

SFT

SAFETY & FIRE TECHNOLOGY

20 YRS

Threats Related to the Operation of Energy Storage Systems, Preventative Measures and Impact Mitigation Methods

p. 106

Zagrożenia związane z eksploatacją magazynów energii elektrycznej oraz środki ich ograniczania

s. 106

Protection of the Population in the 21st Century: the Role of Innovative Technologies in Crisis Response

p. 30

Ochrona ludności w XXI wieku: rola innowacyjnych technologii w reagowaniu kryzysowym

s. 30

Fire Safety of Buildings in the Context of Wildfires

p. 134

Bezpieczeństwo pożarowe budynków w kontekście pożarów lasów

s. 134

Modular Mobile Crisis Management Support Systems – Implementation Prospects Based on the Analysis of the Beirut Explosion (2020)

p. 162

Modułowe mobilne systemy wspomagania zarządzania kryzysowego – perspektywy wdrożenia na podstawie analizy wybuchu w Bejrucie (2020)

s. 162

EDITORIAL COMMITTEE / KOMITET REDAKCYJNY

st. bryg. dr hab. inż. Paweł Janik – Editor-in-Chief / Redaktor Naczelny

st. bryg. dr hab. inż. Jacek Zboina
dr hab. Maria Zielecka
prof. dr hab. Anna Rabajczyk
st. bryg. mgr inż. Daniel Małosiński
nadbryg. w st. spocz. dr inż. Mariusz Feltynowski
prof. Bogdan Z. Długogórski
prof. dr inż. Aleš Dudaček
prof. Arief E. Dahoe
dr Monika Wyszomirska
dr Agnieszka Siłuszka

Language editing / Redakcja językowa:
mgr Aleksandra Grzęda
mgr Anna Golińska
mgr Elżbieta Muszyńska-Połeć

Cover design / Projekt okładki: Małgorzata Żurniewicz-Turno

ISSN 2657-8808

e-ISSN 2658-0810

DOI: 10.12845/sft

© by Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej
im. Józefa Tuliszkowskiego Państwowy Instytut Badawczy, Józefów 2026.
Pewne prawa zastrzeżone. Artykuły udostępnione na licencji CC BY-SA 4.0 /
Scientific and Research Centre for Fire Protection – National Research
Institute, 2026. Some rights reserved. The articles are published under
Creative Commons License the CC BY-SA 4.0

Editorial Office / Redakcja:
ul. Nadwiślańska 213,
05-420 Józefów k. Otwocka

tel. 22 769 33 20
e-mail: sft@cnbop.pl
www.sft.cnbop.pl

Publisher / Wydawca:



Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej
im. Józefa Tuliszkowskiego Państwowy Instytut Badawczy /
Scientific and Research Centre for Fire Protection – National
Research Institute

Circulation / Nakład: 70 egz.

Typesetting / Skład: Małgorzata Żurniewicz-Turno
Print and binding / Druk i oprawa: www.drukujzsensem.pl

EDITORIAL ADVISORY BOARD / RADA NAUKOWA

prof. Andriy Kuzyk
Lviv State University of Life Safety, Ukraine

prof. dr inż. Rainer Koch
the University of Paderborn,
Institute for Fire and Rescue Technology in Dortmund,
Germany

prof. dr inż. Venkatesh Kodur
Michigan State University, USA

prof. Jesús Ignacio Martínez Paricio
the Complutense University of Madrid, Spain

dr inż. Hauke Speth
State Fire Service College of North-Rhine Westphalia,
Germany

dr hab. inż. Lech Starczewski, prof. WITPiS
Military Institute of Armoured and Automotive Technology,
Poland

prof. Asif Usmani
BRE Centre for Fire Safety Engineering
– The University of Edinburgh, UK

dr Ai Sekizawa
prof. Tokyo University of Science, Japan

dr hab. Iwona Szwach
prof. ICSO The Łukasiewicz Research Network
– Institute of Heavy Organic Synthesis "Błachownia",
Poland

dr Jason Yunlong Liu, FIEAust
(<https://www.jasonyunlong.com/>), USA

prof. dr Qiang Xu,
Nanjing University of Science and Technology,
School of Mechanical Engineering, China

prof. Milosh Puchovsky
Worcester Polytechnic Institute, USA

INDEXING IN DATABASES / INDEKSACJA W BAZACH

EBSCO
BazTech
Index Copernicus (ICV 2024: 100)
DOAJ
J-GATE
VINI
Ulrich's Periodicals Directory
ProQuest
SCILIT
Google Books / Google Play
ERIH PLUS

BOOKSTORE PLATFORMS & LIBRARIES /
PLATFORMY KSIĘGARSKIE I BIBLIOTEKI

Electronical Journals Library, University of Regensburg
Vernadsky National Library of Ukraine
Federacja Bibliotek Cyfrowych
Biblioteka Nauki



TWENTY YEARS OF *SAFETY & FIRE TECHNOLOGY*

In 2026, we celebrate the official 20th anniversary of “Safety & Fire Technology”. Official – because its roots date back much further, to 1958 and the title BIT – Fire Science and Technology. However, the journal has existed as a continuous publication since 2006.

This was when the first issue of the quarterly journal “Bezpieczeństwo i Technika Pożarnicza” (“Safety and Fire Technique”) was released, with Eugeniusz W. Roguski, then Director of CNBOP-PIB, serving as Editor-in-Chief. Initially, the journal focused on publishing in-house articles presenting the activities of the Institute, its laboratories, certification issues, and the results of research in the fields of fire protection and civil protection.

Very quickly, however, the periodical evolved into a scientific journal. As early as 2009, it received its first evaluation score from the Ministry responsible for science and higher education. From that point onward, the journal developed dynamically – the number of external authors steadily increased, and in 2012 an international scientific board was established.

The journal consistently followed the development trends of the global scientific publishing market and the guidelines of international editorial standards. It gained recognition both within the scientific community and among representatives of public administration. The special position it holds within the Institute – regardless of changes in leadership – is the result of the determination, expertise, and commitment of successive editors-in-chief and editorial secretaries. Their work made it possible to achieve a high substantive and publishing standard.

In the following years, the journal was indexed in an increasing number of scientific databases, including BazTech, EBSCO, and Index Copernicus, which was reflected in its growing ministerial evaluation score. At the same time, publication ethics standards and peer-review procedures were further developed, and the journal gradually acquired a more international character through publications by foreign authors and articles published in foreign languages.

“Safety & Fire Technology” has existed in its present form since 2019.

The changes introduced in recent years were a deliberate step toward further internationalization of the journal and improving the quality of publishing practices. The periodical began to appear as a semiannual publication, and English became the leading language while maintaining the bilingual character of the journal. A comprehensive restructuring was also carried out, redefining its thematic scope.

The new edition also included graphical changes, greater attention to the linguistic quality of publications, and the development of editorial support infrastructure. Participation in the “Support for Scientific Journals” program of the Ministry of Science and Higher Education enabled the strengthening of the editorial team’s competencies, the development of infrastructure, and more effective international promotion of the journal. The program also formed part of preparations for systemic changes related to the so-called “Act 2.0” and the new evaluation framework for scientific journals.

We continue to maintain the bilingual character of the journal to this day. English translations are financed from the Institute’s own resources, increasing the accessibility of publications for international readers while simultaneously preserving and cultivating the Polish language as an important element of our scientific identity.



DWUDZIESTOLECIE CZASOPISMA „SAFETY & FIRE TECHNOLOGY”

W 2026 roku obchodzimy oficjalne 20-lecie wydawania czasopisma „Safety & Fire Technology”. Oficjalne – gdyż korzenie periodyku sięgają znacznie dalej, aż do 1958 roku i tytułu „BIT – Nauka i Technika Pożarnicza”. Jako wydawnictwo ciągle czasopismo funkcjonuje jednak od 2006 roku.

Właśnie wtedy ukazał się pierwszy numer kwartalnika „Bezpieczeństwo i Technika Pożarnicza”, którego redaktorem naczelnym był ówczesny Dyrektor CNBOP-PIB, Eugeniusz W. Roguski. Początkowo czasopismo koncentrowało się na publikowaniu artykułów własnych, przybliżających działalność Instytutu, jego laboratoriów, zagadnienia certyfikacji oraz wyniki prac badawczych w obszarze ochrony przeciwpożarowej i ochrony ludności.

Bardzo szybko jednak periodyk ewoluował, przekształcając się w czasopismo o charakterze naukowym. Już w 2009 roku uzyskał pierwszą ocenę punktową Ministerstwa właściwego do spraw nauki. Od tego momentu następował jego dynamiczny rozwój – systematycznie rosła liczba autorów zewnętrznych, a w 2012 roku powołano międzynarodową radę naukową.

Czasopismo konsekwentnie podążało za kierunkami rozwoju światowego rynku wydawnictw naukowych oraz wytycznymi międzynarodowych standardów edytorskich. Zyskiwało uznanie zarówno środowiska naukowego, jak i przedstawicieli administracji publicznej. Szczególne miejsce, jakie zajmuje w Instytucie – niezależnie od zmian w jego kierownictwie – jest efektem determinacji, wiedzy i zaangażowania kolejnych redaktorów oraz sekretarzy redakcji. To ich praca pozwoliła osiągnąć wysoki poziom merytoryczny i wydawniczy.

W kolejnych latach periodyk był indeksowany w coraz liczniejszych bazach naukowych, począwszy od BazTech, EBSCO czy Index Copernicus, co znajdowało odzwierciedlenie w rosnącej ocenie ministerialnej. Jednocześnie rozwijano standardy etyki publikacyjnej oraz procedury recenzyjne, a czasopismo stopniowo nabierało charakteru międzynarodowego – pojawiały się publikacje autorów zagranicznych oraz artykuły w językach obcych.

W obecnym kształcie „Safety & Fire Technology” funkcjonuje od roku 2019.

Zmiany z ostatnich lat były świadomym krokiem w kierunku dalszego umiędzynarodowienia czasopisma oraz podniesienia jakości praktyk wydawniczych. Periodyk zaczął ukazywać się jako półrocznik, a językiem wiodącym stał się język angielski, przy jednoczesnym zachowaniu dwujęzycznego charakteru publikacji. Przeprowadzono również gruntowną zmianę struktury czasopisma, redefiniując jego zakres tematyczny.

Nowa odsłona obejmowała także zmiany graficzne, większą dbałość o jakość językową publikacji oraz rozwój zaplecza redakcyjnego. Udział w programie „Wsparcie dla Czasopism Naukowych” Ministerstwa Nauki i Szkolnictwa Wyższego umożliwił wzmocnienie kompetencji zespołu, rozwój infrastruktury oraz skuteczniejszą promocję periodyku na arenie międzynarodowej. Program ten był również elementem przygotowań do zmian systemowych związanych z tzw. „Ustawą 2.0” i nową oceną czasopism naukowych. Dwujęzyczny charakter czasopisma utrzymujemy do dziś. Tłumaczenia na język angielski finansowane są ze środków własnych, co pozwala zwiększać dostępność publikacji dla odbiorców zagranicznych, przy jednoczesnym zachowaniu i kultywowaniu języka polskiego jako ważnego elementu naszej tożsamości naukowej.

Today, "Safety & Fire Technology" is a journal with a broad, multidisciplinary thematic scope. It covers not only fire safety issues, but also the safety of new technologies, civil protection, environmental and industrial safety, rescue operations, legal and organizational aspects, as well as innovative safety-related solutions. Such a broad approach reflects the contemporary understanding of safety as an interdisciplinary category.

The journal's significance within the publishing market is confirmed by its growing visibility and the number of citations in renowned scientific journals such as "Safety Science", "Applied Sciences", "Energies", "Scientific Reports", and the "International Journal of Occupational Medicine and Environmental Health". The presence of articles published in "Safety & Fire Technology" in literature representing such diverse fields as materials engineering, chemistry, energy, construction, and environmental sciences demonstrates its genuine contribution to the development of numerous scientific disciplines. We are also observing a significant increase in citation rates – in the Scopus database, this increase has exceeded 55% over the last three years.

Today, "Safety & Fire Technology" serves as an important platform for the exchange of knowledge and experience in the areas of fire protection, civil protection, and environmental protection. Its strength lies in its multidisciplinary approach, the integration of science and practice, and its focus on applied solutions and innovative technologies serving safety.

The current Editor-in-Chief is Senior Brigadier Paweł Janik, Ph.D., D.Sc., Eng., under whose leadership the journal continues to strengthen its position within the international scientific community.

However, this success would not have been possible without the commitment of authors, reviewers, the scientific board, and entire editorial teams who, over the years, have contributed to the journal's development and reputation. It is thanks to their work that "Safety & Fire Technology" is today a recognized and respected scientific journal.

We warmly invite all of you to continue your cooperation with us – by publishing research results, sharing experiences, and co-creating the next chapters in the history of our journal.

Editorial Committee

Obecnie „Safety & Fire Technology” jest czasopismem o szerokim, multidyscyplinarnym zakresie tematycznym. Obejmuje nie tylko zagadnienia bezpieczeństwa pożarowego, ale również bezpieczeństwo nowych technologii, ochronę ludności, bezpieczeństwo środowiskowe i przemysłowe, działania ratownicze, aspekty prawne i organizacyjne oraz innowacyjne rozwiązania w obszarze bezpieczeństwa. Tak szerokie ujęcie problematyki odzwierciedla współczesne rozumienie bezpieczeństwa jako kategorii interdyscyplinarnej.

Znaczenie czasopisma na rynku wydawniczym potwierdza jego rosnąca widoczność i liczba cytowań w renomowanych czasopismach naukowych, takich jak „Safety Science”, „Applied Sciences”, „Energies”, „Scientific Reports” czy International „Journal of Occupational Medicine and Environmental Health”. Obecność artykułów publikowanych w „Safety & Fire Technology” w literaturze reprezentującej tak różnorodne dziedziny, jak inżynieria materiałowa, chemia, energetyka, budownictwo czy nauki o środowisku, dowodzi jego realnego wkładu w rozwój wielu obszarów nauki. Obserwujemy także wyraźny wzrost cytowalności – w bazie Scopus przekroczył on 55% w ciągu ostatnich trzech lat.

Dziś „Safety & Fire Technology” stanowi istotną platformę wymiany wiedzy i doświadczeń w obszarze ochrony przeciwpożarowej, ochrony ludności oraz ochrony środowiska. Jego siłą jest podejście multidyscyplinarne, łączenie nauki z praktyką oraz koncentracja na rozwiązaniach aplikacyjnych i innowacyjnych technologiach służących bezpieczeństwu.

Funkcję redaktora naczelnego pełni obecnie st. bryg. dr hab. inż. Paweł Janik, pod którego kierunkiem czasopismo konsekwentnie umacnia swoją pozycję w międzynarodowym obiegu naukowym.

Nie byłoby jednak tego sukcesu bez zaangażowania autorów, recenzentów, rady naukowej oraz całych zespołów redakcyjnych, które na przestrzeni lat współtworzyły jego rozwój i renomę. To dzięki ich pracy „Safety & Fire Technology” jest dziś rozpoznawalnym i cenionym czasopismem naukowym.

Zapraszamy wszystkich Państwa do dalszej współpracy – do publikowania wyników badań, dzielenia się doświadczeniem oraz współtworzenia kolejnych rozdziałów historii naszego czasopisma.

Komitet Redakcyjny

CONTENT

- 6** Civil Defense – The Use of LoRa Technology for Effective Warning and Alarm of Threats
Tomasz Popielarczyk, Jacek Zboina, Grzegorz Mroczko, Paweł Bujny
- 30** Protection of the Population in the 21st Century: the Role of Innovative Technologies in Crisis Response
Tomasz Lutoborski, Maciej Zawistowski
- 58** Analysis of Acoustic Anomalies and Speech Artefacts in Synthetic Content
Karol Jędrasiak
- 86** A New Medical Doctrine for CBRNE Threats: a Framework for Developing Poland's Emergency Medical Services, Civil Protection and Civil Defence
Karol Łyziński, Arkadiusz Trzos
- 106** Threats Related to the Operation of Energy Storage Systems, Preventative Measures and Impact Mitigation Methods
Jan Kielin, Jacek Zboina, Paweł Janik, Damian Bąk
- 134** Fire Safety of Buildings in the Context of Wildfires
Łukasz Tyburski
- 146** Firefighter Operational Hygiene as a System for Reducing Secondary Exposure to Hazardous Substances Present in the Fire Environment – Review of Scientific Evidence and Normative Documents
Tomasz Krasowski
- 162** Modular Mobile Crisis Management Support Systems – Implementation Prospects Based on the Analysis of the Beirut Explosion (2020)
Norbert Tuśnio
- 196** Subversive Operations in Cyberspace
Jerzy Kosiński
- 210** Using the Kendrick Extrication Device in the National Rescue and Firefighting System
Sławomir Paszek, Zofia Czaplińska-Paszek

SPIS TREŚCI

- 6** Ochrona ludności – zastosowanie technologii LoRa na potrzeby efektywnego ostrzegania i alarmowania o zagrożeniach
Tomasz Popielarczyk, Jacek Zboina, Grzegorz Mroczko, Paweł Bujny
- 30** Ochrona ludności w XXI wieku: rola innowacyjnych technologii w reagowaniu kryzysowym
Tomasz Lutoborski, Maciej Zawistowski
- 58** Analiza anomalii akustycznych i artefaktów mowy w treściach syntetycznych
Karol Jędrasiak
- 86** Nowa doktryna medyczna wobec zagrożeń CBRNE – kierunek rozwoju systemu ratownictwa medycznego, ochrony ludności i obrony cywilnej w Polsce
Karol Łyziński, Arkadiusz Trzos
- 106** Zagrożenia związane z eksploatacją magazynów energii elektrycznej, środki zapobiegania ich wystąpieniu oraz sposoby ograniczania skutków
Jan Kielin, Jacek Zboina, Paweł Janik, Damian Bąk
- 134** Bezpieczeństwo pożarowe budynków w kontekście pożarów lasów
Łukasz Tyburski
- 146** Higiena operacyjna strażaka jako system ograniczania wtórnej ekspozycji na substancje niebezpieczne obecne w środowisku pożaru – przegląd dowodów naukowych i dokumentów normatywnych
Tomasz Krasowski
- 162** Modułowe mobilne systemy wspomagania zarządzania kryzysowego – perspektywy wdrożenia na podstawie analizy wybuchu w Bejrucie (2020)
Norbert Tuśnio
- 196** Działania dywersyjne w cyberprzestrzeni
Jerzy Kosiński
- 210** Stosowanie kamizelki Kendricka w krajowym systemie ratowniczo-gaśniczym
Sławomir Paszek, Zofia Czaplińska-Paszek

Tomasz Popielarczyk, Jacek Zboina, Grzegorz Mroczko, Paweł Bujny

Scientific and Research Centre for Fire Protection – National Research Institute / Centrum Naukowo-Badawcze Ochrony Przeciwpozarowej – Państwowy Instytut Badawczy
Corresponding author / Autor korespondencyjny: tpopielarczyk@cnbop.pl

Civil Defense – The Use of LoRa Technology for Effective Warning and Alarm of Threats

Ochrona ludności – zastosowanie technologii LoRa na potrzeby efektywnego ostrzegania i alarmowania o zagrożeniach

ABSTRACT

Purpose: The aim of the research carried out together with technological partners in the Otwock district, as well as the manufacturers' own research, was to confirm the possibility of using LoRa technology for the purposes of effective alerting about threats and supporting the evacuation of people, as well as, creating own independent, dedicated crisis communication between entities/facilities.

Project and methods: This research was intended to confirm the correctness of communication by transmitting messages between the base station and the mobile station, and obtaining confirmation of the execution of the alarm siren activation request using radio and LoRa communications. Control signals were sent from the base station via radio and LoRa communications to the mobile station. The mobile station was driven around the local area of the base station to verify the actual range and reception of signals via both types of communication. The transmitting and receiving antennas were placed on the roof to achieve the greatest possible visibility (range). The mobile station (named "OSP" for testing purposes) was mounted on a vehicle, along with elevated transmitting and receiving antennas outside the vehicle, to ensure the best possible "visibility" between the tower station antenna and the mobile station. The tests were carried out together with technological partners in the Otwock district. Manufacturers' own research was also used.

Results: The measurements provided results including transmission time (s) and RSSI (Received Signal Strength Indicator) (dBm) for both DMR radio and LoRa communications. The test system's base station and mobile station were functionally compatible. It is possible to use DMR and LoRa communications in test system – the maximum distance achieved during testing was 15.7 km. The test system's redundancy was also confirmed in real-world conditions.

Conclusions: During all test series, correct redundant DMR and LoRa communication was achieved in 13 out of 16 locations selected for testing (81.25%). Problems with establishing DMR and LoRa communication are influenced by: terrain topography, including the presence of hills between the location of the base station and the mobile station, the degree of forestation/urbanization of the area, including the state of tree foliage, the height of buildings, the presence of high-voltage lines near the masts, the height of antenna masts, local radio communication conditions, including the presence of other radio communication devices, jamming devices.

Keywords: civil protection, security of new technologies, evacuation of population, warning and alarming, technologies for civil protection, communication for civil protection, civil warning and alarm system

Type of article: original scientific article

Received: 19.11.2025; Reviewed: 31.12.2025; Accepted: 12.01.2026;

Authors' ORCID IDs: T. Popielarczyk – 0000-0002-0124-7182; J. Zboina – 0000-0002-9436-5830; G. Mroczko – 0000-0002-9499-539X; P. Bujny – 0009-0007-0588-9135;

The authors contributed equally to this article;

Please cite as: Safety & Fire Technology 2026, 1, 6–28, <https://doi.org/10.12845/sft.67.1.2026.1>;

This is an open access article under the CC BY-SA 4.0 license (<https://creativecommons.org/licenses/by-sa/4.0/>).

ABSTRAKT

Cel: Celem prezentowanych w niniejszej pracy badań było potwierdzenie możliwości wykorzystania technologii LoRa na potrzeby efektywnego alarmowania o zagrożeniach i wspierania ewakuacji ludności, jak również tworzenia własnej niezależnej dedykowanej komunikacji kryzysowej pomiędzy podmiotami i obiektami.

Projekt i metody: Badania miały na celu potwierdzenie poprawności komunikacji poprzez przesyłanie komunikatów pomiędzy stacjami bazową i mobilną oraz uzyskiwanie potwierdzenia realizacji zlecenia uruchomienia syreny alarmowej z wykorzystaniem łączności radiowej i łączności LoRa. Ze stacji bazowej wysyłane były sygnały sterujące drogą komunikacji radiowej oraz komunikacji LoRa do stacji mobilnej. Stacja mobilna przewożona była

po lokalnej okolicy stacji bazowej tak, aby sprawdzić faktyczne możliwości zasięgu i otrzymywania sygnałów poprzez oba typy komunikacji. Anteny nadawczo-odbiorcze zostały wyprowadzone na dach tak, aby uzyskać jak największy zakres widzialności (zasięgu). Stacja mobilna (nazwana na potrzeby testowania „OSP”) była zamontowana na samochodzie, wraz z wyniesionymi antenami nadawczo-odbiorczymi na zewnątrz samochodu w taki sposób, aby zapewnić jak najlepszą, tzw. „widzialność” anteny stacji na wieży i stacji mobilnej. Badania zrealizowano pod afiliacją CNBOP-PIB we współpracy z partnerami technologicznymi w powiecie otwockim. Wykorzystano także rezultaty badań własnych producentów.

Wyniki: Podczas pomiarów uzyskano wyniki na temat czasu transmisji [s] oraz RSSI (ang. *Received Signal Strength Indicator*) [dBm] – zarówno dla komunikacji radiowej DMR, jak i LoRa. Stacja bazowa i stacja mobilna badanego systemu były kompatybilne funkcjonalnie. Potwierdzono możliwość zastosowania w badanym systemie komunikacji DMR oraz LoRa. Odległość maksymalna uzyskana podczas testów wyniosła 15,7 km. Potwierdzono również redundancję badanego systemu w warunkach rzeczywistych.

Wnioski: Podczas wszystkich serii testów uzyskano poprawną redundantną komunikację DMR i LoRa w 13 na 16 lokalizacji wybranych do testów (81,25%). Na problemy z nawiązaniem komunikacji DMR i LoRa wpływ mają: topografia terenu (m.in. występowanie wzniesień pomiędzy lokalizacją stacji bazowej i stacji mobilnej), stopień zalesienia/zurbanizowania terenu (w tym stan ulistnienia drzew, wysokość budynków, obecność linii wysokiego napięcia w pobliżu masztów, wysokości masztów antenowych), a także lokalne warunki radiokomunikacyjne (m.in. obecność innych urządzeń radiokomunikacyjnych, urządzeń zagłuszających).

Słowa kluczowe: ochrona ludności, bezpieczeństwo nowych technologii, ewakuacja ludności, ostrzeżenie i alarmowanie, komunikacja, system ostrzegania i alarmowania ludności

Typ artykułu: oryginalny artykuł naukowy

Przyjęty: 19.11.2025; **Zrecenzowany:** 31.12.2025; **Zaakceptowany:** 12.01.2026;

Identyfikatory ORCID autorów: T. Popielarczyk – 0000-0002-0124-7182; J. Zboina – 0000-0002-9436-5830; G. Mroczko – 0000-0002-9499-539X; P. Bujny – 0009-0007-0588-9135;

Autorzy wnieśli równy wkład merytoryczny w opracowanie artykułu;

Proszę cytować: Safety & Fire Technology 2026, 1, 6–28, <https://doi.org/10.12845/sft.67.1.2026.1>;

Artykuł udostępniany na licencji CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>).

Introduction

Civil protection and civil defence are currently areas of intensive legislative, organisational and systemic works in Poland. They are currently the subject of specialised research, project and programmes. Investments are also made in personnel, its competencies, preparation and equipment with resources and infrastructure, as well as building social resistance to current threats. The numerous needs of the dynamically developed and perfected civil protection in our country are addressed by scientific research, including empirical, aimed at obtaining and disseminating knowledge [1–2], research results, technical and technological solutions [3], systems and products designed to achieve the protection objectives related to broadly understood civil protection and civil defence, property and critical infrastructure [4–5]. The scientific research, the results, the knowledge obtained, the use of experience of other countries and the implementation of own solutions constitute the essential foundations and activities aimed to create effective civil protection mechanisms in Poland.

The needs for products and their properties, dedicated systems and solutions based on new technologies have been the domain of research and activities of CNBOP-PIB for more than 50 years. At present, an urgent need and challenge, apart from fire protection, is the safety of new technologies used for civil protection. It is often by using custom implementations of new technical and technological solutions that we obtain an actual advantage over threats and their potential impact. This is also the case in the area of broadly understood safety: the use of new technologies and their adjustment, implementation and reliability determine the efficiency and effectiveness of protection. A significant part of the scientific research and activities of the Institute

Wprowadzenie

Ochrona ludności i obrona cywilna to aktualnie obszary intensywnych prac w Polsce – zarówno legislacyjnych, organizacyjnych, jak i systemowych. Są one obecnie przedmiotem specjalistycznych badań, projektów i programów. Podejmowane są także inwestycje w personel, jego kompetencje, przygotowanie i wyposażenie, w zasoby i infrastrukturę, a także w budowanie odporności społecznej na aktualne zagrożenia. W liczne potrzeby dynamicznie tworzonej i doskonalonej ochrony ludności w naszym kraju wpisują się badania naukowe, w tym empiryczne, mające na celu pozyskanie i upowszechnianie wiedzy [1–2], wyników badań, rozwiązań technicznych i technologicznych [3], systemów i produktów dedykowanych do realizacji celów ochronnych w odniesieniu do szeroko rozumianej ochrony ludności i obrony cywilnej, mienia i infrastruktury krytycznej [4–5]. To właśnie badania naukowe, ich wyniki, pozyskiwana wiedza, wykorzystanie doświadczeń innych państw i wdrażanie własnych rozwiązań stanowią nieodzowne podstawy i działania mające na celu stworzenie efektywnych mechanizmów ochrony ludności w Polsce.

Potrzeby w zakresie wyrobów i ich właściwości, dedykowanych systemów i rozwiązań opartych na nowych technologiach to domena badań i działalności CNBOP-PIB od ponad 50 lat. Aktualnie pilną potrzebą i wyzwaniem – oprócz ochrony przeciwpożarowej – jest bezpieczeństwo nowych technologii wykorzystywanych do ochrony ludności. To właśnie dzięki zastosowaniu często niestandardowej implementacji nowych rozwiązań technicznych i technologicznych zyskujemy faktyczną przewagę nad zagrożeniami i ich potencjalnymi skutkami. Tak jest i w obszarze szeroko rozumianego bezpieczeństwa – użycie nowych technologii, ich dopasowanie, wdrożenie i niezawodność decydują o skuteczności

is distinguished by being conducted consistently in collaboration with other scientific units, PSP and OSP, as well as industry associations of various technologies and, of course, manufacturers of solutions dedicated to fire protection and civil protection.

The own research presented in this article, as well as the analysis of the research available in literature of the subject was conducted with technological partners, manufacturers and suppliers of products used in warning, alarm and civil protection systems. To prepare the article, the authors used i.a. the results of research carried out by CNBOP-PIB as part of the product and innovation testing procedure, as well as results provided by the manufacturers [6]. They were also presented during subsequent editions of the CNBOP-PIB International Scientific Conference *Bezpieczeństwo Nowych Technologii (BNT, Safety of New Technologies)* where they were discussed in the context of the perspectives for the development and improvement of civil notification and warning systems [7]. The most important conclusions were noted in post-conference reports [8], summarising the presented knowledge and research results in safety of new technologies, improvement of rescue technologies and development of solutions for civil protection.

The aim of both the research conducted with technological partners in the Otwock district and own research of manufacturers was to confirm the possibilities of using the LoRa technology for effective alarm of threats and supporting evacuation, as well as creating own independent dedicated crisis communication between entities/facilities, i.e. in the area, in which this technology had not been previously used.

Independently, the CNBOP-PIB conducts many works aimed at searching for effective technical and technological solutions for fire protection and civil protection. The research and implementation projects already completed by the Institute enable using infrastructure based on LoRa technological solutions, which is on a daily basis used i.a. for supervision (operating status, signalling about threat) of flood detectors, opening/closing, e.g. fire doors, heating control.

Application of the LoRa technology

At present, predominantly analogue systems with alarm sirens located in different city areas and voluntary fire service (OSP) buildings are used for notifying, warning and alarming the population and fire protection units. Every voivodship capital city has this type of system. Digital systems with alarm sirens, as well as telephone communications, SMS, Internet and video surveillance, are increasingly used for warning and alarming. These solutions are used both for informing civilian population and voluntary fire-fighters. PSP rescue and fire-fighting units are alarmed directly from the control room. However, OSP units (except for OSP units on permanent duty) "call" volunteer fire-fighters to the station if a specific unit needs to be dispatched using the alarm

i efektywności ochrony. Znaczną część badań naukowych i działań Instytutu wyróżnia to, że prowadzone są one konsekwentnie we współpracy z innymi jednostkami naukowymi, jednostkami PSP i OSP, a także stowarzyszeniami branżowymi różnych technologii i oczywiście producentami rozwiązań dedykowanych ochronie przeciwpożarowej i ochronie ludności.

Przedstawione w niniejszym artykule badania własne, a także analizę tych dostępnych w literaturze przedmiotu autorzy artykułu prowadzili z partnerami technologicznymi, producentami i dostawcami wyrobów stosowanych w systemach ostrzegania, alarmowania i ochrony ludności. Na potrzeby opracowania artykułu wykorzystano m.in. rezultaty badań prowadzonych przez CNBOP-PIB w ramach procedury testowania wyrobów i rozwiązań innowacyjnych, a także wyniki badań samych producentów [6]. Zaprezentowano je także podczas kolejnych edycji Międzynarodowej Konferencji Naukowej CNBOP-PIB pn. *Bezpieczeństwo Nowych Technologii (BNT)*, gdzie poddano je dyskusji w kontekście perspektyw rozwoju i doskonalenia systemów powiadamiania i ostrzegania ludności [7]. Najważniejsze wnioski odnotowano w raportach [8], będących podsumowaniem prezentowanej wiedzy i wyników badań w zakresie bezpieczeństwa nowych technologii, doskonalenia technologii ratowniczych i rozwoju rozwiązań na potrzeby ochrony ludności.

Celem zarówno badań realizowanych wspólnie z partnerami technologicznymi w powiecie otwockim, jak i badań własnych producentów, było potwierdzenie możliwości wykorzystania technologii LoRa na potrzeby efektywnego alarmowania o zagrożeniach i wspierania ewakuacji ludności, jak również tworzenia własnej niezależnej dedykowanej komunikacji kryzysowej pomiędzy podmiotami/obiektami, tj. w obszarze, w którym technologia ta dotychczas nie była stosowana.

Niezależnie w CNBOP-PIB trwają liczne prace mające na celu poszukiwanie skutecznych rozwiązań technicznych i technologicznych dla ochrony przeciwpożarowej i ochrony ludności. Badania i wdrożenia dotychczas już zrealizowane w Instytucie pozwalają na stosowanie infrastruktury opartej na rozwiązaniach technologicznych LoRa, która na co dzień jest wykorzystywana m.in. do nadzorowania (kontroli stanu pracy, sygnalizacji o zagrożeniu) czujników zalania, otwarcia/zamknięcia – np. drzwi pożarowych, regulacji ogrzewania.

Zastosowanie technologii LoRa

Obecnie do powiadamiania, ostrzegania i alarmowania ludności i jednostek ochrony przeciwpożarowej wykorzystuje się głównie analogowe systemy z syrenami alarmowymi umieszczonymi w różnych częściach miast oraz na budynkach ochotniczych straży pożarnych (OSP). Każde miasto wojewódzkie posiada taki system. Coraz częściej do ostrzegania i alarmowania służą cyfrowe systemy z syrenami alarmowymi, a także łączność telefoniczna, SMS, Internet czy też monitoring wizyjny. Rozwiązania te wykorzystywane są zarówno do informowania ludności cywilnej, jak i strażaków-ochotników. Alarmowanie jednostek ratowniczo-gaśniczych PSP odbywa się bezpośrednio ze stanowiska kierowania. OSP natomiast (pomijając OSP ze stałym dyżurem) w razie

sirens that have been in service for dozens of years, as well as dedicated SMS notifications for telephones and pagers of the OSP fire-fighters entered to the system. An SMS or pager notification is only sent to a specific number of people, considering the time, day of the week and other data on the presence of individual volunteer fire-fighters in town. Newer solutions also enable alarming volunteer firefighters by telephone calls to their mobile phones.

In accordance with *Ramowe wytyczne projektowania strażnic OSP (Framework guidelines for designing OSP stations)* [9], OSP stations must be equipped with communication and alarm equipment and a remote alarm system. In addition, the communication system and the alarm point should have an additional power supply system in case of failure. The alarm siren should be located at the altitude that ensures proper audibility in the town of the OSP headquarters.

A simplified alarm system for fire protection units is presented in figure 1.

konieczności zadysponowania konkretnej jednostki „zwołują” strażaków-ochotników do strażnicy za pomocą wykorzystywanych od kilkudziesięciu lat syren alarmowych, a także dedykowanych powiadomień SMS na telefony lub pagery strażaków OSP zgłoszonych do systemu. Powiadomienie SMS lub na pager wysyłane jest jedynie do określonej liczby osób z uwzględnieniem godziny, dnia w tygodniu i innych danych o przebywaniu w miejscowości poszczególnych strażaków-ochotników. Nowsze rozwiązania umożliwiają również alarmowanie strażaków-ochotników poprzez połączenia telefoniczne na ich telefony komórkowe.

Zgodnie z *Ramowymi wytycznymi projektowania strażnic OSP* [9] strażnice OSP muszą być wyposażone w urządzenia łączności i alarmowania oraz system zdalnego alarmowania. Dodatkowo system łączności i punkt alarmowy na wypadek awarii powinny mieć system zasilania z dodatkowego źródła. Syrena alarmowa powinna być zlokalizowana na wysokości zapewniającej odpowiednią słyszalność w miejscowości będącej siedzibą OSP.

Uproszczony system alarmowania jednostek ochrony przeciwpożarowej przedstawiono na rycinie 1.

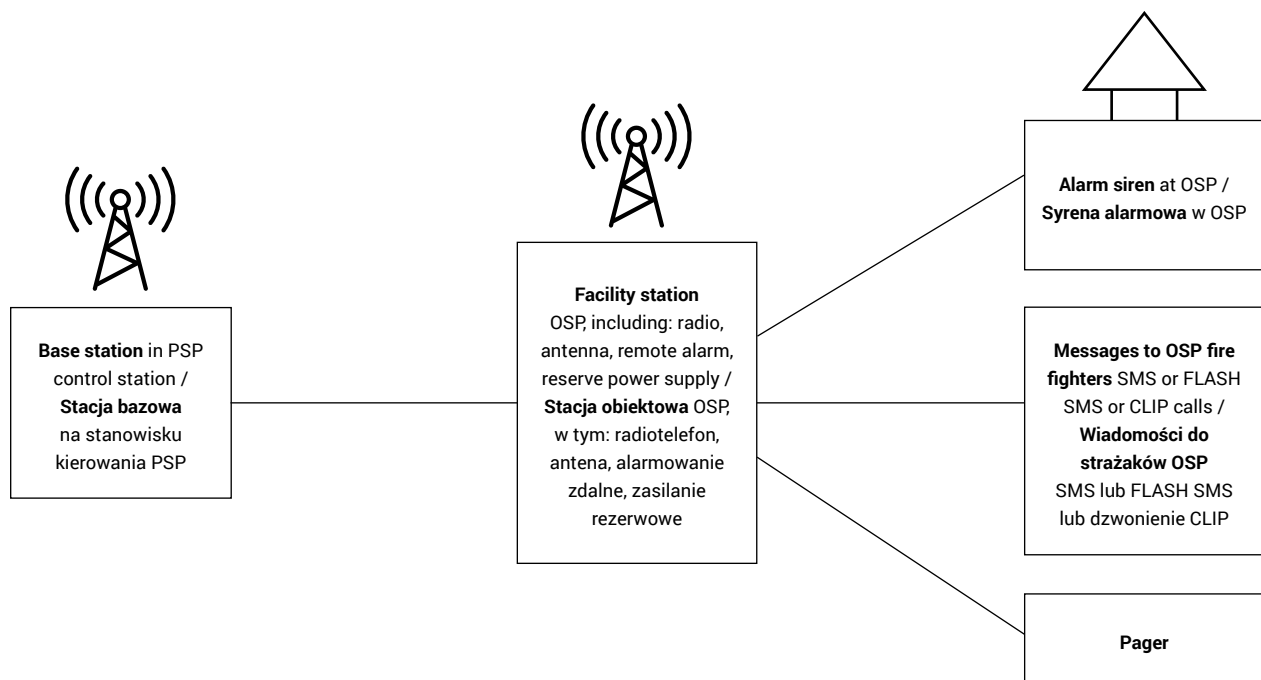


Figure 1. Simplified alarm system for fire protection units
Rycina 1. Uproszczony system alarmowania jednostek ochrony przeciwpożarowej
Source: Own elaboration.
Źródło: Opracowanie własne.

The existing infrastructure for alarming fire protection units is also used for warning and alarming the civilian population of threats. This applies in particular to smaller towns. In cities, there are predominantly systems dedicated exclusively for warning and alarming the civilian population.

Istniejąca infrastruktura do alarmowania jednostek ochrony przeciwpożarowej jest wykorzystywana również do ostrzegania i alarmowania o zagrożeniach ludności cywilnej. Szczególnie dotyczy to mniejszych miejscowości. W miastach najczęściej są to systemy dedykowane tylko ostrzeganiu i alarmowaniu ludności cywilnej.

The communication between the base station and the facility station is conducted primarily using analogue radio communication. Recently, DMR (Digital Mobile Radio) radio communication, which enables higher transmitted audio quality, encryption and power saving, has become increasingly used. In addition, one frequency can support two independent calls at the same time. With the capacity to operate in analogue mode, DMR systems are easier to implement, in particular during migration from existing analogue infrastructure.

Another technology that can be used in this type of systems is the LoRa technology, which enables power-saving and long range radio calls between devices. LoRaWAN (Long Range Wide Area Network) operates in non-licensed radio frequency bands and features long range (up to 15 km in rural areas), low energy consumption and the capability to connect a large number of devices to one network. The architecture includes terminals, gates, network servers and application servers, which enables building a scalable and flexible network for different applications of the Internet of Things (IoT). The term LoRa (Long Range) refers to the physical layer (PHY), which includes the modulation technique used for long range communication with low power consumption. LoRa is a radio signal for wireless data transmission that uses the dispersed spectrum technology. The term LoRaWAN refers to the standard network and system architecture for managing communication between LoRaWAN devices and the network server. It defines the communication standard and system architecture at the level of the MAC (Medium Access Control) layer [10]. LoRa is a radio modulation technique that enables sending small data packages at very long distances, up to a dozen kilometres, with minimal power consumption. This enables the signal sensor or receiver to operate on a single battery for many years. At present, LoRa networks are predominantly used to read parameters from sensors, such as water meters, parking sensors, weather stations, soil humidity sensors or tank, container or basket filling sensors [11]. For example, the proprietary LoRa network at CNBOP-PIB is used i.a. to transmit data from flooding sensors, manage room heating, door opening or closing parameters, including fire doors (with dedicated programmable alarm, after specific opening time), read daily data from the weather station, detection device status information and the local fire-fighting system protecting the electric vehicle charging point. The network use in the institution is tested¹ in other applications as well.

Research has been conducted for many years to implement the LoRa technology in i.a. rescue services and civil protection. The analysis of literature suggests the possible use of this technology in the following areas:

- monitoring natural disasters and disasters caused by human errors [12],
- voice communication (voice processing system for broadband environments, which uses the LoRa dispersed spectrum technology as communication protocol and the voice recognition technology as compression method) to

Łączność między stacją bazową a stacją obiektową odbywa się głównie z wykorzystaniem łączności radiowej analogowej. Od niedawna coraz częściej używana jest łączność radiowa DMR (ang. *Digital Mobile Radio*), która charakteryzuje się lepszą jakością przesyłanego dźwięku, możliwością szyfrowania, oszczędnością zasilania. Ponadto jedna częstotliwość może obsługiwać dwie niezależne rozmowy w tym samym czasie. Dzięki możliwości pracy w trybie analogowym, systemy DMR są łatwiejsze w implementacji, szczególnie podczas migracji z istniejącej infrastruktury analogowej.

Inną technologią możliwą do zastosowania w tego typu systemach jest technologia LoRa, która pozwala na energooszczędne i dalekosiężne połączenia radiowe między urządzeniami. LoRaWAN (ang. *Long Range Wide Area Network*) działa w nielicencjonowanych pasmach częstotliwości radiowych i charakteryzuje się dużym zasięgiem (do 15 km na obszarach wiejskich), niskim poborem energii oraz możliwością podłączenia dużej liczby urządzeń do jednej sieci. Architektura obejmuje urządzenia końcowe, bramy, serwery sieciowe i serwery aplikacji, umożliwiając skalowalną i elastyczną sieć dla różnorodnych aplikacji Internetu Rzeczy (IoT). LoRa (ang. *Long Range*) odnosi się do warstwy fizycznej (PHY), która obejmuje technikę modulacji wykorzystywaną do komunikacji dalekiego zasięgu przy niskim poborze mocy. LoRa to sygnał radiowy, który przesyła dane bezprzewodowo z wykorzystaniem technologii rozproszonego widma. LoRaWAN odnosi się do standardu sieciowego i architektury systemu do zarządzania komunikacją między urządzeniami LoRaWAN a serwerem sieciowym. Definiuje standard komunikacji i architekturę systemu na poziomie warstwy MAC (ang. *Medium Access Control*) [10]. LoRa to technika modulacji radiowej, która pozwala na przesyłanie niewielkich pakietów danych na bardzo duże odległości – nawet kilkanaście kilometrów – przy minimalnym zużyciu energii. Dzięki temu czujnik czy odbiornik sygnału może działać na jednej baterii przez wiele lat. Aktualnie najczęściej sieci LoRa wykorzystuje się do odczytu parametrów z czujników, takich jak wodomierze, czujniki parkingowe, stacje pogodowe, czujniki wilgotności gleby czy czujniki zapełnienia zbiorników, kontenerów bądź koszy [11]. Dla przykładu w CNBOP-PIB własna sieć LoRa wykorzystywana jest m.in. do przesyłania danych z czujników zalania, zarządzania parametrami ogrzewania w pomieszczeniach, otwarcia lub zamknięcia wejść, w tym drzwi przeciwpożarowych (z dedykowanym programowalnym alarmem, po określonym czasie ich otwarcia), odczytu codziennych danych ze stacji pogodowej, informacji o stanie urządzeń detekcyjnych i miejscowego systemu gaszenia chroniącego punkt ładowania pojazdów elektrycznych. Wykorzystanie sieci w instytucji jest testowane¹ również w innych zastosowaniach.

Od wielu lat prowadzone są badania mające na celu wdrożenie technologii LoRa m.in. w ratownictwie i ochronie ludności. Analiza literatury wskazuje na możliwe wykorzystanie tej technologii w następujących obszarach:

- monitorowanie klęsk żywiołowych i katastrof spowodowanych błędami ludzkimi [12],

¹ The testing, research and work areas refer to fire protection, civil protection and rescue services.

¹ Obszary testowania, badań, prac dotyczą ochrony przeciwpożarowej, ochrony ludności i ratownictwa.

enable remote communication for emergency responders during rescue operations, even in environments with no public networks [13],

- alarming the population of threats (on the example of the research conducted in 2025, which indicated the possibility of using an autonomous communication system powered by the LoRa technology and the Arduino platform). With a manual power generator, system operation is uninterrupted, with no external power supply required. The device is equipped with a NEO-6M GPS module and an oxygen sensor, which transmit location and environment information via the LoRaWAN network in real time. The proposed model features pre-formatted alarm messages displayed on the OLED display, transmitted along with sensor readings to the connected LoRa receiver via the web interface and Wi-Fi operation application [14],
- monitoring forests and analysing signals collected from multiple sensors, e.g. the research conducted in 2025 includes a description of the design and development of several portable and wireless systems with sensors, which enable analysing the signals collected from multiple sensors based on the Internet of Things (IoT) in crisis situations. They include fires and earthquakes or situations, when the materials used in buildings and other structures are subject to excessive stress caused by natural disasters. The authors presented innovative sensors with remote operation via Wi-Fi and LoRa [15].

The research on radio communication and LoRa communication [16–17] shows that when there is a straight radio route between the transmitting antenna and the receiving antenna (the so-called Line-of-sight, LoS), both communications can be operated over long distances from a dozen to several dozens of kilometres. If the buildings, topography or forestation obstruct the direct radio route, the range drops dramatically (the so-called Non-Line-of-Sight, NLoS). In urban areas, where obstacles are many, LoRaWAN networks can operate efficiently over the distances of more than 1 km (due to high sensitivity of the receiver), but phenomena like diffraction and reflection are critical.

Methods

As mentioned above, the research results presented in the subject article and the resulting conclusions and recommendations for civil protection solutions related to the use of the LoRa technology for efficient alarming of threats and supporting evacuation, were developed with technological partners, manufacturers and suppliers in this range of products and dedicated solutions. To prepare the article, the authors used the results of the research conducted by CNBOP-PIB as part of the product and

- zapewnienie łączności głosowej (system przetwarzania głosu dla środowisk wąskopasmowych, który wykorzystuje technologię rozproszonego widma LoRa jako protokół komunikacyjny oraz technologię rozpoznawania mowy jako metodę kompresji), umożliwiając zdalną komunikację ratowników podczas działań ratowniczych, nawet w środowiskach pozbawionych sieci publicznych [13],
- alarmowania ludności o zagrożeniach (na przykładzie badań prowadzonych w 2025 r., wskazujących na możliwość zastosowania autonomicznego systemu komunikacji wykorzystującego technologię LoRa i platformę Arduino). Dzięki ręcznemu generatorowi prądu system działa nieprzerwanie, bez potrzeby zewnętrznego źródła zasilania. Urządzenie jest wyposażone w układ GPS NEO-6M i czujnik tlenu, które przekazują w czasie rzeczywistym informacje o położeniu i środowisku za pośrednictwem sieci LoRaWAN. Proponowany model posiada wstępnie sformatowane komunikaty alarmowe wyświetlane na wyświetlaczu OLED, które wraz z odczytami czujników są przekazywane do podłączonego odbiornika LoRa za pośrednictwem interfejsu internetowego i aplikacji obsługującej Wi-Fi [14],
- monitorowanie lasów i analiza sygnałów zebranych z wielu czujników – np. badania prowadzone w 2025 r. opisują budowę i rozwój kilku przenośnych i bezprzewodowych systemów z czujnikami, które umożliwiają analizę sygnałów zebranych z wielu czujników opartych na Internecie Rzeczy (IoT) w sytuacjach kryzysowych. Należą do nich pożary i trzęsienia ziemi lub przypadki, w których materiały używane w budynkach i innych konstrukcjach są poddawane dużemu naprężeniu z powodu katastrof naturalnych. Autorzy przedstawili nowatorskie czujniki działające zdalnie za pośrednictwem Wi-Fi i LoRa [15].

Badania komunikacji radiowej oraz komunikacji LoRa [16–17] wykazują, że w przypadku gdy istnieje prosta droga radiowa między anteną nadawczą a odbiorczą (tzw. *Line-of-sight*, LoS), obie komunikacje mogą być realizowane na znaczne odległości sięgające od kilkunastu do kilkudziesięciu kilometrów. W warunkach, gdy budynki, ukształtowanie terenu, czy zalesienia zasłaniają bezpośredni tor radiowy, zasięg drastycznie spada (tzw. *Non-Line-of-Sight*, NLoS). W zabudowie miejskiej natomiast, gdzie przeszkody są częste, sieci LoRaWAN mogą działać sprawnie na odległości ponad 1 km (dzięki dużej czułości odbiornika), ale kluczowe są tam zjawiska takie jak dyfrakcja i odbicia.

Metody

Jak już wspomniano powyżej, wnioski i rekomendacje przedstawione w niniejszym artykule sformułowano na podstawie badań prowadzonych z partnerami technologicznymi, producentami i dostawcami rozwiązań wykorzystujących technologię LoRa. Analizowano w nich możliwość użycia przedmiotowych rozwiązań na potrzeby efektywnego alarmowania o zagrożeniach i wspierania ewakuacji. W celu opracowania artykułu wykorzystano także wyniki badań realizowanych przez CNBOP-PIB

innovation testing procedure, as well as own research made available by manufacturers [6].

As a reminder, exactly to enable testing the products used in fire protection, more than 10 years ago the State Fire Service introduced the innovative product testing procedure [18]. The procedure assumes practical testing of products or solutions by the firefighters serving in Testing Units, the rescue and firefighting units of the PSP selected for testing. It involves the manufacturer of the product/solution, JRG PSP and CNBOP-PIB. As a rule, the procedure enables the manufacturers to collect feedback on the manufactured products and the fire-fighters to express opinions on them. In practice, however, it is a unique tool for empirical research, testing and implementing new solutions both for fire protection and civil protection.

The confirmation of meeting the requirements and expectations of the end user of the products (which is PSP in this case) is critical for introducing products to the market and use. This is particularly significant for innovative products and technical innovations that are yet to be checked in practice and reviewed for usability, functionality and workmanship. In such situation, it is critical for the manufacturer to obtain direct opinions from the users of the product. This procedure is described in CNBOP-PIB and has been tested by PSP for more than 10 years, it is flexible and “capacious” enough to address new needs and challenges, such as testing new technologies. Thus, under the above-mentioned Testing Innovative Products Procedure at PSP, NEURON in collaboration with DIGITEX submitted the Hybrid Communication System HSR, which is designed for notifying and alarming the population by starting alarm sirens and for dispatching OSP units from the PSP Command Support System.

The Hybrid Communication System HSR consists of two components: the PSP base station and the OSP mobile station. The communication between the PSP base station and the OSP mobile station is operated in two ways:

- 1) digital radio communication DMR – using TDMA MotoTRBO modulation with AES encryption in a channel within the VHF range, e.g. 148.725MHz. Transmission in a radio channel (data frames additionally secured with AES encryption and authorisation keys as Digitex protocol functionality);
- 2) LoRa digital radio communication – low power long range wireless communication protocol and system. The maximum distances between devices and base stations are 10–15 km. The data transmission rate in the LoRa system is from 0.3 kb/s to 37.5 kb/s. LoRa uses licence-free sub-Gigahertz radio frequency bands, such as 169 MHz, 433 MHz, 868 Mhz.

The Hybrid Communication System HSR was tested in accordance with the testing programme approved by the Chief of PSP in the CNBOP-PIB Testing Unit². The tests were completed by the Laboratory of Fire Alarm Systems and Fire Automation – BA, CNBOP-PIB, in collaboration with the manufacturers of the system. The tests were conducted from 23.05.2024 to 26.06.2024.

² Given the specifics of the tested product/technology, it was decided that the testing required specific qualifications and competencies of the Laboratory of Fire Alarm Systems and Fire Automation – BA, CNBOP-PIB. Thus, in this testing process, the testing unit was CNBOP-PIB, not JRG PSP.

w ramach procedury testowania wyrobów i rozwiązań innowacyjnych, a także udostępnionych przez producentów ich badań własnych [6].

Dla przypomnienia, właśnie w celu umożliwienia testowania wyrobów stosowanych w ochronie przeciwpożarowej ponad 10 lat temu w Państwowej Straży Pożarnej wdrożono procedurę testowania wyrobów innowacyjnych [18]. Procedura ta zakłada praktyczne testowanie wyrobów lub rozwiązań przez strażaków pełniących służbę w Jednostkach Testujących – jednostkach ratowniczo-gaśniczych PSP wytypowanych do testowania. Biorą w niej udział producent wyrobu/rozwiązania, JRG PSP oraz CNBOP-PIB. Procedura co do zasady umożliwia producentom zebranie opinii o produkowanych wyrobach, a strażakom wyrażanie opinii o nich. W praktyce jest to jednak unikalne narzędzie do badań empirycznych, testowania i wdrażania nowych rozwiązań zarówno na potrzeby ochrony przeciwpożarowej, jak i ochrony ludności.

Potwierdzenie spełnienia wymagań i oczekiwań użytkownika końcowego wyrobów (którym w tym przypadku jest PSP) jest kluczowe z punktu widzenia wprowadzenia wyrobów do sprzedaży i stosowania. Jest to szczególnie istotne w przypadku wyrobów innowacyjnych i nowości technicznych, które jeszcze nie sprawdzono w praktyce i nie sformułowano opinii w zakresie ich przydatności, funkcjonalności i wykonania. W takiej sytuacji niezwykle ważne dla producenta jest uzyskanie bezpośredniej opinii użytkowników wyrobu. Procedura ta, opracowana w CNBOP-PIB, a testowana w PSP już przez ponad 10 lat, jest na tyle elastyczna i „pojemna”, iż pozwala wychodzić naprzeciw nowym potrzebom i wyzwaniom, takim jak m.in. testowanie technologii. Dlatego do przywołanej powyżej procedury Testowania Wyrobów Innowacyjnych w PSP firma NEURON we współpracy z firmą DIGITEX zgłosiła Hybrydowy System Komunikacji HSR, który przeznaczony jest do powiadamiania i alarmowania ludności poprzez uruchamianie syren alarmowych oraz do dysponowania jednostek OSP z poziomu Systemu Wspomagania Dowodzenia PSP.

Hybrydowy System Komunikacji HSR składa się z dwóch elementów – stacji bazowej PSP oraz stacji mobilnej OSP. Komunikacja między stacją bazową PSP a stacją mobilną OSP jest realizowana dwiema drogami:

- 1) cyfrowa komunikacja radiowa DMR – wykorzystanie modulacji TDMA MotoTRBO, z użyciem szyfrowania AES, na kanale z zakresu VHF np. 148.725MHz. Transmisja w kanale radiowym (ramki danych dodatkowo zabezpieczono szyfrowaniem AES i kluczami autoryzacyjnymi jako funkcjonalność protokołu Digitex);
- 2) cyfrowa komunikacja radiowa LoRa – protokół i system komunikacji bezprzewodowej dalekiego zasięgu o małej mocy. Maksymalne odległości między urządzeniami a stacjami bazowymi wynoszą 10–15 km. Szybkość transmisji danych w systemie LoRa wynosi między 0,3 kb/s a 37,5 kb/s. LoRa wykorzystuje wolne od licencji sub-gigahercowe pasma częstotliwości radiowych, takie jak 169 MHz, 433 MHz, 868 MHz.

Testowanie Hybrydowego Systemu Komunikacji HSR odbywało się zgodnie z programem testowania zatwierdzonym przez Komendanta Głównego PSP w CNBOP-PIB – Jednostce

The purpose was to confirm the possibility of using the Hybrid Communication System HSR for sending communications for the purposes of notifying and alarming the population by starting alarm sirens and dispatching OSP units.

Under this testing programme, the following additional verification and test procedures were conducted:

- assessment of the functional compatibility of devices,
- check of the DMR radio communication in selected locations in the Otwock district and assessment of the range,
- check of the LoRa communication in selected locations in the Otwock district and assessment of the range,
- check of the DMR and LoRa radio communication redundancy.

This research was intended to confirm the correctness of communication by transmitting messages between the base station and the mobile station, and obtaining confirmation of the execution of the alarm siren activation request using radio and LoRa communications. Control signals were sent from the base station via radio and LoRa communications to the mobile station. The mobile station was driven around the local area of the base station to verify the actual range and reception of signals via both types of communication. The mobile station was receiving control signals from the main station, to confirm them or not in two ways the reception of control signals and order completion.

The base station (referred to as "District PSP" for testing purposes) was installed in the following locations:

- geographical coordinates 52°06'58.6"N 21°12'43.6"E, ul. Nadwiślańska 213, Józefów;
- geographical coordinates 49°51'40.0"N 19°20'20.0"E, ul. Batorego 14, Andrychów.

The transmitting and receiving antennas were placed on the roof to achieve the greatest possible visibility (range) with other stations (the mobile station). The tests in Andrychów only included the measurement of LoRa communication. The measurements of radio communication were not completed due to the terrain characteristics and the assumption that in this terrain achieving radio communication could be achieved without difficulty.

The mobile station (named "OSP" for testing purposes) was mounted on a vehicle, along with elevated transmitting and receiving antennas outside the vehicle, to ensure the best possible "visibility" between the tower station antenna and the mobile station.

Detailed test procedure:

- 1) Initiate signal transmission from the base station;
- 2) Check if the signal was sent by both communication routes;
- 3) Check if the signal was received by the mobile station for each route and record the signal transmission time for each communication route;
- 4) Confirm if the signal was received in the mobile station;
- 5) Check if the confirmation signal was sent by both communication routes;
- 6) Check if the confirmation signal was received by the base station for each route and record the signal transmission time for each communication route;

Testującej². Testy zostały wykonane przez Zespół Laboratoriów Sygnalizacji Alarmu Pożaru i Automatyki Pożarniczej – BA, CNBOP-PIB przy współudziale producentów systemu. Testowanie odbywało się w dniach od 23.05.2024 do 26.06.2024 roku. Jego celem było potwierdzenie możliwości wykorzystania Hybridowego Systemu Komunikacji HSR do przesyłania komunikatów na potrzeby powiadamiania i alarmowania ludności poprzez uruchamianie syren alarmowych oraz do dysponowania jednostek OSP.

W ramach tego programu testowania prowadzono dodatkowe następujące procedury weryfikacji i badań:

- ocena kompatybilności funkcjonalnej urządzeń,
- sprawdzenie komunikacji radiowej DMR w wybranych miejscach na terenie powiatu otwockiego i ocena zasięgu,
- sprawdzenie komunikacji LoRa w wybranych miejscach na terenie powiatu otwockiego i ocena zasięgu,
- sprawdzenie redundancji komunikacji radiowej DMR i LoRa.

Badania te miały na celu potwierdzenie poprawności komunikacji poprzez przesyłanie komunikatów pomiędzy stacjami bazową i mobilną oraz uzyskiwanie potwierdzenia realizacji zlecenia uruchomienia syreny alarmowej z wykorzystaniem łączności radiowej i łączności LoRa. Ze stacji bazowej wysyłane były sygnały sterujące drogą komunikacji radiowej oraz komunikacji LoRa do stacji mobilnej. Stacja mobilna przewożona była po lokalnej okolicy stacji bazowej tak, aby sprawdzić faktyczne możliwości zasięgu i otrzymywania sygnałów poprzez oba typy komunikacji. Stacja mobilna odbierała sygnały sterujące od stacji głównej, po czym potwierdzała lub nie dwiema drogami odebranie sygnałów sterujących oraz realizację zlecenia.

Stacja bazowa (nazwana na potrzeby testowania „Powiatowa PSP”) zamontowana została w następujących lokalizacjach:

- współrzędne geograficzne 52°06'58.6"N 21°12'43.6"E, ul. Nadwiślańska 213, Józefów;
- współrzędne geograficzne 49°51'40.0"N 19°20'20.0"E, ul. Batorego 14, Andrychów.

Anteny nadawczo-odbiorcze zostały wyprowadzone na dach tak, aby uzyskać jak największy zakres widzialności (zasięgu) z innymi stacjami (stacją mobilną). W przypadku badań na terenie Andrychowa wykonano pomiar tylko łączności LoRa. Odstąpiono od pomiarów łączności radiowej z uwagi na charakterystykę terenu i przyjęte założenie, że w tym terenie nie będzie trudności z uzyskaniem łączności radiowej.

Stacja mobilna (nazwana na potrzeby testowania „OSP”) była zamontowana na samochodzie, wraz z wyniesionymi antenami nadawczo-odbiorczymi na zewnątrz samochodu w taki sposób, aby zapewnić jak najlepszą, tak zwaną „widzialność” anteny stacji na wieży i stacji mobilnej.

Szczegółowy przebieg badania:

- 1) Zainicjowano transmisję sygnału w stacji bazowej;
- 2) Sprawdzone, czy sygnał został wysłany obiema drogami komunikacji;

² Z uwagi na specyfikę testowanego wyrobu/technologii uznano, iż to testowania niezbędne są określone kwalifikacje i kompetencje, którymi dysponuje Zespół Laboratoriów Sygnalizacji Alarmu Pożaru i Automatyki Pożarniczej - BA, CNBOP-PIB. Dlatego w tym procesie testowania jednostką testującą było CNBOP-PIB, a nie JRG PSP.

- 7) For each measurement point, record the presence of communication in both communication routes or the fact of no communication for the given route.

The general diagram of the test station was presented in figure 2.

The test station consisted of the following components:

- 3) Sprawdzone, czy sygnał został odebrany przez stację mobilną dla każdej drogi i odnotowano czas transmisji sygnału dla każdej z dróg komunikacji;
- 4) Potwierdzono odbiór sygnału na stacji mobilnej;
- 5) Sprawdzone, czy sygnał potwierdzenia został wysłany obiema drogami komunikacji;
- 6) Sprawdzone, czy sygnał potwierdzenia został odebrany przez stację bazową dla każdej drogi i odnotowano czas transmisji sygnału dla każdej z dróg komunikacji;
- 7) Dla każdego z punktów pomiarowych odnotowano obecność komunikacji dla obydwu dróg komunikacji lub fakt braku komunikacji dla danej drogi.

Ogólny schemat stanowiska badawczego przedstawiono na rycinie 2.

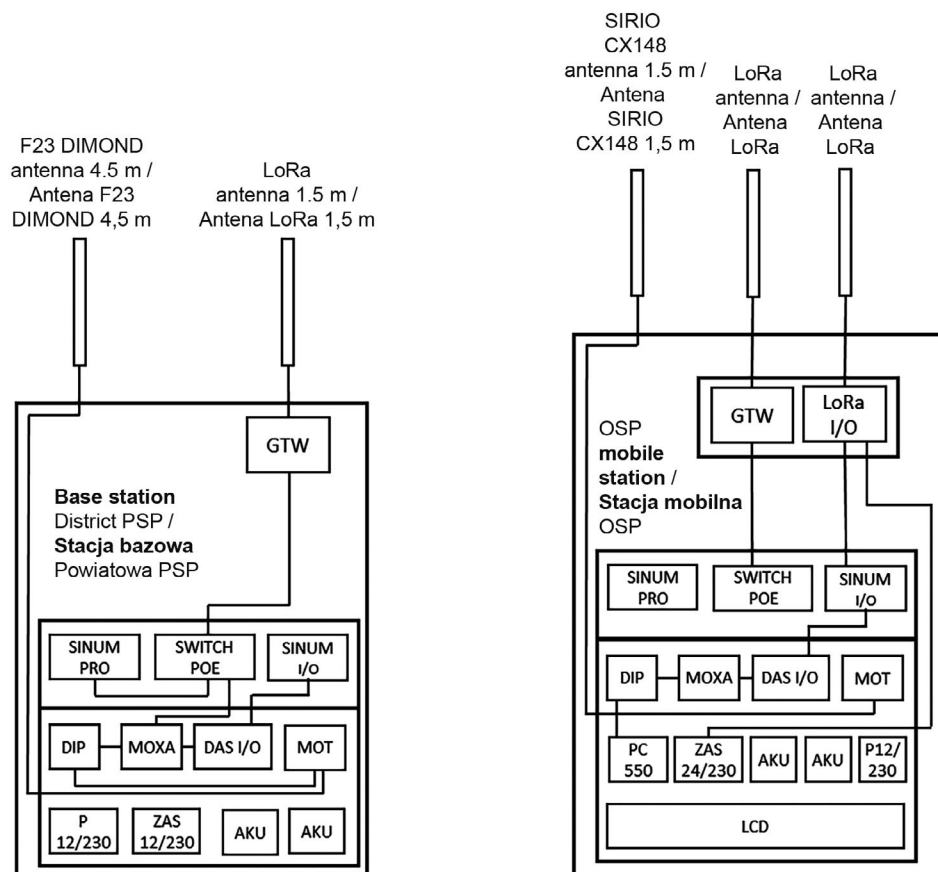


Figure 2. Diagram of the test station, in which: MOT – Motorola radio, DIP – industrial computer, MOXA – RS485 ports server, DAS I/O – Digitex digital input/output module, P 12/230 – 12VDC/230VAC converter, ZAS – 24VDC power supply, AKU – batteries, GTW – LoRa gateway, SINUM PRO – Sinum control panel, SINUM I/O – Sinum Pro input/output card, SWITCH POE – switch with POE 24VDC power output, PC 550 – alarm siren controller, LCD – display

Rycina 2. Schemat stanowiska badawczego, gdzie MOT – radio Motorola, DIP – komputer przemysłowy, MOXA – serwer portów RS485, DAS I/O – moduł wejść/wyjść cyfrowych Digitex, P 12/230 – przetwornica 12VDC/230VAC, ZAS – zasilacz 24VDC, AKU – akumulatory, GTW – bramka LoRa, SINUM PRO – centrala Sinum, SINUM I/O – karta wejść/wyjść Sinum Pro, SWITCH POE – switch z wyjściem zasilania POE 24VDC, PC 550 – sterownik syreny alarmowej, LCD – wyświetlacz

Source: Own elaboration.

Źródło: Opracowanie własne.

- antennas:
 - base station: building roof, radio antenna 4.5 m (3 x 5/8), Lora antenna 1.5 m with MikroTik LtAP LTE6 kit access point,
 - mobile station: 4 m mast (first attempt) or 19 m lift (second attempt), radio antenna 1.5 m, Lora antenna 1.5 m with MikroTik LtAP LTE6 kit access point and Sinum KW-22L;
- base station – 19" PILO 9U rack:
 - DSP-16 control panel (digitex CZK/IP) with Motorola DM4400e radio and Motorola RMN5052A microphone,
 - DSP-16 MAZ panel,
 - MeanWell HDR-100-24N power supply,
 - TECH SinumPro EH-02PRO,
 - TECH SinumPro MB-04m (2 pcs.),
 - PoE ISFG64-BT Pulsar industrial switch,
 - ZM12V10A-151B-000 power supply,
 - Digitex DAS-8180,
 - Digitex DAS-4R04AI,
 - Auspicious button,
 - MOXA NPort 5232,
 - Europower EV-33-12 battery,
 - fans with temperature sensor;
- mobile station, DSP-62C rack:
 - Motorola DM4600e radio with Motorola RMN 5127c microphone,
 - DDM-07 Digitex,
 - Digitex signalling and operation panel,
 - Digitex DAS-8180,
 - Digitex DAS-4R04AI,
 - Digitex DMS-62,
 - TECH SinumPro EH-02PRO,
 - TECH SinumPro MB-04m (2 pcs.),
 - loudspeaker (alarm siren simulator),
 - PE-16D voltage converter,
 - Digitex ZSE24 power supply,
 - TST160/012/2 transformer,
 - PC-550A Digitex,
 - Digitex Switch,
 - MOXA NPort 5232,
 - switch,
 - 230 VAC outlet,
 - Europower EV-33-12 battery (2 pcs.).

The view of individual components of the test station is presented in figures 3–5.

In addition, the following measurement devices were used

W skład stanowiska badawczego wchodziły następujące elementy:

- anteny:
 - stacja bazowa: dach budynku, antena radio 4,5 m (3 x 5/8), antena Lora 1,5 m z punktem dostępowym MikroTik LtAP LTE6 kit,
 - stacja mobilna: maszt 4 m (pierwsza próba) lub podnośnik zwyżka 19 m (druga próba), antena radio 1,5 m, antena Lora 1,5 m z punktem dostępowym MikroTik LtAP LTE6 kit i Sinum KW-22L;
- stacja bazowa – szafa 19" PILO 9U:
 - centrala alarmowa DSP-16 (digitex CZK/IP) z radiem Motorola DM4400e z mikrofonem Motorola RMN 5052A,
 - panel DSP-16 MAZ,
 - zasilacz MeanWell HDR-100-24N,
 - TECH SinumPro EH-02PRO,
 - TECH SinumPro MB-04m (2 szt.),
 - PoE Switch przemysłowy ISFG64-BT Pulsar,
 - zasilacz ZM12V10A-151B-000,
 - Digitex DAS-8180,
 - Digitex DAS-4R04AI,
 - przycisk Auspicious,
 - MOXA NPort 5232,
 - bateria Europower EV-33-12,
 - wentylatory z czujnikiem temepatury;
- stacja mobilna, szafa DSP-62C:
 - radio Motorola DM4600e z mikrofonem Motorola RMN5127c,
 - DDM-07 Digitex,
 - panel sygnalizacji i obsługi Digitex,
 - Digitex DAS-8180,
 - Digitex DAS-4R04AI,
 - Digitex DMS-62,
 - TECH SinumPro EH-02PRO,
 - TECH SinumPro MB-04m (2 szt.),
 - głośnik (symulator syreny alarmowej),
 - przetwornica napięcia PE-16D
 - zasilacz Digitex ZSE24,
 - transformator TST160/012/2,
 - PC-550A Digitex,
 - Digitex Switch,
 - MOXA NPort 5232,
 - przełącznik,
 - gniazdo 230 V AC,
 - bateria Europower EV-33-12 (2 szt.).

Widok poszczególnych elementów stanowiska badawczego przedstawiono na rycinach 3–5.



Figure 3. View of the base station
Rycina 3. Widok stacji bazowej

Source: Own elaboration.
Źródło: Opracowanie własne.

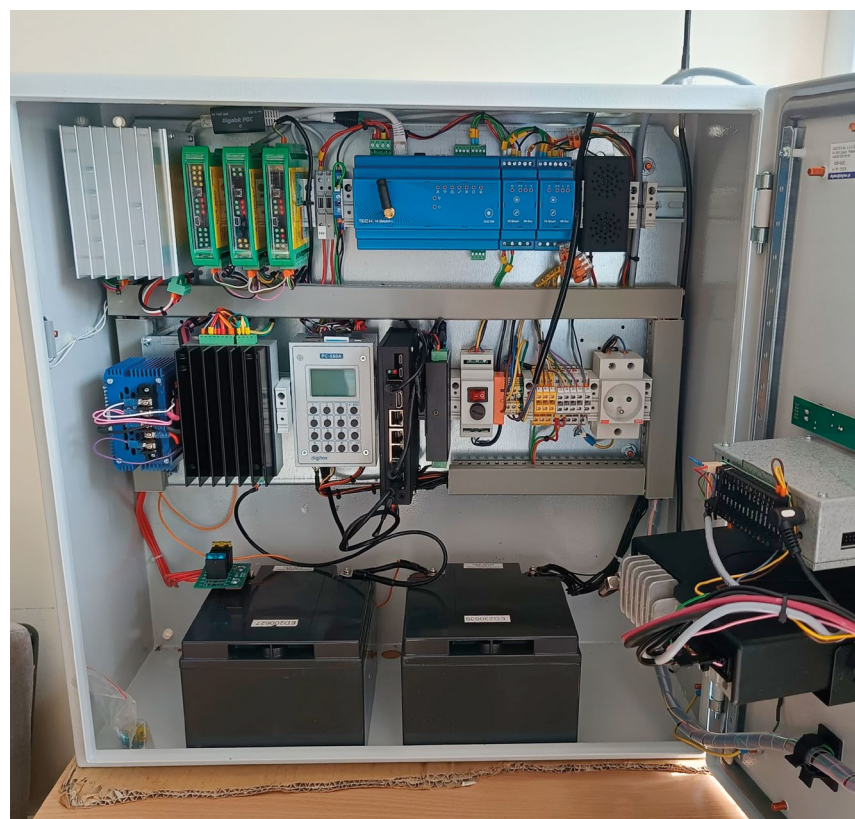


Figure 4. View of the mobile station
Rycina 4. Widok stacji mobilnej

Source: Own elaboration.
Źródło: Opracowanie własne.



Figure 5. View of antennas: a) base station, b) 4 m mast of the mobile station, c) 19 m lift of the mobile station
Rycina 5. Widok anten w: a) stacji bazowej, b) stacji mobilnej maszt 4 m, c) stacji mobilnej

Source: Own elaboration.

Źródło: Opracowanie własne.

for the tests:

- 8) time measurement: at the base station, the electronic stopwatch type HS-80TW, no. 406Q05R, and in addition, at the mobile station, the electronic stopwatch type Fenix 6X PRO,
- 9) altitude measurement: FLUKE 424D range finder,
- 10) RSSI and SNR: indications of the devices included in the tested communication system,
- 11) mobile station altitude reading: Fenix 6X PRO altimeter.

Ponadto do badań wykorzystano następujące wyposażenie pomiarowe:

- 8) pomiar czasu: przy stacji bazowej sekundomierz elektroniczny typu HS-80TW, nr 406Q05R oraz dodatkowo przy stacji mobilnej sekundomierz elektroniczny Fenix 6X PRO,
- 9) pomiar wysokości: dalmierz FLUKE 424D,
- 10) RSSI i SNR: wskazania z urządzeń wchodzących w skład badanego systemu komunikacji,
- 11) odczyt wysokości stacji mobilnej: wysokościomierz elektroniczny Fenix 6X PRO.

Results

The results of measurements are presented in tables 1–3.

The tests also verified the cooperation between individual

Wyniki

Wyniki przeprowadzonych pomiarów zaprezentowano w tabelach 1–3.

Table 1. The results of measurements in and around the Otwock district – mobile station antenna on the 4 m mast

Tabela 1. Wynik pomiarów w powiecie otwockim i okolicach – antena stacji mobilnej na maszcie 4 m

No. / Lp.	Location (name, GPS coordinates) / Miejsce (nazwa, współrzędne GPS)	Line- of-sight distance from the base station [km] / Odległość w linii prostej od stacji bazowej [km]	Altitude above the sea level [m] / Wysokość n.p.m. [m]	Radio communication / Komunikacja radiowa		LoRa communication / Komunikacja LoRa		
				Transmission time [s] / Czas transmisji [s]	RSSI [dBm]	Transmission time [s] / Czas transmisji [s]	RSSI [dBm]	SNR [dB]
1	52°02'13.0"N 21°20'58.5"E	12.9	99	> 1	-96	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji

No. / Lp.	Location (name, GPS coordinates) / Miejsce (nazwa, współrzędne GPS)	Line- of-sight distance from the base station [km] / Odległość w linii prostej od stacji bazowej [km]	Altitude above the sea level [m] / Wysokość n.p.m. [m]	Radio communication / Komunikacja radiowa		LoRa communication / Komunikacja LoRa		
				Transmission time [s] / Czas transmisji [s]	RSSI [dBm]	Transmission time [s] / Czas transmisji [s]	RSSI [dBm]	SNR [dB]
2	52°02'22.1"N 21°17'50.1"E	10.4	93	> 1	-82	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
3	52°04'32.9"N 21°14'53.1"E	5.1	76	> 1 / > 1	-81	19	-113	-20
4	52°02'53.8"N 21°14'49.4"E	8.0	88	> 1	-81	20	-115	-16
5	52°02'22.1"N 21°17'50.1"E	10.4	93	> 1	-84	2	-113	-11
6	52°02'13.0"N 21°20'58.5"E	12.9	99	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
7	52°01'35.4"N 21°18'33.5"E	12.0	90	> 1	-89	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
8	52°00'47.6"N 21°22'03.9"E	15.7	98	> 1	-97	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
9	52°07'53.9"N 21°24'58.8"E	14.0	108	> 1	-104	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
10	52°08'11.5"N 21°19'59.4"E	8.6	107	2	-92	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
11	52°06'43.9"N 21°18'38.6"E	6.7	106	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
12	52°09'30.8"N 21°12'55.0"E	4.7	90	2	-76	10	-110	-19
13	52°10'32.9"N 21°11'51.9"E	6.7	94	> 1	-89	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
14	52°10'25.1"N 21°09'11.2"E	7.5	86	> 1	-81	2	-108	-120
15	52°06'36.0"N 21°08'03.5"E	5.4	84	> 1	-69	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
16	52°05'46.0"N 21°07'04.2"E	6.8	87	> 1	-74	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
17	51°59'00.5"N 21°13'09.6"E	14.8	118	> 1	-88	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji

Source: Own elaboration.
Źródło: Opracowanie własne.

Table 2. The results of measurements in and around the Otwock district – mobile station antenna on the 19 m lift
Tabela 2. Wynik pomiarów w powiecie otwockim i okolicach – antena stacji mobilnej na podnośniku powyżej 19 m

No. / Lp.	Location (name, GPS coordinates) / Miejsce (nazwa, współrzędne GPS)	Line-of-sight distance from the base station [km] / Odległość w linii prostej od stacji bazowej [km]	Altitude above the sea level [m] / Wysokość n.p.m. [m]	Radio communication / Komunikacja radiowa		LoRa communication / Komunikacja LoRa		
				Transmission time [s] / Czas transmisji [s]	RSSI [dBm]	Transmission time [s] / Czas transmisji [s]	RSSI [dBm]	SNR [dB]
1	52°01'21.9"N 21°17'16.0"E	11.7	91	< 1	-78	4.5	-107	-2
2	52°01'35.4"N 21°18'33.5"E	12.0	90	< 1	-87	6	-112	-8
3	52°02'13.0"N 21°20'58.5"E	12.9	99	< 1	-87	3	-111	-16
4	52°00'47.6"N 21°22'03.9"E	15.7	98	< 1	-89	3	-113	-9
			98 (lift at 12 m) / 98 (zwyczajka na 12 m)	< 1	-94	3	-113	-12
			98 (lift at 4 m) / 98 (zwyczajka na 12 m)	< 1	-100	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
5	52°03'58.3"N 21°21'23.7"E	11.4	118	< 1	-88	3	-111	-10
6	52°06'43.9"N 21°18'38.6"E	6.7	106	< 1	-92	3	-114	-17
7	52°11'03.0"N 21°10'07.5"E	8.1	84	< 1	-74	2.5	-106	-11
8	52°08'13.7"N 21°14'02.0"E	2.7	93	< 1	-60	3	-96	-1

Source: Own elaboration.
 Źródło: Opracowanie własne.

Table 3. The results of measurements in the Wadowice district – mobile station antenna on the 4 m mast
Tabela 3. Wynik pomiarów w powiecie wadowickim – antena stacji mobilnej na maszcie 4 m

No. / Lp.	Location (name, GPS coordinates) / Miejsce (nazwa, współrzędne GPS)	Line-of-sight distance from the base station [km] / Odległość w linii prostej od stacji bazowej [km]	Altitude above the sea level [m] / Wysokość n.p.m. [m]	Radio communication / Komunikacja radiowa		LoRa communication / Komunikacja LoRa		
				Transmission time [s] / Czas transmisji [s]	RSSI [dBm]	Transmission time [s] / Czas transmisji [s]	RSSI [dBm]	SNR [dB]
1	49°52'12.00"N 19°18'10.80"E	2.9	329	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
2	49°51'33.48"N 19°19'28.20"E	1.1	345	-	-	> 20	-84	-10
3	49°52'39.36"N 19°17'26.52"E	4.1	318	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji

No. / Lp.	Location (name, GPS coordinates) / Miejsce (nazwa, współrzędne GPS)	Line-of-sight distance from the base station [km] / Odległość w linii prostej od stacji bazowej [km]	Altitude above the sea level [m] / Wysokość n.p.m. [m]	Radio communication / Komunikacja radiowa		LoRa communication / Komunikacja LoRa		
				Transmission time [s] / Czas transmisji [s]	RSSI [dBm]	Transmission time [s] / Czas transmisji [s]	RSSI [dBm]	SNR [dB]
4	49°51'49.68"N 19°18'46.80"E	2.0	337	-	-	> 20	-115	-7.5
5	49°51'14.76"N 19°18'54.36"E	1.8	339	-	-	> 20	-114	-5.3
6	49°50'46.32"N 19°18'36.72"E	2.5	357	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
7	49°50'30.12"N 19°17'24.72"E	4.0	367	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
8	49°49'57.72"N 19°18'17.28"E	3.8	392	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
9	49°49'51.60"N 19°18'25.20"E	3.8	415	-	-	> 20	-115	-7.3
10	49°49'37.20"N 19°19'7.68"E	3.8	398	-	-	> 20	-112	-2
11	49°49'55.20"N 19°20'13.20"E	3.0	357	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
12	49°49'8.40"N 19°20'2.40"E	4.4	384	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
13	49°48'23.76"N 19°19'7.32"E	6.0	440	-	-	> 20	-112	-5.8
14	49°48'3.60"N 19°18'21.60"E	6.8	483	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
15	49°47'9.60"N 19°19'26.40"E	8.1	556	-	-	> 20	-110	-1.5
16	49°46'32.52"N 19°19'31.08"E	9.3	708	-	-	> 20	-115	-7.3
17	49°53'20.04"N 19°22'19.56"E	4.1	326	-	-	> 20	-105	-3.8
18	49°53'53.16"N 19°24'57.24"E	7.1	279	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
19	49°52'44.40"N 19°24'36.00"E	5.6	313	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
20	49°52'12.72"N 19°24'26.64"E	5.1	319	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
21	49°51'54.36"N 19°23'56.04"E	4.4	322	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji

No. / Lp.	Location (name, GPS coordinates) / Miejsce (nazwa, współrzędne GPS)	Line-of-sight distance from the base station [km] / Odległość w linii prostej od stacji bazowej [km]	Altitude above the sea level [m] / Wysokość n.p.m. [m]	Radio communication / Komunikacja radiowa		LoRa communication / Komunikacja LoRa		
				Transmission time [s] / Czas transmisji [s]	RSSI [dBm]	Transmission time [s] / Czas transmisji [s]	RSSI [dBm]	SNR [dB]
22	49°51'29.88"N 19°22'24.96"E	2.5	336	-	-	> 20	-114	-6.3
23	49°51'11.16"N 19°21'36.00"E	1.6	390	-	-	> 20	-110	-1.8
24	49°50'56.40"N 19°21'36.00"E	1.8	397	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
25	49°50'16.80"N 19°22'40.80"E	3.6	397	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
26	49°49'37.20"N 19°23'24.00"E	5.1	479	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
27	49°49'55.20"N 19°22'26.40"E	3.9	383	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
28	49°48'57.96"N 19°23'45.60"E	6.2	438	-	-	> 20	-114	-5.5
29	49°47'57.12"N 19°24'50.76"E	8.5	473	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
30	49°47'42.00"N 19°23'16.80"E	7.9	465	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
31	49°48'21.60"N 19°22'4.80"E	6.2	447	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
32	49°49'41.88"N 19°20'40.56"E	3.4	402	-	-	> 20	-103	-6.3
33	49°51'44.64"N 19°21'9.00"E	1.1	327	-	-	> 20	-99	-7
34	49°51'38.88"N 19°21'31.32"E	1.4	326	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
35	49°51'27.72"N 19°21'15.12"E	1.1	342	-	-	> 20	-110	-2.3
36	49°51'19.08"N 19°21'4.68"E	0.9	346	-	-	> 20	-107	-3.5
37	49°51'0.00"N 19°20'51.00"E	1.1	338	-	-	> 20	-115	-7
38	49°50'38.04"N 19°20'45.96"E	1.7	338	-	-	> 20	-107	-9.5
39	49°50'35.16"N 19°20'12.12"E	1.7	340	-	-	> 20	-114	-1
40	49°51'4.68"N 19°19'37.20"E	1.2	352	-	-	> 20	-95	-9.8

No. / Lp.	Location (name, GPS coordinates) / Miejsce (nazwa, współrzędne GPS)	Line-of-sight distance from the base station [km] / Odległość w linii prostej od stacji bazowej [km]	Altitude above the sea level [m] / Wysokość n.p.m. [m]	Radio communication / Komunikacja radiowa		LoRa communication / Komunikacja LoRa		
				Transmission time [s] / Czas transmisji [s]	RSSI [dBm]	Transmission time [s] / Czas transmisji [s]	RSSI [dBm]	SNR [dB]
41	49°53'5.64"N 19°21'10.44"E	3.1	294	-	-	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji	no communi- cation / brak komunikacji
42	49°52'44.04"N 19°21'16.92"E	2.5	330	-	-	> 20	-109	-1.8
43	49°52'14.16"N 19°20'37.32"E	1.4	310	-	-	> 20	-105	-5.3

Source: Own elaboration based on [5].

Źródło: Opracowanie własne na podstawie [5].

components. The devices cooperated and were compatible with one another. In addition, the transmission of signals between the base station and the mobile station after simulated failure of one transmission route was checked. The redundancy of radio and LoRa communication was maintained.

Podczas badań zweryfikowano również współpracę poszczególnych elementów. Urządzenia współpracowały ze sobą i były ze sobą kompatybilne. Sprawdzone również przesyłanie sygnałów między stacją bazową a stacją mobilną po zasymulowaniu uszkodzenia jednego z torów transmisji. Redundancja komunikacji radiowej i LoRa została zachowana.

Discussion of methods and results

The first series of tests in the Otwock district enabled the following conclusions:

- 1) The base station and the mobile station of the HSR system are functionally compatible with each other;
- 2) It is possible to use DMR communication in HSR – distance obtained during the tests: 15.7 km;
- 3) It is possible to use LoRa communication in HSR – distance obtained during the tests: 10.4 km;
- 4) In laboratory conditions, the HSR system ensures communication redundancy; the redundancy of the HSR system was not confirmed in real conditions;
- 5) In five locations, correct DMR and LoRa communication was obtained; in five locations, correct DMR communication was obtained, no LoRa communication; in two locations neither DMR, nor LoRa communication was obtained;
- 6) Problems with establishing DMR and LoRa communication are influenced by:
 - terrain topography, i.a. the existence of hills between the location of the base station and mobile station,
 - the terrain forestation/urbanisation degree, including i.a. the condition of tree foliage, the height of buildings,
 - the presence of high voltage lines near the masts,
 - the height of antenna masts,
 - local radio communication conditions, including i.a. the presence of other radio communication devices, jamming devices etc.;

Dyskusja nad metodami i wynikami

Przeprowadzone badania pierwszej serii testów w powiecie otwockim pozwoliły na sformułowanie następujących wniosków:

- 1) Stacja bazowa i stacja mobilna systemu HSR są ze sobą kompatybilne funkcjonalnie;
- 2) Istnieje możliwość zastosowania w HSR komunikacji DMR – odległość uzyskana podczas testów: 15,7 km;
- 3) Istnieje możliwość zastosowania w HSR komunikacji LoRa – odległość uzyskana podczas testów: 10,4 km;
- 4) System HSR w warunkach laboratoryjnych zapewnia redundancję komunikacji; nie potwierdzono redundancji systemu HSR w warunkach rzeczywistych;
- 5) W pięciu lokalizacjach uzyskano poprawną komunikację DMR i LoRa; w pięciu lokalizacjach uzyskano poprawną komunikację DMR, brak komunikacji LoRa; w dwóch lokalizacjach nie uzyskano komunikacji DMR ani LoRa;
- 6) Na problemy z nawiązaniem komunikacji DMR i LoRa wpływ mają:
 - topografia terenu m.in. występowanie wzniesień pomiędzy lokalizacją stacji bazowej i stacji mobilnej,
 - stopień zalesienia/zurbanizowania terenu w tym m.in. stan ulistnienia drzew, wysokość budynków,
 - obecność linii wysokiego napięcia w pobliżu masztów,
 - wysokości masztów antenowych,
 - lokalne warunki radiokomunikacyjne w tym m.in. obecność innych urządzeń radiokomunikacyjnych, urządzeń zagłuszających itp.;

- 7) Another series of tests using a higher mobile station mast is needed, which should have a positive impact on the measurement results.

The second series of tests in the Otwock district enabled the following conclusions:

- 1) The base station and the mobile station of the HSR system are functionally compatible with each other;
- 2) It is possible to use LoRa communication in DMR – distance obtained during the tests: 15.7 km;
- 3) It is possible to use LoRa communication in HSR – distance obtained during the tests; 15.7 km;
- 4) In laboratory conditions, the HSR system ensures communication redundancy; the redundancy of the HSR system was also confirmed in real conditions ;
- 5) In eight locations, correct DMR and LoRa communication was obtained;
- 6) Increasing the mobile station mast height improved the radio communication conditions and enabled establishing DMR and LoRa communication in locations, in which it was not established during the first series of tests;
- 7) in total, during the two series of tests, correct DMR and LoRa communication with redundancy was obtained in sixteen test locations (81.25%), the greatest communication distance with redundancy obtained during the tests was 15.7 km.

The tests conducted in the Wadowice district enabled the following conclusions [6]:

- 1) The LoRa network range in the Wadowice district covers the area within approx. 10 km radius from the base station;
- 2) In most cases, the RSSI signal level is higher than -100 dBm, which ensures correct data reception;
- 3) At some points, located on the outskirts of town, RSSI can drop to -115 dBm, which can result in unstable data reception;
- 4) The LoRa network range is influenced by multiple factors, i.a.: base station antenna gain, base station antenna installation height, topography, development density and the radio noise level;
- 5) The test proved that the LoRa network near Andrychów provides a satisfactory range in developed areas, the data reception is mostly correct, however it should be noted that at some points in the outskirts of town the range can be unstable;
- 6) To improve the LoRa network range near Andrychów, the following solutions can be considered:
 - increase the base station antenna gain,
 - install the base station antenna on a higher mast,
 - use directional antennas.

Based on research and tests of the LoRa technology for use for effective alarming of threats and supporting evacuation, of which the results are described above, and based on the tested product, in accordance with the TWI procedure, on 09/07/2024 CNBOP-PIB granted the Fire Protection Usability Recommendation no. RP-00172024 to the Hybrid Communication System.

The recommendation includes the description of completed tests, their results and evaluation of usability for use in the

- 7) Istnieje potrzeba wykonania kolejnej serii testów z wykorzystaniem wyższego masztu stacji mobilnej, co powinno mieć pozytywny wpływ na uzyskiwane wyniki pomiarów.

Przeprowadzone badania drugiej serii testów w powiecie otwockim pozwoliły na sformułowanie następujących wniosków:

- 1) Stacja bazowa i stacja mobilna systemu HSR są ze sobą kompatybilne funkcjonalnie;
- 2) Istnieje możliwość zastosowania w HSR komunikacji DMR – odległość uzyskana podczas testów: 15,7 km;
- 3) Istnieje możliwość zastosowania w HSR komunikacji LoRa _ odległość uzyskana podczas testów: 15,7 km;
- 4) System HSR w warunkach laboratoryjnych zapewnia redundancję komunikacji, potwierdzono również redundancję systemu HSR w warunkach rzeczywistych;
- 5) W ośmiu lokalizacjach uzyskano poprawną komunikację DMR i LoRa;
- 6) Zwiększenie wysokości masztu stacji mobilnej poprawiło warunki radiokomunikacyjne i pozwoliło na nawiązanie komunikacji DMR i LoRa w lokalizacjach, w których podczas pierwszej serii testów nie udało się jej nawiązać;
- 7) Łącznie podczas obu serii testów uzyskano poprawną redundantną komunikację DMR i LoRa w trzynastu na szesnaście lokalizacji wybranych do testów (81,25%), największa uzyskana podczas testów odległość redundantnej komunikacji to 15,7 km.

Przeprowadzone badania w powiecie wadowickim pozwoliły na sformułowanie następujących wniosków [6]:

- 1) Zasięg sieci LoRa w powiecie wadowickim obejmuje obszar o promieniu około 10 km od stacji bazowej;
- 2) W większości przypadków poziom sygnału RSSI jest wyższy niż -100 dBm, co zapewnia prawidłowy odbiór danych;
- 3) W niektórych punktach, zlokalizowanych na obrzeżach miasta, RSSI może spadać do wartości -115 dBm, co może prowadzić do niestabilnego odbioru danych;
- 4) Na zasięg sieci LoRa wpływa wiele czynników, m.in.: zysk anteny stacji bazowej, wysokość montażu anteny stacji bazowej, ukształtowanie terenu, zagęszczenie zabudowy oraz poziom zakłóceń radiowych;
- 5) Przeprowadzone badanie wykazało, że sieć LoRa w okolicy Andrychowa zapewnia zadowalający zasięg w obrębie terenów zabudowanych, w większości przypadków odbiór danych jest prawidłowy, należy jednak zwrócić uwagę, że w niektórych punktach na obrzeżach miasta zasięg może być niestabilny;
- 6) W celu poprawy zasięgu sieci LoRa w okolicy Andrychowa można rozważyć:
 - zwiększenie zysku anteny stacji bazowej,
 - montaż anteny stacji bazowej na wyższym maszcie,
 - zastosowanie anten kierunkowych.

Na podstawie przeprowadzonych badań i testów technologii LoRa pod kątem wykorzystania jej do efektywnego alarmowania o zagrożeniach i wspierania ewakuacji, których wyniki opisano powyżej, oraz na podstawie oceny testowanego wyrobu, zgodnie z procedurą TWI, CNBOP-PIB udzieliło w dniu 09.07.2024 r. dla Hybrydowego Systemu Komunikacji HSR Rekomendacji Przydatności do stosowania w ochronie przeciwpożarowej nr RP-0017/2024.

declared scope. The recommendation is available to download from the website of the Institute [19]. Obtaining that recommendation authorises the manufacturers to mark the product with the TESTOWANIE REKOMENDACJA mark, both on the product and in the accompanying documentation.

Rekomendacja zawiera opis przeprowadzonych testów, ich wyniki oraz ocenę przydatności do zastosowania w deklarowanym zakresie. Rekomendacja jest dostępna do pobrania ze strony internetowej Instytutu [19]. Uzyskanie takiej rekomendacji upoważnia producentów do znakowania wyrobu znakiem TESTOWANIE REKOMENDACJA zarówno na wyrobie, jak i na towarzyszącej mu dokumentacji.



Figure 6. "TESTOWANIE REKOMENDACJA" mark design
Rycina 6. Wzór znaku „TESTOWANIE REKOMENDACJA”

Source: Own elaboration.

Źródło: Opracowanie własne.

Conclusion

Civil protection and civil defence are currently the areas of intensive works in our country. They require applying new technical and technological solutions, which enable effective protection from new and evolving threats. In this article, the authors focused on the need for civil protection by alarming, warning and enabling communication during threat elimination. The tested solution was the LoRa technology, tested for effective alarming of threats and supporting evacuation and protection operations. LoRa uses licence-free sub-Gigahertz radio frequency bands, such as 169 MHz, 433 MHz, 868 MHz. The described tests confirmed the effectiveness of the tested technology. Additional product capabilities were identified and presented in the article.

The own research of the Institute, research in collaboration with technological partners, as well as the research of product manufacturers and specific solution suppliers provide the material basis for using these solutions to improve concepts and the effectiveness of the Warning and Alarm System in our country by implementing specific new solutions. The currently public contract³ for the delivery of complete sets of devices in the quantity of 3711 pcs. consisting of the Remote Siren Controller and LoRaWAN Gateway, used for the remote control of existing alarm sirens, creates new opportunities for a significant improvement of efficiency of warning and alarming the population of threats. Such expansion of the warning and alarm system also provides the foundation for broader concept and implementation works to use the potential of solutions based on the LoRa technology for

Podsumowanie

Ochrona ludności i obrona cywilna to aktualnie obszary intensywnych prac w naszym kraju. Wymagają one zastosowania nowoczesnych rozwiązań technicznych i technologicznych, które pozwolą na zapewnienie efektywnej ochrony przed nowymi i ewoluującymi zagrożeniami. W niniejszym artykule autorzy skupili się na potrzebie ochrony ludności poprzez jej alarmowanie, ostrzeganie, a także umożliwienie komunikowania się podczas likwidacji zagrożeń. Badanym rozwiązaniem była technologia LoRa, testowana pod kątem efektywnego alarmowania o zagrożeniach i wspierania ewakuacji, działań ochronnych. LoRa wykorzystuje wolne od licencji sub-gigahercowe pasma częstotliwości radiowych takie jak 169 MHz, 433 MHz, 868 MHz. Poprzez opisane badania potwierdzono efektywność testowanej technologii. Ujawniono dodatkowe możliwości wyrobów, które przedstawiono w artykule.

Badania własne Instytutu, badania we współpracy z partnerami technologicznymi, a także badania producentów wyrobów i dostawców konkretnych już rozwiązań dają merytoryczne podstawy do wykorzystania tych rozwiązań do doskonalenia koncepcji i poprzez wdrażanie konkretnych nowych rozwiązań efektywności Systemu Ostrzegania i Alarmowania w naszym kraju. Zamówienie publiczne³ realizowane aktualnie na dostarczenie kompletnych zestawów urządzeń w ilości 3711 szt. składających się ze Zdalnego Sterownika Syreny oraz Bramki LoRaWAN, służących do zdalnego sterowania istniejącymi syrenami alarmowymi stwarza nowe możliwości istotnej poprawy skuteczności

³ Related to the task – delivery, installation and configuration of the SOiA AlertController and Gateway hubs of the LoRa/LoRaWAN system expanding the Warning and Alarm System under the National Recovery and Resilience Plan.

³ Dotyczące zadania – dostawy, instalacji i konfiguracji Kontrolerów Ostrzegania SOiA AlertController oraz koncentratorów Gateway systemu LoRa/LoRaWAN stanowiącego rozbudowę Systemu Ostrzegania i Alarmowania w ramach Krajowego Planu Odbudowy i Zwiększenia Odporności.

civil protection. In addition to the improved systems, e.g. RCB⁴ alert, the authors believe this solution has very high potential for effective improvement of the effectiveness of warning the population of various threats. In relation to the advantages of mobile carrier networks used for SMS-based RCB alerts, the LoRa technology shows advantage in the following aspects:

- 1) It can be the network used for communication and warning and alarming the population, with specific resistance, including back-up power parameters;
- 2) It is characterised by low power requirement during basic operation;
- 3) It includes the designed functionalities;
- 4) It is resistant to noise;
- 5) It enables sending basic text information;
- 6) It has a large number of end points.

The primary disadvantages of the LoRa technology are low throughput and restricted line-of-sight (LoS) communication.

The obtained test results presented in the article in tables enable specific conclusions and recommendations on the usability of solutions based on the LoRa technology for effective alarming of threats and supporting evacuation. The tested Hybrid Communication System HSR can be used for sending messages for notifying and alarming the population by starting alarm sirens and for dispatching OSP units. The availability of DMR and LoRa communication channels should be confirmed at every base station and mobile/OSP facility station installation point. The establishment of DMR and LoRa communication and their range depend i.a. on: topography, terrain forestation/urbanisation degree, presence of high voltage lines, height of antenna masts, local radio communication conditions.

The solution being the subject of this article enables building own autonomous and redundant communication and information transmission networks for the purposes of civil defence and basic crisis communication (when another fails), both with the population and between rescue service entities. While seeing this potential, in confrontation with identified limitations, which exist for every technical and technological solution, the authors of the article hope that in Polish conditions it will be possible to implement new nation-wide and effective solutions also in this area. Especially today, civil protection needs ideas, solutions and quick implementation. The experiences acquired in the improvement and rationality of products and solutions used for fire protection are invaluable for current use for the purposes of building more efficient civil protection and civil defence.

The pursued research on the usability of the LoRa technology revealed its capabilities, but also needs for use for effective transmission of key information during rescue operations. In particular, they apply to basic fire-fighter life parameters, location information under restricted communication conditions, e.g. in disaster areas or collapsed facilities. It enables treating that technology as independent and noise-resistant foundation of communication. Looking into near future, combining technologies into

ostrzegania i alarmowania o zagrożeniach ludności. Taka rozbudowa systemu ostrzegania i alarmowania daje również podstawy do szerszego koncepcyjnego i wdrożeniowego podejmowania prac na rzecz wykorzystania potencjału rozwiązań opartych na technologii LoRa na potrzeby ochrony ludności. Obok doskonałych systemów, np. alertu RCB⁴, właśnie to rozwiązanie – zdaniem autorów – ma bardzo duży potencjał dla skutecznego poprawienia efektywności ostrzegania ludności o różnorodnych zagrożeniach. W odniesieniu do zalet sieci operatorów komórkowych wykorzystywanych w przypadku SMS-owych alertów RCB technologia LoRa wykazuje przewagę w poniższych aspektach:

- 1) Może być siecią wykorzystywaną do komunikacji i ostrzegania i alarmowania ludności, o określonej odporności, w tym parametrach zasilania awaryjnego;
- 2) Charakteryzuje się niedużym zapotrzebowaniem na energię, przy podstawowym działaniu;
- 3) Zawiera zaprojektowane funkcjonalności;
- 4) Jest odporna na zakłócenia;
- 5) Pozwala na przesyłanie podstawowych informacji tekstowych;
- 6) Ma dużą liczbę punktów końcowych.

Wady technologii LoRa to głównie niska przepustowość oraz ograniczona komunikacja w linii wzroku (LoS).

Uzyskane wyniki badań przedstawione w artykule w zestawieniu tabelarycznym upoważniają do sformułowania konkretnych wniosków i rekomendacji w zakresie przydatności zastosowania rozwiązań opartych na technologii LoRa na potrzeby efektywnego alarmowania o zagrożeniach i wspierania ewakuacji. Testowany Hybrydowy System Komunikacji HSR może być wykorzystywany do przesyłania komunikatów na potrzeby powiadamiania i alarmowania ludności poprzez uruchamianie syren alarmowych oraz do dysponowania jednostek OSP – dostępność kanałów komunikacji DMR i LoRa należy potwierdzać w każdym miejscu instalacji stacji bazowej i stacji mobilnych/objektowych OSP. Nawiązanie komunikacji DMR i LoRa i jej zasięg są uzależnione m.in. od: topografii terenu, stopnia zalesienia/zurbanizowania terenu, obecności linii wysokiego napięcia, wysokości masztów antenowych, lokalnych warunków radiokomunikacyjnych.

Rozwiązanie będące przedmiotem niniejszej pracy pozwala na tworzenie własnych autonomicznych, redundantnych sieci komunikacji i przekazu informacji na potrzeby ochrony ludności i podstawowej komunikacji kryzysowej (gdy inna zawiedzie) – zarówno z ludnością, jak i pomiędzy podmiotami ratowniczymi. Dostrzegając ten potencjał, w konfrontacji ze wskazanymi ograniczeniami, występującymi w przypadku każdego rozwiązania technicznego i technologicznego, autorzy artykułu wyrażają nadzieję, iż w warunkach polskich możliwe będzie wdrażanie nowych, krajowych i efektywnych rozwiązań również w tym zakresie. Ochrona ludności szczególnie potrzebuje dzisiaj pomysłów, rozwiązań i szybkich wdrożeń. Doświadczenia zdobyte w doskonaleniu i racjonalności stosowanych wyrobów i rozwiązań na

⁴ RCB alert is a SMS system used to notify the population of threats. It is used in extraordinary situations, in which there is probability of imminent threat to life or health in the given area. The RCB website <https://www.gov.pl/web/rcb/alert-rcb---najwazniejsze-pytania-i-odpowiedzi> [access: 10/11/2025].

⁴ Alert RCB to system SMS-owego powiadamiania ludności o zagrożeniach. Jest wykorzystywany w sytuacjach nadzwyczajnych, wtedy, gdy występuje prawdopodobieństwo bezpośredniego zagrożenia życia lub zdrowia na znaczącym obszarze. Strona RCB <https://www.gov.pl/web/rcb/alert-rcb---najwazniejsze-pytania-i-odpowiedzi> [dostęp: 10.11.2025].

hybrids (LoRa + 5G/6G, LoRa + satellite connection) may increase the safety level of operations. Research on predictive fire spreading, remote control over rescue teams in difficult-to-access areas or AI-assisted-assisted evacuation systems will become promising. It is predicted that the LoRa system will evolve from an alarm utility into a key rescue safety solution. However, its further development will depend on the strengthening of the cybersecurity pillar, standardisation of protocols or closer collaboration between science and market solutions. The authors plan on submitting the CNBOP-PIB research and results in this field for publication in subsequent issues of the SFT scientific journal.

potrzeby ochrony przeciwpożarowej są bezcenne dla wykorzystania ich obecnie na potrzeby budowania skutecznej ochrony ludności i obrony cywilnej.

Podczas realizowanych badań z zakresu użyteczności technologii LoRa ujawnione zostały jej możliwości, a także potrzeby pod kątem wykorzystania tego rozwiązania do efektywnego przesyłania kluczowych informacji podczas działań ratowniczych. W szczególności dotyczą one podstawowych parametrów życia strażaka, informacji o jego lokalizacji w warunkach ograniczonej łączności, np. w strefie katastrof czy zawalonych obiektach. Pozwala to traktować tę technologię jako niezależny, odporny na zakłócenia fundament komunikacyjny. Patrząc w niedaleką przyszłość, połączenie technologii w hybrydy (LoRa + 5G/6G, LoRa + satelitarne połączenie) może podnieść poziom bezpieczeństwa prowadzonych działań. Obiecujące staną się badania z zakresu predykcyjnego rozprzestrzeniania się pożarów, zdalnego sterowania zespołami ratowniczymi w miejscach trudno dostępnych czy systemach ewakuacji wspomaganych SI. Przewiduje się, że system LoRa ewoluuje od narzędzia alarmowego do kluczowego rozwiązania z zakresu bezpieczeństwa ratowniczego. Dalszy jej rozwój zależy jednak od wzmocnienia filaru cyberbezpieczeństwa, standaryzacji protokołów czy ścisłej współpracy nauki z rozwiązaniami rynkowymi. Badania CNBOP-PIB oraz wyniki w tym zakresie autorzy planują zgłosić do publikacji w kolejnych wydaniach czasopisma naukowego SFT.

List of abbreviations

AES	Advanced Encryption Standard – symmetrical block encryption
BNT	Safety of New Technologies
DMR	Digital Mobile Radio – open digital radio communication standard
HSR	Hybrid System
IoT	Internet of Things
JRG PSP	PSP Rescue and Fire-Fighting Unit
LoRa	Long Range
LoRaWAN	Long Range Wide Area Network – long range communication system
LoS	Line-of-sight
MAC	Medium Access Control
NLoS	Non-Line-of-Sight
OSP	Voluntary Fire Service
PSP	State Fire Service
RCB	Government Safety Centre
RSSI	Received Signal Strength Indicator
AI	Artificial intelligence
TWI	Testing of innovative products
TDMA	Time Division Multiple Access
VHF	Very High Frequency – radio wave range with frequency from 30 to 300 MHz

Wykaz skrótów

AES	zaawansowany standard szyfrowania
BNT	bezpieczeństwo nowych technologii
DMR	otwarty standard cyfrowej łączności radiowej
HSR	hybrydowy system komunikacji
IoT	internet rzeczy
JRG PSP	jednostka ratowniczo-gaśnicza PSP
LoRa	daleki zasięg
LoRaWAN	System komunikacji dalekiego zasięgu w zasięgu widzenia
LoS	
MAC	Medium Access Control
NLoS	poza linią wzroku
OSP	Ochotnicza straż pożarna
PSP	Państwowa Straż Pożarna
RCB	Rządowe Centrum Bezpieczeństwa
RSSI	Wskaźnik siły odbieranego sygnału
SI	sztuczna inteligencja
TWI	Testowanie Wyrobów Innowacyjnych
TDMA	wielodostęp z podziałem czasowym
VHF	bardzo wysoka częstotliwość, zakres fal radiowych o częstotliwości od 30 do 300 MHz

AI Use Statement

The authors declare that no artificial intelligence tools were used in the preparation of this article to generate text, analyses, graphics, or other elements of the publication.

The authors take full responsibility for the content of the publication, including the scientific accuracy, interpretation of results, and the final editing of the manuscript.

According to the journal's editorial policy, the uncritical copying of AI-generated content and its inclusion in a publication without proper critical analysis, verification, and revision by the authors is prohibited.

Oświadczenie dotyczące wykorzystania AI

Autorzy oświadczają, że w procesie przygotowania niniejszego artykułu nie korzystano z narzędzi opartych na sztucznej inteligencji do generowania treści, analiz, grafik ani innych elementów publikacji.

Autorzy ponoszą pełną odpowiedzialność za treść publikacji, w tym za poprawność merytoryczną, interpretację wyników oraz redakcję tekstu.

Zgodnie z polityką redakcyjną czasopisma zabronione jest bezrefleksyjne kopiowanie treści wygenerowanych przez narzędzia AI oraz pozostawianie ich w publikacji bez krytycznej analizy, weryfikacji i redakcji przez autora(ów).

Literature / Literatura

- [1] Terlikowski T., *Inżynieria bezpieczeństwa cywilnego czy inżynieria ochrony ludności?*, „Safety & Fire Technology” 2020, 55, 1, 48–61, <https://doi.org/10.12845/sft.55.1.2020.4>.
- [2] Gromek P., Sobolewski G., *Risk-Based Approach for Informing Sustainable Infrastructure Resilience Enhancement and Potential Resilience Implication in Terms of Emergency Service Perspective*, „Sustainability” 2020, 12(11), 4530, <https://doi.org/10.3390/su12114530>.
- [3] Florek P., Kołodziejczyk T., *Wsparcie ewakuacji osób niepełnosprawnych – wyzwania organizacyjne i technologiczne*, „Safety & Fire Technology” 2021, 57, 1, 134–144, <https://doi.org/10.12845/sft.57.1.2021.9>.
- [4] Garlińska U., Popielarczyk T., Sowa T., Śliwiński R., *Wytyczne stosowania dźwiękowych systemów ostrzegawczych na podstawie analizy dokumentów normatywnych i prawnych stosowanych w wybranych krajach Europy*, „Safety & Fire Technology” 2021, 57, 1, 6–24, <https://doi.org/10.12845/sft.57.1.2021.1>.
- [5] Popielarczyk T., Stępień P., Chmiel M., Iwanska M., *Tests of Fire Circuit Breakers (FCBs) to Assess Their Suitability for Use in Construction Objects*, „ELECTRONICS” 2024, 13, 9, 1633, <https://doi.org/10.3390/electronics13091633>.
- [6] *Raport z badania zasięgu sieci LoRaWAN w okolicy Andrychowa*, 2024, Wyniki badań firmy Neuron Sp. z o. o. sp. k. pt. (materiały niepublikowane).
- [7] Strona MSWiA, <https://www.gov.pl/web/mswia/alarmowanie-i-ostrzezenie> [dostęp: 10.11.2025].
- [8] Konferencje BNT, <https://cnbop.pl/nauka/konferencje/konferencje-bnt> [dostęp: 10.11.2025].
- [9] Ramowe wytyczne projektowania strażnic OSP – załącznik do Uchwały nr 283/34/2012 Prezydium ZG ZOŚP RP z 19.04.2012 r.
- [10] Strona internetowa Lora Alliance, <https://lora-alliance.org/about-lorawan> [dostęp: 13.11.2025].
- [11] Ruban D., *LoRa pod lupą*, Zakład Kompatybilności Elektromagnetycznej IŁ-PIB we Wrocławiu, <https://www.gov.pl/web/instytut-laczynosci/lora-pod-lupa> [dostęp: 13.11.2025].
- [12] Lopes I.R., Coelho P.R.d.S.L., Pasquini R., Miani R.S., *Evaluating the Performance of LoRa Networks: A Study on Disaster Monitoring Scenarios*, „IoT” 2025, 6, 1, 14, <https://doi.org/10.3390/iot6010014>.
- [13] Li J., *Design of LoRa Communication System Based on Speech Recognition in Emergency Rescue Environment*, w: *Proceedings of the 2nd International Conference on Signal Processing, Computer Networks and Communications (SPCNC '23)*, 2023, 215–219, <https://doi.org/10.1145/3654446.3654484>.
- [14] Pradeep Kumar R., Selvarathinam D.K.P., Gnanaprakasam C.N., *A LoRa Based Emergency Communication Device for Disaster Response*, w: *Proceedings of the 5th International Conference on Trends in Material Science and Inventive Materials (ICTMIM)*, 2025, 1074–1081.
- [15] del Río Sáez J.S., Aragonés V., Villaluenga T. S., Davila-Gomez L., Paramio Martínez S., Vázquez-López A., Ballesteros Y., Martínez V., Jiménez J.L., Abdulmalik Yusuf, Li X., Ao X., Xiu J., Wang D.-Y., *Wi-Fi/LoRa communication systems for fire and seismic-risk mitigation and health monitoring*, *Front. Detect. Sci. Technol.*, 07 February 2025, Sec. Data Acquisitions Methods and Readout Electronics, 2025, 3, <https://doi.org/10.3389/fdest.2025.1484647>.
- [16] Jimenez M., Medina A., Navarro L., Osorio A., Robles D., Calle M., Candelo-Becerra J. E., *Obstacles, Speed and Spreading Factor: Insights in LoRa Mobile Performance*, „International Journal on Communications Antenna and Propagation” (IRECAP) 9(3):228-235, <https://doi.org/10.15866/irecap.v9i3.17296>.
- [17] Abdallah B., Khriji S., Chéour R., Lahoud C., Moessner K., Kanoun O., *Improving the Reliability of Long-Range Communication against Interference for Non-Line-of-Sight Conditions in Industrial Internet of Things Applications*, „Applied Science” 2024, 14, 868, <https://doi.org/10.3390/app14020868>.
- [18] Procedura testowania wyrobów innowacyjnych, Wyd. 2, CNBOP-PIB, Józefów 2015.
- [19] Rekomendacja przydatności do stosowania w ochronie przeciwpożarowej nr RP-0017/2024, https://cnbop.pl/app/uploads/2024/09/rp_0017_2024.pdf [dostęp: 13.11.2025].

TOMASZ POPIELARCZYK, PH.D. ENG. – graduate of the Faculty of Fire Safety Engineering of the Fire University in Warszawa and Faculty of Management and Command of the War Studies University in Warsaw. He works in the Laboratory of Fire Alarm Systems and Fire Automation in the Scientific and Research Centre for Fire Protection – National Research Institute in Józefów. He conducts scientific research in the following fields: fire safety of buildings, design of technical fire protection systems and their use during rescue operations.

SEN. BRIG. JACEK ZBOINA, D.SC. ENG. – Deputy Director for Certification and Admittance of CNBOP-PIB. Graduate of the Fire University in Warszawa, Warsaw School of Economics and Naval Academy in Gdynia. In 2023, he obtained the post-doctoral degree (dr hab.) in social sciences, in the discipline of safety sciences in the Department of Naval Command and Operations of the Naval Academy in Gdynia. Expert of the Chief of the State Fire Service for fire protections. His research, scientific and professional interests are related to safety, fire protection, techniques and new technologies and assessment of conformity. Author and co-author of dozens of scientific and branch publications in the field of fire safety, safety of new technologies, implementations and innovations, technical protection systems, research, testing and certification of products, as well as practical use of new technologies. In his research and professional activity, he is involved in implementation works and research and research and development projects – both as contractor and manager.

JR. BRIG. GRZEGORZ MROCZKO, M.SC. ENG. – graduate of the Fire University in Warszawa, officer of State Fire Service, representative of Poland in TC 72 of the European Technical Committee (CEN), representative of CNBOP-PIB in the European Organisation for Technical Assessment (EOTA), member of KT 264 and KT 323 of the Polish Committee for Standardisation (Polski Komitet Normalizacyjny, PKN). Involved in technical assessment of construction products used for the fire protection of buildings at the CNBOP-PIB Technical Assessment Department for many years.

PAWEŁ BUJNY, M.SC. ENG. – graduate of computer science in the Faculty of Electrical Engineering, Automatic Control and Computer Science of the Kielce University of Technology. Head of the IT Department and Chief Network and System Security Specialist at CNBOP-PIB. Expert with more than 12 years of experience in cybersecurity, computer forensics and offensive security. Holder of multiple training and branch certificates, i.a. CEH (Certified Ethical Hacker), CompTIA Security+, RHCSA, RHCE and ISO 27001 auditor. At present, he pursues his interdisciplinary doctoral dissertation on using artificial intelligence to support fire service rescue operations. Participant of post-graduate studies in AI in cybersecurity (ARISA). Member of the KT 338 Technical Committee for Artificial Intelligence and Head of the CNBOP-PIB Scientific Club. Speaker at branch conferences on new technologies.

DR INŻ. TOMASZ POPIELARCZYK – absolwent Wydziału Inżynierii Bezpieczeństwa Pożarowego Szkoły Głównej Służby Pożarniczej w Warszawie oraz Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej w Warszawie. Pracuje w Zespole Laboratoriów Sygnalizacji Alarmu Pożaru i Automatyki Pożarniczej w Centrum Naukowo-Badawczym Ochrony Przeciwpowodziowej – Państwowym Instytucie Badawczym w Józefowie. Prowadzi badania naukowe w następujących obszarach: bezpieczeństwo pożarowe obiektów budowlanych, projektowanie technicznych systemów zabezpieczeń przeciwpowodziowych oraz ich wykorzystanie podczas działań ratowniczych.

ST. BRYG. DR HAB. INŻ. JACEK ZBOINA – Z-ca Dyrektora ds. Certyfikacji i Dopuszczeń CNBOP-PIB. Absolwent Szkoły Głównej Służby Pożarniczej, Szkoły Głównej Handlowej w Warszawie oraz Akademii Marynarki Wojennej w Gdyni. W 2023 roku uzyskał stopień doktora habilitowanego w dziedzinie nauk społecznych w dyscyplinie nauk o bezpieczeństwie na Wydziale Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej w Gdyni. Rzeczoznawca Komendanta Głównego PSP ds. zabezpieczeń przeciwpowodziowych. Jego zainteresowania badawcze, naukowe oraz zawodowe dotyczą bezpieczeństwa, ochrony przeciwpowodziowej, techniki i nowych technologii oraz oceny zgodności. Autor i współautor kilkudziesięciu publikacji naukowych oraz branżowych w zakresie bezpieczeństwa pożarowego, bezpieczeństwa nowych technologii, wdrożeń i innowacji, technicznych systemów zabezpieczeń, badań, testowania i certyfikacji wyrobów, a także wykorzystania w praktyce nowych technologii. W działalności badawczej i zawodowej uczestniczy w pracach wdrożeniowych i projektach badawczych i badawczo-rozwojowych – zarówno w roli wykonawcy, jak i kierownika.

ML. BRYG. MGR INŻ. GRZEGORZ MROCZKO – absolwent SGSP, oficer Państwowej Straży Pożarnej, przedstawiciel Polski w TC 72 Europejskiego Komitetu Technicznego (CEN), przedstawiciel CNBOP-PIB w Europejskiej Organizacji ds. Oceny Technicznej (EOTA), członek KT 264 i KT 323 Polskiego Komitetu Normalizacyjnego (PKN). Od lat związany z oceną techniczną wyrobów budowlanych służących do ochrony przeciwpowodziowej budynków w Zakładzie Ocen Technicznych CNBOP-PIB.

MGR INŻ. PAWEŁ BUJNY – absolwent Wydziału Elektroniki, Automatyki i Informatyki Politechniki Świętokrzyskiej na kierunku informatyka. Kierownik Działu IT oraz główny specjalista ds. bezpieczeństwa sieci i systemów w CNBOP – PIB. Ekspert z ponad 12-letnim doświadczeniem w obszarze cyberbezpieczeństwa, informatyki śledczej i bezpieczeństwa ofensywnego. Posiadacz licznych szkoleń i certyfikatów branżowych, m.in. CEH (Certified Ethical Hacker), CompTIA Security+, RHCSA, RHCE oraz audytora ISO 27001. Obecnie realizuje interdyscyplinarną pracę doktorską dotyczącą wykorzystania sztucznej inteligencji do wsparcia czynności ratowniczych straży pożarnej. Słuchacz studiów podyplomowych w zakresie AI w cyberbezpieczeństwie (program ARISA). Członek Komitetu Technicznego KT 338 ds. Sztucznej Inteligencji oraz Przewodniczący Koła Naukowego CNBOP-PIB. Prelegent na konferencjach branżowych dotyczących nowych technologii.



od 2019

2018-2006



SFT (wcześniej BiTP) jest recenzowanym czasopismem naukowym, którego głównym założeniem jest publikowanie w otwartym dostępie oryginalnych badań, artykułów przeglądowych oraz studiów przypadków z zakresu szeroko rozumianego bezpieczeństwa i ochrony przeciwpożarowej. Pismo koncentruje się na transferze wiedzy między nauką a praktyką oraz promowaniu innowacyjnych rozwiązań technicznych. Pełni rolę platformy wymiany wiedzy naukowej w obszarze inżynierii bezpieczeństwa i nauk pokrewnych, wspierając rozwój badań oraz praktyki w dziedzinie ochrony przeciwpożarowej.



tak się zaczęło...

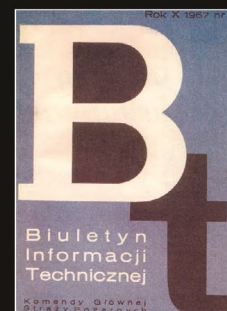
1958-1966

Czasopismo powstało w 1958 roku jako miesięcznik poświęcony upowszechnianiu wiedzy z zakresu ochrony przeciwpożarowej, ze szczególnym uwzględnieniem postępu technicznego, materiałów normatywnych oraz zasad zapobiegania pożarom w budownictwie i procesach technologicznych. Początkowo na jego łamach ukazywały się również tłumaczenia zagranicznej literatury fachowej.



1967-1985

W kolejnych latach periodyk przekształcił się w kwartalnik o charakterze naukowo-technicznym, koncentrujący się na aktualnych problemach ochrony przeciwpożarowej, rozwoju techniki pożarniczej oraz działalności profilaktycznej i operacyjnej. Publikowano w nim także informacje o normach, wymaganiach technicznych, sprzęcie pożarniczym oraz przeglądy literatury branżowej.



1986-1989

Z biegiem czasu czasopismo zmieniało nazwę i formułę, rozszerzając zakres tematyczny o zagadnienia ratownictwa technicznego i chemicznego oraz prezentację wyników badań prowadzonych w kraju i za granicą. Stało się forum wymiany wiedzy naukowej i praktycznej, wspierając rozwój ochrony przeciwpożarowej oraz popularyzację nowoczesnych rozwiązań w tej dziedzinie.



ZAPRASZAMY DO WSPÓŁPRACY



www.sft.cnbp.pl

Tomasz Lutoborski, Maciej Zawistowski

Scientific and Research Centre for Fire Protection – National Research Institute / Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej – Państwowy Instytut Badawczy
Corresponding author / Autor korespondencyjny: tlutoborski@cnbop.pl

Protection of the Population in the 21st Century: the Role of Innovative Technologies in Crisis Response

Ochrona ludności w XXI wieku: rola innowacyjnych technologii w reagowaniu kryzysowym

ABSTRACT

Purpose: The purpose of the paper is to discuss contemporary organisational and technological solutions within the system of civil protection and civil defence in Poland, and to indicate the role of modern technologies in enhancing citizens' safety. The authors put forward a thesis assuming that effective civil protection and civil defence are based on increased civic engagement, with citizens using modern technologies to help build a safe environment.

Introduction: In the 21st century, public safety is changing faster than ever before. Extreme weather phenomena, hybrid warfare, and disinformation show that the state and society must be prepared for a wide range of threats. Modern technologies – monitoring and alerting systems, IoT, mobile applications, VR/AR tools, and drones – have become a response to these challenges. However, their effectiveness depends on one key factor: a society that is aware of and prepared for threats. The article analyses the role of technology in civil protection in Poland, presents the organizational and legal foundations of the system, and discusses the importance of modern solutions in building social resilience.

Methodology: The study uses both quantitative and qualitative analysis of public data to assess public interest in topics related to civil protection and the role of modern technologies in public safety. The quantitative part included an analysis of Google Trends and Wikipedia Pageviews data for selected safety-related terms. The qualitative part included a formal and legal analysis and a review of expert sources. Theoretical methods were applied, including the analysis of legal acts, government documents, websites of institutions responsible for security, and industry articles.

Conclusions: Modern technologies significantly strengthen public safety by providing continuous environmental monitoring and rapid alerting of the population about threats. However, the tools themselves do not guarantee effectiveness—the key lies in their conscious and responsible use by citizens. Social engagement improves system response, enables data exchange, faster threat detection, and better decision-making by emergency services. A clear trend of growing public interest in civil defence is visible, supporting the development of social resilience. At the same time, it remains important to reduce barriers such as digital exclusion, telecommunication failures, low quality of some mobile applications, and the need to counter disinformation. At the foundation of the entire system lie education, awareness of threats, and information resilience. The effectiveness of civil protection depends on systematic training, public education, and trust in the actions of state institutions.

Keywords: public safety, civil defence, civil protection, modern technologies

Type of article: review article

Received: 20.11.2025; Reviewed: 28.12.2025; Accepted: 16.01.2026;

Authors' ORCID IDs: T. Lutoborski – 0009-0004-5122-2874; M. Zawistowski – 0000-0001-9832-0376;

Percentage contribution: T. Lutoborski – 55%; M. Zawistowski – 45%;

Please cite as: Safety & Fire Technology 2026, 1, 30–57, <https://doi.org/10.12845/sft.67.1.2026.2>;

This is an open access article under the CC BY-SA 4.0 license (<https://creativecommons.org/licenses/by-sa/4.0/>).

ABSTRAKT

Cel: Celem pracy jest omówienie współczesnych rozwiązań organizacyjno-technicznych w systemie ochrony ludności i obrony cywilnej w Polsce oraz wskazanie roli nowoczesnych technologii w zwiększeniu bezpieczeństwa obywateli. Autorzy postawili tezę, w której zakłada się, że skuteczna ochrona ludności i obrona cywilna opierają się na zwiększonej aktywności obywateli, którzy wykorzystują nowoczesne technologie do budowy bezpiecznego środowiska.

Wprowadzenie: W XXI wieku bezpieczeństwo powszechne zmienia się szybciej niż kiedykolwiek wcześniej. Ekstremalne zjawiska pogodowe, wojna hybrydowa, dezinformacja pokazują, że państwo i społeczeństwo muszą być przygotowane na szeroki wachlarz zagrożeń. Odpowiedzią na te wyzwania stają się nowoczesne technologie: systemy monitorowania i alarmowania, IoT, aplikacje mobilne, narzędzia VR/AR czy drony. Ich skuteczność zależy jednak

od jednego kluczowego czynnika – przygotowanego na zagrożenia i świadomego społeczeństwa. Artykuł analizuje rolę technologii w ochronie ludności w Polsce, przedstawia podstawy organizacyjno-prawne systemu oraz omawia znaczenie nowoczesnych rozwiązań w budowaniu odporności społecznej.

Metodologia: W pracy zastosowano zarówno analizę ilościową, jak i analizę jakościową danych publicznych, w celu oceny zainteresowania społecznego tematami związanymi z ochroną ludności oraz rolą nowoczesnych technologii w bezpieczeństwie powszechnym. Część ilościowa obejmowała analizę danych z Google Trends oraz Wikipedia Pageviews dla wybranych haseł dotyczących bezpieczeństwa. Część jakościowa obejmowała analizę formalno-prawną oraz przegląd źródeł eksperckich. Wykorzystano metody teoretyczne, w tym analizę aktów prawnych, dokumentów rządowych, portali instytucji odpowiedzialnych za bezpieczeństwo oraz artykułów branżowych.

Wnioski: Nowoczesne technologie znacząco wzmacniają bezpieczeństwo powszechne oraz szybkie alarmowanie społeczeństwa o zagrożeniach. Same narzędzia nie gwarantują jednak skuteczności – kluczowe jest ich świadome i odpowiedzialne wykorzystanie przez obywateli. Zaangażowanie społeczne poprawia reakcję systemu i umożliwia wymianę danych, szybsze wykrywanie zagrożeń oraz lepsze podejmowanie decyzji przez służby. Dostrzegalny jest wyraźny trend wzrostu zainteresowania obroną cywilną, co sprzyja budowaniu odporności społecznej. Jednocześnie istotne pozostaje niwelowanie barier, takich jak wykluczenie cyfrowe, awarie telekomunikacyjne, niska jakość części aplikacji mobilnych oraz konieczność przeciwdziałania dezinformacji. U podstaw całego systemu stoi edukacja, świadomość zagrożeń i odporność informacyjna. Skuteczność ochrony ludności zależy od systematycznych szkoleń, edukacji publicznej oraz zaufania do działań instytucji państwowych.

Słowa kluczowe: bezpieczeństwo powszechne, ochrona ludności, obrona cywilna, nowoczesne technologie

Typ artykułu: artykuł przeglądowy

Przyjęty: 20.11.2025; **Zrecenzowany:** 28.12.2025; **Zaakceptowany:** 16.01.2026;

Identyfikatory ORCID autorów: T. Lutoborski – 0009-0004-5122-2874; M. Zawistowski – 0000-0001-9832-0376;

Procentowy wkład merytoryczny: T. Lutoborski – 55%; M. Zawistowski – 45%;

Proszę cytować: Safety & Fire Technology 2026, 1, 30–57, <https://doi.org/10.12845/sft.67.1.2026.2>;

Artykuł udostępniany na licencji CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>).

Introduction

The purpose of this article is to present the issues of civil protection and civil defence in the context of contemporary legal conditions and to explain the basic terms related to that field. Particular focus was on discussing the essence of modern technologies and on reviewing technological solutions that really support the functioning of civil protection and civil defence, including monitoring systems, alarm systems and crisis communication applications. The article also presents practical examples of such tools and points to the directions and opportunities for their further development in view of increasing safety challenges. In addition, the significance of innovative technologies, such as alarm telecommunications, mobile applications, IoT and VR/AR tools, for building national and social resistance to natural and man-made threats, including armed conflicts. It was also assumed that the effectiveness of the civil protection system is to a significant extent determined by the level of engagement and awareness of the citizens.

The terms of civil protection and civil defence have been specified and defined in the Civil Protection and Civil Defence Act of 5 December 2024. Pursuant to Article 2(1) of that Act, Civil Protection is a system consisting of public administration bodies in charge of tasks intended to civil safety by protecting human life and health, property, including animals, infrastructure necessary for living purposes, cultural property and the environment in hazardous situations, hereinafter referred to “civil protection bodies”, entities in charge of these tasks, hereinafter referred to “civil protection entities” and civil protection resources [1].

Civil defence is defined in Article 2(2) as fulfilment of the tasks specified in Article 61 letter a of the Protocol Additional to the Geneva Conventions of 12 August 1949 relating to the Protection of Victims of International Armed Conflicts (Protocol I), drafted in Geneva on 8 June 1977 (Journal of Laws 1992, item 175, and 2015, item 1056), hereinafter referred to as “the First

Wprowadzenie

Celem niniejszego artykułu jest przedstawienie zagadnień Ochrony ludności i obrony cywilnej (OLiOC) w kontekście współczesnych uwarunkowań prawnych oraz wyjaśnienie podstawowych pojęć związanych z tym obszarem. Szczególny nacisk położono na omówienie istoty nowoczesnych technologii oraz na przegląd rozwiązań technologicznych, które realnie wspierają funkcjonowanie OLiOC, obejmujących m.in. systemy monitorowania, alarmowania oraz aplikacje służące komunikacji kryzysowej. Artykuł prezentuje również praktyczne przykłady takich narzędzi oraz wskazuje kierunki i możliwości ich dalszego rozwoju w świetle rosnących wyzwań bezpieczeństwa. Podkreślono ponadto znaczenie innowacyjnych technologii – takich jak telekomunikacja alarmowa, aplikacje mobilne, IoT oraz narzędzia VR/AR – w budowaniu odporności państwa i społeczeństwa na zagrożenia naturalne i wywołane przez człowieka, w tym konflikty zbrojne. Założono przy tym, że efektywność systemu ochrony ludności jest w znacznym stopniu uzależniona od poziomu zaangażowania i świadomości obywateli.

Pojęcia ochrony ludności oraz obrony cywilnej zostały określone i zdefiniowane w Ustawie z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej. Zgodnie z treścią ustawy art. 2 pkt 1 Ochrona ludności to system składający się z organów administracji publicznej wykonujących zadania mające na celu zapewnienie bezpieczeństwa ludności przez ochronę życia i zdrowia ludzi, mienia, w tym zwierząt, infrastruktury niezbędnej do zaspokojenia potrzeb bytowych, dóbr kultury i środowiska w sytuacji zagrożenia, zwanych dalej „organami ochrony ludności”, podmiotów wykonujących te zadania, zwanych dalej „podmiotami ochrony ludności”, oraz zasobów ochrony ludności [1].

Obrona cywilna została zdefiniowana w art. 2 pkt 2 jako realizacja zadań określonych w art. 61 lit. a Protokołu dodatkowego do Konwencji Genewskich z 12 sierpnia 1949 r. dotyczącego ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół I),

Protocol Additional to the Geneva Conventions of 12 August 1949”, intended to protect civilian population from hazards arising from armed operations and their consequences [2].

The legal framework organise the responsibility of institutions, but their effectiveness in the field is also determined under interconnected conditions, quickly escalating events: from disinformation campaigns and cyberattacks (hybrid warfare), to floods, draughts and fires related to climate change, to power and telecommunications failures. In this reality, network collaboration between services and citizens, based on effective warning channels, credible bottom-up data and operational readiness increasing tools, is necessary.

In the remainder of the article, the terms “civil protection” and “civil defence” are treated as synonyms and written in lower-case letters, except for quotes from legal acts, relating to the same functional system of operations focused on the protection of life, health and property of civilian population. Both civil protection and civil defence pursue the same objectives, using similar organisational, technical and social resources, in particular to reduce human and property losses. The differences between these terms are primarily related to the context of their formal initiation, not the essence of the undertaken protection operations. Consequently, the authors of the article assumed a functional perspective, from which both terms describe a cohesive and continuous civil protection system.

Based on the above considerations, including both the legal framework and the increasing complexity of risks characteristic of the 21st Century (such as hybrid warfare, extreme climate phenomena, critical infrastructure failures), the authors put forward a thesis assuming that effective civil defence is based on active involvement of citizens and support of technologies.

Methodology

The chapter describes the method of assessment of the dynamics and meanings of the terms related to civil protection and civil defence in Poland, based on data from open Internet sources, including Google Trends and Wikipedia Pageviews. The analysis only relates to the national context and covers the period from January 2022 to November 2025. The main purpose is to determine, which of the terms related to public safety remain of permanent social interest, which only occur in response to specific events. This data is considered as indicator of attention of citizens, which may indirectly reflect the effectiveness of institutional communication and hazard awareness level.

The study used both Topics and Search Terms. Topics are related to general themes (“civil defence”, “112”, “IMGW-PIB”), while Search Terms include specific system and application names (“Alert RCB”, “RSO”). Three time horizons are used: 2022–2025 (long-term analysis; see Fig. 1), last 12 months (see Fig. 2) and last 90 days (see Fig. 3) (episodic analyses). This approach enables distinguishing permanent trends from short-term media reactions.

sporządzonego w Genewie dnia 8 czerwca 1977 r. (Dz.U. 1992 poz. 175 oraz 2015, poz. 1056), zwanego dalej „Pierwszym Protokołem dodatkowym do Konwencji Genewskich z 12 sierpnia 1949 r.”, mająca na celu ochronę ludności cywilnej przed zagrożeniami wynikającymi z działań zbrojnych i ich następstw [2].

Ramy ustawowe porządkują odpowiedzialność instytucji, ale skuteczność w terenie rozstrzyga się w warunkach wielowątkowych, szybko eskalujących zdarzeń: od kampanii dezinformacyjnych i cyberataków (wojna hybrydowa), przez powodzie, susze i pożary związane ze zmianą klimatu, po awarie energetyczne i telekomunikacyjne. W takiej rzeczywistości niezbędna jest sieciowa współpraca służb z obywatelami, oparta na sprawnych kanałach ostrzegania, wiarygodnych danych oddolnych i narzędziach podnoszących gotowość do działania.

W dalszej części artykułu terminy ochrona ludności i obrona cywilna traktuje się jako synonimy i zapisuje małymi literami, o ile nie wynikają z cytatów aktów prawnych, odnosząc je do tego samego funkcjonalnego systemu działań ukierunkowanych na ochronę życia, zdrowia oraz mienia ludności cywilnej. Zarówno ochrona ludności, jak i obrona cywilna realizują tożsame cele, wykorzystując zbliżone zasoby organizacyjne, techniczne i społeczne, w szczególności w zakresie ograniczania strat w ludziach i mieniu. Różnice pomiędzy tymi pojęciami dotyczą przede wszystkim kontekstu ich formalnego uruchomienia, a nie istoty podejmowanych działań ochronnych. Z tego względu w pracy przyjęto perspektywę funkcjonalną, w której oba pojęcia opisują spójny i ciągły system bezpieczeństwa ludności.

Na podstawie powyższych rozważań, uwzględniających zarówno ramy prawne, jak i rosnącą złożoność ryzyk charakterystycznych dla XXI wieku) jak wojna hybrydowa, ekstremalne zjawiska klimatyczne, awarie infrastruktury krytycznej), postawiono tezę, w której zakłada się, że skuteczna obrona cywilna opiera się na aktywnym udziale obywateli i wsparciu technologii.

Metodologia

Rozdział opisuje sposób oceny dynamiki i znaczenia pojęć związanych z ochroną ludności oraz obroną cywilną w Polsce, bazujący na danych pochodzących z otwartych źródeł internetowych, w tym Google Trends i Wikipedia Pageviews. Analiza dotyczy wyłącznie kontekstu krajowego i obejmuje okres od stycznia 2022 r. do listopada 2025 roku. Głównym celem jest określenie, które z pojęć związanych z bezpieczeństwem powszechnym pozostają w trwałym zainteresowaniu społecznym, a które pojawiają się jedynie w reakcji na konkretne wydarzenia. Dane te traktowane są jako wskaźnik uwagi obywateli, mogący pośrednio odzwierciedlać skuteczność komunikacji instytucjonalnej oraz poziom świadomości zagrożeń.

W badaniu wykorzystano zarówno tematy (Topics), jak i wyszukiwane hasła (Search Terms). Tematy odnoszą się do ujęć ogólnych („obrona cywilna”, „112”, „IMGW-PIB”), natomiast wyszukiwane hasła obejmują konkretne nazwy systemów i aplikacji („Alert RCB”, „RSO”). Zastosowano trzy horyzonty czasowe: 2022–2025 (analiza długookresowa; zob. Ryc. 1), ostatnie 12 miesięcy (zob. Ryc. 2) i ostatnie 90 dni (zob. Ryc. 3) (analiza epizodyczna). Takie podejście pozwala na odróżnienie trendów stałych od krótkotrwałych reakcji medialnych.

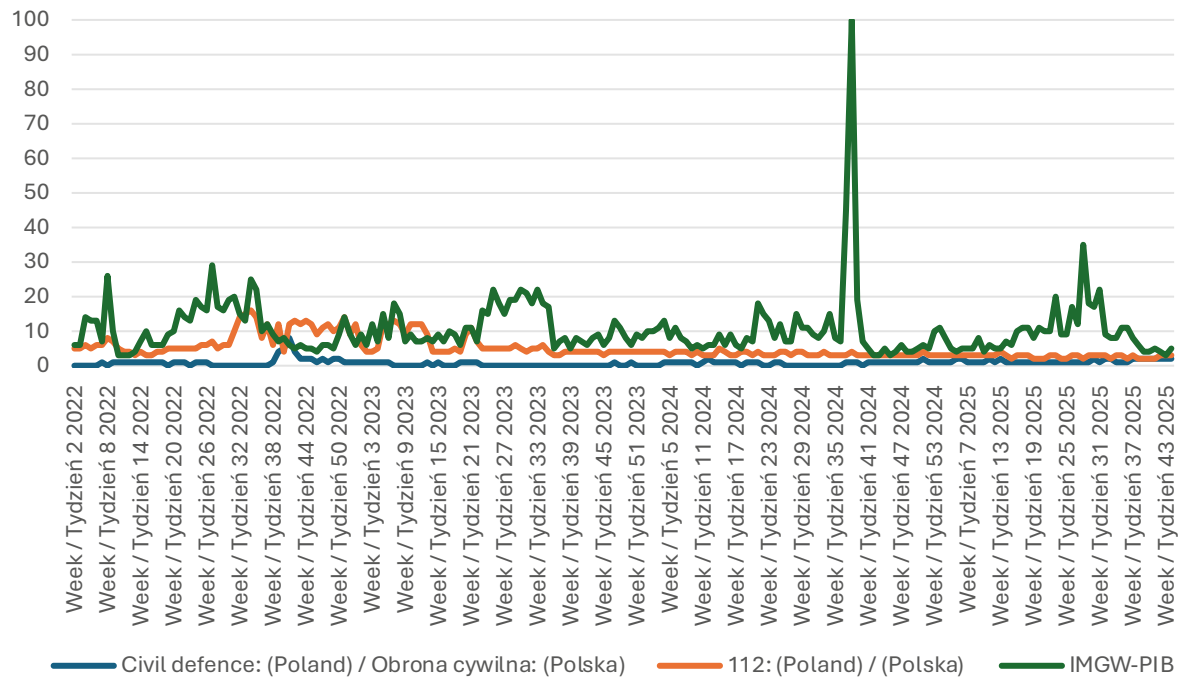


Figure 1. Google Trends – Poland (period of 01/2022-10/2025). Search Terms: obrona cywilna (civil defence) / 112 / IMGW-PIB
Rycina 1. Google Trends – Polska (okres 01.2022-10.2025). Hasła: obrona cywilna / 112 / IMGW-PIB

Source: Own elaboration.

Źródło: Opracowanie własne.

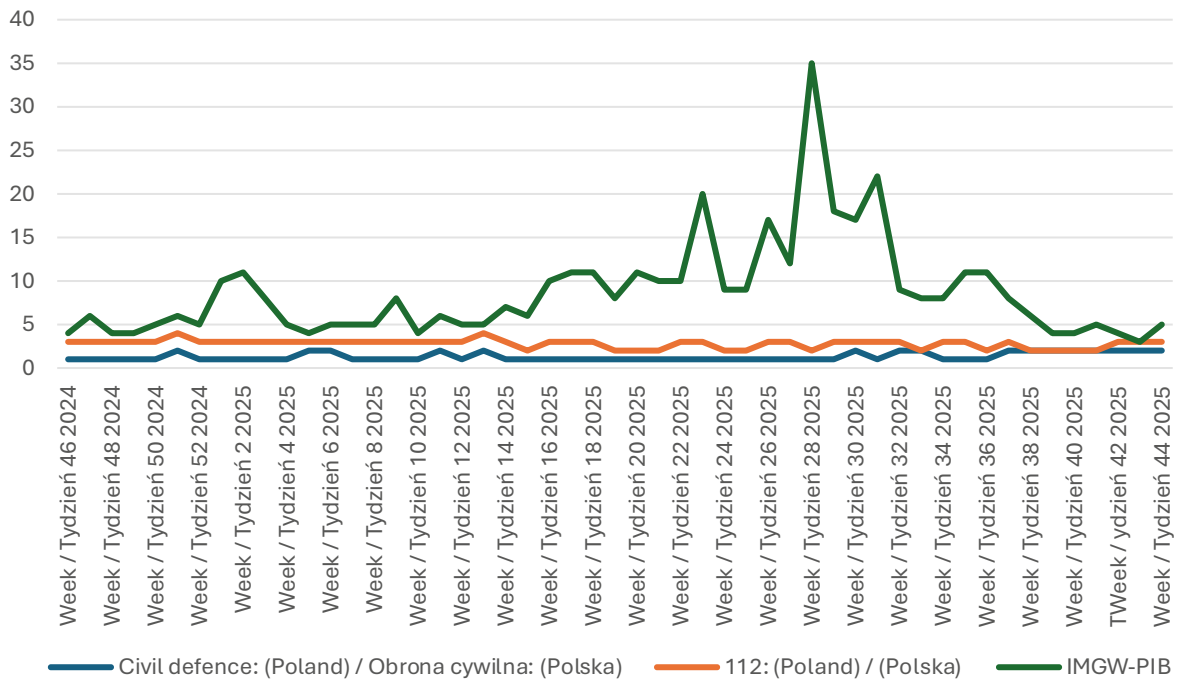


Figure 2. Google Trends – Poland (period of last 12 months – 11/2024-11/2025). Search Terms: obrona cywilna (civil defence) / 112 / IMGW-PIB
Rycina 2. Google Trends – Polska (okres ostatnie 12-mcy – 11.2024-11.2025). Hasła: obrona cywilna / 112 / IMGW-PIB

Source: Own elaboration.

Źródło: Opracowanie własne.

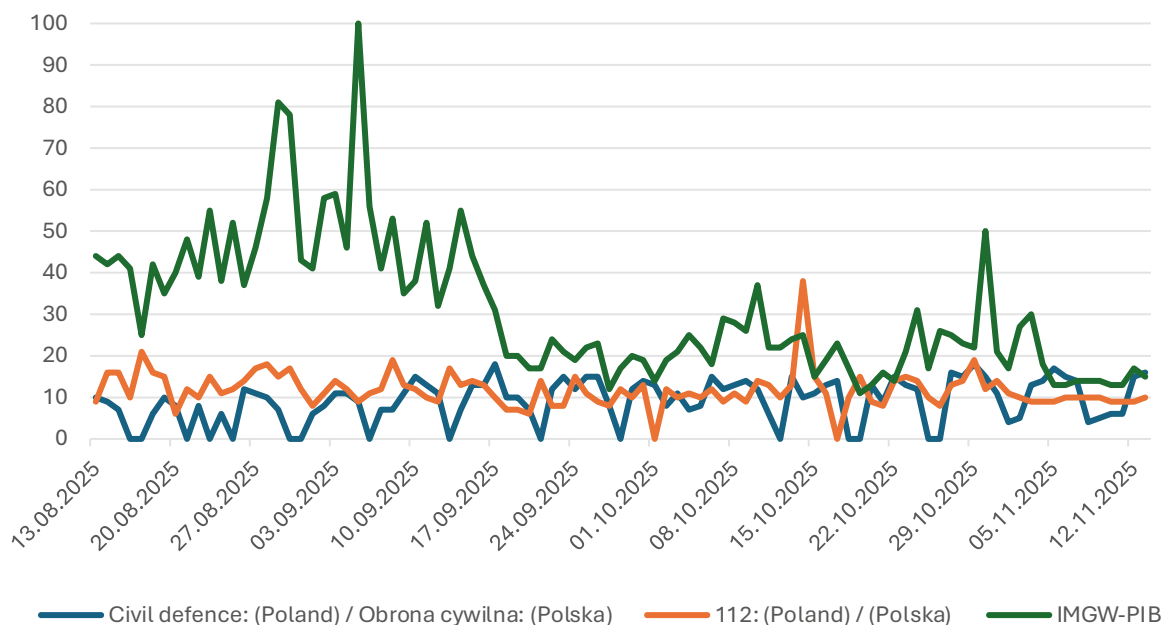


Figure 3. Google Trends – Poland (period of last 90 months days – 08-11/2025). Search Terms: obrona cywilna (civil defence) / 112 / IMGW-PIB
Rycina 3. Google Trends – Polska (okres ostatnie 90 dni – 08-11.2025). Hasła: obrona cywilna / 112 / IMGW-PIB

Source: Own elaboration.

Źródło: Opracowanie własne.

The data from Google Trends was processed in a spreadsheet and presented in a layout enabling a comparative analysis. Index values (0–100) were scaled in relation to reference period and then four indicators were calculated:

- currency index (average of the last 90 days to average of the entire period),
- peak ratio (maximum of the last 12 months to median),
- annual trend (linear regression inclination for annual presentation),
- diffusion indicator (number of voivodeships with ≥ 50 in the peak week).

The results are presented in table 1 below (diffusion value calculated for Search Terms IMGW-PIB, 112, *obrona cywilna* «civil defence»).

Dane z Google Trends zostały przetworzone w arkuszu kalkulacyjnym i zestawione w układzie umożliwiającym analizę porównawczą. Wartości indeksu (0–100) przeskalowano względem okresu referencyjnego, a następnie obliczono cztery wskaźniki:

- indeks aktualności (średnia z ostatnich 90 dni do średniej z całego okresu),
- *peak ratio* (maksimum z ostatnich 12 miesięcy do mediany),
- trend roczny (nachylenie regresji liniowej dla ujęcia rocznego),
- wskaźnik dyfuzji (liczba województw z wartością ≥ 50 w tygodniu piku).

Wyniki przedstawiono w tabeli 1 poniżej (wartości dyfuzji obliczono dla haseł IMGW-PIB, 112, obrona cywilna).

Table 1. Indicator values (currency index, peak ratio, annual trend and diffusion indicator) for selected search terms

Tabela 1. Wartości wskaźników (indeks aktualności, peak ratio, trend roczny i wskaźnik dyfuzji) dla wybranych haseł

	Average of 2022–2025 / Średnia 2022–2025	Average of 90 days / Średnia 90 dni	Currency index / Indeks aktualności	Peak ratio	Annual trend – inclination / Trend roczny – nachylenie	Diffusion / Dyfuzja
Alert RCB	8.89	3.63	0.41	16.67	0.380	-
RSO	4.05	5.23	1.29	4.00	0.019	-
Meteo IMGW	13.99	29.54	2.11	3.09	0.099	-
IMGW-PIB	10.54	30.88	2.93	4.38	0.093	2
112	5.05	2.54	0.50	1.33	-0.014	2
Obrona cywilna (civil defence)	0.82	9.11	11.11	2.00	0.013	2

Source: Own elaboration.

Źródło: Opracowanie własne.

The currency index describes how the current interest (last 90 days) compares to values typical of the entire period of 2022–2025; values above 1.0 indicate that the subject is currently “above standard” and reinforced by current events. The peak ratio, calculated as the ratio of the current maximum value to the median of the last 12 months, enables determining if the increase in interest is stable or episodic. High values designate one-time surges caused by an incident or warning communication. The annual trend, determined based on the linear regression inclination for data from the last 12 months, indicates the general change direction: positive values indicate an increasing interest and gradual activation of the recipients, while negative values prove the withdrawal of attention. The diffusion indicator shows the number of voivodeships, in which the index value exceeded 50 in the week of the highest interest. The more voivodeships meet that threshold, the more nationwide the nature of the given phenomenon or communication. However, a low number of voivodeships indicates that the interest was restricted to some regions.

The presentation of indicators clearly shows that “Alert RCB” is highly abrupt, a relatively low average in the entire period, a high currency index and a high peak ratio, which entails short and very strong surges in interest related to specific events. “Meteo IMGW” and “IMGW-PIB” are more stable in nature. Their currency index is raised, while the peak ratio is moderate, which proves a permanent presence in social awareness and frequent returns to these sources in weather-related crisis situations. For terms “112” and “obrona cywilna” (civil defence), the base level is low, but the annual trend is positive, which suggests a gradual increase of interest in the last 12 months, probably in connection with the reform of the system and the discussion about the new act. The diffusion indicator shows that content related to IMGW-PIB and number 112 have a clearly nationwide coverage, while the interest in civil defence remains more spatially varied and more strongly concentrated in some regions. Collectively, it means that mass warning systems (Alert RCB) generate abrupt, yet short-term peaks in attention, while analytical institutions and key alarm numbers build their position by through stable presence and gradual awareness growth. For designing crisis communication, it is suggested that both approaches must be combined: quick, one-time alerts with long-term education around the terms of “112”, “civil defence” and role of institutions, such as IMGW-PIB.

The data obtained allow noting differences in the nature of interest in individual topics. “Alert RCB” is characterised by clear peaks during intensive weather and crisis situations (e.g. floods, gales), while “civil defence” maintains a stable, yet low, interest background with a visible increase in the second half of 2024. This, in turn, may be connected with the entry into force of the new Civil Protection and Civil Defence Act. “RSO” is characterised by moderate activity and low variation dynamics, which suggests smaller awareness among citizens, despite major operational significance. “IMGW-PIB” records a systematic increase in interest, in particular weather warning periods, but its values often coincide with “Alert RCB” peaks, which points to the correlation of communications and confirms that the citizen responds to a consistent institutional message.

Indeks aktualności opisuje, jak obecne zainteresowanie (ostatnie 90 dni) wypada na tle wartości typowych dla całego okresu 2022–2025; wartości powyżej 1,0 wskazują na temat, który znajduje się aktualnie „powyżej normy” i jest wzmacniany przez bieżące wydarzenia. Peak ratio, obliczany jako stosunek wartości maksymalnej do mediany z ostatnich 12 miesięcy, pozwala określić, czy wzrosty zainteresowania mają charakter stabilny, czy epizodyczny – wysokie wartości oznaczają jednorazowe skoki wywołane incydentem lub komunikatem ostrzegawczym. Trend roczny, wyznaczony na podstawie nachylenia regresji liniowej dla danych z ostatnich 12 miesięcy, pokazuje ogólny kierunek zmiany: wartości dodatnie oznaczają narastające zainteresowanie i stopniową aktywizację odbiorców, a wartości ujemne świadczą o wygaszaniu uwagi. Wskaźnik dyfuzji pokazuje, w ilu województwach w tygodniu największego zainteresowania wartość indeksu przekroczyła poziom 50. Im więcej województw osiąga ten próg, tym bardziej ogólnokrajowy charakter ma dane zjawisko lub komunikat. Niska liczba województw oznacza natomiast, że zainteresowanie ograniczało się do wybranych regionów.

Z zestawienia wskaźników widać wyraźnie, że „Alert RCB” ma charakter silnie skokowy, relatywnie niską średnią w całym okresie, wysoki indeks aktualności oraz wysokie *peak ratio*, co oznacza krótkie, bardzo mocne skoki zainteresowania powiązane z konkretnymi zdarzeniami. „Meteo IMGW” i „IMGW-PIB” wykazują bardziej stabilny charakter – ich indeks aktualności jest podwyższony, ale *peak ratio* umiarkowane, co świadczy o stałej obecności w świadomości społecznej i częstym powracaniu do tych źródeł w sytuacjach kryzysowych związanych z pogodą. Dla pojęć „112” i „obrona cywilna” widoczny jest niski poziom bazowy, ale dodatni trend roczny, co sugeruje stopniowy wzrost zainteresowania w ostatnich 12 miesiącach, prawdopodobnie w związku z reformą systemu i dyskusją wokół nowej ustawy. Wskaźnik dyfuzji pokazuje, że treści związane z IMGW-PIB i numerem 112 mają wyraźny zasięg ogólnokrajowy, podczas gdy zainteresowanie obroną cywilną wciąż jest bardziej zróżnicowane przestrzennie i silniej koncentruje się w wybranych regionach. Łącznie oznacza to, że systemy ostrzegania masowego (Alert RCB) generują gwałtowne, ale krótkotrwałe piki uwagi, natomiast instytucje analityczne i kluczowe numery alarmowe budują swoją pozycję poprzez stabilną obecność i stopniowy wzrost rozpoznawalności. Dla projektowania komunikacji kryzysowej sugeruje to konieczność łączenia obu podejść: szybkich, jednorazowych alertów z długofalową edukacją wokół pojęć „112”, „obrona cywilna” i roli instytucji takich jak IMGW-PIB.

Uzyskane dane pozwalają zauważyć wyraźne różnice w charakterze zainteresowania poszczególnymi tematami. „Alert RCB” cechuje się wyraźnymi pikami w okresach intensywnych zjawisk pogodowych oraz sytuacji kryzysowych (np. powódzie, wichury), natomiast „obrona cywilna” utrzymuje stabilne, choć niskie, tło zainteresowania z widocznym wzrostem w drugiej połowie 2024 roku. Ten można z kolei wiązać z wejściem w życie nowej ustawy o ochronie ludności i obronie cywilnej. „RSO” charakteryzuje się umiarkowaną aktywnością i słabą dynamiką zmian, co sugeruje jego mniejszą rozpoznawalność wśród obywateli, mimo dużego znaczenia operacyjnego. „IMGW-PIB” notuje systematyczny wzrost zainteresowania, szczególnie w okresach ostrzeżeń pogodowych,

The data indicates that warning systems based on SMS messages and mobile applications (Alert RCB, RSO) trigger short-term, yet high surges in attention, however analytical and scientific institutions (IMGW-PIB) receive stable long-term interest level. In a long-term view, an growth trend is visible for Search Terms “civil defence” and “System 112”, which may be interpreted as a result of legislative changes and increased number of media communications on the reform of the civil protection system.

For the purposes of spatial assessment, the “Interest by sub-region” Google Trends module was used, which enabled a geographical distribution of the interest in the Topic of “Alert RCB” in the period of 90 days. Values above 50 were recorded in all eastern and southern voivodeships, with particular intensity in Lubelskie and Podlaskie voivodeships. This distribution coincided with areas connected to war (Lubelskie) and difficult border situation.

a jego wartości często pokrywają się z pikami „Alertu RCB”, co wskazuje na współzależność komunikatów i potwierdza, że obywatel reaguje na spójny przekaz instytucjonalny.

Dane wskazują, że systemy ostrzegania bazujące na komunikatach SMS i aplikacjach mobilnych (Alert RCB, RSO) wywołują krótkotrwale, wysokie skoki uwagi, natomiast instytucje o charakterze analityczno-naukowym (IMGW-PIB) utrzymują stabilny, długoterminowy poziom zainteresowania. W ujęciu długookresowym widoczny jest trend wzrostowy dla pojęcia „obrona cywilna” oraz „System 112”, co można interpretować jako efekt zmian legislacyjnych i wzrostu liczby komunikatów medialnych dotyczących reformy systemu ochrony ludności.

Na potrzeby oceny przestrzennej wykorzystano moduł „Interest by subregion” z Google Trends, co pozwoliło określić rozmieszczenie geograficzne zainteresowania tematem „Alert RCB” w okresie 90 dni. Wartości powyżej 50 odnotowano we wszystkich województwach wschodnich i południowych, ze szczególnym natężeniem w województwach lubelskim i podlaskim. Dystrybucja ta pokrywa się z obszarami, które są związane z wojną (lubelskie) oraz trudną sytuacją graniczną.

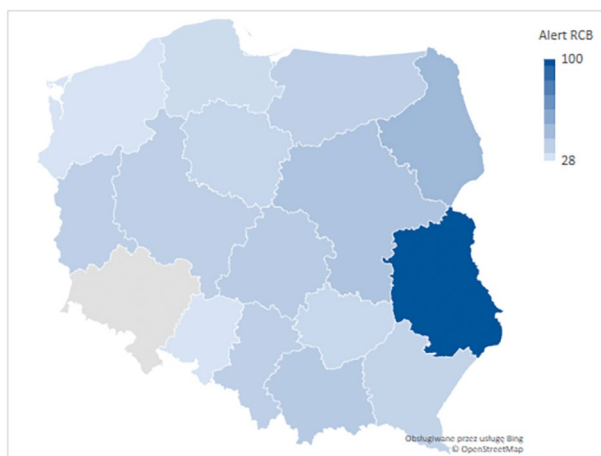


Figure 4. The diffusion map of interest in Search Term “Alert RCB” by voivodeship in the period of 90 days (from 14.08.2025). The colours represent the relative intensity of queries

Rycina 4. Mapa dyfuzji zainteresowania hasłem Alert RCB według województw w okresie 90 dni (od 14.08.2025). Kolorystyka przedstawia względną intensywność zapytań

Source: Google Trends [access: 13.11.2025].

Źródło: Google Trends [dostęp: 13.11.2025].

To verify the persistence of the phenomena observed, Google Trends data was matched with the number of views of appropriate Search Terms in Wikipedia Pageviews in Polish (see Fig. 5). The analysis showed that increases for “Alert RCB” and “IMGW” in Google Trends are correlated with increased numbers of views of their Wikipedii pages, which proves that recipients move from current information (alert) to in-depth information (description of the system or institutions).

W celu weryfikacji trwałości obserwowanych zjawisk dane z Google Trends zestawiono z liczbą odsłon odpowiednich haseł w Wikipedia Pageviews w języku polskim (zob. Ryc. 5). Analiza wykazała, że wzrosty w Google Trends dla „Alertu RCB” i „IMGW” korelują ze zwiększoną liczbą odsłon ich stron w Wikipedii, co świadczy o przechodzeniu odbiorców od informacji bieżącej (alertu) do informacji pogłębionej (opis systemu lub instytucji).

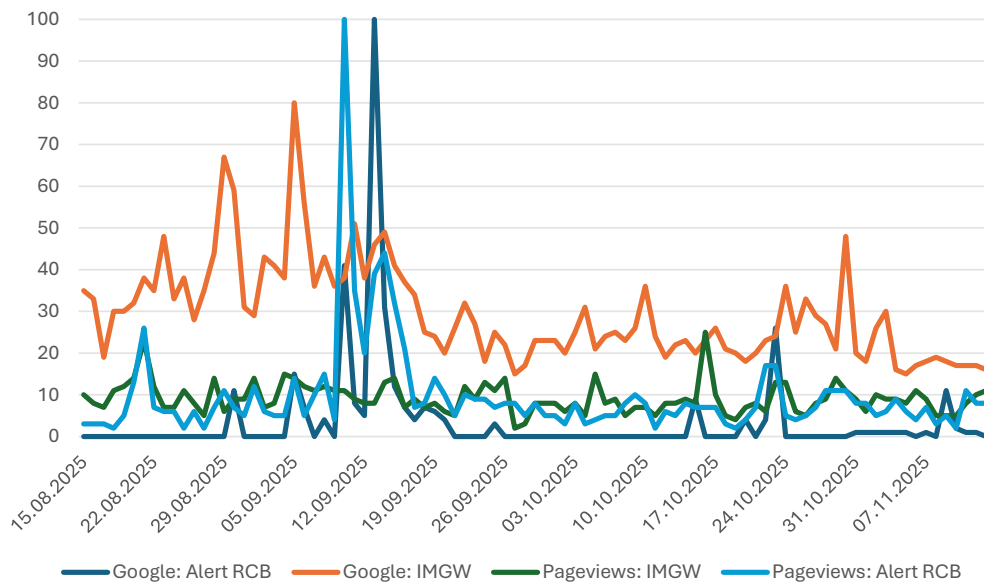


Figure 5. The comparison of the popularity of Search Terms Alert RCB and IMGW in the period of 90 days (08–11.2025) in the Google and Wikipedia browser

Rycina 5. Porównanie popularności haseł Alert RCB i IMGW w okresie 90 dni (08–11.2025) w przeglądarce Google i Wikipedia

Source: Google Trends [access: 13.11.2025].

Źródło: Google Trends [dostęp: 13.11.2025].

The qualitative analysis also included the assessment of availability and update of national information systems (Alert RCB, RSO, IMGW application, Airly and other). For each of them, it included: the number of downloads, average user rating (see Table 2). This enabled connecting the dynamics of social interest with real availability of tools.

Do analizy jakościowej włączono również ocenę dostępności i aktualności krajowych systemów informacyjnych (Alert RCB, RSO, aplikacja IMGW, Airly i inne). Dla każdego z nich uwzględniono: liczbę pobrań, średnią ocenę użytkowników (zob. Tabela 2). Dzięki temu możliwe było powiązanie dynamiki zainteresowania społecznego z rzeczywistą dostępnością narzędzi.

Table 2. Selected applications with comparison of ratings and number of downloads (data as of 14.11.2025)

Tabela 2. Wybrane aplikacje wraz z porównaniem ocen i liczby pobrań (dane na dzień 14.11.2025)

No. / Lp.	Name / Nazwa	Administrator / Administrator	Purchase platform / Platforma zakupowa	Rating / Ocena	Number of ratings / Liczba ocen	Number of downloads / Liczba pobrań
1	RSO	MSWIA/RCB	App Store	2.3/5.0	128	n/a
			Google Play	3.2/5.0	1.84k	+100k
2	Meteo IMGW	IMGW PIB	App Store	3.2/5.0	204	n/a
			Google Play	4.0/5.0	2.26k	+100k
3	BLISKO	AMM Systems Sp. z o.o.	App Store	3.0/5.0	41	n/a
			Google Play	2.9/5.0	1.35k	+100k
4	Alarm 112	MSWIA	App Store	2.6/5.0	40	n/a
			Google Play	2.5/5.0	295	+50k
5	Ratunek	Polkomtel Sp. z o.o. Fundacja GOPR	App Store	2.1/5.0	152	n/a
			Google Play	3.8/5.0	1.28k	+500k
6	Ratownik	Centrum Ratownictwa Sp. z o.o.	App Store	4.7/5.0	110	n/a
			Google Play	4.1/5.0	1.2k	+100k
7	Airly	Airly Sp. z o.o.	App Store	4.7/5.0	43k	n/a
			Google Play	3.7/5.0	6.91k	+500k

Source / Źródło: <https://www.apple.com/pl/app-store/> and <https://play.google.com/store/games?hl=pl>

The proposed methodological model integrates quantitative and qualitative data, combining the analysis of search trends, information activity of public institutions and availability of digital tools. This enables capturing the dynamics of social perception of safety in Poland and indicating areas, in which education, communication and new technologies may really increase the effectiveness of civil protection.

New technologies as tools of engagement of the citizens

The purpose of this chapter is to define, what is considered as “new technology” in civil protection and indicating its main categories, useful for engagement of citizens, with short examples of applications. Detailed case studies were elaborated in the remainder of the article. In this study, a “new technology” is understood not as an innovative gadget, but as a digital, telecommunication or hardware solution that really streamlines the key functions of civil protection, such as: monitoring, warning, information exchange, recognition of situation, prevention and training.

For a given technology to be effective, it must be above all generally available, i.e. work on devices already owned by most citizens, require minimum operating skills and be familiar enough for the recipients to know, how to use it under time pressure. Reliability, interoperability with systems of services and care for privacy and simplicity of communication are equally important.

The contemporary ecosystem of solutions that engage citizens consists above all of public warning systems, to a large extent Local Based or based on Cell Broadcast SMS and mobile applications. They are often complemented by crisis applications enabling two-way communication, as well as IoT and data crowdsourcing mechanisms (e.g. air quality sensors, simple water level sensors and inhabitant reports). An increasing role is also played by VR/AR tools and gamification, which enable training correct behaviours and procedures in a short time, especially in rare yet high risk situations. The following chapters present detailed descriptions of implementation, here the authors only point to the directions and logic of their use.

For example, firstly, the warning system connecting Cell Broadcast and SMS with a simple application may deliver a consistent message to all telephones in the hazard zone within minutes and, secondly, through the application, show the map, short FAQ and three most important action steps. From the perspective of services, it relieves emergency numbers and enables more precise evacuation control.

Secondly, a two-way “report and check” application shortens the time from event to decision: the citizen sends the description and picture, the location is attached automatically and the system pre-classifies the report and routes it to the right station; the officer on duty sees the locations, in which similar signals multiply, on the map.

Thirdly, the combination of cheap IoT sensors (e.g. precipitation and water level at local culverts) with inhabitant reports forms the flood early warning system, which can detect an increasing surge quicker than the thinner measurement network,

Zaproponowany model metodologiczny integruje dane ilościowe i jakościowe, łącząc analizę trendów wyszukiwań, aktywność informacyjną instytucji publicznych oraz dostępność narzędzi cyfrowych. Dzięki temu możliwe jest uchwycenie dynamiki społecznego postrzegania bezpieczeństwa w Polsce i wskazanie obszarów, w których edukacja, komunikacja i nowe technologie mogą realnie zwiększyć skuteczność ochrony ludności.

Nowe technologie jako narzędzie zaangażowania obywateli

Celem rozdziału jest zdefiniowanie, co rozumiemy przez „nową technologię” w ochronie ludności oraz wskazanie jej głównych kategorii, użytecznych do angażowania obywateli, z krótkimi przykładami zastosowań. Szczegółowe studia przypadków rozwinięto w dalszej części artykułu. W niniejszej pracy „nową technologię” rozumiemy nie jako innowacyjny gadżet, lecz jako rozwiązanie cyfrowe, telekomunikacyjne lub sprzętowe, które realnie usprawnia kluczowe funkcje ochrony ludności, takie jak: monitorowanie, ostrzeganie, wymianę informacji, rozpoznanie sytuacji, prewencja i szkolenia.

Aby dana technologia była skuteczna, musi być przede wszystkim ogólnodostępna – czyli działać na urządzeniach, które większość obywateli już posiada, wymagać minimalnych umiejętności obsługi i być rozpoznawalna na tyle, by odbiorcy wiedzieli, jak z niej skorzystać pod presją czasu. Równie ważne są niezawodność, interoperacyjność z systemami służb oraz dbałość o kwestię prywatności i prostotę przekazu.

Współczesny ekosystem rozwiązań, które angażują obywateli, tworzą przede wszystkim publiczne systemy ostrzegania, które w dużej mierze oparte są na Local Based lub Cell Broadcast SMS i aplikacjach mobilnych. Są one często uzupełniane przez aplikacje kryzysowe umożliwiające komunikację dwustronną, a także przez IoT i mechanizmy crowdsourcingu danych (np. sensory jakości powietrza, proste czujniki poziomu wody oraz raporty mieszkańców). Coraz większą rolę odgrywają również narzędzia VR/AR oraz grywalizacja, które pozwalają w krótkim czasie trenować poprawne zachowania i procedury, zwłaszcza w sytuacjach rzadkich, ale obarczonych wysokim ryzykiem. Szczegółowe opisy wdrożeń przedstawiono w kolejnych rozdziałach – tutaj autorzy wskazują jedynie kierunki i logikę ich użycia.

Ilustracyjnie, po pierwsze, system ostrzegania łączący Cell Broadcast i SMS z prostą aplikacją może w ciągu minut dostarczyć spójny komunikat do wszystkich telefonów przebywających w strefie zagrożenia, a następnie – poprzez aplikację – pokazać mapę, krótkie FAQ i trzy najważniejsze kroki działania. Z perspektywy służb oznacza to odciążenie numerów alarmowych i możliwość precyzyjniejszego kierowania ewakuacją.

Po drugie, aplikacja dwukierunkowa „zgłoś i sprawdź” skraca czas od zdarzenia do decyzji: obywatel wysyła opis i zdjęcie, lokalizacja dołącza się automatycznie, a system wstępnie klasyfikuje zgłoszenie i kieruje je do właściwego stanowiska; dyżurny widzi na mapie miejsca, w których mnożą się podobne sygnały.

Po trzecie, połączenie tanich czujników IoT (np. opadów i poziomu wody na lokalnych przepustach) z raportami mieszkańców tworzy

which really helps in dispatching patrols and logistics (sand bags, detours) and builds a database for post-event analysis.

A common denominator of these solutions is the shortening of the “information → decision → action” and moving some of the burden from the technology itself to more common use and simple procedures. The technology only reinforces the resistance when it is familiar, easy and available to many and when it smoothly connects with existing infrastructure and operational practices of services.

The following chapters present the examples of Polish technological solutions aimed to strengthen the civil safety and protection.

Polish systemic solutions – monitoring hazards and alarming the population

In connection with ensuring the safety of citizens, the public administration is entrusted with clear legal obligations in terms of hazard monitoring, notification and alarms. They are a foundation of the civil protection and civil defence system and their fulfilment is based on the principle of uninterrupted flow of information between state bodies, services and society.

The primary obligation of the state in this area arises already from Article 5 of the Constitution of the Republic of Poland, which stipulates that “The Republic of Poland ensures the freedom and human and citizen rights and safety of citizens”. This stipulation results in the constitutional obligation of the state to undertake actions aimed at protecting the life, health and property of the population in case of natural, technical, environmental or military hazard [3].

These obligations are detailed in the Civil Protection and Civil Defence Act of 5 December 2024 (Journal of Laws 2024, item 1907). Section 8 of that Act defines the following specific tasks of public administration bodies and other entities in charge of safety: “detecting hazards, notification, hazard warnings and alarms and the safe state communication system”. In accordance with the above regulations, every administration body or civil protection entity that obtains the hazard information first is obliged to immediately notify appropriate services and populations, as well as to initiate appropriate alarm procedures. These obligations are fulfilled at all levels of public administration, in close collaboration with entities in charge of safety, public order, environmental protection and crisis response. Broadly understood monitoring hazards and alarming the population are an essential component of the civil protection and civil defence system. They are the basic tool for the fulfilment of the constitutional obligation of the state to ensure the safety of citizens.

Civil protection and civil defence tasks include five interconnected, but separate functions: monitoring, detection, notification, warning and alarming. The monitoring and detection of hazards are processes of continuous monitoring, collection and analysis of data on potential and existing hazards. They cover both the analysis of meteorological, hydrological, geological or epidemiological data and monitoring of critical infrastructure.

wczesne ostrzeganie powodziowe, które potrafi wykryć narastające wezbranie szybciej niż rzadsza sieć pomiarowa – co realnie pomaga w kierowaniu patroli i logistyki (worki z piaskiem, objazdy) oraz buduje bazę danych do analiz po zdarzeniu.

Wspólnym mianownikiem tych rozwiązań jest skrócenie drogi „informacja → decyzja → działanie” oraz przeniesienie części ciężaru z samej technologii na powszechne użycie i proste procedury. Technologia wzmacnia odporność dopiero wtedy, gdy jest znana, łatwa i dostępna dla wielu – i gdy bez trudu łączy się z istniejącą infrastrukturą i praktykami operacyjnymi służb.

W rozdziałach poniżej przedstawiono przykłady polskich rozwiązań technologicznych, które mają na celu zwiększenie bezpieczeństwa i ochrony ludności.

Polskie rozwiązania systemowe – monitorowanie zagrożeń i alarmowanie ludności

W związku z zapewnieniem bezpieczeństwa obywateli na administrację publiczną nałożone są jednoznaczne obowiązki prawne w zakresie monitorowania, powiadamiania i alarmowania o zagrożeniach. Są one fundamentem systemu ochrony ludności i obrony cywilnej, a ich realizacja opiera się na zasadzie nieprzerwanego przepływu informacji między organami państwa, służbami i społeczeństwem.

Podstawowy obowiązek państwa w tym zakresie wynika już z art. 5 Konstytucji Rzeczypospolitej Polskiej, który stanowi, że „Rzeczpospolita Polska zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli”. Z przepisu tego wynika konstytucyjna powinność państwa do podejmowania działań służących ochronie życia, zdrowia i mienia ludności w sytuacjach zagrożenia naturalnego, technicznego, ekologicznego czy militarnego [3].

Uszczegółowienie tych obowiązków zawiera Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907). W rozdziale 8 tej ustawy określono następujące szczegółowe zadania organów administracji publicznej i innych podmiotów odpowiedzialnych za bezpieczeństwo: „wykrywanie zagrożeń, powiadamianie, ostrzeganie i alarmowanie o zagrożeniach oraz system bezpiecznej łączności państwowej”. Zgodnie z ww. przepisami, każdy organ administracji lub podmiot ochrony ludności, który jako pierwszy uzyska informację o zagrożeniu, jest zobowiązany do niezwłocznego powiadomienia właściwych służb oraz ludności, a także do uruchomienia odpowiednich procedur alarmowych. Obowiązki te realizowane są na wszystkich poziomach zarządzania publicznego w ścisłej współpracy z podmiotami odpowiedzialnymi za bezpieczeństwo, porządek publiczny, ochronę środowiska i reagowanie kryzysowe. Szeroko rozumiane monitorowanie zagrożeń oraz alarmowanie ludności stanowią kluczowy element systemu ochrony ludności i obrony cywilnej. Są one podstawowym narzędziem realizacji konstytucyjnego obowiązku państwa zapewnienia bezpieczeństwa obywateli.

Zadania z zakresu ochrony ludności i obrony cywilnej obejmują pięć powiązanych ze sobą, lecz odrębnych funkcji: monitorowanie, wykrywanie, powiadamianie, ostrzeganie i alarmowanie. Monitorowanie i wykrywanie zagrożeń to procesy ciągłego obserwowania,

Although the Civil Protection and Civil Defence Act of 2024 does not define the term hazard monitoring directly, this activity is an integral component of the hazard detection process, which is referred to in section 8 of the Act. The obligation to conduct monitoring in specific fields arises from other legal acts, such as the Crisis Management Act, the Environmental Protection Law, the Water Law and the Atomic Law. The monitoring is continuous and preventative, it includes ongoing tracking of environmental parameters and enables predicting the potential occurrence of the hazard in advance. The essence of monitoring is the possibility of early-warning of citizens [4].

Detection is the statement of factual occurrence of the hazard or its direct consequences. This operation is reactive in nature and consists in determining that the hazard has already occurred. Subsequently, the hazard is identified and the impact range and hazard intensity are evaluated. The detection of the hazard is the basis for initiating the alarm and starting rescue operations.

The notification consists in communicating, using all available means of communication, the information on the possibility of occurrence, the occurrence or the cessation of the risk. The purpose of notification is to inform the authorities and rescue services, as well as the society of the situation, and specifying the procedure.

Warning is the stage that precedes alarming and consists in informing of probable hazards and recommending preventative activities. The purpose of warning messages is to increase the readiness of the society and services to respond, as well as to reduce the potential impact of hazards.

Alarming, in turn, is an urgent activity. It consists in transmitting signals and alarm messages related to an event that is a direct hazard to life, health and property. Alarming initiates evacuation procedures, mobilisation of services and communication of procedural instructions.

A common feature of all five operations is effective communication and quick flow of information, based on both organisational and technological solutions.

Monitoring and alarming tasks are divided into public administration levels and specialised institutions:

1. Government administration – in particular the Minister of Internal Affairs and Administration, responsible for coordinating civil protection operations, the Government Centre for Security, managing the national warning system (Alert RCB and RSO, and the Minister of Climate and Environment, supervising environmental monitoring systems.
2. Local administration – voivodeships, starostes, commune administrators, mayors and city presidents, organising local alarm and crisis communication systems, in collaboration with their subordinate crisis management centres.
3. Specialised services and inspections – i.a. the State Fire Service, Police, State Sanitary Inspection, Polish Waters, Polish Geological Institute, communal guards.
4. Scientific and technical institutions – conducting research and developing technologies to support early warning, predicting hazards and analysis of spatial data, i.a. the Institute of Meteorology and Water Management

gromadzenia i analizowania danych dotyczących potencjalnych i występujących zagrożeń. Obejmują one zarówno analizę danych meteorologicznych, hydrologicznych, geologicznych czy epidemiologicznych, jak i obserwację infrastruktury krytycznej.

Choć ustawa o ochronie ludności i obronie cywilnej z 2024 r. nie definiuje wprost pojęcia monitorowania zagrożeń, to czynność ta stanowi nieodłączny element procesu wykrywania zagrożeń, o którym mowa w rozdziale 8 ustawy. Obowiązek prowadzenia monitoringu w określonych dziedzinach wynika z innych aktów prawnych, takich jak ustawa o zarządzaniu kryzysowym, Prawo ochrony środowiska, Prawo wodne, Prawo atomowe. Monitorowanie ma charakter ciągły i prewencyjny – obejmuje bieżące śledzenie parametrów środowiskowych, pozwala z wyprzedzeniem przewidzieć możliwość wystąpienia zagrożenia. Istotą monitorowania jest możliwość wczesnego ostrzegania obywateli [4].

Wykrywanie to stwierdzenie faktycznego wystąpienia zagrożenia lub jego bezpośrednich skutków. Działanie to ma charakter reaktywny, polega na ustaleniu, że zagrożenie już nastąpiło. W dalszej kolejności zagrożenie jest identyfikowane, następuje ocena jego zasięgu oddziaływania i natężenia. Wykrycie zagrożenia jest podstawą do uruchomienia alarmowania i rozpoczęcia działań ratowniczych.

Powiadamianie polega na przekazywaniu – przy użyciu wszelkich dostępnych środków łączności – informacji o możliwości wystąpienia, wystąpieniu lub ustąpieniu zagrożenia. Celem powiadamiania jest poinformowanie zarówno władz i służb ratowniczych, jak i społeczeństwa o sytuacji oraz wskazanie sposobu postępowania.

Ostrzeganie to etap uprzedzający alarmowanie, polegający na informowaniu o prawdopodobnych zagrożeniach i zalecaniu działań prewencyjnych. Komunikaty ostrzegawcze mają na celu zwiększenie gotowości społeczeństwa i służb do reagowania, a także ograniczenie potencjalnych skutków zagrożeń.

Alarmowanie natomiast jest działaniem o charakterze pilnym – polega na natychmiastowym przekazaniu sygnałów i komunikatów alarmowych o zdarzeniu, które bezpośrednio zagraża życiu, zdrowiu lub mieniu. Alarmowanie uruchamia procedury ewakuacji, mobilizacji służb oraz przekazywania instrukcji postępowania.

Wspólną cechą wszystkich pięciu działań jest skuteczna komunikacja i szybki obieg informacji, oparty zarówno na rozwiązaniach organizacyjnych, jak i technologicznych.

Zadania w zakresie monitorowania i alarmowania zostały podzielone na poziomy administracji publicznej oraz wyspecjalizowane instytucje:

1. Administracja rządowa – w szczególności Minister Spraw Wewnętrznych i Administracji, odpowiedzialny za koordynację działań z zakresu ochrony ludności; Rządowe Centrum Bezpieczeństwa, które zarządza krajowym systemem ostrzegania (Alert RCB i RSO); oraz Minister Klimatu i Środowiska, nadzorujący systemy monitoringu środowiska.
2. Administracja terenowa – wojewodowie, starostowie, wójtowie, burmistrzowie i prezydenci miast, którzy organizują lokalne systemy alarmowania i komunikacji kryzysowej, współpracując z podporządkowanymi im centrami zarządzania kryzysowego.
3. Służby i inspekcje specjalistyczne – m.in. Państwowa Straż Pożarna, Policja, Państwowa Inspekcja Sanitarna,

of the National Research Institute, the Polish Geological Institute of the National Research Institute, the National Atomic Energy Agency and the Scientific and Research Centre for Fire Protection of the National Research Institute.

The collaboration between these entities are based on a cohesive information exchange and mutual support system, in which every rung of administration plays a clearly defined role.

The Polish ecosystem of solutions for monitoring and alarming the population covers a wide spectrum of technological and organisational tools. It consists, public warning systems, civic collaboration platforms, environmental sensor networks and modern forms of education.

The most important components of this system are:

1. The Alert RCB system – the mass SMS notification system, operating in collaboration with mobile network operators. It enables instant transmission of warning messages to the inhabitants of specific hazard area.
2. Geographic Information Systems (GIS) and spatial data analytics – used to predict the consequences of events (e.g. floods, fires, pollution) and modelling response scenarios.
3. IoT sensors and telemetric networks – enable continuous monitoring of air quality, water level, temperature, radiation or seismic activity. The data from these systems is transmitted to crisis management centres in real time.
4. Mobile applications and warning portals – such as “Regionalny System Ostrzegania” (RSO, Regional Warning System), which provides two-directional communication with citizens and enables reporting incidents.
5. Artificial intelligence and data analysis automation – they increasingly support the process of detecting anomalies, predicting hazards and personalising warning communications.
6. Modern education tools – using virtual reality and augmented reality (VR/AR) in crisis response and social education.

Monitoring and alarming the population are fundamental instruments of civil protection, based on solid legal foundation and supported by modern information technologies. This system is a dynamically developing ecosystem, in which teleinformatics technologies, data analysis and social communication combine into a cohesive civil protection mechanism. Their effectiveness depends on the agility of administration structures, integration of technical systems and social awareness of citizens.

Wody Polskie, Państwowy Instytut Geologiczny, strażę gminne.

4. Instytucje naukowe i techniczne – prowadzące badania i rozwijające technologie wspierające wczesne ostrzeganie, prognozowanie zagrożeń oraz analizę danych przestrzennych m.in. Instytut Meteorologii i Gospodarki Wodnej PIB, Państwowy Instytut Geologiczny PIB, Państwowa Agencja Atomistyki, Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej PIB.

Współpraca między tymi podmiotami opiera się na zasadzie wspólnego systemu wymiany informacji i wzajemnego wsparcia, w którym każdy szczebel administracji odgrywa jasno określoną rolę.

Polski ekosystem rozwiązań w zakresie monitorowania i alarmowania ludności obejmuje szerokie spektrum narzędzi technologicznych i organizacyjnych. Tworzą go zarówno publiczne systemy ostrzegania, jak i platformy współpracy z obywatelami, sieci czujników środowiskowych oraz nowoczesne formy edukacji.

Najważniejsze elementy tego systemu to:

1. System Alert RCB – masowy system powiadamiania SMS-owego, działający we współpracy z operatorami sieci komórkowych. Umożliwia błyskawiczne przekazywanie komunikatów ostrzegawczych mieszkańcom określonego obszaru zagrożenia.
2. Systemy Informacji Geograficznej (GIS) i analityka danych przestrzennych – wykorzystywane do prognozowania skutków zdarzeń (np. powodzi, pożarów, skażeń) i modelowania scenariuszy reagowania.
3. Czujniki IoT i sieci telemetryczne – umożliwiają stałe monitorowanie jakości powietrza, poziomu wód, temperatury, promieniowania czy ruchów sejsmicznych. Dane z tych systemów trafiają do centrów zarządzania kryzysowego w czasie rzeczywistym.
4. Aplikacje mobilne i portale ostrzegawcze – takie jak „Regionalny System Ostrzegania” (RSO), które zapewniają dwukierunkową komunikację z obywatelami, umożliwiając im także zgłaszanie incydentów.
5. Sztuczna inteligencja i automatyzacja analizy danych – coraz częściej wspierają proces wykrywania anomalii, prognozowania zagrożeń oraz personalizowania komunikatów ostrzegawczych.
6. Nowoczesne narzędzia edukacyjne – wykorzystujące rzeczywistość wirtualną i rozszerzoną (VR/AR) w szkoleniach z zakresu reagowania kryzysowego i edukacji społecznej.

Monitorowanie i alarmowanie ludności to fundamentalne instrumenty ochrony ludności, oparte na solidnych podstawach prawnych i wspierane przez nowoczesne technologie informacyjne. System ten stanowi dynamicznie rozwijający się ekosystem, w którym technologie teleinformatyczne, analiza danych i komunikacja społeczna łączą się w spójny mechanizm ochrony ludności. Ich skuteczność zależy od sprawności struktur administracyjnych, integracji systemów technicznych oraz świadomości społecznej obywateli.

Tools and applications supporting safety of citizens – Alert RCB and RSO

Poland has a wide public warning system, however its most known form is Alert RCB, using the Location Based SMS technology. It is a state system of mass notifications routed to mobile telephones for people in the hazard zone. Warnings are received by users within the area of occurrence or potential occurrence of danger and communications are prepared by the Government Centre for Security in collaboration e.g. with IMGW, ministries, voivodeships and services, such as the Police, State Fire Service and Border Guard. The system is only activated in extraordinary situations, when there is very high probability (above 80%), direct hazard to life or health of people within a significant area [5].

A direct impulse to start the SMS hazard information system was the storm of the night of 11/12 August 2017 and the tragedy at the Suszek (Pomorskie voivodeship), where two teenage girls died. Alert RCB was started in July 2018 as a pilot programme and following changes in the Telecommunication Law it became a fully-fledged solution. In the first months of operation, 29 activations were initiated and approx. 220M SMS messages were sent [6]. In 2020–2023, the Alert RCB system was intensively developed and modernised. In that period, its frequency of use was primarily connected with the COVID-19 pandemic and extreme weather phenomena, as well as technical or environmental hazards (river poisoning). In parallel, works were conducted to adjust the system to the European Union requirements arising from the European Electronic Communications Code, which obliged the member states to introduce national notification systems based on telecommunication infrastructure [7].

Alert RCB is dedicated to dynamic incidents, such as storms, gales, heavy rains, floods, but also informing of planned detonation of unexploded ordinance, water contamination, CBRNE hazards or epidemic regulations. A message, usually consisting of 160 characters (in exceptional circumstances: up to 320), includes the type of hazard and the most important recommended procedures and often also the link to gov.pl with additional information. The messages are sent to every telephone in hazard area – in Polish to numbers with +48 prefix, in English to other numbers. Messages are distributed by mobile network operators in Poland and the service itself is completely free of charge. In exceptional cases, Alert RCB may be also sent to users with Polish numbers abroad, to provide a quick and consistent message “to everyone in range”.

At present, the technological migration from LB-SMS to Cell Broadcast SMS (CB-SMS) is discussed. This solution enables quicker and more reliable delivery of communications to users in the given area without loading the network. At present, RCB maintains Alert RCB in its current SMS-based form, however works are conducted to expand system functionality, i.e. to the so-called recall alerts on the cessation of hazard [8–9].

Another example of a public warning system in Poland may be Regionalny System Ostrzegania (RSO, Regional Warning System). It is an extended system used to inform and warn the population in Poland of local and regional hazards. RSO is a project of the Government Centre for Security, pursued in collaboration with

Narzędzia i aplikacje wspierające bezpieczeństwo obywateli – Alert RCB i RSO

Polska posiada szeroki system ostrzegania publicznego, jednak jego najbardziej znaną formą jest Alert RCB, wykorzystujący technologię Location Based SMS. Jest to państwowy system masowych powiadomień kierowanych na telefony komórkowe osób przebywających w strefie zagrożenia. Ostrzeżenia otrzymują użytkownicy znajdujący się w obszarze występowania lub potencjalnego wystąpienia niebezpieczeństwa, a komunikaty przygotowuje Rządowe Centrum Bezpieczeństwa we współpracy m.in. z IMGW, ministerstwami, wojewodami oraz służbami takimi jak Policja, Państwowa Straż Pożarna czy Straż Graniczna. System uruchamiany jest wyłącznie w sytuacjach nadzwyczajnych, gdy istnieje bardzo duże prawdopodobieństwo (ponad 80%) bezpośredniego zagrożenia życia lub zdrowia osób przebywających na znaczącym obszarze [5].

Bezpośrednim impulsem uruchomienia SMS-owego systemu informowania o zagrożeniach była nawałnica z nocy 11/12 sierpnia 2017 r. i tragedia na obozie harcerskim w Suszku (woj. pomorskie), gdzie zginęły dwie nastolatki. Alert RCB ruszył w lipcu 2018 r. jako program pilotażowy, a po zmianach w Prawie telekomunikacyjnym stał się pełnoprawnym rozwiązaniem. W pierwszych miesiącach jego działania zainicjowano 29 uruchomień i wysłano ok. 220 mln SMS-ów [6]. W latach 2020–2023 system Alert RCB był intensywnie rozwijany i modernizowany. W tym czasie wzrosła częstotliwość jego wykorzystania związana głównie z pandemią COVID-19 oraz ekstremalnymi zjawiskami pogodowymi, a także zagrożeniami o charakterze technicznym lub środowiskowym (zatrucia rzek). Równoległe trwały prace nad dostosowaniem systemu do wymogów Unii Europejskiej wynikających z Europejskiego Kodeksu Łączności Elektronicznej, który zobowiązał państwa członkowskie do wprowadzenia krajowych systemów powiadamiania opartych o infrastrukturę telekomunikacyjną [7].

Alert RCB dedykowany jest zdarzeniom dynamicznym, takim jak burze, wichury, intensywne opady deszczu, powódzie, ale również informuje o planowanych detonacjach niewybuchów, skażeniu wody, zagrożeniach CBRNE czy regulacjach związanych z epidemią. Komunikat, liczący zwykle 160 znaków (w wyjątkowych sytuacjach do 320), zawiera rodzaj zagrożenia oraz najważniejsze zalecenia postępowania, a często także link do strony gov.pl z dodatkowymi informacjami. Wiadomości są przesyłane na każdy telefon znajdujący się na zagrożonym terenie – na numery z prefixem +48 w języku polskim, a na pozostałe w języku angielskim. Dystrybucją komunikatów zajmują się operatorzy sieci komórkowych w Polsce, a sama usługa jest całkowicie bezpłatna. W wyjątkowych przypadkach Alert RCB może być również wysyłany do użytkowników z polskim numerem przebywających za granicą, zapewniając szybki, jednolity przekaz „dla wszystkich w zasięgu”.

Obecnie trwają dyskusje o przejściu technologii LB-SMS na Cell Broadcast SMS (CB-SMS) – rozwiązanie to umożliwi szybsze, bardziej niezawodne rozsyłanie komunikatów do użytkowników na danym obszarze bez obciążenia sieci. Obecnie RCB utrzymuje Alert RCB w obecnej formie SMS-owej, jednak prowadzone są prace na rozszerzeniu funkcjonalności systemu, m.in. o tzw. alerty odwoławcze, informujące o ustaniu zagrożenia [8–9].

voivodes and Telewizja Polska (Polish Television). RSO transfers different types of messages, including meteorological and hydrological warnings and other warnings of local hazards, e.g. road accidents. The system also features a map presenting the condition of waters in selected water gauges of Polish rivers and guidelines in crisis situations, e.g. how to provide first aid, how to behave during a storm, flood or terrorist attack [10].

Warnings are delivered to the inhabitants of the given region by different channels: RSO mobile application, RSO website, voivodeship office websites, DVB-T radio and television, on TVP – HbbTV hybrid platforms, teletext.

RSO was integrated with hybrid television, meaning that hazard communications were displayed on the screens of TV sets connected to the Internet that received the terrestrial television signal (i.e. via DVB-T). In practice, it was resolved that the television signal delivered video and audio of TV programmes, while the HbbTV layer enables adding interactive RSO communications. Legacy TV sets without HbbTV support are unable to receive RSO communications in the form of interactive notifications. In such situations, warnings are transmitted in traditional mode – by information strips or warning boards broadcast in television.

The free RSO application is available in application stores for different platforms (Google Play, App Store, Windows Phone Store). It can be found easily by typing the keywords “RSO” or “Regionalny System Ostrzegania” in the search engine. The communications published in the system are introduced and activated by officers on duty in Voivodeship Crisis Management Centre in every voivodeship, according to territorial competence. In the Google Play store, information can be found that the application was downloaded more than 100,000 times and users rate it at 3.2 in a five-point scale. The application received 1790 reviews in total. Most of them are under responsibility of the administrator at the Ministry of Internal Affairs and Administrator, who thanks for the rating and informs that the application will be updated to have new functions added, bugs fixed and procedures simplified if possible – data as of 12/11/2025 [11].

The main advantages of the application include the option to set the range and type of communications, enabling the user to control the information obtained. The user may select regions (voivodeships) to receive notifications or to enable notifications or to enable the geolocation function, enabling the adjustment of the communications to the current location.

A disadvantage of the system is that its effectiveness depends on the engagement of the user to receive warnings, the user must download and install the application on the smartphone. Without active involvement of a conscious citizen, effective hazard notification is impossible, unlike in the automatic Alert RCB system.

Innym przykładem systemu ostrzegania publicznego w Polsce może być Regionalny System Ostrzegania (RSO). To rozszerzony system informowania i ostrzegania ludności w Polsce o zagrożeniach o charakterze lokalnym i regionalnym. RSO jest projektem Rządowego Centrum Bezpieczeństwa, realizowanym we współpracy z wojewodami oraz Telewizją Polską. Za pośrednictwem RSO przekazywane są różnego rodzaju komunikaty, w tym ostrzeżenia meteorologiczne, hydrologiczne lub inne ostrzeżenia odwołujące się do miejscowych zagrożeń, np. wypadków drogowych. W systemie dostępna jest również mapa prezentująca stan wód na wybranych wodowskazach polskich rzek oraz poradniki postępowania w sytuacjach kryzysowych, np. jak udzielić pierwszej pomocy, jak zachować się podczas burzy, powodzi czy ataku terrorystycznego [10].

Ostrzeżenia są przekazywane mieszkańcom danego regionu przez różne kanały: aplikacja mobilna RSO, strona internetowa RSO, strony internetowe urzędów wojewódzkich, radio i telewizja DVB-T, na platformach hybrydowej TVP – HbbTV, telegazeta.

RSO zostało zintegrowane z telewizją hybrydową, co oznacza, że komunikaty o zagrożeniach są wyświetlane na ekranach telewizorów podłączonych do Internetu, odbierających sygnał telewizji naziemnej (czyli przez DVB-T). W praktyce zostało to rozwiązane tak, że sygnał telewizyjny dostarcza obraz i dźwięk programów TV, a warstwa HbbTV umożliwia dodanie interaktywnych komunikatów RSO. W przypadku starszych odbiorników telewizyjnych, które nie obsługują technologii HbbTV, odbiór komunikatów RSO w formie interaktywnych powiadomień nie jest możliwy. W takich sytuacjach ostrzeżenia są przekazywane w sposób tradycyjny – poprzez paski informacyjne lub plansze ostrzegawcze emitowane na antenie telewizji.

Bezpłatna aplikacja RSO jest dostępna w sklepach z aplikacjami dla różnych platform (Google Play, App Store, Windows Phone Store). Można ją łatwo odnaleźć, wpisując w wyszukiwarce słowa kluczowe „RSO” lub „Regionalny System Ostrzegania”. Komunikaty publikowane w systemie są wprowadzane i aktywowane przez dyżurnych Wojewódzkich Centrów Zarządzania Kryzysowego w każdym województwie, zgodnie z ich właściwością terytorialną. W sklepie Google Play można znaleźć informację, że aplikacja została pobrana ponad 100 tys. razy, a użytkownicy oceniają ją na 3,2 w pięciostopniowej skali. Aplikacja zebrała łącznie 1790 opinii. Na większość z nich odpowiada administrator z Ministerstwa Spraw Wewnętrznych i Administracji, dziękując za ocenę oraz informując, że aplikacja zostanie w miarę możliwości rozszerzona o nowe funkcje, błędy naprawione, a procedury uproszczone – dane na dzień 12.11.2025 roku [11].

Do głównych zalet aplikacji należy możliwość samodzielnego ustawienia zakresu i rodzaju komunikatów, co pozwala użytkownikowi kontrolować otrzymywane informacje. Użytkownik może wybrać regiony (województwa), z których chce otrzymywać powiadomienia, lub włączyć funkcję geolokalizacji, dzięki czemu komunikaty będą dopasowane do jego aktualnego miejsca pobytu.

Wadą systemu jest to, że jego skuteczność zależy od zaangażowania użytkownika – aby otrzymywać ostrzeżenia, należy samodzielnie pobrać i zainstalować aplikację na smartfonie. Bez aktywnego udziału świadomego obywatela – nie ma mowy o skutecznym informowaniu o zagrożeniach, tak jak ma to miejsce w przypadku automatycznego systemu Alert RCB.

SWOT analysis of the RCB and RSO alert

This subchapter summarises weak and strong points and development opportunities and threats of the key solution classes described above. The strong points of these technologies include above all mass coverage without installing the application, only applicable to Alert RCB, the possibility of geotargeting and quick delivery of short messages. It is also worth noting that despite these advantages, the restricted content length, lack of multimedia, possible LB-SMS delays and the risk of "alert fatigue" with language availability problems may weaken the impact of the communication. The development opportunities include a fuller migration to CB, standardisation of *call-to-action* patterns, distribution expansion to HbbTV, mObywatel or TTS, and recall automation in the CAP standard with personalisation components. Important threats are power and telecommunication failures, disinformation campaigns, digital exclusion and fragmentation of responsibility of broadcasters.

Other solutions supporting the safety of citizens

The contemporary information society should be characterised by high awareness of environmental and civilisation hazards. To obtain that effect, it is important to provide the society with tools and sources of knowledge on where to obtain reliable information. One of the key components to provide civil protection is to enable ongoing monitoring of crisis situation and transmitting warning communications using generally available means. In this context, Internet websites and public institution portals are particularly important, which make available the current data on the environment, natural hazards and extraordinary situations. Each of the institutions responsible for monitoring specific areas of the environment operates its own news portals and often also mobile applications, which provide the society with easy and direct access to current environmental information.

Both Alert RCB and the Regional Warning System play a key role in informing the citizens of predicted or existing hazards. Their effectiveness is based on collaboration with extensive environmental monitoring and analysis systems that provide the data necessary to issue warnings. These systems function under the responsibility of specialised national institutions and services. A perfect example of this mechanism is the Institute of Meteorology and Water Management, which conducts ongoing surveillance of meteorological conditions and provides weather forecasts in Poland through a network of weather stations, radars and measurement stations. Based on the data collected, IMGW prepares and publishes warnings, which are sent directly to RCB and to voivodeship crisis management centres. After receiving the information, the RCB conducts quick risk assessment and makes a decision, the situation requires the activation of systems to warn the population [12].

The Institute of Meteorology and Water Management of the National Research Institute operates an extensive news website, which is one of key tools for monitoring and analysing

Analiza SWOT Alertu RCB i RSO

W podrozdziale tym zestawiono mocne i słabe strony oraz szanse rozwojowe i zagrożenia kluczowych klas rozwiązań opisanych powyżej. Do mocnych stron tych technologii należą przede wszystkim masowy zasięg bez konieczności instalacji aplikacji – dot. wyłącznie Alertu RCB, możliwość geotargetowania oraz szybkie dostarczanie krótkich komunikatów. Warto zaznaczyć, że pomimo tych zalet ograniczona długość treści, brak multimediów, możliwe opóźnienia w LB-SMS oraz ryzyko „zmęczenia alertami” wraz z problemami dostępności językowej mogą osłabiać efekt komunikatu. Szanse rozwojowe obejmują pełniejsze przejście na CB, ujednolicenie wzorców *call-to-action*, rozszerzenie dystrybucji o HbbTV, mObywatel lub TTS oraz automatyzację odwołań w standardzie CAP z elementami personalizacji. Za istotne zagrożenia uznaje się awarie energetyczno-telekomunikacyjne, kampanie dezinformacyjne, wykluczenie cyfrowe oraz fragmentację odpowiedzialności nadawców.

Pozostałe rozwiązania wspierające bezpieczeństwo obywateli

Współczesne społeczeństwo informacyjne powinno charakteryzować się wysoką świadomością zagrożeń środowiskowych i cywilizacyjnych. W celu uzyskania tego efektu ważne jest, by udostępnić społeczeństwu narzędzia i źródła wiedzy na temat tego, skąd czerpać rzetelne informacje. Jednym z kluczowych elementów zapewnienia bezpieczeństwa ludności jest możliwość bieżącego monitorowania sytuacji kryzysowej i przekazywania komunikatów ostrzegawczych w sposób powszechnie dostępny. W tym kontekście szczególne znaczenie mają internetowe serwisy i portale instytucji publicznych, które udostępniają aktualne dane o stanie środowiska, zagrożeniach naturalnych oraz sytuacjach nadzwyczajnych. Każda z instytucji odpowiedzialna za monitorowanie określonych obszarów środowiska prowadzi własne portale informacyjne, a często również aplikacje mobilne, które umożliwiają społeczeństwu łatwy i bezpośredni dostęp do aktualnych informacji środowiskowych.

Zarówno Alert RCB, jak i Regionalny System Ostrzegania pełnią kluczową rolę w informowaniu obywateli o prognozowanych lub zaistniałych zagrożeniach. Ich skuteczność opiera się na współpracy z rozbudowanymi systemami monitorowania i analizowania środowiska, które dostarczają danych niezbędnych do wydawania ostrzeżeń. Za funkcjonowanie tych systemów odpowiadają wyspecjalizowane instytucje państwowe i służby. Idealnym przykładem tego mechanizmu jest Instytut Meteorologii i Gospodarki Wodnej, który prowadzi stały nadzór nad warunkami meteorologicznymi lub zajmuje się prognozowaniem pogody w Polsce poprzez sieć stacji meteo, radarów i posterunków pomiarowych. Na podstawie zebranych danych IMGW opracowuje i publikuje ostrzeżenia, które przesyłane są bezpośrednio do RCB oraz do wojewódzkich centrów zarządzania kryzysowego. Po otrzymaniu informacji RCB dokonuje szybkiej oceny ryzyka i podejmuje decyzję, czy sytuacja wymaga uruchomienia systemów ostrzegania ludności [12].

environmental hazards in Poland. The imgw.pl website makes available several specialised thematic platforms.

One of primary tools is the Hydro portal, which enables ongoing monitoring of surface water levels, river flows and hydrological conditions. The data is presented in the form of dynamic maps and charts, which enables quick identification of flood hazard and assessment of tendencies for water level changes. This website is a component of the National Flood and Other Hydrological Phenomena Early Warning System [13].

In addition to the Hydro module, the imgw.pl portal also includes websites dedicated to other environmental aspects. They include i.a. Meteo, which presents data on the current and forecasted weather conditions, weather warnings and communications on weather hazards, such as storms, strong winds, heats or heavy precipitation [14].

Another significant component of the website is the Agrometeo module, designed for the agricultural sector. It includes data on soil temperature, air humidity, precipitation and other meteorological parameters that affect agricultural production. This information enables farmers and advisory institutions to properly plan the field work and respond to hazards related to draughts, frosts or excessive precipitation [15].

Attention should also be paid to the Baltic section, which covers data on the sea level, including water temperature, wind force, waviness and salinity level. This module is particularly significant for the safety of sailing, fishing and port operations, as well as services responsible for responding to potential environmental hazards, such as leaks of oil derivatives [16].

Another integral part of the website is the air quality monitoring system, which provides information on the concentrations of suspended particulates, carbon, sulphur and nitrogen oxides and other air contaminants. This data is necessary for health risk assessment and planning preventative operations related to public health protection [17].

IMGW-PIB also created an application presented the weather forecast, which is available to download free of charge from Google Play and App Store. The application achieved significant interest (more than 100,000 downloads from Google Play) and high ratings, 4.0 in Google Play (2.25k ratings) and App Store 3.2 (204 ratings), respectively.

It is worth emphasising that all IMGW-PIB modules form a cohesive and integrated system, which not only informs of current environmental conditions, but also predicts their short- and medium-term changes.

In 2022-2023, the State Fire Service conducted a nationwide inventory of building structures under the so-called operational reconnaissance. The purpose of this activity was to identify the buildings that can be classified as temporary refuge (MDS), hide-out (U) or shelter (S). The inventory covered i.a. facilities owned by state institutions, local government, housing communities and business entities.

Based on the collected data, a free-of-charge "Schrony" (Shelters) application was developed, available in browser version. Its central component is an interactive map that enables finding the nearest locations, divided into MDS, U and S categories, in an easy and intuitive manner. The system presents the results of inventory

Instytut Meteorologii i Gospodarki Wodnej – PIB prowadzi rozbudowany serwis informacyjny, który stanowi jedno z kluczowych narzędzi w zakresie monitorowania i analizowania zagrożeń środowiskowych w Polsce. Na stronie internetowej imgw.pl dostępnych jest kilka wyspecjalizowanych platform tematycznych.

Jednym z podstawowych narzędzi jest portal Hydro, umożliwiający bieżące monitorowanie stanów wód powierzchniowych, przepływów rzecznych oraz warunków hydrologicznych. Dane prezentowane są w formie dynamicznych map i wykresów, co pozwala na szybkie zidentyfikowanie zagrożeń powodziowych i ocenę tendencji zmian poziomu wód. Serwis ten stanowi element Krajowego Systemu Wczesnego Ostrzegania Przed Powodziami i Innymi Zjawiskami Hydrologicznymi [13].

Oprócz modułu Hydro, portal imgw.pl obejmuje również serwisy dedykowane pozostałym aspektom środowiska. Wśród nich znajduje się m.in. Meteo, prezentujący dane o aktualnych i prognozowanych warunkach atmosferycznych, ostrzeżenia meteorologiczne, a także komunikaty o zagrożeniach pogodowych, takich jak burze, silny wiatr, upały czy intensywne opady [14].

Istotnym elementem serwisu jest także moduł Agrometeo, skierowany do sektora rolniczego. Zawiera on dane dotyczące temperatury gleby, wilgotności powietrza, opadów i innych parametrów meteorologicznych wpływających na produkcję rolną. Informacje te pozwalają rolnikom i instytucjom doradczym odpowiednio planować prace polowe oraz reagować na zagrożenia związane z suszą, przymrozkami czy nadmiernymi opadami [15].

Na uwagę zasługuje również sekcja Bałtyk, obejmująca dane o stanie morza, w tym o temperaturze wody, sile wiatru, stanie falowania oraz poziomie zasolenia. Moduł ten ma szczególne znaczenie dla bezpieczeństwa żeglugi, rybołówstwa oraz działalności portowej, a także dla służb odpowiedzialnych za reagowanie na potencjalne zagrożenia ekologiczne, takie jak wycieki substancji ropopochodnych [16].

Integralną część portalu stanowi także system monitorowania jakości powietrza, który udostępnia informacje o stężeniach pyłów zawieszonych, tlenków węgla, siarki, azotu oraz innych zanieczyszczeń atmosferycznych. Dane te są niezbędne dla oceny ryzyka zdrowotnego oraz planowania działań prewencyjnych w zakresie ochrony zdrowia publicznego [17].

IMGW-PIB stworzyła również aplikację prezentującą prognozę pogody, która dostępna jest do pobrania za darmo ze sklepów Google Play i App Store. Aplikacja osiąga znaczne zainteresowanie (ponad 100 tys. pobrań z Google Play) i wysokie oceny, odpowiednio 4,0 w Google Play (2,25 tys. ocen) i App Store 3,2 (204 oceny).

Warto podkreślić, że wszystkie moduły IMGW-PIB tworzą spójny, zintegrowany system, który nie tylko informuje o aktualnych warunkach środowiskowych, ale także prognozuje ich zmiany w krótkim i średnim okresie.

W latach 2022–2023 Państwowa Straż Pożarna przeprowadziła ogólnopolską inwentaryzację obiektów budowlanych w ramach tzw. rozpoznania operacyjnego. Celem tego działania było wskazanie budynków, które mogą zostać zakwalifikowane jako miejsca doraźnego schronienia (MDS), ukrycia (U) lub schrony (S). Inwentaryzacja objęła m.in. obiekty należące do instytucji państwowych, samorządowych, wspólnot mieszkaniowych oraz podmiotów gospodarczych.

covering both protection buildings for extreme weather conditions and civilian shelters as defined in the Geneva Conventions. The application developed by the Security Office of the Headquarters of the State Fire Service presents the locations of temporary refuge and hideout, i.e. non-hermetic protection buildings, and shelters, i.e. closed and hermetic design structures. The users may search shelters by address or current location. The results are presented on the map and as a list of structures with information on i.a. the estimated capacity, area and quality rating. The application provides inhabitants with direct access to the data that was difficult to access earlier. For local governments and rescue services, it is a valuable planning and analytical tool [20].

Another entity fulfilling hydrological safety tasks is Państwowe Gospodarstwo Wodne Wody Polskie. The official website of the institution includes the “Hydrological situation” service, which publishes communications on the current status of rivers, flood prevention reservoirs and the level of preparation of water infrastructure to surges [21].

The Chief Inspectorate of Environmental Protection (GIOŚ) plays a key role in monitoring the status of environment by conducting the National Environmental Monitoring, which includes measurements, assessments and forecasts related to air, water, soil and forest quality. The inspectorate collects, processes and releases the data necessary to assess the environmental policy and to inform the society. With regards to air quality, GIOŚ publishes current measurement results of contamination levels, such as PM10 and PM2.5 particulates, nitrogen oxide (NO_x) or sulphur oxide (SO₂), while water monitoring also includes the analysis of bottom sediments, which enable determining the level of ecosystem contamination and degradation [22]. To provide wide access to environmental information, GIOŚ also operates the INSPIRE platform, which is part of the European spatial data release system. This data is significant both for public health protection and planning prevention activities in case of environmental hazards [23].

A special category of monitoring is radiation surveillance, conducted by the National Atomic Energy Agency. The agency website makes available the radiation map of Poland, updated in real time, which presents the indications of radioactive contaminants early detection stations and the radiation dose rate value [24].

In the context of geological safety, the Landslide Counteracting System, conducted by the State Geological Institute of the National Research Institute. This system enables identification and monitoring areas with landslide hazards and collects data on their activity [25].

In turn, the Agricultural Drought Monitoring System (SMSR) delivers information on hazards related to precipitation deficiency, which is crucial for food security and agricultural economy [26].

In the area of public health, an important source of information is the National Public Health Institute – National Institute of Hygiene that operates websites on nationwide epidemic monitoring. The data published there enables evaluating health hazards, which is important both for administration bodies and for citizens in the context of response to biological hazards.

It is also worth noting that the IT Country Protection System (Informatyczny System Oslony Kraju, ISOK) that integrates meteorological, hydrological and geological data by supporting

Na podstawie zebranych danych opracowano darmową aplikację „Schrony”, dostępną w wersji przeglądarkowej. Jej centralnym elementem jest interaktywna mapa, umożliwiająca łatwe i intuicyjne wyszukiwanie najbliższych miejsc schronienia w podziale na kategorie MDS, U oraz S. System prezentuje wyniki inwentaryzacji obejmującej zarówno budowle ochronne pełniące funkcję osłony przed ekstremalnymi zjawiskami pogodowymi, jak i obiekty mogące służyć jako schrony cywilne, zgodnie z definicjami określonymi w Konwencji Genewskiej. Aplikacja, stworzona przez Biuro Bezpieczeństwa Komendy Głównej PSP, prezentuje na mapie miejsca doraźnego schronienia i ukrycia – czyli budowle ochronne niehermetyczne – oraz schrony, będące obiektami o zamkniętej, hermetycznej konstrukcji. Użytkownicy mogą wyszukiwać schrony według adresu lub bieżącej lokalizacji. Wyniki prezentowane są na mapie oraz w formie listy obiektów zawierającej informacje m.in. o szacowanej pojemności, powierzchni i ocenie jakościowej. Aplikacja zapewnia mieszkańcom bezpośredni dostęp do danych, które dotychczas były trudno dostępne. Dla samorządów i służb ratowniczych stanowi zaś cenne narzędzie planistyczne i analityczne [20].

Kolejnym podmiotem realizującym zadania w zakresie bezpieczeństwa hydrologicznego jest Państwowe Gospodarstwo Wodne Wody Polskie. Na oficjalnej stronie instytucji znajduje się serwis „Sytuacja hydrologiczna”, w którym publikowane są komunikaty dotyczące aktualnego stanu rzek, zbiorników przeciwpowodziowych oraz stopnia przygotowania infrastruktury wodnej na wystąpienie wzbrań [21].

Główny Inspektorat Ochrony Środowiska (GIOŚ) pełni kluczową rolę w monitorowaniu stanu środowiska poprzez prowadzenie Państwowego Monitoringu Środowiska, obejmującego pomiary, oceny i prognozy dotyczące jakości powietrza, wód, gleb i lasów. Inspektorat gromadzi, przetwarza i udostępnia dane niezbędne do oceny polityki ekologicznej oraz informowania społeczeństwa. W zakresie jakości powietrza GIOŚ publikuje bieżące wyniki pomiarów poziomu zanieczyszczeń, takich jak pyły PM10 i PM2.5, dwutlenek azotu (NO_x) czy dwutlenek siarki (SO₂), natomiast monitoring wód obejmuje również analizę osadów dennych, pozwalającą ocenić stopień zanieczyszczenia i degradacji ekosystemów [22]. Dla zapewnienia szerokiego dostępu do informacji środowiskowych GIOŚ prowadzi także platformę INSPIRE, będącą częścią europejskiego systemu udostępniania danych przestrzennych. Dane te mają znaczenie zarówno dla ochrony zdrowia publicznego, jak i planowania działań prewencyjnych w sytuacjach zagrożeń ekologicznych [23].

Szczególną kategorię monitoringu stanowi nadzór radiacyjny, realizowany przez Państwową Agencję Atomistyki. Na stronie agencji udostępniona jest aktualizowana w czasie rzeczywistym mapa radiacyjna Polski, przedstawiająca wskazania stacji wczesnego wykrywania skażeń promieniotwórczych oraz wartości mocy dawki promieniowania [24].

W kontekście bezpieczeństwa geologicznego szczególne znaczenie ma System Osłony Przeciwosuwiskowej, prowadzony przez Państwowy Instytut Geologiczny – PIB. System ten umożliwia identyfikację i monitorowanie terenów zagrożonych osuwiskami oraz gromadzi dane o ich aktywności [25].

Z kolei System Monitoringu Suszy Rolniczej (SMSR) dostarcza informacji o zagrożeniach związanych z niedoborem opadów,

the operations of administration in predicting and preventing the consequences of natural disasters.

To conclude, the websites and online systems listed are the foundation of the modern system for monitoring and alarming the population, based on the principle of public access to information. The integration of data from different institutional sources and transparently releasing it in the public space contribute to the increase of safety of citizens by enabling them to make conscious decisions in hazard situations. In future, the development of these tools, based on IT technologies and artificial intelligence, may create one of the key directions of development of the national civil protection system.

Two-way applications and report channels for citizens

Two-way applications enable information exchange between the user and the administrator, i.e. between the citizen and services, local governments or crisis management centres. In traditional systems, the warnings, such as SMS alerts and media communications, the information is transmitted one-way, only from institutions to citizens. In case of two-way applications, communication is conducted in both directions: public services can send hazard notifications and users can report hazardous situations and send location data or multimedia materials to help in quicker response and more effective operation of the services.

An example of such system in Poland can be the National Map of Safety Hazards (Krajowa Mapa Zagrożeń Bezpieczeństwa). It is a tool developed for the Police that enables indicating local hazards nearby. The Police verifies the reports and undertakes appropriate operations. Here one should note that the tool is not intended for urgent reports, which should be made to number 112. Notwithstanding, the application is very effective in mapping "chronic" phenomena, such as e.g. illegal landfills [27].

Another example of using two-way application solutions is mObywatel – the official mobile application managed by the Ministry of Digitalisation. It enables storing the digital versions of identity documents, such as mDowód Osobisty (ID) or mPrawo Jazdy (Driver's Licence), and enable convenient handling of official matters in electronic form. As of August 2024, the application was expanded to the "Safe Online" (Bezpiecznie w sieci) service, which is an important component of the cybersecurity of citizens. It enables the users to report suspicious websites, emails or SMS messages, as well as receive notifications on current online

co ma kluczowe znaczenie dla bezpieczeństwa żywnościowego i gospodarki rolnej [26].

W obszarze zdrowia publicznego istotnym źródłem informacji jest Narodowy Instytut Zdrowia Publicznego – Państwowy Zakład Higieny, który prowadzi serwisy dotyczące monitorowania sytuacji epidemicznej w kraju. Publikowane tam dane umożliwiają ocenę zagrożeń zdrowotnych, co ma znaczenie zarówno dla organów administracji, jak i dla obywateli w kontekście reagowania na zagrożenia biologiczne.

Warto również wskazać Informatyczny System Oslony Kraju (ISOK), który integruje dane meteorologiczne, hydrologiczne i geologiczne, wspierając działania administracji w zakresie prognozowania i zapobiegania skutkom klęsk żywiołowych.

Podsumowując, wymienione serwisy i systemy online stanowią fundament nowoczesnego systemu monitorowania i alarmowania ludności, opartego na zasadzie powszechnego dostępu do informacji. Integracja danych pochodzących z różnych źródeł instytucjonalnych oraz ich transparentne udostępnianie w przestrzeni publicznej przyczyniają się do wzrostu bezpieczeństwa obywateli, umożliwiając im podejmowanie świadomych decyzji w sytuacjach zagrożenia. W przyszłości rozwój tych narzędzi, oparty o technologie informatyczne i sztuczną inteligencję, może stanowić jeden z kluczowych kierunków rozwoju krajowego systemu ochrony ludności.

Aplikacje dwukierunkowe i kanały zgłoszeń obywateli

Aplikacje dwukierunkowe umożliwiają wymianę informacji pomiędzy użytkownikiem a administratorem, czyli obywatelem a służbami, samorządami lub centrami zarządzania kryzysowego. W tradycyjnych systemach ostrzegania – takich jak alerty SMS czy komunikaty w mediach – informacja przekazywana jest jednostronnie, wyłącznie od instytucji do obywateli. W przypadku aplikacji dwukierunkowych komunikacja przebiega w obie strony: służby publiczne mogą wysyłać powiadomienia o zagrożeniach, a użytkownicy mają możliwość samodzielnego zgłaszania niebezpiecznych sytuacji oraz przesyłania danych lokalizacyjnych lub materiałów multimedialnych, które pomagają w szybszej reakcji i skuteczniejszym działaniu służb.

Przykładem takiego systemu w Polsce może być Krajowa Mapa Zagrożeń Bezpieczeństwa. Jest to narzędzie stworzone dla Policji, które umożliwia wskazywanie miejscowych zagrożeń w okolicy. Policja weryfikuje sygnały i podejmuje odpowiednie działania. Należy przy tym zwrócić uwagę, że to narzędzie nie jest przeznaczone do zgłoszeń nagłych, o których należy zawiadamiać poprzez numer 112. Pomimo to aplikacja bardzo dobrze sprawdza się przy mapowaniu zjawisk „przewlekłych” jak np. nielegalne wysypiska [27].

Kolejnym przykładem wykorzystującym rozwiązania aplikacji dwukierunkowej jest mObywatel – oficjalna aplikacja mobilna zarządzana przez Ministerstwo Cyfryzacji. Umożliwia ona przechowywanie cyfrowych wersji dokumentów tożsamości, takich jak mDowód Osobisty czy mPrawo Jazdy, a także pozwala na wygodne załatwianie spraw urzędowych w formie elektronicznej. Od sierpnia 2024 r. aplikacja została rozszerzona o usługę „Bezpiecznie w sieci”, która

hazards. The system operates in two-way mode – the citizens send information on potential incidents, which is then routed to appropriate state institutions for analysis (i.a. CERT Polska). After assessing the report, if the hazard is confirmed, the application enables sending warning alerts to users, thus increasing the level of digital safety of the society [28].

The SMS Information System (System Informacji SMS, SISMS) is a crisis and warning communication system that enables two-way information exchange between local government units and inhabitants. This solution is implemented in many Polish towns, i.a. Gdańsk, Wrocław and Ciechocinek. The communications are transmitted by multiple channels – by SMS, email and “BLISKO” mobile application, which is a modern evolution of the SISMS system. The introduction of the mobile application created a new communication channel, which made the information transmission quicker, cheaper and more interactive. The users can not only receive notifications, but also respond to them by providing feedback, e.g. report local problems, accidents or difficulties. With this solution, information on events, such as sudden water supply failures, planned maintenance breaks, strong winds and road detours, can reach both active Internet users and users that prefer the traditional SMS channel.

The application also aggregates communications of the Regional Warning System (RSO) and selected broadcasters, while organising them by subject and area, which enables quickly noting the really relevant news. In addition, the user can decide, which channels and categories are relevant, and the local government can determine whom and where send the alert, sending the message precisely to a specific town, street or housing complex [29]. The BLISKO application can be downloaded from Google Play and App Store. It achieves moderate results, the rating of 2.9/5.0 on Google Play (1,35k ratings and more than 100,000 downloads) and the rating of 3.0/5.0 on App Store (41 reviews).

Another example of a two-way application in Poland can certainly be Alarm112, in particular because it is dedicated for persons with certain dysfunctions that restrict their ability to use traditional media channels. The application supported by Rescue Notification Centres is an alternative report channel for people that cannot or are unable to make a voice call at the moment. In particular for deaf people, people with hearing impairment or speaking difficulties, but also for someone, who must remain silent or who is in a high noise area. A report consists of simple selections based on pictograms (event type, number of victims, basic hazards) and automatically attached location, which enables the Rescue Notification Centre dispatcher to quickly understand the situation and dispatch appropriate forces and resources without having a conversation. Thus, the application is worth promoting even as an emergency solution that can save precious time in crisis after prior installation and activation of location services, by minimising linguistic and technological barriers and risk of losing contact [30].

The Alarm112 application can be downloaded from Google Play and App Store. It achieves moderate results, the rating of 2.5/5.0 on Google Play (295 ratings and more than 50,000 downloads) and 2.6/5.0 on App Store (40 reviews). The points and comments indicate that the application requires improvement,

stanowi ważny element w zakresie cyberbezpieczeństwa obywateli. Dzięki niej użytkownicy mogą zgłaszać podejrzane strony internetowe, wiadomości e-mail lub SMS-y, a także otrzymywać powiadomienia o aktualnych zagrożeniach w sieci. System działa w sposób dwukierunkowy – obywatele przekazują informacje o potencjalnych incydentach, które następnie trafiają do odpowiednich instytucji państwowych zajmujących się ich analizą (m.in. CERT Polska). Po dokonaniu oceny zgłoszenia, w przypadku potwierdzenia zagrożenia, aplikacja umożliwia rozsyłanie alertów ostrzegawczych do użytkowników, zwiększając tym samym poziom bezpieczeństwa cyfrowego społeczeństwa [28].

System Informacji SMS (SISMS) to system komunikacji kryzysowej i ostrzegawczej, umożliwiający dwukierunkową wymianę informacji pomiędzy jednostkami samorządu terytorialnego a mieszkańcami. Rozwiązanie to zostało wdrożone w wielu polskich miastach, m.in. w Gdańsku, Wrocławiu i Ciechocinku. Komunikaty przekazywane są wielokanałowo – za pomocą wiadomości SMS, poczty elektronicznej oraz poprzez aplikację mobilną „BLISKO”, będącą nowoczesnym rozwinięciem systemu SISMS. Wprowadzenie aplikacji mobilnej stworzyło nowy kanał komunikacji, dzięki czemu przekazywanie informacji stało się szybsze, tańsze i bardziej interaktywne. Użytkownicy mogą nie tylko otrzymywać powiadomienia, ale również reagować na nie, dostarczając informacji zwrotnych – np. zgłaszać lokalne problemy, wypadki czy utrudnienia. Dzięki temu rozwiązaniu informacje o takich zdarzeniach jak nagłe awarie wodociągowe, planowane przerwy techniczne, silny wiatr czy objazdy drogowe mogą dotrzeć zarówno do osób aktywnie korzystających z Internetu, jak i do tych, które preferują tradycyjny kanał SMS.

Aplikacja agreguje także komunikaty Regionalnego Systemu Ostrzegania (RSO) oraz wybranych nadawców, porządkując je tematycznie i terytorialnie, co ułatwia szybkie wychwytywanie naprawdę ważnych wiadomości. Dodatkowo użytkownik ma możliwość samodzielnej decyzji, które kanały i kategorie są dla niego istotne, a samorząd komu i gdzie wysłać alert, precyzyjnie adresując przekaz do konkretnej miejscowości, ulicy czy osiedla [29]. Aplikację BLISKO można pobrać ze sklepu Google Play i App Store. Osiąga umiarkowane wyniki, osiągając ocenę 2,9/5,0 w Google Play (1,35 tys. opinii i ponad 100 tys. pobrań) i ocenę 3,0/5,0 w App Store (41 opinii).

Kolejnym przykładem aplikacji dwukierunkowej stosowanej w Polsce z pewnością może być Alarm112, szczególnie dlatego, że jest ona dedykowana dla osób posiadających pewne dysfunkcje ograniczające ich możliwość w korzystaniu z tradycyjnych środków przekazu. Aplikacja obsługiwana przez Centra Powiadamiania Ratunkowego to alternatywny kanał zgłoszeniowy dla osób, które w danej chwili nie mogą lub nie są w stanie wykonać połączenia głosowego. W szczególności dla osób głuchych, niedosłyszących czy z trudnościami w mówieniu, ale też dla kogoś, kto musi zachować ciszę albo znajduje się w miejscu o dużym hałasie. Zgłoszenie składa się z prostych wyborów opartych na piktogramach (rodzaj zdarzenia, liczba poszkodowanych, podstawowe zagrożenia) oraz automatycznie dołączonej lokalizacji, co pozwala dyspozytorowi CPR szybko zrozumieć sytuację i wysłać odpowiednie siły i środki bez konieczności prowadzenia rozmowy. Dlatego aplikację warto promować nawet

i.a. with regards to registration and correct transmission of information, to be trusted by more people.

„Ratunek” (Rescue) is an application intended primarily for people in the mountains or by the water, which integrates the emergency numbers of services, such as: GOPR, TOPR, WOPR, MOPR. The application automatically sends the geolocation data of the person calling for help, which enables the rescuers to respond quickly and effectively [31]. The „Ratownik” (Rescuer) application is a mobile tool that enables the user to call for help quickly by calling the 112 emergency number and reporting to the citizen rescuer network near the place of event. The application includes the map of locations of AED defibrillators in public space. The users can add new devices or suggest, where another AED should be installed [32].

In emergency situations of life or health hazard always contact the rescue services directly at 112. The applications are only a supplement that in certain situations expedite the help by making available geolocation data or standardising reports.

jako rozwiązanie awaryjne, które po wcześniejszej instalacji i włączeniu usług lokalizacyjnych może uratować cenny czas w kryzysie, minimalizując bariery językowe i technologiczne oraz ryzyko utraty kontaktu [30].

Aplikację Alarm112 można pobrać ze sklepu Google Play i App Store. Osiąga umiarkowane wyniki – ocenę 2,5/5,0 w Google Play (295 opinii i ponad 50 tys. pobrań) i 2,6/5,0 w App Store (40 opinii). Punkty i komentarze wskazują, że aplikacja musi być poprawiona m.in. w zakresie rejestracji i poprawnego przesyłania informacji, aby więcej osób mogło jej zaufać.

„Ratunek” jest to aplikacja skierowana głównie do osób przebywających w górach lub nad wodą, integrująca numery ratunkowe służb, takich jak: GOPR, TOPR, WOPR, MOPR. Aplikacja automatycznie przesyła dane geolokalizacyjne osoby wzywającej pomoc, co umożliwia szybką i skuteczną reakcję ratowników [31]. Aplikacja „Ratownik” to mobilne narzędzie pozwalające użytkownikowi na szybkie wezwanie pomocy – poprzez połączenie z numerem alarmowym 112 oraz powiadomienie sieci ratowników obywatelskich w pobliżu miejsca zdarzenia. Aplikacja zawiera mapę lokalizacji defibrylatorów AED rozmieszczonych w przestrzeni publicznej. Użytkownicy mogą dodawać nowe urządzenia lub sugerować, gdzie powinien być zainstalowany kolejny AED [32].

W nagłych sytuacjach zagrożenia życia lub zdrowia należy zawsze kontaktować się z służbami ratunkowymi bezpośrednio pod numerem 112. Aplikacje są wyłącznie uzupełnieniem, które w konkretnych sytuacjach przyspieszają udzielenie pomocy dzięki udostępnianiu danych geolokalizacyjnych lub standaryzacji zgłoszeń.

SWOT analysis of two-way applications and report channels for citizens

For this group of technologies, the strengths include the ability to send reports with location and photo/video material, shorter path to operational decisions, discrete communication and handling low urgency notifications at the local level. Despite all advantages, the barriers are the requirements of installation and permanent Internet access, variable quality of report verification, privacy concerns and unequal adaptation to different age groups. The opportunity is integration with the public warning system and data standardisation, as well as use of algorithms to prevent duplication and prioritisation of reports, supplemented by educational programmes and gamification components. The hazards are connected with abuse and false reports, peak overload of service providers, changes in mobile system policies and data security concerns.

Analiza SWOT aplikacji dwukierunkowych i kanałów zgłoszeń obywateli

W przypadku tej grupy technologii do jej mocnych stron zalicza się możliwość przesyłania zgłoszeń z lokalizacją i materiałem foto/wideo, krótszą ścieżkę decyzji operacyjnych, komunikację dyskretną oraz obsługę powiadomień o niskiej pilności na poziomie lokalnym. Pomimo wielu zalet barierą pozostaje konieczność instalacji i stałego dostępu do Internetu, zmienna jakość weryfikacji zgłoszeń, obawy o prywatność oraz nierówne przystosowanie się w różnych grupach wiekowych. Szansą jest integracja z publicznym systemem ostrzegania i standaryzacja danych oraz wykorzystanie algorytmów do unikania powielania i priorytetyzacji zgłoszeń, uzupełnione programami edukacyjnymi i elementami grywalizacji. Zagrożenia wiążą się z nadużyciami i fałszywymi zgłoszeniami, przeciążeniem operatorów w piku, zmianami polityk systemów mobilnych oraz kwestiami bezpieczeństwa danych.

IoT and environmental data crowdsourcing

Internet of Things (IoT) is a network of devices connected to the Internet that automatically collect and process data without human intervention. IoT may include smoke detectors, surveillance cameras, weather stations, alarm systems, electricity meters and air quality sensors. IoT enables early detection of

IoT i crowdsourcing danych środowiskowych

Internet of Things (IoT) to sieć urządzeń połączonych z Internetem, które automatycznie gromadzą, przetwarzają dane bez udziału człowieka. Do IoT mogą należeć czujniki dymu, kamery monitoringu, stacje pogodowe, systemy alarmowe, liczniki energii czy sensory jakości powietrza. Dzięki IoT możliwe jest wczesne

hazards – seismic sensors and flood sensors send data to managing institutions in real time. In turn, *crowdsourcing* consists in obtaining information or help from a wide group of people, most often via Internet or mobile applications. Instead of relying only on data from institutions, the authorities can use the reports, photos and observations sent by citizens.

There are many applications based on the Internet of Things or *crowdsourcing*, however the most popular application is Airly. As of the day of writing of this article, the application has more than 13,000 measurement points in more than 50 countries (including more than 2,800 installed in Poland), which makes it a dense, publicly available network of air quality sensors built by society, which enables tracking data on the interactive map and in the application, but also downloading. Its strength is the very large number of sensors, so indications from nearby points enable quickly assessing, what we breathe in here and now, without waiting for the daily average reports. However, Airly should be considered above all as a tool for awareness and prevention and for ongoing warnings and building of habits, not as a substitute to the reference measurements of the Natural Environmental Monitoring (GIOŚ/PMŚ). This results from the primary problem of such systems, i.e. the data from low-cost sensors are only indicative and depend i.a. on the calibration, local conditions and correct installation [33].

SWOT analysis of IoT and environmental data crowdsourcing

A strength of this technology is dense and hyperlocal “here and now” information, high educational and preventative value at low unit costs and community activation. However, it should be remembered that low-cost sensors are characterised by variable quality and drift. They are not equivalent to reference methods, require maintenance and data can be misinterpreted by users. The opportunities are calibration and merger with reference data (PMŚ/GIOŚ), detecting anomalies using ML methods and combining environmental communications with health recommendations and evacuation plans. The threats include over-interpretation of single measurement points, power supply and communication failures, metadata inconsistencies and disputes related to responsibility for measurement contents.

VR/AR and gamification (education and training)

Virtual reality and augmented reality are entering the daily training repertoire of services and prevention programmes for citizens. In the State Fire Service, today VR solutions really supplement and add variation to the standard demonstrations and training sessions. They enable increasing the interest among the youth and safe processing of different scenarios, correcting wrong attitudes and all that in safe conditions, without creating specialised demonstrations.

The State Fire Service in Lubuskie Voivodeship demonstrated how virtual reality can support preventative operations

wykrywanie zagrożeń – czujniki sejsmiczne, powodziowe przesyłają dane w czasie rzeczywistym do instytucji nimi zarządzającymi. Natomiast *crowdsourcing* polega na pozyskiwaniu informacji lub pomocy od szerokiej grupy ludzi – najczęściej za pośrednictwem Internetu lub aplikacji mobilnych. Zamiast opierać się tylko na danych z instytucji, władze mogą korzystać z raportów, zdjęć i obserwacji przesyłanych przez obywateli.

Istnieje wiele aplikacji opartych na Internet of Things czy *crowdsourcingu*, jednak najbardziej popularną jest aplikacja Airly. Na dzień pisania artykułu aplikacja posiada ponad 13 000 punktów pomiarowych w ponad 50 krajach (z czego ponad 2800 zamontowanych jest w Polsce), przez co jest to gęsta, ogólnodostępna sieć czujników jakości powietrza zbudowana przez społeczeństwo, której dane można śledzić na interaktywnej mapie i w aplikacji, a także pobierać. Jej siłą jest bardzo duża liczba czujników, przez co wskazania z pobliskich punktów pozwalają szybko ocenić, czym oddychamy tu i teraz, bez czekania na raporty dobowej średniej. Warto jednak traktować Airly przede wszystkim jako narzędzie świadomości i prewencji oraz do bieżącego ostrzegania i budowania nawyków, a nie jako substytut pomiarów referencyjnych Państwowego Monitoringu Środowiska (GIOŚ/PMŚ). Wynika to z głównego problemu takich systemów – dane z czujników niskokosztowych są orientacyjne i zależą m.in. od kalibracji oraz warunków lokalnych i ich poprawnego zamontowania [33].

Analiza SWOT IoT i crowdsourcing danych środowiskowych

Mocną stroną tej technologii jest gęsta, hiperlokalna informacja „tu i teraz”, wysoka wartość edukacyjna i prewencyjna przy niskich kosztach jednostkowych oraz aktywizacja społeczności. Należy jednak pamiętać, że czujniki niskokosztowe charakteryzują się zmienną jakością i dryftem. Nie są równoważne metodom referencyjnym, wymagają utrzymania, a dane bywają błędnie interpretowane przez użytkowników. Szanse obejmują kalibrację i fuzję z danymi referencyjnymi (PMŚ/GIOŚ), wykrywanie anomalii z użyciem metod ML oraz łączenie komunikatów środowiskowych z zaleceniami zdrowotnymi i planami ewakuacji. Do zagrożeń zalicza się nadinterpretację pojedynczych punktów pomiarowych, awarie zasilania i łączności, niespójność metadanych oraz spory o odpowiedzialność za treść pomiarów.

VR/AR i grywalizacja (edukacja i trening)

Wirtualna i rozszerzona rzeczywistość wchodzi do codziennego arsenału szkoleniowego służb oraz programów prewencyjnych dla obywateli. W Państwowej Straży Pożarnej rozwiązania VR są dziś realnym uzupełnieniem i urozmaicheniem standardowych pokazów i ćwiczeń. Pozwalają na zwiększenie zainteresowania młodzieży oraz bezpieczne powtarzanie różnorodnych scenariuszy, korygowanie błędnych postaw, a wszystko w bezpiecznych warunkach bez konieczności tworzenia specjalistycznych pokazów.

Lubuska PSP pokazała, jak wirtualna rzeczywistość może wspierać działania profilaktyczne i budowanie kultury bezpieczeństwa.

and building the culture of safety. During the meetings with inhabitants, simulations allow “experiencing” hazard situations and reinforcing good habits from evacuation to first decisions in the place of event. This type of initiatives increase the understanding of risk, while being attractive to the youth and people that learn easier through action. An important partner for the development and standardisation of such solutions is CNBOP-PIB – the State Fire Service Research Institute that has been conducting training sessions, conferences and development projects at the interface of fire protection, civil protection and new technologies for years.

In parallel, there is a dynamic growth of commercial VR programmes for OHS and public education (see Fig. 6). Finished modules for evacuation from buildings, fire protection exercises, first aid education and work in high risk environments are available. Such tools, implemented in schools, public offices, local government units and enterprises, increase engagement, enable measuring progress and comfortably scaling the training, however they are not substitutes for practical training sessions, but only reasonably supplement them. In Poland, there are many suppliers and performers, while example modules are easily available.

W czasie spotkań z mieszkańcami symulacje pomagają „przeżyć” sytuacje zagrożenia i utrwalić dobre nawyki od ewakuacji po pierwsze decyzje na miejscu zdarzenia. Tego typu inicjatywy zwiększają zrozumienie ryzyka, a jednocześnie są atrakcyjne dla młodzieży i osób, które łatwiej uczą się przez działanie. Ważnym partnerem dla rozwoju i standaryzacji takich rozwiązań jest CNBOP-PIB – instytut badawczy PSP, który od lat prowadzi szkolenia, konferencje i projekty rozwojowe na styku ochrony przeciwpożarowej, ochrony ludności i nowych technologii.

Równolegle dynamicznie rośnie oferta komercyjnych programów VR dla BHP i edukacji publicznej (zob. Ryc. 6). Dostępne są gotowe moduły do ewakuacji z budynków, ćwiczeń ochrony przeciwpożarowej, nauki pierwszej pomocy czy pracy w środowiskach o podwyższonym ryzyku. Takie narzędzia – wdrażane w szkołach, urzędach, jednostkach samorządu terytorialnego i przedsiębiorstwach – zwiększają zaangażowanie, pozwalają mierzyć postępy i wygodnie skalować szkolenia, a przy tym nie zastępują ćwiczeń praktycznych, tylko je rozsądnie uzupełniają. W Polsce działa wielu dostawców i realizatorów, a przykładowe moduły są łatwo dostępne.



Figure 6. Example screenshot from VR scenario used in VR training sessions conducted by CNBOP-PIB

Rycina 6. Przykładowy screen scenariusza VR wykorzystywany przy szkoleniach VR prowadzonych przez CNBOP-PIB

Source: Own archives.

Źródło: Archiwum własne.

VR/AR and gamification components move education and training from the boring safety lectures level to the safe training level. For services, it means more frequent, more measurable, cheaper and simpler organisation of training sessions, without real hazards. For citizens, it means more engaging prevention programmes that translate to better decisions in danger. It remains crucial to smartly combine virtual tools with practice and collaboration of PSP, CNBOP-PIB, local governments and the market on standards.

VR/AR i elementy grywalizacji przenoszą edukację i trening z poziomu nużącego mówienia o bezpieczeństwie na poziom bezpiecznych ćwiczeń. Dla służb oznacza to częstsze, bardziej mierzalne, tańsze i prostsze w organizacji szkolenia, bez realnego zagrożenia. Dla obywateli oznaczają one bardziej angażujące programy prewencyjne, które przekładają się na lepsze decyzje w obliczu niebezpieczeństwa. Kluczem pozostaje jednak mądre łączenie wirtualnych narzędzi z praktyką i wspólna praca środowiska PSP, CNBOP-PIB, samorządów i rynku nad standardami.

SWOT analysis of VR/AR and gamification

The strengths of virtual reality and augmented reality include the possibility of safe training of rare and complex scenarios, high retention of knowledge in short 10–20 minute modules, objective assessment of competences and reduction of costs and

Analiza SWOT VR/AR i grywalizacji

Do mocnych stron wirtualnej i rozszerzonej rzeczywistości zalicza się możliwość bezpiecznego ćwiczenia rzadkich, złożonych scenariuszy, wysoką retencję wiedzy w krótkich modułach 10–20 minut, obiektywizację oceny kompetencji oraz ograniczenie

logistics of live training sessions. Despite these advantages, it is necessary to mention hardware and venue requirements, need for adjusting scenarios to Polish procedures, the risk of “novelty effect” without continued implementation and the need to prepare instructors. The development opportunities for this technology include standardisation and certification of modules, combination with e-learning and multiplayer mode and integration with real data (maps, 3D object models, telemetry). The threats include quick ageing of hardware and content (quality, immersion), inadequate implementation scale, the risk of drawing inadequate conclusions from “idealised” simulations and the risk of simulator disease in some participants.

Robots and UAVs

Operationally, the robots used by the State Fire Service are highly specialised, remote controlled vehicles designed to work in a high risk environment: extreme temperatures, smoking, collapsing structures or hazardous substances. Their tasks include feeding fire jets, reconnaissance (daylight/IR cameras), transport of equipment and evacuation of loads in zones, where sending rescuers is disproportionately risky. A good example of such use is the fire of the shopping complex at ul. Marywilska 44 in Warszawa (12 May 2024), where to work inside a ruined, heavily heated hall, the firefighting robot Colossus was sent [34] to reduce the exposure of humans to danger.

It is worth noting that in the end of 2023, the State Fire Service purchased eight of such firefighting robots [35] and distributed them among selected units nationwide, while systematically increasing the ability to work in CBRNE environment and large structures. Tragic events, such as the fire of the poultry processing plant in Kawle (August 2025), where a firefighter died, show the scale of structural hazards (structure instability, demolition with heavy machines) and justify the development of tools that enable indirect reconnaissance and operation, while maintaining the highest safety level.

kosztów i logistyki ćwiczeń na żywo. Pomimo tych zalet należy wspomnieć o wymaganiach sprzętowych i lokalowych, potrzebie dostosowania scenariuszy do polskich procedur, ryzyku „efektu nowości” bez ciągłości wdrożenia oraz konieczności przygotowania instruktorów. Do szans rozwojowych tej technologii należą standaryzacja i certyfikacja modułów, łączenie z e-learningiem i trybem wieloosobowym oraz integracja z danymi rzeczywistymi (mapy, modele 3D obiektów, telemetria). Do zagrożeń należą szybkie starzenie się sprzętu i treści (jakość, imersja), zbyt mała skala wdrożenia, możliwość wyciągania nieadekwatnych wniosków z „idealizowanych” symulacji oraz ryzyko choroby symulatorowej u części uczestników.

Roboty i BSP

W ujęciu operacyjnym stosowane przez Państwową Straż Pożarną roboty to wysoce wyspecjalizowane, zdalnie sterowane pojazdy przeznaczone do pracy w środowisku o podwyższonym ryzyku: przy ekstremalnych temperaturach, zadymieniu, zawalających się konstrukcjach, czy w obecności substancji niebezpiecznych. Ich zadaniem jest m.in. podanie prądu gaśniczego, rozpoznanie (kamery dzień/IR), transport wyposażenia i ewakuacja ładunków w strefach, do których wysyłanie ratowników byłoby nieproporcjonalnie ryzykowne. Dobrym przykładem takiego użycia jest pożar kompleksu handlowego przy ul. Marywilskiej 44 w Warszawie (12 maja 2024 r.), gdzie do pracy wewnątrz zrujnowanej, silnie nagrzonej hali wprowadzono robota gaśniczego Colossus [34], aby ograniczyć ekspozycję ludzi na niebezpieczeństwo.

Warto odnotować, że pod koniec 2023 r. PSP zakupiła osiem takich robotów gaśniczych [35] i rozdzieliła je do wybranych jednostek w kraju, systematycznie zwiększając zdolności do pracy w środowisku CBRNE i w obiektach wielokubaturowych. Tragiczne zdarzenia, takie jak pożar zakładu przetwórstwa drobiu w Kawłach (sierpień 2025 r.), w którym zginął strażak, pokazują skalę zagrożeń strukturalnych (niestabilność konstrukcji, rozbiorczy ciężki sprzęt) i uzasadniają rozwój narzędzi pozwalających na rozpoznanie oraz działania w sposób pośredni, z zachowaniem możliwie najwyższego poziomu bezpieczeństwa.



Figure 7. Robot Colossus in operation during the fire of the Marywilska
Rycina 7. Robot Colossus w trakcie działań przy pożarze hali Marywilska

Source/Źródło: <https://www.gov.pl/web/kgpsp/pozar-hali-handlowej-w-warszawie> [access/dostęp: 12.11.2025].

Today Unmanned Aerial Vehicles play a crucial role in the reconnaissance, documenting events and supporting decisions (daylight/thermal imaging, orthophotos, 3D models – see Fig. 8). However, their use during rescue operations is subject to strict legal restrictions: in accordance with EU regulations (2019/947, UAS.OPEN.060(3)) [36], the pilot and the operator cannot fly “near or within areas of crisis response operations”, unless approved by appropriate services. Air traffic violations, including violations of such prohibitions, can result in criminal sanctions pursuant to Article 212 of the Aviation Law Act. In practice, it means that civilians cannot fly above/nearby the action area: the only exceptions are formally authorised operations, integrated into the structure of activities and conducted by authorised entities. In addition, in Poland “geographical zones” can be delimited (e.g. DRA-R temporary restriction zones), which enables operational security of the space above the operation area – applicable competencies are held by Polish Air Navigation Services Agency.

In the absence of conflict with the regulations and operational needs, UAVs are very effective in civil defence and preparation and reconstruction phase: quick inspections of critical objects, documentation of damage, photogrammetric 3D models and maps for post-completion analyses, as well as training sessions and prior planning. The increasingly wide availability of quick RGB or IR data processing software enables creating geoinformation products in time frames that are operationally useful.

Bezzałogowe statki powietrzne pełnią dziś kluczową rolę w rozpoznaniu sytuacji, dokumentacji zdarzeń i wsparciu decyzji (obrazowanie dzień/termiczne, ortofotomapy, modele 3D – zob. Ryc. 8). W toku akcji ratowniczej ich użycie podlega jednak ścisłym ograniczeniom prawnym: zgodnie z przepisami UE (2019/947, UAS.OPEN.060(3)) [36] pilot i operator nie mogą wykonywać lotu „blisko lub wewnątrz obszarów, gdzie prowadzone są działania reagowania kryzysowego”, o ile nie uzyskali na to zgody właściwych służb. Naruszenia przepisów ruchu lotniczego, w tym takich zakazów, mogą skutkować odpowiedzialnością karną na podstawie art. 212 ust. 1 ustawy – Prawo lotnicze. W praktyce oznacza to, że osoby cywilne nie mogą latać nad/obok miejsc akcji: wyjątkiem są wyłącznie operacje formalnie upoważnione, włączone w strukturę działań i prowadzone przez uprawnione podmioty. Dodatkowo, w Polsce możliwe jest wyznaczanie „stref geograficznych” (np. czasowych stref ograniczeń DRA-R), co pozwala operacyjnie zabezpieczać przestrzeń nad rejonem działań – kompetencje w tym zakresie posiada Polska Agencja Żeglugi Powietrznej.

Tam, gdzie nie ma konfliktu z przepisami i potrzebami operacyjnymi, BSP bardzo dobrze sprawdzą się w obronie cywilnej i fazie przygotowania i odbudowy: szybkie inspekcje obiektów krytycznych, dokumentacja szkód, fotogrametryczne modele 3D i mapy na potrzeby analiz powykonalawczych, a także treningów i wcześniejszego planowania. Coraz szersza dostępność oprogramowania do szybkiej obróbki danych RGB lub IR umożliwia tworzenie produktów geoinformacyjnych w oknach czasowych użytecznych operacyjnie.



Figure 8. Aerial photograph made in 2024.

Rycina 8. Zdjęcie lotnicze wykonane w trakcie w 2024 r.

Source/Źródło: <https://300gospodarka.pl/news/polska-walczy-z-powodzia-będzie-nadzwyczajne-posiedzenie-rządu> [access/dostęp: 16.11.2025].

SWOT analysis of robots and UAVs

Based on the presented description of applications of robots and unmanned aerial vehicles (UAV) in rescue operations, their strengths and weaknesses were synthetically assessed and key opportunities and threats were identified.

The robots used by the State Fire Service are specialised in working in the most difficult conditions, high temperature, smoking, collapse risk zones or hazardous substances. It enables

Analiza SWOT robotów i BSP

Na podstawie przedstawionego opisu zastosowań robotów oraz bezzałogowych statków powietrznych (BSP) w działaniach ratowniczych dokonano syntetycznej oceny ich mocnych i słabych stron oraz wskazano kluczowe szanse i zagrożenia.

Roboty wykorzystywane w PSP to pojazdy wyspecjalizowane do pracy w najtrudniejszych warunkach – wysokiej temperaturze, zadymieniu, w strefach z ryzykiem zawalenia lub występowania

feeding fire jets, visual reconnaissance (RGB/IR) and transport of equipment without exposing rescuers, which is confirmed by experience from major fires of large structures. In turn, UAVs ensure quick reconnaissance, documentation of events and creation of geoinformation products (orthophotos, 3D models, RGB/IR analyses), important both for current decisions and for later assessment of operations. The increasingly available software expedites data processing, which enables feeding useful operational information in short time frames. From the systemic perspective, another advantage is the possibility of operational safeguarding of the airspace (geographical zones), which organises the responsibility and facilitates the work of the Rescue Operation Commander.

Despite numerous advantages, robots and UAVs require specialised personnel, training and continuous equipment maintenance, while the equipment itself can be expensive and subject to operational limitations (power supply, communication, environmental resistance). For UAVs, an additional obstacle are regulations that prohibit civilian flights in the operation area, which restricts the use to the authorised entities formally included in the operation. The legal and insurance requirements and trust of the Rescue Operation Commander in the pilot's competences make it difficult to change. In practice, sometimes another problem is the standardisation of data products (formats, metadata, quality) and their quick inclusion in the decision-making, in particular in the absence of pre-defined integration procedures.

The expanding catalogue of possible uses and improvement of procedures enable better integration of robots and UAVs into the reconnaissance → decision → operation chain. The progress in software (automatic photogrammetry, integration of RGB and thermovision data, semi-automatic image interpretation) favours quick production of maps and 3D models for planning, assessment of damage and post-completion analysis. Increasing the availability of unmanned aerial vehicles and their increasing technical advancement combined with experienced instructors and pilots and refinement of standards (technical and training) reinforces the predictability of results and facilitates scaling the capacity nationwide. Another opportunity is closer integration of UAV products with command systems and operation maps, which increases the value of information at the tactical and staff level.

The most important risks are communication and power supply failures (in particular in case of infrastructural events), difficult environmental conditions exceeding equipment parameters and the risk of collision of regulations and responsibilities (unauthorised flights, zone violations). In the organisational area, the threat is competence dispersion and inconsistency of standards between entities, which impedes the data exchange and mutual support. Finally, the quick pace of technological changes results in the need for frequent updates and changes of hardware and software, thus increasing the maintenance costs and risk of solution incompatibility in a longer time horizon.

substancji niebezpiecznych. Umożliwiają podanie prądów gaśniczych, rozpoznanie wizyjne (RGB/IR) i transport wyposażenia bez narażania ratowników, co potwierdzają doświadczenia z dużych pożarów obiektów wielkokubaturowych. BSP zapewniają z kolei szybkie rozpoznanie sytuacji, dokumentację zdarzeń oraz tworzenie produktów geoinformacyjnych (ortofotomapy, modele 3D, analizy RGB/IR), istotnych zarówno dla bieżących decyzji, jak i dla późniejszej oceny działań. Coraz lepiej dostępne oprogramowanie przyspiesza obróbkę danych, dzięki czemu możliwe jest dostarczanie użytecznych operacyjnie informacji w krótkich oknach czasowych. W ujęciu systemowym atutem jest też możliwość operacyjnego zabezpieczania przestrzeni powietrznej (strefy geograficzne), co porządkuje odpowiedzialność i ułatwia pracę KDR.

Pomimo licznych zalet, roboty i BSP wymagają wyspecjalizowanego personelu, przeszkolenia i stałego utrzymania sprzętu, a sam sprzęt bywa kosztowny i podatny na ograniczenia eksploatacyjne (zasilanie, łączność, odporność na środowisko). W przypadku BSP dodatkową przeszkodą są przepisy zabraniające lotów cywilnych w rejonie działań, co zawęża użycie do podmiotów uprawnionych i formalnie włączonych do akcji. Wymogi prawne i ubezpieczeniowe oraz zaufanie KDR do kompetencji pilota sprawiają, że jest to kwestia trudna do zmiany. W praktyce problemem bywa także standaryzacja produktów danych (formaty, metadane, jakość) oraz ich szybkie włączenie do obiegu decyzyjnego, zwłaszcza gdy brakuje z góry zdefiniowanych procedur integracji.

Rosnący katalog możliwego użycia i doskonalenie procedur, pozwala lepiej „wbudować” roboty i BSP w łańcuch rozpoznania → decyzja → działanie. Postęp w oprogramowaniu (automatyczna fotogrametria, łączenie danych RGB i termowizyjnych, półautomatyczna interpretacja obrazu) sprzyja szybkiej produkcji map i modeli 3D do planowania, oceny szkód czy analiz powypadkowych. Zwiększanie dostępności bezzałogowych statków powietrznych wraz z ich rosnącym zaawansowaniem technicznym w połączeniu z doświadczoną kadrą instruktorów i pilotów oraz doprecyzowanie standardów (technicznych i szkoleniowych) wzmacnia przewidywalność rezultatów i ułatwia skalowanie zdolności w skali kraju. Szansą jest także ściślejsza integracja produktów BSP z systemami dowodzenia i mapami operacyjnymi, co podnosi wartość informacji na poziomie taktycznym i sztabowym.

Najistotniejsze ryzyka to zakłócenia łączności i zasilania (zwłaszcza w zdarzeniach o charakterze infrastrukturalnym), trudne warunki środowiskowe przekraczające parametry sprzętu oraz ryzyko kolizji przepisów i odpowiedzialności (loty nieuprawnione, naruszenia stref). W obszarze organizacyjnym zagrożeniem jest rozproszenie kompetencji i brak spójności standardów między podmiotami, co utrudnia wymianę danych i wzajemne wsparcie. Wreszcie, szybkie tempo zmian technologicznych powoduje konieczność częstych aktualizacji i wymiany sprzętu oraz oprogramowania, a tym samym zwiększa koszty utrzymania i ryzyko niekompatybilności rozwiązań w dłuższym horyzoncie czasowym.

Conclusion

The primary research problem addressed by the authors is the assumption that effective civil defence is based on active involvement of citizens and use of modern technologies. Based on the conducted analyses and assessments, the conclusions confirm that effective civil protection and civil defence really requires engaging the society. At present, contemporary technologies, such as the Internet of Things (IoT), monitoring systems, two-way communication applications or unmanned aerial vehicles (UAV), are a key factor increasing the effectiveness of operations. However, the technology itself does not guarantee the success. To really increase the safety, real crowdsourcing must occur, namely engagement of the society in transmitting information on hazards. This requires awareness, education and building social resistance based on collaboration and responsibility. It is also necessary to ensure the trust and transparency of system operation, user privacy protection and availability of alternative forms of communication for people in digital exclusion, with disabilities or without knowledge of the Polish language. Another key factor is infrastructural resilience, capability to operate under network or power supply failure, and information hygiene, including report moderation and disinformation prevention. Finally, systemic education, training sessions and practical preparation of citizens are what decides if technology becomes a real support, rather than merely a tool. Only a conscious and well-prepared society using modern solutions responsibly can form an effective and resistant civil defence system.

The material prepared, due to its volume, was divided into two parts. The first presents examples of modern technologies supporting civil protection and civil defence used in Poland, while the second describes the organisational and technical solutions operating in Europe and worldwide.

The thesis put forward in the content of the study will be complemented by the presentation of survey results. Therefore, we kindly ask the readers to spend a few minutes and submit their answers. The purpose of the survey is to learn the opinions on the use of modern technologies in civil protection and civil defence. The data collected will be used for the analysis of the level of social awareness and the technological development of tools supporting public safety. Thank you for your time.

<https://forms.gle/QppnijVmzVbzKK828>



Podsumowanie

Głównym problemem badawczym, nad którym pochyłili się autorzy, jest założenie, że skuteczna obrona cywilna opiera się na aktywnym udziale obywateli oraz wykorzystaniu nowoczesnych technologii. Przeprowadzone analizy i oceny pozwoliły na sformułowanie wniosków potwierdzających, że efektywna ochrona ludności i obrona cywilna rzeczywiście wymagają zaangażowania społeczeństwa. Współczesne technologie, takie jak Internet Rzeczy (IoT), systemy monitoringu, aplikacje komunikacji dwukierunkowej czy bezzałogowe statki powietrzne (BSP), stanowią obecnie kluczowy czynnik zwiększający skuteczność podejmowanych działań. Jednak sama technologia nie gwarantuje sukcesu. Aby mogła realnie zwiększać bezpieczeństwo, konieczne jest zaistnienie rzeczywistego crowdsourcingu, czyli zaangażowania społeczeństwa w przekazywanie informacji o zagrożeniach. Wymaga to świadomości, edukacji i budowania odporności społecznej, opartej na współpracy i odpowiedzialności. Niezbędne jest również zapewnienie zaufania i przejrzystości działania systemów, ochrony prywatności użytkowników, a także dostępności alternatywnych form komunikacji dla osób wykluczonych cyfrowo, z niepełnosprawnościami lub osób nie znających języka polskiego. Kluczowe znaczenie ma także odporność infrastruktury – zdolność do działania w warunkach awarii sieci lub zasilania – oraz higiena informacyjna, obejmująca moderację zgłoszeń i przeciwdziałanie dezinformacji. Ostatecznie to systematyczna edukacja, ćwiczenia i praktyczne przygotowanie obywateli decydują o tym, czy technologia stanie się rzeczywistym wsparciem, a nie jedynie narzędziem. Tylko świadome i dobrze przygotowane społeczeństwo, korzystające z nowoczesnych rozwiązań w sposób odpowiedzialny, może stworzyć skuteczny i odporny system obrony cywilnej.

Opracowany materiał ze względu na swoją objętość został podzielony na dwie części. Pierwsza służy prezentacji przykładów nowoczesnych technologii wspierających ochronę ludności i obronę cywilną stosowane w Polsce, zaś w części drugiej opisane zostaną rozwiązania organizacyjno-techniczne funkcjonujące w Europie i na świecie.

Uzupełnieniem tezy postawionej w treści pracy będzie przedstawienie wyników ankiety. W związku z tym prosimy czytelników o poświęcenie kilku minut i przesłanie swoich odpowiedzi. Celem ankiety jest poznanie opinii na temat wykorzystania nowoczesnych technologii w Ochronie Ludności i obronie cywilnej. Zebrane dane posłużą do analizy poziomu świadomości społecznej oraz oceny skuteczności i rozwoju technologicznych narzędzi wspierających bezpieczeństwo powszechne. Z góry dziękujemy za poświęcony czas.

<https://forms.gle/QppnijVmzVbzKK828>



AI Use Statement

The authors declare that artificial intelligence tools were used in the preparation of this article only within the scope indicated below:

- language and stylistic verification of the manuscript,
- data analysis supporting interpretation of results,
- searching for and identifying potential bibliographic sources.

The authors take full responsibility for the content of the publication, including the scientific accuracy, interpretation of results, and final editing of the manuscript. Artificial intelligence tools were used solely as supporting instruments.

The journal's editorial policy prohibits the uncritical copying of AI-generated content and its inclusion in a publication without proper critical analysis, verification, and revision by the authors.

Oświadczenie dotyczące wykorzystania AI

Autorzy oświadczają, że w procesie przygotowania niniejszego artykułu wykorzystano narzędzia oparte na sztucznej inteligencji wyłącznie w zakresie wskazanym poniżej:

- weryfikacja językowa i stylistyczna tekstu,
- analiza danych wspomagająca interpretację wyników,
- wyszukiwanie i identyfikacja potencjalnych źródeł bibliograficznych.

Autorzy ponoszą pełną odpowiedzialność za treść publikacji, w tym za poprawność merytoryczną, interpretację wyników oraz ostateczną redakcję tekstu. Narzędzia sztucznej inteligencji były wykorzystywane wyłącznie jako narzędzia pomocnicze.

Polityka redakcyjna czasopisma zabrania bezrefleksyjnego kopiowania treści wygenerowanych przez narzędzia AI oraz pozostawiania ich w publikacji bez krytycznej analizy, weryfikacji i redakcji przez autorów.

Literature / Literatura

- [1] Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907).
- [2] Konwencje o ochronie ofiar wojny, podpisane w Genewie dnia 12 sierpnia 1949 roku (Dz.U. 1956 nr 38 poz. 171).
- [3] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483).
- [4] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590).
- [5] <https://www.gov.pl/web/rcb/alertrcb> [dostęp: 10.10.2025].
- [6] https://archiwum.rcb.gov.pl/alert-rcb-dotychczasowe-dowiadzenia-i-perspektywy-rozwoju/?utm_source [dostęp: 10.10.2025].
- [7] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej.
- [8] https://komorkomania.pl/alert-rcb-przejdzie-duze-zmiany-ta-technologie-zastapi-sms-y-o-zagrozeniach-2C6900753254054816a?utm_ [dostęp: 10.10.2025].
- [9] https://wiadomosci.wp.pl/resort-szykuje-zmiany-w-planach-nowa-funkcja-alertow-rcb-7200884320094816a?utm_ [dostęp: 10.10.2025].
- [10] <https://www.gov.pl/web/uw-mazowiecki/regionalny-system-ostrzegania2> [dostęp: 10.10.2025].
- [11] <https://play.google.com/store/apps/details?id=mswiarso&hl=pl> [dostęp: 17.11.2025].
- [12] <https://imgw.pl/> [dostęp: 15.10.2025].
- [13] <https://hydro.imgw.pl/#/> [dostęp: 15.10.2025].
- [14] <https://meteo.imgw.pl/> [dostęp: 15.10.2025].
- [15] <https://agrometeo.imgw.pl/> [dostęp: 15.10.2025].
- [16] <https://baltyk.imgw.pl/> [dostęp: 15.10.2025].
- [17] <https://powietrze.imgw.pl/#group=smog¶m=o3&loc=52.24,21.034,7> [dostęp: 15.10.2025].
- [18] <https://play.google.com/store/apps/details?hl=pl&id=pl.imgw.meteo> [dostęp: 20.10.2025].
- [19] <https://apps.apple.com/pl/app/meteo-imgw-prognoza-dla-polski/id1530352176> [dostęp: 20.10.2025].
- [20] <http://schrony.straz.gov.pl> [dostęp: 20.10.2025].
- [21] <https://www.gov.pl/web/wody-polskie/sytuacja-hydrologiczna> [dostęp: 20.10.2025].
- [22] <https://www.gov.pl/web/gios> [dostęp: 20.10.2025].
- [23] <https://inspire.gios.gov.pl/portal/> [dostęp: 20.10.2025].
- [24] <https://monitoring.paa.gov.pl/maps-portal/> [dostęp: 20.10.2025].
- [25] <https://www.pgi.gov.pl/osuwiska/123/aplikacja.html> [dostęp: 21.10.2025].
- [26] <https://isok.gov.pl/index.html> [dostęp: 21.10.2025].
- [27] <https://mapy.geoportal.gov.pl/iMapLite/KMZBPublic.html> [dostęp: 21.10.2025].
- [28] <https://www.gov.pl/web/mobywatel> [dostęp: 21.10.2025].
- [29] <https://sisms.pl/> [dostęp: 05.11.2025].
- [30] <https://www.gov.pl/web/numer-alarmowy-112/aplikacja-moblina-alarm112> [dostęp: 05.11.2025].
- [31] <https://www.ratunek.eu/> [dostęp: 05.11.2025].
- [32] <https://ratownikpp.pl/aplikacja-ratownik> [dostęp: 17.11.2025].
- [33] <https://airly.org/map/pl/> [dostęp: 17.11.2025].
- [34] <https://www.gov.pl/web/kmpsp-warszawa/pozar-hali-handlowej-na-ul-marywilskiej-44> [dostęp: 17.11.2025].
- [35] <https://www.gov.pl/web/kgpsp-nowe-roboty-colossus-w-psp> [dostęp: 17.11.2025].
- [36] <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32020R0639> [dostęp: 17.11.2025].

TOMASZ LUTOBORSKI, M.A. – graduate of the Warsaw Technical University, Faculty of Administration and Social Sciences. Since 2022, linked with the Scientific and Research Centre for Fire Protection – National Research Institute in Józefów, where he conducts research on handheld fire-extinguishing equipment and fixed fire-extinguishing equipment in the Laboratory Of Fire Extinguishing Agents and Equipment. He is also responsible for testing innovative solutions in fire-extinguishing technology. In 2025, he completed post-graduate studies in Civil Protection, Civil Defence and Crisis Management at the Fire University. Volunteer firefighter, Volunteer Fire Service in Józefów.

MACIEJ ZAWISTOWSKI, M.SC. ENG. – pilot of unmanned aerial vehicles, instructor and specialist in using unmanned systems in rescue operations. Graduate of the Faculty of Electrical Engineering in the Warsaw University of Technology. In 2013-2018, he worked in the Institute of Electrical Engineering in Międzyzlesie, in teams in charge of measurement and diagnostics systems and electrical drives and control. Since 2018, he is linked with the Scientific and Research Centre for Fire Protection – National Research Institute in Józefów, where in the Drone Centre he conducts research on using unmanned aerial vehicles and RGB and thermal cameras in fire service and civil defence operations. Participant of national and international projects, ex-head of the international project Horizon 2020 „ASSISTANCE – Adapted Situation Awareness tools and tailored training scenarios for increasing capabilities and enhancing the protection of First Responders”. Author and co-author of many publications on UAV parameters and settings, BSP operation risk assessment and use of drones in fire protection. Member of the Volunteer Fire Service in Józefów.

MGR TOMASZ LUTOBORSKI – absolwent Politechniki Warszawskiej, Wydziału Administracji i Nauk Społecznych. Od 2022 r. związany z Centrum Naukowo-Badawczym Ochrony Przeciwpowarowej im. Józefa Tuliszkowskiego – Państwowym Instytutem Badawczym w Józefowie, gdzie w Zespole Laboratoriów Urządzeń i Środków Gaśniczych prowadzi badania nad podręcznym sprzętem gaśniczym oraz stałymi urządzeniami gaśniczymi. Zajmuje się również testowaniem innowacyjnych rozwiązań w dziedzinie techniki gaśniczej. W 2025 r. ukończył studia podyplomowe na Akademii Pożarniczej na kierunku ochrona ludności, obrona cywilna i zarządzanie kryzysowe. Strażak ochotnik w OSP Józefów.

MGR INŻ. MACIEJ ZAWISTOWSKI – pilot bezałogowych statków powietrznych, instruktor i specjalista w zakresie wykorzystania systemów bezałogowych w działaniach ratowniczych. Absolwent Wydziału Elektrycznego Politechniki Warszawskiej. W latach 2013–2018 pracował w Instytucie Elektrotechniki w Międzyzlesiu, w zespołach zajmujących się systemami pomiarowo-diagnostycznymi oraz napędami elektrycznymi i sterowaniem. Od 2018 r. związany jest z Centrum Naukowo-Badawczym Ochrony Przeciwpowarowej im. Józefa Tuliszkowskiego – Państwowym Instytutem Badawczym w Józefowie, gdzie w Centrum Dronów prowadzi badania nad zastosowaniem bezałogowych statków powietrznych oraz kamer RGB i termowizyjnych w działaniach straży pożarnej i obronie cywilnej. Uczestnik projektów krajowych i międzynarodowych. Był kierownikiem międzynarodowego projektu Horyzont 2020 „ASSISTANCE – Adapted Situation Awareness tools and tailored training scenarios for increasing capabilities and enhancing the protection of First Responders”. Autor i współautor licznych publikacji dotyczących parametrów i ustawień BSP, oceny ryzyka operacji BSP oraz wykorzystania dronów w ochronie przeciwpożarowej. Druh Ochotniczej Straży Pożarnej w Józefowie.

Karol Jędrasiak

WSB University / Akademia WSB

Corresponding author / Autor korespondencyjny: kjedrasiak@wsb.edu.pl

Analysis of Acoustic Anomalies and Speech Artefacts in Synthetic Content

Analiza anomalii akustycznych i artefaktów mowy w treściach syntetycznych

ABSTRACT

Purpose: The purpose of the study was to empirically confirm that acoustic anomalies and speech artefacts may constitute interpretable and robust descriptors used to detect audio deepfakes. The study focused on identifying typical deviations in voice, prosody and acoustic spectrum parameters, which result from synthetic speech generation by TTS models and voice conversion, in particular in the sound source and articulation track mirroring layers. The following stage was to assess the stability of these characteristics in realistic distribution of the content (in the wild), including recompression, variable band and typical noise.

Project and methods: A full framework was developed for unification, extraction and selection of acoustic characteristics, independent of classifiers. The analysis included the impact of the signal to noise ratio (SNR), which determines the quality of audio recording, where a low SNR value indicates strong impact of the background noise and significantly decreases the effectiveness of phase, cepstral and modulation characteristics. 46,371 clips from the DeepFake RealWorld (DFRW) set were analysed, which includes authentic and synthetic recordings, generated using various technologies (GAN, diffusion models, TTS, voice conversion). Five descriptor families were defined: tonal-glottal, cepstral-spectral, phase, energy-dynamic and prosodic-modulatory. The selection was completed without using neural networks, using differential factors $\Delta p = p_{df} - p_{real}$ and $PR = p_{df} / p_{real}$ with thresholds $\Delta p \geq 0.15$ or $PR \geq 1.5$ and validity control FDR ($q < 5\%$).

Results: The analysis revealed significant differences between authentic and synthetic speech. The highest differentiation effectiveness was obtained for characteristics LFCC, CQCC and MFCC (Δp to 0.25; $PR \approx 1.6$ –1.8), which maintained stability after degradations typical of social media. The jitter/shimmer, HNR/CPP and modulation characteristics showed smoothing of prosody and excessive voice regularity ($\Delta p \approx 0.17$ –0.23). Phase characteristics were useful in detecting harmonic discontinuities, however their effectiveness dropped at low SNR. The combination of acoustic analysis with audio-video synchronisation metrics (LSE-C/LSE-D) increased the resistance to single modality disturbance attacks.

Conclusions: The identified speech anomalies and artefacts are a credible and interpretable foundation of audio deepfake detection. The results have a direct application value for public safety and civil protection, because they enable building an auditable audio content layer for voice impersonation and message manipulations. In operating scenarios, such as crisis communication of public institutions, verification of authenticity of recordings disseminated in social media and analysis of sociotechnical incidents, interpretable descriptors may shorten the triage time, support the early warning and reduce the escalation risk of voice misinformation. They can be used as basis for hybrid forensic systems that combine classic acoustic descriptors with deep learning models to ensure interpretability and resistance to technological drift. The DFRW set and the applied selection method enable a comparable and repeatable evaluation of the effectiveness of characteristics in various distribution conditions. The continuation of the project (DFRWv2) will include database extension to $\geq 500,000$ clips and multi-modal audio-video analyses, which will enable standardisation of the reporting of indicators Δp , PR , p_{real} , p_{df} and 95% CI in forensic studies and security engineering.

Keywords: audio deepfake, speech artefacts, acoustic anomalies, modulation spectrum, audio-video synchronisation, public safety, cybersecurity, civil protection, crisis communication, acoustic forensics

Type of article: original scientific article

Received: 27.10.2025; Reviewed: 13.11.2025; Accepted: 07.01.2026;

Author's ORCID ID: 0000-0002-2254-1030;

Please cite as: Safety & Fire Technology 2026, 1, 58–84, <https://doi.org/10.12845/sft.67.1.2026.3>;

This is an open access article under the CC BY-SA 4.0 license (<https://creativecommons.org/licenses/by-sa/4.0/>).

ABSTRAKT

Cel: Celem badania było empiryczne potwierdzenie, że anomalie akustyczne i artefakty mowy mogą stanowić interpretowalne i odporne deskryptory służące do detekcji audio deepfake'ów. Praca koncentrowała się na identyfikacji charakterystycznych odchył w parametrach głosu, prozodii i widma akustycznego, które powstają w wyniku syntetycznego generowania mowy przez modele TTS i konwersji głosu, szczególnie w warstwie odwzorowania źródła dźwięku i toru artykulacyjnego. Dalszym etapem była ocena stabilności tych cech w warunkach realistycznej dystrybucji materiałów (ang. *in the wild*), obejmującej rekompresję, zmienne pasmo oraz typowe szумы.

Projekt i metody: Opracowano kompletną ramę unifikacji, ekstrakcji i selekcji cech akustycznych, niezależną od klasyfikatorów. W analizie uwzględniono wpływ stosunku sygnału do szumu (SNR), który określa jakość nagrania audio, przy czym niski SNR oznacza silny wpływ szumu tła i istotnie obniża skuteczność cech fazowych, cepstralnych i modulacyjnych. Analizie poddano 46 371 klipów ze zbioru DeepFake RealWorld (DFRW), obejmującego nagrania autentyczne i syntetyczne, wygenerowane różnymi technologiami (GAN, modele dyfuzyjne, TTS, voice conversion). Zdefiniowano pięć rodzin deskryptorów: tonalno-glottalne, cepstralne i widmowe, fazowe, energetyczno-dynamiczne oraz prozodyczno-modulacyjne. Selekcję prowadzono bez użycia sieci neuronowych, wykorzystując wskaźniki różnicowe $\Delta p = p_{df} - p_{real}$ i $PR = p_{df} / p_{real}$ przy progach $\Delta p \geq 0,15$ lub $PR \geq 1,5$ oraz kontroli istotności FDR ($q < 5\%$).

Wyniki: Analiza ujawniła istotne różnice między mową autentyczną a syntetyczną. Najwyższą skuteczność rozróżniania uzyskano dla cech LFCC, CQCC i MFCC (Δp do 0,25; $PR \approx 1,6-1,8$), które zachowały stabilność po degradacjach typowych dla mediów społecznościowych. Wskaźniki jitter/shimmer, HNR/ CPP i cechy modulacyjne wskazały na wygładzenie prozodyki i nadmierną regularność głosu ($\Delta p \approx 0,17-0,23$). Cechy fazowe były użyteczne w wykrywaniu nieciągłości harmonicznych, choć ich skuteczność spadała przy niskim SNR. Połączenie analizy akustycznej z metrykami spójności audio-wideo (LSE-C/LSE-D) zwiększyło odporność na ataki zakłócające jedną modalność.

Wnioski: Zidentyfikowane anomalie i artefakty mowy stanowią wiarygodny, interpretowalny fundament detekcji audio deepfake'ów. Wyniki mają bezpośrednią wartość aplikacyjną dla bezpieczeństwa publicznego, cyberbezpieczeństwa oraz ochrony ludności, ponieważ umożliwiają budowę audytowalnej warstwy preselekcji materiału audio pod kątem podszywania się głosem i manipulacji komunikatami. W scenariuszach operacyjnych, takich jak komunikacja kryzysowa instytucji publicznych, weryfikacja autentyczności nagrań rozpowszechnianych w mediach społecznościowych oraz analiza incydentów socjotechnicznych, interpretowalne deskryptory mogą skracać czas triage, wspierać wczesne ostrzeganie i ograniczać ryzyko eskalacji dezinformacji głosowej. Mogą służyć jako podstawa hybrydowych systemów forensycznych łączących klasyczne deskryptory akustyczne z modelami uczenia głębokiego, zapewniając interpretowalność i odporność na dryf technologiczny. Zbiór DFRW i zastosowana metoda selekcji umożliwiają porównywalną, powtarzalną ocenę skuteczności cech w różnych warunkach dystrybucyjnych. Kontynuacja projektu (DFRWv2) obejmie rozszerzenie bazy do $\geq 500\,000$ klipów i analiz multimodalnych audio-wideo, co pozwoli na standaryzację raportowania wskaźników Δp , PR , p_{real} , p_{df} i 95% CI w badaniach forensycznych i inżynierii bezpieczeństwa.

Słowa kluczowe: audio deepfake'i, artefakty mowy, anomalie akustyczne, widmo modulacyjne, spójność audio-wideo, bezpieczeństwo publiczne, cyberbezpieczeństwo, ochrona ludności, komunikacja kryzysowa, forensyka akustyczna

Typ artykułu: oryginalny artykuł naukowy

Przyjęty: 27.10.2025; **Zrecenzowany:** 13.11.2025; **Zaakceptowany:** 07.01.2026;

Identyfikator ORCID autora: 0000-0002-2254-1030;

Proszę cytować: Safety & Fire Technology 2026, 1, 58–84, <https://doi.org/10.12845/sft.67.1.2026.3>;

Artykuł udostępniany na licencji CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>).

Introduction

The dynamic development of artificial intelligence in the last decade led to an important shift of paradigm in the generation of synthetic content, including images, video and speech. The phenomenon referred to as deepfakes intensified with the increase of deep learning model complexity, of which the rate can be comparable with Moore's law for artificial intelligence [1–2]. The number of parameters of generative models increased abruptly from the range of 10^{11} – 10^{12} parameters in 2018 to more than 10^{11} – 10^{12} in 2024 [3–4]. In parallel, the development of hardware infrastructure, in particular GPUs (Graphics Processing Unit) and machine learning accelerators, enabled running advanced models on consumer hardware, contributing to wide commercialisation of generative technologies.

Although the diffusion of deepfakes in the visual area is described extensively in literature [5–6], the development of acoustic content and speech synthesis is equally dynamic. Models, such as WaveNet, Tacotron 2, FastSpeech and transformer architectures [7–8], enabled generating voice in quality similar to natural human articulation. As a result, synthetic voice recordings were found useful both in positive areas, such as personalisation of services or support for people with speech disorders, and in harmful activities, including fraud, information manipulation and public safety hazards [9–10].

Wprowadzenie

Dynamiczny rozwój sztucznej inteligencji w ostatniej dekadzie doprowadził do istotnej zmiany paradygmatu w generowaniu treści syntetycznych, obejmujących obrazy, wideo oraz mowę. Zjawisko określane mianem deepfake nasiliło się wraz ze wzrostem złożoności modeli głębokiego uczenia, którego tempo bywa porównywane do prawa Moore'a dla sztucznej inteligencji [1–2]. Liczba parametrów modeli generatywnych wzrosła skokowo z rzędu 10^{11} – 10^{12} parametrów w roku 2018 do ponad 10^{11} – 10^{12} w roku 2024 [3–4]. Równolegle rozwój infrastruktury sprzętowej, w szczególności układów GPU (ang. *Graphics Processing Unit*) i akceleratorów uczenia maszynowego, umożliwił uruchamianie zaawansowanych modeli na sprzęcie konsumenckim, przyczyniając się do szerokiej komercjalizacji technologii generatywnych.

Choć rozpowszechnienie deepfake'ów w obszarze wizualnym jest szeroko opisane w literaturze [5–6], również dynamiczny rozwój dotyczy treści akustycznych i syntezy mowy. Modele, takie jak WaveNet, Tacotron 2, FastSpeech oraz architektury transformatorowe [7–8], umożliwiły generowanie głosu o jakości zbliżonej do naturalnej artykulacji człowieka. W efekcie syntetyczne nagrania głosowe znalazły zastosowanie zarówno w obszarach pozytywnych, jak personalizacja usług czy wsparcie osób z zaburzeniami mowy, jak i w działaniach szkodliwych, obejmujących oszustwa, manipulacje informacyjne oraz zagrożenia dla bezpieczeństwa publicznego [9–10].

The scale of the phenomenon finds confirmation in empirical data. The Sumsb Report 2023 indicated a tenfold increase in the use of deepfakes in identity verification systems compared to 2022 and another fourfold increase was recorded in 2024 [11]. The Regula Report (2024) indicated that approx. 50% of analysed enterprises experienced incidents related to synthetic content [12]. In Europe, the dynamics of the phenomenon in 2023 increased by 780% in a year, which translated to increasing expectations for security systems and forensic solutions.

The ease of generation of acoustic materials results from the availability of open source tools and commercialisation of cloud services. Applications, such as VALL-E, ElevenLabs or Descript, and SaaS platforms, including HeyGen and Synthesia, enable quick creation of audio and audio-video content based on short voice samples. The democratisation of these technologies lowers the barrier of entry, but also increases the scale of hazards from the security engineering perspective.

Unlike for image, for which detection is based on visual and spectral markers [13–14], for acoustic content the analysis requires identification of specific anomalies resulting from the synthesis process. The most commonly described include frequency spectrum irregularities, lack of microdetails related to speech apparatus physiology, prosodic disruptions, unnatural transitions between phonemes and temporal and amplitudinal artefacts [10], [15]. The research indicates that even advanced models fail to fully reflect the physical processes of speech activation, which leads to systematic signal deviations [16].

The rate and scale of distribution of synthetic recordings remains a significant challenge. The analyses by Kumar et al. [17] based on 2,3M tweets showed that fake contents reach a million views in 2.3 hours on average, with most interactions occurring within 30 minutes of posting. This creates a temporal asymmetry with detection and moderation systems, which need a few hours to respond in operating conditions [18]. Within that time, content can be replicated and archived multiple times, which significantly impedes eliminating it.

The consequences of the phenomenon include both reputation and financial losses. In 2024, Europol recorded a significant 850% increase in losses due to corporate CEO fraud based on audio deepfakes, up to more than USD 100M [19]. Moreover, the TNO simulations [20] show that fake voice messages can have a significant impact on collective behaviour in crisis situations. From the civil protection perspective, the risk of impersonating institutions responsible for warning and crisis response coordination is particularly critical, because synthetic voice messages may undermine trust in information channels and impede the enforcement of safety guidelines. In cybersecurity, the same attack class reinforced the effectiveness of sociotechnics, including fraud targeting decision-making and authorisation processes, which increases the demand for detection methods resistant to channel degradation and possible to explain in the course of incident analysis.

In this context, the key research problem remains to develop interpretable and stable acoustic characteristics that could be used as universal detection descriptors. Until now, approaches based on black box classifiers have been dominant, which are

Skala zjawiska znajduje potwierdzenie w danych empirycznych. Raport Sumsb z 2023 roku wskazuje na dziesięciokrotny wzrost użycia deepfake'ów w systemach weryfikacji tożsamości względem roku 2022, a w roku 2024 odnotowano kolejny czterokrotny wzrost [11]. W raporcie Regula (2024) wykazano, że około 50% analizowanych przedsiębiorstw doświadczyło incydentów związanych z treściami syntetycznymi [12]. W Europie dynamika zjawiska w 2023 roku wzrosła o 780% w ciągu roku, co przekłada się na rosnące oczekiwania względem systemów bezpieczeństwa i rozwiązań forensycznych.

Łatwość generowania materiałów akustycznych wynika z dostępności narzędzi otwartoźródłowych oraz komercjalizacji usług chmurowych. Aplikacje, takie jak VALL-E, ElevenLabs czy Descript oraz platformy SaaS, w tym HeyGen i Synthesia, umożliwiają szybkie tworzenie treści audio i audio-wideo na bazie krótkich próbek głosu. Demokratyzacja tych technologii obniża barierę wejścia, lecz jednocześnie zwiększa skalę zagrożeń z punktu widzenia inżynierii bezpieczeństwa.

W odróżnieniu od obrazu, w przypadku którego detekcja opiera się na markerach wizualnych i spektralnych [13–14], analiza treści akustycznych wymaga identyfikacji specyficznych anomalii wynikających z procesu syntezy. Do najczęściej opisywanych należą nieregularności widma częstotliwościowego, brak mikrodetali związanych z fizjologią aparatu mowy, zaburzenia prozodyczne, nienaturalne przejścia między fonemami oraz artefakty temporalne i amplitudowe [10], [15]. Badania wskazują, że nawet zaawansowane modele nie odtwarzają w pełni fizycznych procesów akwizycji mowy, co prowadzi do systematycznych odchyłen sygnału [16].

Istotnym wyzwaniem pozostaje tempo i skala dystrybucji syntetycznych nagrań. Analizy Kumar i in. [17] oparte na 2,3 mln tweetów wykazały, że fałszywe materiały osiągają milion wyświetleń średnio w czasie 2,3 godziny, przy czym większość interakcji występuje w pierwszych 30 minutach od publikacji. Tworzy to asymetrię czasową względem systemów detekcji i moderacji, które w warunkach operacyjnych wymagają kilku godzin na reakcję [18]. W tym czasie treści mogą być wielokrotnie replikowane i archiwizowane, co znacząco utrudnia ich eliminację.

Konsekwencje zjawiska obejmują zarówno straty reputacyjne, jak i finansowe. W 2024 roku Europol odnotował wzrost strat z tytułu oszustw korporacyjnych typu CEO fraud opartych na audio deepfake'ach o 850%, do poziomu ponad 100 mln USD [19]. Symulacje TNO [20] wskazują ponadto, że fałszywe komunikaty głosowe mogą istotnie wpływać na zachowania zbiorowe w sytuacjach kryzysowych. Z perspektywy ochrony ludności szczególnie krytyczne jest ryzyko podszywania się pod instytucje odpowiedzialne za ostrzeganie i koordynację działań w kryzysie, ponieważ syntetyczne komunikaty głosowe mogą zaburzać zaufanie do kanałów informacyjnych i utrudniać egzekucję zaleceń bezpieczeństwa. W obszarze cyberbezpieczeństwa ta sama klasa ataków wzmacnia skuteczność socjotechniki, w tym oszustw nakierowanych na procesy decyzyjne oraz autoryzacyjne, co zwiększa zapotrzebowanie na metody detekcji odporne na degradację kanałowe i możliwe do wyjaśnienia w toku analizy incydentu.

W tym kontekście kluczowym problemem badawczym pozostaje opracowanie interpretowalnych i stabilnych cech akustycznych, które mogłyby pełnić rolę uniwersalnych deskryptorów

characterised by high effectiveness on training data, but limited robustness in real distribution conditions [9], [21]. Thus it was necessary to shift the focus towards transparent methods, covering a wide spectrum of acoustic anomalies and degradations typical of social media platforms [22].

The purpose of this study is to develop an empirically verified set of descriptors to enable differentiating authentic voice recordings from synthetic content. The analysis is focused on the identification of acoustic anomalies, prosodic disruptions and artefacts of synthesis and on the evaluation of the stability of characteristics in typical signal degradations conditions. The result is the extraction of a set of characteristics with high application potential, constituting the basis for explicable audio deepfake detection methods in security engineering and acoustic forensics.

Data sets and research challenges

The effectiveness of detection of synthetic content in the acoustic domain is directly determined by the quality and structure of the data sets used for training and evaluation of methods. In literature, there are three primary benchmark classes: visual sets with audio component, acoustic sets dedicated to synthetic speech detection and multi-modal audio-video sets. Each of these categories contributes important information, but also generates limitations for the analysis of acoustic anomalies and speech artefacts.

Visual sets with audio, such as DFDC [23], FaceForensics++ [24], DeeperForensics-1.0 [25] and Celeb-DF v2 [26], played an important role in the development of video deepfake detection, however they were not designed as acoustic benchmarks. The lack of control over audio channel parameters and degradation scenarios limits their usability in synthetic speech detection. The models trained on this data show a visual bias and significant effectiveness drops in inter-set and inter-generator transfer [6], [21].

The standard in synthetic speech detection remains the ASVspoof benchmark family, which includes logical access and physical access scenarios and EER (Equal Error Rate) and min t-DCF metrics [27–28]. The post-2019 editions include a wide range of TTS and VC models and channel variants, enabling the analysis of the stability of spectral, cepstral and phase characteristics in near-real conditions. They are complemented by in-the-wild sets, however they remain limited by the lack of uniform channel descriptions and consistent evaluation protocols [10], [15].

In practice, two approaches are followed as reference methods. The first includes standardised ASVspoof protocols, which clearly prove that high effectiveness in laboratory conditions does not translate to stability in real distribution conditions [29]. The second includes trained detectors, such as RawNet2 and AASIST [30], and self-supervised models, including wav2vec 2.0 and WavLM, which increase the resistance to channel variability [31].

dotekcji. Dotychczas dominowały podejścia oparte na klasyfikatorach typu czarna skrzynka, charakteryzujące się wysoką skutecznością na danych treningowych, lecz ograniczoną odpornością w warunkach rzeczywistej dystrybucji [9], [21]. Konieczne jest zatem przesunięcie akcentu w stronę metod transparentnych, uwzględniających szerokie spektrum anomalii akustycznych oraz degradacje charakterystyczne dla platform społecznościowych [22].

Celem niniejszej pracy jest opracowanie empirycznie zweryfikowanego zbioru deskryptorów umożliwiających rozróżnianie autentycznych nagrań głosowych od treści syntetycznych. Analiza koncentruje się na identyfikacji anomalii akustycznych, zaburzeń prozodycznych i artefaktów syntezy oraz na ocenie stabilności cech w warunkach typowych degradacji sygnału. Rezultatem jest wyodrębnienie zbioru cech o wysokim potencjale aplikacyjnym, stanowiący podstawę dla wyjaśnialnych metod detekcji audio deepfake'ów w inżynierii bezpieczeństwa i forensyce akustycznej.

Zbiory danych i wyzwania badawcze

Skuteczność detekcji treści syntetycznych w domenie akustycznej jest bezpośrednio uzależniona od jakości i konstrukcji zbiorów danych wykorzystywanych do uczenia oraz ewaluacji metod. W literaturze funkcjonują trzy główne klasy benchmarków: zbiory wizualne z komponentem audio, zbiory akustyczne dedykowane detekcji mowy syntetycznej oraz zestawy multimodalne audio-wideo. Każda z tych kategorii wnosi istotne informacje, lecz jednocześnie generuje ograniczenia w kontekście analizy anomalii akustycznych i artefaktów mowy.

Zbiory wizualne z dźwiękiem, takie jak DFDC [23], FaceForensics++ [24], DeeperForensics-1.0 [25] oraz Celeb-DF v2 [26], odegrały istotną rolę w rozwoju detekcji wideo deepfake'ów, jednak nie były projektowane jako benchmarki akustyczne. Brak kontroli nad parametrami kanału audio i scenariuszami degradacji powoduje, że ich użyteczność w detekcji mowy syntetycznej jest ograniczona. Modele uczone na tych danych wykazują bias wizualny oraz istotne spadki skuteczności w transferze międzyzbiorowym i międzygeneratorowym [6], [21].

Standardem w detekcji mowy syntetycznej pozostaje rodzina benchmarków ASVspoof, obejmująca scenariusze dostępu logicznego (ang. *logical access*) i fizycznego (ang. *physical access*) oraz metryki EER (ang. *Equal Error Rate*) i min t-DCF [27–28]. Edycje po 2019 roku uwzględniają szeroki zakres modeli TTS i VC oraz warianty kanałowe, pozwalające na analizę stabilności cech widmowych, cepstralnych i fazowych w warunkach zbliżonych do rzeczywistych. Uzupełnieniem są zbiory *in-the-wild*, jednak ich ograniczeniem pozostaje brak jednorodnych opisów kanału i spójnych protokołów oceny [10], [15].

W praktyce jako metody odniesienia funkcjonują dwa podejścia. Pierwsze obejmuje standaryzowane protokoły ASVspoof, które jednoznacznie wykazały, że wysoka skuteczność laboratoryjna nie przekłada się na stabilność w warunkach rzeczywistej dystrybucji [29]. Drugie obejmuje uczone detektory, takie jak RawNet2 i AASIST [30], oraz modele wykorzystujące reprezentacje

These approaches, however, mostly remain black box classifiers, which limits their forensic usability.

Platform distribution and channel variation remain a key challenge. In real conditions, audio signal is subject to cascade transcoding, band filtering, volume normalisation, SNR variables and secondary recording. These factors also affect the amplitude, phase, time and frequency domain. According to literature, relatively high robustness is found in characteristics related to articulation microdetails, formant structures, phase coherence and prosodic micro-differences with proper channel normalisation [10].

Inter-generator generalisation and technological drift remain an important problem. The detectors trained on data based on vocoders and GAN architecture lose effectiveness in view of diffusion and hybrid models. As a result, we record drops in AUC (area under curve) in the range of 20–50% and deteriorating calibration in OOD scenarios (Out Of Distribution) [6], [21], [32–33]. From the security engineering perspective, it is necessary to report metrics at low FPR (False Positive Rate) and conduct regular calibration around EER (Equal Error Rate) and min t-DCF (Minimum tandem Detection Cost Function).

Anti-forensics and adaptive attacks are an additional hazard. Simple masking transformations and attacks minimising detector losses effectively reduce diagnostic artefacts, while retaining perceptive speech quality [34–36]. For that reason, data sets should include controlled degradation scenarios and adversarial texts.

Forensic applications require interpretability and evidence track buildability. In audio detection, it entails linking detection to anomaly classes, such as formant instability, $F0$ – energy relationship disruptions, phonemic discontinuities and phase decoherence, and presenting them clearly in reports [10], [37]. The reviews of commercial systems indicate inadequate use of XAI methods and the lack of standard report protocols [38–39].

In this study, the selection of data sets was determined by identification of stable acoustic anomalies and synthetic speech artefacts. Natural speech reference material, synthetic samples from various generation paradigms, channel degradation scenarios and the multi-modal component were used. A key role is played by the DFRW set, which constitutes the *in-the-wild* data source and the basis for the robustness of characteristics in real distribution conditions. Its use enables the selection of descriptors with high operating usability [21], [36], [40].

The DFRW set

Due to the lack of a single current and representative set combining the newest generation techniques with realistic platform degradation chains, the DeepFake RealWorld (DFRW) set with 46,371 clips was developed. The construction was completed in two stages. The first stage consisted in systematic acquisition

samonadzorowane (ang. *self supervised*), w tym wav2vec 2.0 i WavLM, zwiększające odporność na zmienność kanału [31]. Podejścia te pozostają jednak w większości klasyfikatorami czarnej skrzynki, co ogranicza ich przydatność forensyczną.

Kluczowym wyzwaniem pozostaje dystrybucja platformowa i zmienność kanału. W warunkach rzeczywistych sygnał audio podlega kaskadowym transkodowaniom, filtracji pasmowej, normalizacji głośności, zmiennym SNR oraz wtórnej rejestracji. Czynniki te wpływają jednocześnie na domenę amplitudy, fazy, czasu i częstotliwości. Literatura wskazuje, że relatywnie odporne są cechy związane z mikrodetaliami artykulacyjnymi, strukturą formantów, koherencją fazową i mikroróżnicami prozodycznymi, przy odpowiedniej normalizacji kanału [10].

Istotnym problemem pozostaje generalizacja międzygeneratorowa i dryf technologiczny. Detektory trenowane na danych opartych na wokoderach i architekturach GAN tracą skuteczność wobec modeli dyfuzyjnych i hybrydowych. W efekcie odnotowujemy spadki AUC (ang. *area under curve* – obszar pod krzywą) rzędu 20–50% oraz pogorszenie kalibracji w scenariuszach OOD (ang. *Out Of Distribution*) [6], [21], [32–33]. Z perspektywy inżynierii bezpieczeństwa konieczne jest raportowanie metryk przy niskim FPR (ang. *False Positive Rate*) oraz regularna kalibracja obok EER (ang. *Equal Error Rate*) i min t-DCF (ang. *Minimum tandem Detection Cost Function*).

Dodatkowym zagrożeniem jest antyforensyka i ataki adaptacyjne. Proste transformacje maskujące oraz ataki minimalizujące stratę detektora skutecznie redukują diagnostyczne artefakty, przy zachowaniu jakości percepcyjnej mowy [34–36]. Z tego powodu zbiory danych powinny obejmować kontrolowane scenariusze degradacji i testy adversarialne.

Zastosowania forensyczne wymagają interpretowalności i możliwości budowy ścieżki dowodowej. W detekcji audio oznacza to powiązanie decyzji z klasami anomalii, takimi jak niestabilność formantów, zaburzenia relacji $F0$ – energia, nieciągłości fonemiczne czy dekoherencja fazy, oraz ich czytelną prezentację w raportach [10], [37]. Przeglądy systemów komercyjnych wskazują na niedostateczne wykorzystanie metod XAI i brak standardowych protokołów raportowych [38–39].

W niniejszej pracy dobór zbiorów danych podporządkowano identyfikacji stabilnych anomalii akustycznych i artefaktów mowy syntetycznej. Wykorzystano materiał referencyjny mowy naturalnej, próbki syntetyczne z różnych paradygmatów generacyjnych, scenariusze degradacji kanałowej oraz komponent multimodalny. Kluczową rolę pełni zbiór DFRW, stanowiący źródło danych *in-the-wild* i podstawę oceny odporności cech w warunkach rzeczywistej dystrybucji. Jego zastosowanie umożliwia selekcję deskryptorów o wysokiej użyteczności operacyjnej [21], [36], [40].

Zbiór DFRW

Wobec braku jednego, aktualnego i reprezentatywnego zbioru łączącego najnowsze techniki generacji z realistycznymi łańcuchami degradacji platformowej opracowano zbiór DeepFake RealWorld (DFRW) obejmujący 46 371 klipów. Konstrukcja odbywała się dwuetapowo. Etap pierwszy polegał na systematycznym

of “wild” deepfakes from open OSINT sources from social services and video aggregators by tracking hashtags (#deepfake, #fakespeech, #faceswap), not GIS analyses in fact-checking reports (PolitiFact, Snopes, AFP FactCheck), queries in Reddit r/deepfakes and correlation of pHash perceptive signatures. 4186 original clips were acquired, subject to pseudonymisation and context review in accordance with the principles of permissible scientific use and research ethics [41–42].

The second stage included controlled expansion of the set to synthetic variants and degradation scenarios for sustainable representation of technologies and distribution conditions. 42,185 additional clips were generated using tools representative of 2025, including full-frame diffusion video models (Stable Video Diffusion, Runway Gen 2 Gen 3, Pika Labs, Sora Beta), new generation *face swap* systems (SimSwap++, DeepFaceLab 2.0, InsightFaceSwap), audio- or video-controlled *lip sync* and *reenactment* methods (Wav2Lip++, SadTalker, EMO LipSync) and scene and face editors (Face2Face Enhanced, First Order Motion Model 2025). To replicate the platform chain, H.264 H.265 (CRF 18–32) multiple recoding, mobile filters and AR, resolution and aspect ratio changes, secondary screen recording and audio channel degradations were used. DFRW includes 4,186 “wild” deepfakes (9%) and 42,185 synthetic or transformed variants (91%), which enables replication of real content circulation and controlled tests of detector robustness [6], [23–24].

Finally, the DFRWv2 version is planned with scale $\geq 500,000$ clips and extended representation of diffusion models (Stable Diffusion 3.x, Runway Gen 3, Sora), multi-modal variants with dedicated audio track and continuous evaluation of platform degradations. It will enable conducting robustness and transfer tests and validation in OSINT forensics scenarios [6], [21].

The total material time is 229,28 hours. The average clip duration is 17.8 ± 12.3 s, 95% CI [17.69 s, 17.91 s]; the median is 12.4 s, IQR from 7.1 to 22.9 s. Duration distribution: < 5 s – 22% (10,202), from 5 to 15 s – 41% (19,012), from 15 to 60 s – 27% (12,520), > 60 s – 10% (4,637). Technology category: *face swap* – 35% (16,230), *reenactment* expression – 28% (12,984), full-frame diffusion – 25% (11,593), complex scene manipulations – 12% (5,564) [43–44]. For diffusion variants, the following process parameters were recorded: step median – 30, *guidance scale* – 4.5. In *reenactment*, 57% clips were audio driven, 43% were video driven. It enabled conducting a temporal inconsistencies and AV synchrony [21].

Distribution conditions are as follows: high quality – 15% (6,956), medium – 60% (27,823), high degradation – 25% (11,592). Video codecs: H.264 AVC – 71%, H.265 HEVC – 19%, VP9 – 7%, AV1 – 3%. Containers: MP4 – 84%, WebM – 10%, MOV – 6%. Median video bitrate – 1.6 Mb/s, IQR – from 0.9 to 2.8 Mb/s. GOP length: median – 60, Q1 30, Q3 120. Resolution: ≤ 480 p – 14%, 720p – 45%, 1080p – 33%, ≥ 1440 p – 8%. Orientation: horizontal – 59%, vertical – 36%, square – 5%. FPS (frames per second): 30 fps – 62%, 24 fps – 21%, 60 fps – 7%, 25 fps – 7%, other – 3%. Secondary recording was identified in 12% samples. Average subsequent 2.1 recodings: one – 36%, two – 31%, three – 23% ≥ 4 – 10%. AR mobile filters – 28%, platform watermark – 19%.

Reference-less image metrics: NIQE (Natural Image Quality Evaluator) – median 4.1/3.2/2.6 for high degradation / medium /

pozyскиwaniu „dzikich” deepfake’ów z otwartych źródeł OSINT z serwisów społecznościowych i agregatorów wideo, z wykorzystaniem śledzenia hashtagów (#deepfake, #fakespeech, #faceswap), analizy nie-GIS (ang. *not GIS*) w raportach weryfikujących fakty (PolitiFact, Snopes, AFP FactCheck), kwerend w Reddit r/deepfakes oraz korelacji percepcyjnych sygnatur pHash. Pozy-skano 4186 oryginalnych klipów poddanych pseudonimizacji i przeglądowi kontekstowemu zgodnie z zasadami dozwolonego użytku naukowego oraz etyki badań [41–42].

Etap drugi obejmował kontrolowane powiększenie zbioru o warianty syntetyczne i scenariusze degradacyjne dla zrównoważonej reprezentacji technologii i warunków dystrybucji. Wygenerowano 42 185 dodatkowych klipów z użyciem narzędzi reprezentatywnych dla roku 2025, w tym pełnoklatkowych modeli dyfuzyjnych wideo (Stable Video Diffusion, Runway Gen 2 Gen 3, Pika Labs, Sora Beta), systemów *face swap* nowej generacji (SimSwap++, DeepFaceLab 2.0, InsightFaceSwap), metod *lip sync* i *reenactment* sterowanych audio lub wideo (Wav2Lip++, SadTalker, EMO LipSync) oraz edytorów scen i twarzy (Face2Face Enhanced, First Order Motion Model 2025). Dla odtworzenia łańcucha platformowego zastosowano wielokrotne rekodowanie H.264 H.265 (CRF 18 do 32), filtry mobilne i AR, zmiany rozdzielczości i proporcji, wtórną rejestrację z ekranów oraz degradację kanałowe audio. DFRW obejmuje 4186 „dzikich” deepfake’ów (9%) oraz 42 185 wariantów syntetycznych lub przekształconych (91%), co umożliwia jednocześnie odwzorowanie realnego obiegu treści i kontrolowane testy odporności detektorów [6], [23–24].

Docelowo planowana jest wersja DFRWv2 o skali $\geq 500\,000$ klipów z rozszerzoną reprezentacją modeli dyfuzyjnych (Stable Diffusion 3.x, Runway Gen 3, Sora), wariantami multimodalnymi z dedykowaną ścieżką audio oraz ewaluacją ciągłą degradacji platformowych. Pozwoli ona na przeprowadzenie badań odpornościowych i transferowych oraz walidację w scenariuszach OSINT forensics [6], [21].

Łączny czas materiału wynosi 229,28 godzin. Średnia długość klipu to $17,8 \pm 12,3$ s, 95% CI [17,69 s, 17,91 s]; mediana to 12,4 s, IQR od 7,1 do 22,9 sekund. Rozkład długości: < 5 s – 22% (10 202), od 5 do 15 s – 41% (19 012), od 15 do 60 s – 27% (12 520), > 60 s – 10% (4637). Kategorie technologii: *face swap* – 35% (16 230), *reenactment* ekspresja – 28% (12 984), pełnoklatkowa dyfuzja – 25% (11 593), złożone manipulacje scenowe – 12% (5564) [43–44]. Dla wariantów dyfuzyjnych rejestrowano następujące parametry procesu: mediana kroków – 30, *guidance scale* – 4,5. W *reenactment* 57% klipów zawierało sterowanie mową (ang. *audio driven*), 43% – sterowanie wideo (ang. *video driven*). Umożliwiło to przeprowadzenie analizy niespójności temporalnej i synchronii AV [21].

Warunki dystrybucyjne przedstawiają się następująco: jakość wysoka – 15% (6956), średnia – 60% (27 823), wysoka degradacja – 25% (11 592). Kodeki wideo: H.264 AVC – 71%, H.265 HEVC – 19%, VP9 – 7%, AV1 – 3%. Kontenery: MP4 – 84%, WebM – 10%, MOV – 6%. Mediana bitrate wideo – 1,6 Mb/s, IQR – od 0,9 do 2,8 Mb/s. Długość GOP: mediana – 60, Q1 30, Q3 120. Rozdzielczości: ≤ 480 p – 14%, 720p – 45%, 1080p – 33%, ≥ 1440 p – 8%. Orientacja: pozioma – 59%, pionowa – 36%, kwadrat – 5%. FPS (ang. *frames per second*; klatki na sekundę): 30 fps – 62%, 24 fps – 21%, 60 fps – 7%, 25 fps – 7%, inne – 3%. Wtórną rejestrację rozpoznano

high quality, respectively; BRISQUE – 42/31/24. Correlation: $\rho(\text{CRF}, \text{LPIPS}) = 0.82, p < 0.001$; $\rho(\text{CRF}, \text{VMAF}) = -0.79, p < 0.001$. For reference subset: PSNR 33.8 dB, SSIM 0.926, LPIPS 0.193, as per platform chain profiles [26], [45–47].

Scenic and demographic attributes: men – 52% (24,113), women – 48% (22,258). Age: < 25 years – 25% (11,592), from 25 to 50 – 60% (27,822), > 50 – 15% (6,957). Scene: studio – 40% (18,548), outdoor – 35% (16,230), home – 25% (11,593). Number of people: 1 face – 72%, 2 faces – 23%, ≥ 3 faces – 5%. Relative face area: $14\% \pm 9\%$ (median 11%). Extreme head positions: $|\text{yaw}| > 30^\circ$ in 41%, $|\text{pitch}| > 20^\circ$ in 18%. Obstructions $\geq 5\%$ frames: hand object – 27%, sunglasses – 12%, masks – 3%. RAFT movement intensity: median 2.3 px/frame, P90 6.8 px, which supports temporal robustness characteristic tests [48–49].

In the acoustic layer, 77% clips include the audio track. Sampling frequency: 44.1 kHz (in 58% clips), 48 kHz (40%), other (2%). Channels: mono – 63%, stereo – 37%. The lips and speech synchronisation indicators as per LSE C (Equal Error Rate) and LSE D (Lip Sync Error Distance) are as follows: 18% clips with LSE D desynchronisation > 0.7 ; the average LSE C indicator value is 8.1 and the standard deviation is 1.6. This *audio driven* method artefacts and secondary recording [50–51]. Source and simulated platforms: TikTok – 33%, YouTube Shorts – 28%, X Twitter – 18%, Reddit – 12%, other – 9%. Inter-network duplicates with Hamming pHash threshold ≤ 10 constituted 1.3% and were removed. The metadata includes model family and version, generation parameters, list and order of degradation transformations and AV synchrony indicators.

Source and location identification data was removed. The 70%/15%/15% distribution was completed with stratification in relation to generator, scene, degradation level, duration and with strict identity distinction. The face embedding clustering (OpenFace) showed $8,740 \pm 210$ unique identities; average cluster size – 3.2, median – 2. The test of identity leak between splits at cosine distance < 0.3 : 0%, which reduces overstated results and favours cause and effect analyses [24], [52]. The validation was designed independent of automatic detectors to reduce the feedback loop and methodological bias in the conditions of distribution drift and emergence of new generators [6], [32], [44], [53–54].

Every clip was evaluated by two forensic expert in double blind mode after calibration session, with technological metadata masking: discrepancies were resolved by consensus with arbiter. The reliability was reported with Cohen's kappa and Krippendorff's alpha coefficients, in accordance with methodological guidelines [55–57]. The quality control was based on signal inspection in multiple representations and tests of stability under typical transmission and editing degradations, which enabled reducing the evaluation artefacts observed with heuristics specific for a single family of generators [23–24], [58].

The registered degradation profile is consistent with literature, which indicates that even moderate recompression and multi-stage transcoding cause AUC drops in the range of 10–25 pp and EER increases of 5–18 pp, in particular for diffusion families and for temporal artefacts and AR filters [6], [32], [44], [53]. The important factors for audio are: band limitation by lossy codecs, volume normalisation, variable SNR, room impulse response and A/D track

w 12% próbek. Średnia liczba kolejnych rekodowań 2.1: jedno – 36%, dwa – 31%, trzy – 23% ≥ 4 – 10%. Filtry mobilne AR – 28%, watermark platformowy – 19%.

Metryki bezreferencyjne obrazu: NIQE (ang. *Natural Image Quality Evaluator*) – mediana 4,1/3,2/2,6 odpowiednio dla wysokiej degradacji / średniej/wysokiej jakości; BRISQUE – 42/31/24. Korelacje: $\rho(\text{CRF}, \text{LPIPS}) = 0.82, p < 0.001$; $\rho(\text{CRF}, \text{VMAF}) = -0.79, p < 0.001$. Dla podzbioru referencyjnego: PSNR 33,8 dB, SSIM 0,926, LPIPS 0,193, zgodnie z profilami łańcuchów platformowych [26], [45–47].

Atrybuty sceniczne i demograficzne: mężczyźni – 52% (24 113), kobiety – 48% (22 258). Wiek: < 25 lat – 25% (11 592), od 25 do 50 lat – 60% (27 822), > 50 lat – 15% (6 957). Scena: studio – 40% (18 548), plener – 35% (16 230), dom – 25% (11 593). Liczba osób: 1 twarz – 72%, 2 twarze – 23%, ≥ 3 twarze – 5%. Relatywna powierzchnia twarzy: $14\% \pm 9\%$ (mediana 11%). Ekstremalne położenia głowy: $|\text{yaw}| > 30^\circ$ w 41%, $|\text{pitch}| > 20^\circ$ w 18%. Zastłonięcia $\geq 5\%$ klatek: ręka obiekt – 27%, okulary przeciwsłoneczne – 12%, maski – 3%. Intensywność ruchu RAFT: mediana 2,3 px/klatkę, P90 6,8 px, co wspiera testy odporności cech temporalnych [48–49].

Jeśli chodzi o warstwę akustyczną, 77% klipów zawiera ścieżkę audio. Częstotliwości próbkowania: 44,1 kHz (w 58% klipów), 48 kHz (40%), inne (2%). Kanały: mono – 63%, stereo – 37%. Wskaźniki spójności ust z mową wg LSE C (ang. *Equal Error Rate*) LSE D (ang. *Lip Sync Error Distance*) wyglądają następująco: 18% klipów z niespójnością LSE D $> 0,7$; średnia wartość wskaźnika LSE C wynosi 8,1, a odchylenie standardowe 1,6. Odzwierciedla to artefakty metod *audio driven* oraz wtórną rejestrację [50–51]. Platformy źródłowe i symulowane: TikTok – 33%, YouTube Shorts – 28%, X Twitter – 18%, Reddit – 12%, inne – 9%. Duplikaty międzysieciowe przy progu Hamming pHash ≤ 10 wyniosły 1,3% i zostały usunięte. Metadane obejmują rodzinę i wersję modelu, parametry generacji, listę i kolejność transformacji degradacyjnych oraz wskaźniki synchronii AV.

Dane identyfikujące źródła i lokalizacje usuwano. Podział 70%/15%/15% wykonano ze stratyfikacją względem generatora, sceny, poziomu degradacji, długości i ze ścisłym rozdzieleniem tożsamości. Klasteryzacja embeddingów twarzowych (OpenFace) wskazała $8\,740 \pm 210$ unikatowych tożsamości; średni rozmiar klastra – 3,2, mediana – 2. Test przecieku tożsamości między splitami przy odległości kosinusowej $< 0,3$: 0%, co ogranicza zawyżanie wyników i sprzyja analizom przyczynowo-skutkowym [24], [52]. Walidację zaprojektowano niezależnie od automatycznych detektorów w celu ograniczenia pętli zwrotnej i biasu metodologicznego w warunkach dryfu dystrybucyjnego i pojawiania się nowych generatorów [6], [32], [44], [53–54].

Każdy klip oceniali dwaj eksperci forensyczni w trybie podwójnie ślepy po sesji kalibracyjnej, przy maskowaniu metadanych technologicznych; rozbieżności rozstrzygano konsensem z arbitrem. Rzetelność raportowano współczynnikami kappa Cohena i alfa Krippendorffa, zgodnie z zaleceniami metodologicznymi [55–57]. Kontrolę jakości oparto na inspekcji sygnału w wielu reprezentacjach oraz testach stabilności pod typowymi degradacjami transmisyjnymi i edycyjnymi, co pozwoliło ograniczyć artefakty ewaluacyjne obserwowane przy heurystykach specyficznych dla jednej rodziny generatorów [23–24], [58].

non-linearity. Therefore, metrics LSE C and LSE D, phase coherence, formant stability and prosodic micro-fluctuations were included in metadata as stratification factors, supporting the selection of characteristics resistant to platform chains and anti-forensic attacks, including *time stretch* with formant correction, *pitch shift*, band filtering and secondary recording [10], [34], [36].

The set was developed only for scientific purposes, based on publicly available OSINT materials without access to private accounts, on the legal basis of Article 6 section 1 letter e or f and Article 89 of the GDPR. Minimisation was used: no storage of personal identifiers and source links, pseudonymisation by hashing with salt, removal of location and EXIF fields, retaining technical metadata only. Only metadata are publicly released and access to the content requires a formal application, which may be denied subject to increased re-identification risk.

The DFRW combines in the wild material with controlled generation and degradation variants, stresses the acoustic layer and AV synchronisation, and constitutes the basis for selecting sound characteristics and evaluating their stability in OOD protocols, considering uncertainty calibration and resistance to anti-forensic attacks [6], [10], [21], [36].

Zarejestrowany profil degradacji jest spójny z literaturą wskazującą, że nawet umiarkowana rekompresja i wieloetapowe transkodowanie powodują spadki AUC rzędu 10–25 pp oraz wzrost EER o 5–18 pp, szczególnie dla rodzin dyfuzyjnych oraz przy artefaktach temporalnych i filtrach AR [6], [32], [44], [53]. W audio istotne są: ograniczenie pasma przez kodeki stratne, normalizacja głośności, zmienny SNR, odpowiedź impulsowa pomieszczenia i nieliniowości toru A/D. W związku z powyższym metryki LSE C LSE D, koherencję fazową, stabilność formantów i mikrofluktuacje prozodyczne ujęto w metadanych jako czynniki stratyfikujące, wspierające selekcję cech odpornych na łańcuchy platformowe i ataki antyforensyczne, w tym *time stretch* z korekcją formantów, *pitch shift*, filtracje pasmowe i wtórną rejestrację [10], [34], [36].

Zbiór utworzono wyłącznie do celów naukowych na podstawie publicznie dostępnych materiałów OSINT bez dostępu do kont prywatnych, przy podstawie prawnej art. 6 ust. 1 lit. e lub f oraz art. 89 RODO. Zastosowano minimalizację: brak przechowywania identyfikatorów osobowych i linków źródłowych, pseudonimizację przez haszowanie z solą, usunięcie pól lokalizacyjnych i EXIF oraz zachowanie wyłącznie metadanych technicznych. Publicznie udostępniane są jedynie metadane, a dostęp do treści wymaga formalnego wniosku, który może zostać odrzucony przy podwyższonym ryzyku reidentyfikacji.

DFRW łączy materiał *in the wild* z kontrolowanymi wariantami generacyjnymi i degradacyjnymi, akcentuje warstwę akustyczną oraz synchronię AV i stanowi podstawę selekcji cech dźwiękowych oraz oceny ich stabilności w protokołach OOD, z uwzględnieniem kalibracji niepewności i odporności na ataki antyforensyczne [6], [10], [21], [36].

```
{
  "clip_id": "7c2b1f0e-5a5a-4f7a-8a4c-9b0a9f0a2f21",
  "sha256_content": "e7f5b5c9...d1a",
  "dataset_version": "DFRW-1.0",
  "source_platform": "YouTube",
  "source_url_hash": "SHA256:8b1e...f93",
  "license_category": "OSINT-fair-use",
  "legal_basis": "art.6.1.e RODO badania",
  "publisher_id_hash": "SHA256:1f3a...c0d",
  "modality": "AV",
  "label_authenticity": "synthetic",
  "manipulation_type": "B",
  "generation_family": "dyfuzja",
  "generator_model": "Stable Diffusion video deriver",
  "postproc_ops": ["rekodowanie", "filtr AR"],
  "width_px": 1280,
  "height_px": 720,
  "fps_nominal": 30.0,
  "codec_video": "H.264",
  "profile_level": "High@4.1",
  "container_brand": "isom",
  "bitrate_video_kbps": 1850,
  "gop_length": 48,
  "nal_stats": {"idr_interval": 48, "sps_count": 1, "pps_count": 1},
```

```

"colr_box": {"primaries": "BT.709", "transfer": "BT.709", "matrix": "BT.709"},
"pts_dts_consistency": "niespójne",
"encoder_fingerprint": "Lavf59.27.100 x264 core164",
"exif_present": false,
"integrity_flags": ["nietyпова kolejność atomów", "niespójność colr vs SPS"],
"audio_codec": "AAC",
"audio_sr_hz": 48000,
"audio_channels": 2,

// ciąg dalszy pliku JSON pominięty

```

Figure 1. Example of metadata record in JSON

Rycina 1. Przykład rekordu metadanych w JSON

Source: Own elaboration.

Źródło: Opracowanie własne.

Sound characteristics and synthetic speech artefact characteristics

This chapter defines the framework for extraction, normalisation and selection of acoustic descriptors and synthetic speech artefacts for the DFRW set. The purpose is to develop a set of characteristics with high stability and resistance to platform degradation, while retaining the forensic interpretability and replicability of procedures [6], [23], [59]. Stability was defined as the characteristic effectiveness decline of up to 15% in the degradation set. Robustness is simultaneous meeting of the low stability decrease and the low PR coefficient variance requirements across scenarios, with $p_{\text{real}} \leq 20\%$ and at least one criterion $\Delta p \geq 0.15$ or $PR \geq 1.5$. The degradation set included H.264 and H.265 recoding, 480–1440p resolution, platform operations and *re-upload*.

The unification was conducted in two tracks. The video track included transcoding up to MP4 and H.264 as per ITU T H.264 and ISO/IEC 14496 10 AVC, luminance and contrast normalisation, 30 fps setting and resolution scaling to 1280 × 720 px with fixed aspect ratio. Temporal sampling every 0.5 s and Intra coded frame extraction were used to capture spatio-temporal consistency and DCT quantisation codes [24], [63]. The audio path included demultiplexing to WAV 48 kHz, volume normalisation as per EBU R128 with ITU R BS.1770 measurement, active speech level standardisation as per ITU T P.56 and phoneme segmentation with an automatic adjustment tool. Unification restricts variance caused by platform chains and ensures the comparability of descriptors [26], [60–62].

The extraction frame includes five families of descriptors calculated in 20–30 ms frames with 50% overlap, with pre-sampling to 48 kHz and pre-emphasis of 0.97, unless the characteristic standard states otherwise. The characteristics were reported as aggregated statistics at the recording level, including the medial, quartiles and percentage of frames exceeding the anomaly threshold θ determined on real class.

The first family includes tonal and glottal characteristics. $F0$ was tracked using the YIN method with median filtering of

Cechy dźwiękowe oraz cechy artefaktów mowy syntetycznej

Rozdział definiuje ramę ekstrakcji, normalizacji i selekcji deskryptorów akustycznych oraz artefaktów mowy syntetycznej dla zbioru DFRW. Celem jest stworzenie zbioru cech o wysokiej stabilności i odporności na degradację platformowe przy zachowaniu interpretowalności forensycznej i replikowalności procedur [6], [23], [59]. Stabilność zdefiniowano jako spadek skuteczności cechy nieprzekraczający 15% w zestawie degradacji. Odporność oznacza jednocześnie spełnienie warunku niskiego spadku stabilności oraz niskiej wariancji współczynnika PR między scenariuszami, przy $p_{\text{real}} \leq 20\%$ oraz co najmniej jednym kryterium $\Delta p \geq 0.15$ lub $PR \geq 1.5$. Zestaw degradacji obejmował rekodowanie H.264 i H.265, skalowanie rozdzielczości 480–1440p, operacje platformowe oraz *re-upload*.

Unifikację przeprowadzono w dwóch torach. Tor wideo obejmował transkodowanie do MP4 i H.264 zgodnego z ITU T H.264 oraz ISO/IEC 14496 10 AVC, normalizację luminancji i kontrastu, ustalenie 30 fps oraz skalowanie do 1280 × 720 px z zachowaniem proporcji. Próbkowanie temporalne co 0,5 s i wydzielenie ramek I (ang. *Intra coded frame*) służyły uchwyceniu spójności przestrzenno-czasowej i śladów kwantyzacji DCT [24], [63]. Tor audio obejmował demultipleksowanie do WAV 48 kHz, normalizację głośności wg EBU R128 z pomiarem ITU R BS.1770, standaryzację poziomu mowy aktywnej wg ITU T P.56 oraz segmentację fonemową z użyciem automatycznego narzędzia dopasowującego. Unifikacja ogranicza wariancję wynikającą z łańcuchów platformowych i zapewnia porównywalność deskryptorów [26], [60–62].

Rama ekstrakcji obejmuje pięć rodzin deskryptorów obliczanych w ramach 20–30 ms z 50% nakładaniem, po przedpróbkowaniu do 48 kHz i z pre-emfazą 0,97, o ile standard cechy nie stanowi inaczej. Cechy raportowano jako statystyki zagregowane na poziomie nagrania, w tym medianę, kwartyle oraz odsetek ramek przekraczających próg anomalii θ wyznaczony na klasie rzeczywistej.

Pierwsza rodzina obejmuje cechy tonalne i glottalne. $F0$ śledzono metodą YIN z filtrowaniem medianowym outlierów w oknie

outliers in 150 ms window [64]. The $F0$ average and variance, change range and rate, jitter RAP and PPQ5, shimmer APQ3 and APQ5 and HNR as per de Krom were reported. Synthetic speech usually shows excessive regularity and overstated HNR, which reflects limitations of non-stationary larynx modelling [65–68].

The second family are cepstral and spectral characteristics. MFCC with delta and delta-delta, LFCC and CQCC were used, which are sensitive to non-physical energy distributions in high bands and vocoder filtering traces [69–71]. They were complemented with LPC, F1–F3 formant estimation with band widths, spectral inclination > 4 kHz and spectral flatness, which reveal spectrum smoothing [72–74].

The third family includes phase characteristics. MGD, phase cepstrum and instantaneous frequency smoothness measures were included, because phase is sensitive to phase relationship discontinuities and inconsistencies typical of reconstructions without a realistic voice source and tract model [75].

The fourth family includes energetic and dynamic characteristics. Spectral centroid, *roll off*, *flux* and HNR in temporal view, integrated LUFS volume and LRA volume range as per ITU R BS.1770 and EBU R128 were included. Synthetic signals often show lowered dynamics variance and excessively stationary energy outlines [60–62], [68].

The fifth family includes prosodic characteristics. The articulation rate, phoneme length variance, silence share and energy envelope were determined in 2–20 Hz bands, because TTS and VC models usually generate uniform prosody and narrowed pause distribution [76–77].

Artefacts specific for TTS and VC result from model approximations, vocoders and phase reconstruction, so their operationalisation includes phase, modulation, prosodic characteristics and harmonicity-noise relationships, resistant to lossy compression and background mix [78–80]. The transient indicator based on short-time energy kurtosis and phase coherence between harmonics were recorded. High kurtosis values and coherence drops indicate vocoder clicks and non-physical amplitude-phase relationships, also detectable by MGD and phase cepstrum [28], [75]. The $F0$ change range and rate, intonation outline entropy, pause length distributions and Mel scale outline modulation energy were measured, in which synthetic speech shows modulation complexity drops and excessive regularity [77], [81–82]. In addition, HNR, CPP and spectral inclination > 4 kHz were used, where CQCC and LFCC complemented phase and modulation characteristics as smoothing indicators and non-physical band filtering [67–68], [70–71], [83].

To capture multi-modal anomalies, acoustic characteristics were matched with lip and phoneme articulation synchronisation metrics, including LSE C and LSE D, and articulation rhythmic consistency indicators with $F0$ outline and energy envelope. Synchrony inconsistencies facilitate *audio driven* control and secondary registration effects [21], [50–51].

The selection was conducted without building classifiers. For each f characteristic, the effect direction was set based on the median difference between classes and the anomaly threshold θ was determined based on the *real* class only. For overstated effects in deepfake, $\theta = \text{medianareal} + 2 \cdot \text{MADreal}$ or the 95th

150 ms [64]. Raportowano średnią i wariancję $F0$, zakres i tempo zmian, jitter RAP i PPQ5, shimmer APQ3 i APQ5 oraz HNR wg de Kroma. Mowa syntetyczna wykazuje zwykle nadmierną regularność i zawyżony HNR, co odzwierciedla ograniczone modelowanie niestacjonarności krtani [65–68].

Druga rodzina to cechy cepstralne i widmowe. Zastosowano MFCC z deltami i delta-deltami, LFCC oraz CQCC, które są czułe na niefizyczne rozkłady energii w pasmach wysokich i ślady filtracji wokoderowej [69–71]. Uzupełniono je o LPC, estymację formantów F1–F3 z szerokościami pasm, nachylenie widmowe > 4 kHz oraz płaskość widmową (ang. *spectra flatness*) ujawniające wygładzanie widma [72–74].

Trzecia rodzina obejmuje cechy fazowe. Włączono MGD, cepstrum fazowe oraz miary płynności częstotliwości chwilowej, ponieważ faza jest wrażliwa na nieciągłości i niespójności relacji fazowych typowe dla rekonstrukcji bez realistycznego modelu źródła i traktu głosowego [75].

Czwarta rodzina obejmuje cechy energetyczno-dynamiczne. Raportowano centroidę spektralną (ang. *spectral centroid*), *roll off*, *flux* i HNR w ujęciu czasowym oraz głośność zintegrowaną LUFS i zakres głośności LRA zgodnie z ITU R BS.1770 i EBU R128. Sygnały syntetyczne często wykazują obniżoną wariancję dynamiki i nadmierną stacjonarność konturów energii [60–62], [68].

Piąta rodzina obejmuje cechy prozodyczne. Wyznaczano tempo artykulacji, wariancję długości fonemów, udział ciszy oraz obwiednię energii w pasmach 2–20 Hz, ponieważ modele TTS i VC generują zwykle jednorodną prozodię i pauzy o zawężonej dystrybucji [76–77].

Artefakty specyficzne dla TTS i VC wynikają z przybliżenia modeli, wokoderów i rekonstrukcji fazy, dlatego ich operacjonalizacja obejmuje cechy fazowe, modulacyjne, prozodyczne oraz relacje harmoniczność–szum, odporne na kompresję stratną i miks tła [78–80]. Rejestrowano wskaźnik transjentów oparty na kurtozie krótkoczasowej energii oraz koherencję fazową między harmonicznymi; wysokie wartości kurtozy i spadki koherencji wskazują na kliknięcia wokoderowe oraz niefizyczne relacje amplituda–faza, wykrywalne także przez MGD i cepstrum fazowe [28], [75]. Mierzono rozstęp i tempo zmian $F0$, entropię konturu intonacyjnego, rozkłady długości pauz oraz energię modulacyjną obwiedni w skalach Mel, gdzie mowa syntetyczna ujawnia spadek złożoności modulacji i nadmierną regularność [77], [81–82]. Użyto także HNR, CPP oraz nachylenia widmowego > 4 kHz, przy czym CQCC i LFCC uzupełniały cechy fazowe i modulacyjne jako wskaźniki wygładzania i niefizycznych filtracji pasmowych [67–68], [70–71], [83].

W celu uchwycenia anomalii multimodalnych zestawiono cechy akustyczne z metrykami spójności artykulacji ust i fonemów, w tym LSE C i LSE D, oraz wskaźnikami zgodności rytmiki artykulacyjnej z konturem $F0$ i obwiednią energii. Niespójności synchronii ujawniają sterowanie *audio driven* i efekty wtórnej rejestracji [21], [50–51].

Selekcję przeprowadzono bez budowy klasyfikatorów. Dla każdej cechy f ustalano kierunek efektu na podstawie różnicy median między klasami, a próg anomalii θ wyznaczano wyłącznie na klasie *real*. Dla efektów zawyżonych w deepfake stosowano $\theta = \text{medianareal} + 2 \cdot \text{MADreal}$ lub 95 percentyl klasy *real*, dla efektów

percentile of real class was used, for understated effects the 5th percentile was used. Then, p_df was determined as percentage of deepfake samples of $f \geq \theta$ and p_real as percentage of real samples of $f \geq \theta$, while difference measures were defined as $\Delta p = p_df - p_real$ and $PR = p_df / p_real$, with 95% CI using the percentile bootstrap method. Multiple comparisons were controlled using the Benjamini-Hochberg procedure with $q < 5\%$ [84–85].

Robustness standardisation was based on *robust z-score* in relation to the real class. Set entry criteria included validity after FDR correction and magnitude thresholds: $\Delta p \geq 0.15$ or $PR \geq 1.5$ with $p_real \leq 20\%$. The thresholds were justified empirically, because metric fluctuations arising from H.264 H.265 codec artefacts only reach 5–10 pp, while $\Delta p = 0.15$ is the margin differentiating generative anomalies from channel noise. The $PR \geq 1.5$ requirement corresponds to at least 50% increase in anomaly frequency in synthetic class and it is treated as the minimum practical effect magnitude. Characteristics with $p_df \geq 30\%$ and $p_real \leq 20\%$ were preferred. For sequential characteristics, the percentage of frames with $f \geq \theta$ was aggregated and the sample was considered as positive with the 10% frames threshold. The results were also reported in cross-sections by unification parameters to exclude apparent technical effects. The ranking was built by Δp and by preferring low p_real with high p_df in case of draws by PR . For each characteristic, the forensic mechanism, units and θ determination rule were reported to ensure full replicability.

The set included tonal and glottal characteristics: F_0 , jitter RAP, PPQ5, shimmer APQ3, APQ5, HNR [65–68]; cepstral and spectral characteristics: MFCC + Δ + $\Delta\Delta$, LFCC, CQCC, LPC, F1–F3 formants with bandwidths, spectral inclination > 4 kHz, spectral flatness [69–74]; phase characteristics: MGD, phase cepstrum, instantaneous frequency smoothness, phase coherence [75]; energetic-dynamic characteristics: centroid, roll-off, flux, HNR, LUFS, LRA, ASL as per ITU T P.56 [60–62], [68]; prosodic characteristics: articulation rate, phoneme length variance, silence share, F_0 outline change range and rate, energy envelope 2–20 Hz, outline entropy [76–77]; synthetic artefacts: CPP and variance, transient kurtosis, Mel scale envelope modulation spectrum, modulation depth, modulation correlation between bands, modulation inconsistency index, formant path smoothness measured by energy of the second derivative of F1–F3 and LSE C and LSE D for AV synchronisation [28], [81–83], [50–51].

Cepstral characteristics based on LFCC and CQCC, combined with phase and modulation descriptors, show increased stability after multiple recompression and with background noise and secondary recording, as long as channel normalisation and phoneme segmentation are retained [10], [28], [86]. Prosody and modulation remain distinguishable in *time-stretch* and *pitch-shift* scenarios with formant correction, however they are particularly sensitive to adaptive attacks optimised for detector loss functions, which justifies combining them with phase and multi-modal characteristics and regular OOD tests with controlled degradations and *re-upload* [21], [34], [36].

To match the frame with the current state of knowledge, the post-completion report was assumed as reference, focused on complementarity, in which the set is an independent layer of evidence, stable in degradations and useful for explaining the errors

zaniżonych 5 percentyl. Następnie wyznaczano p_df jako odsetek próbek deepfake z $f \geq \theta$ oraz p_real jako odsetek próbek real z $f \geq \theta$, a miary różnicowania definiowano jako $\Delta p = p_df - p_real$ oraz $PR = p_df / p_real$, z 95% CI metodą bootstrapu persentylowego. Wielokrotne porównania kontrolowano procedurą Benjamini Hochberg z $q < 5\%$ [84–85].

Standaryzację odpornościową oparto na *robust z-score* względem klasy real. Kryteria wejścia do zbioru obejmowały istotność po korekcie FDR oraz progi magnitude: $\Delta p \geq 0,15$ lub $PR \geq 1,5$ przy $p_real \leq 20\%$. Progi uzasadniono empirycznie, ponieważ fluktuacje metryk wynikające wyłącznie z artektów kodeka H.264 H.265 sięgają 5–10 pp, a $\Delta p = 0,15$ stanowi margines odróżniający anomalie generatywne od szumu kanałowego. Wymóg $PR \geq 1,5$ odpowiada co najmniej 50% wzrostowi częstości anomalii w klasie syntetycznej i jest traktowany jako minimalna praktyczna wielkość efektu. Preferowano cechy o $p_df \geq 30\%$ i $p_real \leq 20\%$. Dla cech sekwencyjnych agregowano odsetek ramek z $f \geq \theta$ i uznawano próbkę za pozytywną przy progu 10% ramek. Wyniki raportowano także w przekrojach po parametrach unifikacji, aby wykluczyć pozorne efekty techniczne. Ranking budowano według Δp , a przy remisach według PR , preferując niskie p_real przy wysokim p_df . Dla każdej cechy raportowano mechanizm forensyczny, jednostki i regułę wyznaczania θ , aby zapewnić pełną replikowalność.

Zestaw obejmował cechy tonalne i glottalne: F_0 , jitter RAP, PPQ5, shimmer APQ3, APQ5, HNR [65–68]; cechy cepstralne i widmowe: MFCC + Δ + $\Delta\Delta$, LFCC, CQCC, LPC, formanty F1–F3 z szerokościami pasm, nachylenie widmowe > 4 kHz, spectral flatness [69–74]; cechy fazowe: MGD, cepstrum fazowe, płynność częstotliwości chwilowej, koherencja fazowa [75]; cechy energetyczno-dynamiczne: centroid, roll-off, flux, HNR, LUFS, LRA, ASL wg ITU T P.56 [60–62], [68]; cechy prozodyczne: tempo artykulacji, wariancja długości fonemów, udział ciszy, zakres i tempo zmian konturu F_0 , obwiednia energii 2–20 Hz, entropia konturu [76–77]; artefakty syntetyczne: CPP i wariancja, kurtoza transjentów, widmo modulacyjne obwiedni w skalach Mel, głębokość modulacji, korelacja modulacyjna między pasmami, indeks niespójności modulacyjnej, gładkość torów formantowych mierzona energią drugiej pochodnej F1–F3 oraz LSE C i LSE D dla spójności AV [28], [81–83], [50–51].

Cechy cepstralne oparte na LFCC i CQCC, w połączeniu z deskryptorami fazowymi i modulacyjnymi, wykazują podwyższoną stabilność po wielokrotnej rekompresji oraz w obecności szumu tła i wtórnej rejestracji, o ile zachowana jest normalizacja kanałowa i segmentacja fonemowa [10], [28], [86]. Artefakty prozodyczne i modulacyjne pozostają rozróżnialne w scenariuszach *time-stretch* oraz *pitch-shift* z korekcją formantów, natomiast są szczególnie wrażliwe na ataki adaptacyjne optymalizowane względem funkcji strat detektora, co uzasadnia ich łączenie z cechami fazowymi i multimodalnymi oraz regularne testy OOD z kontrolowanymi degradacjami i *re-uploadem* [21], [34], [36].

W celu zestawienia ramy z aktualnym stanem wiedzy, jako punkt odniesienia przyjęto protokół porównawczy ukierunkowany na komplementarność, gdzie zbiór stanowi niezależną warstwę materiałów dowodowych stabilną w degradacjach i użyteczną do wyjaśniania błędów modeli uczonych w OOD. Jako punkt

of models trained in OOD. The specified reference point were *end to end* architectures, reported to ASVspoof, including RawNet2 and AASIST, and the *self supervised approach* with wav2vec 2.0 or WavLM embeddings and a simple classification head [30–31].

The evaluation was conducted by layer for quality and degradation in DFRW, including the number of recodings and presence of secondary recording. For the reference point, the reports include EER, pAUC in the low FPR area and uncertainty calibration measure, including ECE, often after temperature calibration, which meets the requirements of high responsibility environments [33]. For the set of characteristics, the reports included Δp and PR stability in the same sub-sets and pre-selection effectiveness with fixed FPR limitation, according to thresholds based on the real class. The complementarity benchmark included the analysis of error coverage, i.e. the percentage of reference point errors captured by the set as anomalies for at least one family of characteristics and reverse analysis, while matching characteristic family indications with channel degradation type. The framework defines the chain of unification, extraction and selection of the descriptors for synthetic speech and ensures interpretability and operational usability in real distribution. The following chapter presents the empirical results for DFRW with the ranking of characteristics meeting Δp and PR thresholds and the analysis of their stability in OOD scenarios.

Results of tests and selection on the DFRW set

The following presents the results of the analysis of the DeepFake RealWorld (DFRW) set described in the previous part of this study. This set includes 46,371 video clips, including 4,186 “wild” deepfakes and 42,185 synthetically generated or transformed variants. The primary classes of generation technologies, including *face swap*, *reenactment*, full-frame diffusion models and lips movement and mimic expressions synchronisation tools are included.

To replicate distribution conditions, the set includes recordings with varied duration (median: 12.4 s), resolution (480–1440p), number of recodings, degradation levels and scene types. In 77% of samples, an audio track is available, which enables an analysis of acoustic modality and audio-video synchronisation. This variety is the basis for the evaluation of the characteristics discussed in the chapter above and selection leading to the set of deepfake characteristics. Synthetic results for groups of characteristics are presented in column layout:

- group of characteristics / descriptors, name of characteristic or group of characteristics,
- p_{df} [%], percentage of values typical of deepfakes,
- p_{real} [%], percentage of values typical of authentic materials,
- Δp , $p_{df}-p_{real}$ frequency difference,
- PR, p_{df}/p_{real} prevalence coefficient,
- notes on stability, description of robustness or sensitivity to quality degradations.

Results for sound characteristics

The analysis includes the set of acoustic descriptors describing both tonal characteristics and spectral, phase, dynamic and

odniesienia wskazano architektury *end to end* raportowane na ASVspoof, w tym RawNet2 i AASIST, oraz *podjęcie self supervised* z embeddingami wav2vec 2.0 lub WavLM i prostą głowicą klasyfikacyjną [30–31].

Ocenę prowadzono warstwowo względem jakości i degradacji w DFRW, w tym liczby rekodowań i obecności wtórnej rejestracji. Dla punktu odniesienia raportuje się EER, pAUC w obszarze niskich FPR oraz miary kalibracji niepewności, w tym ECE często po kalibracji temperaturowej, co odpowiada wymaganiom środowisk wysokiej odpowiedzialności [33]. Dla zbioru cech raportowano stabilność Δp i PR w tych samych podzbiorach oraz skuteczność preselekcji przy stałym ograniczeniu FPR zgodnie z progami opartymi na klasie real. Benchmark komplementarności obejmował analizę pokrycia błędów, czyli odsetek błędów punktu odniesienia przechwyconych przez zbiór jako anomalie co najmniej jednej rodziny cech oraz analizę odwrotną, wraz z powiązaniem wskazań rodzin cech z typem degradacji kanałowej. Rama definiuje łańcuch unifikacji, ekstrakcji i selekcji deskryptorów dla mowy syntetycznej oraz zapewnia interpretowalność i użyteczność operacyjną w dystrybucji rzeczywistej. W rozdziale niżej przedstawiono wyniki empiryczne dla DFRW z rankingiem cech spełniających progi Δp i PR oraz analizą ich stabilności w scenariuszach OOD.

Wyniki Badań i Selekcji na zbiorze DFRW

Poniżej przedstawiono wyniki analizy zbioru DeepFake RealWorld (DFRW) opisanego w poprzedniej części niniejszej pracy. Zbiór ten obejmuje 46 371 klipów wideo, w tym 4 186 „dzikich” deepfake oraz 42 185 syntetycznie wygenerowanych lub przekształconych wariantów. Ujęto główne klasy technologii generacyjnych, w tym *face swap*, *reenactment*, pełnoklatkowe modele dyfuzyjne oraz narzędzia synchronizacji ruchu ust i ekspresji mimicznych.

Aby odwzorować warunki dystrybucji, w zbiorze występuje zróżnicowanie długości nagrań (mediana 12,4 s), rozdzielczości (480–1440p), liczby rekodowań, poziomów degradacji oraz typów scen. W 77% próbek dostępna jest ścieżka audio, co umożliwia analizę modalności akustycznej i synchronizacji audio-wideo. Różnorodność ta stanowi podstawę oceny cech omawianych w rozdziale wyżej oraz selekcji prowadzącej do zbioru cech deepfake. Wyniki syntetyczne dla grup cech przedstawiono w układzie kolumn:

- grupa cech / deskryptor, nazwa cechy lub grupy cech,
- p_{df} [%], procentowy udział wartości charakterystycznych dla deepfake,
- p_{real} [%], procentowy udział wartości charakterystycznych dla materiałów autentycznych,
- Δp , różnica częstości $p_{df}-p_{real}$,
- PR, współczynnik przewagi p_{df}/p_{real} ,
- uwagi o stabilności, opis odporności lub wrażliwości na degradację jakościowe.

Wyniki dla cech dźwiękowych

Analiza obejmowała zestaw deskryptorów akustycznych opisujących zarówno cechy tonalne, jak i parametry widmowe,

prosodic parameters. The average and variance of the primary frequency (F_0), jitter (RAP, PPQ5) and shimmer (APQ3, APQ5), as well as the harmonic-noise ratio (HNR) were included. With regards to spectral characteristics, MFCC cepstral coefficients with deltas and delta deltas, LFCC, CQCC, LPC vectors, F1–F3 formants and their bandwidth, spectral inclination above 4 kHz and measure of *spectral flatness* were used. The phase analysis was based on the modified spectrum of group delay, phase cepstrum and instantaneous frequency smoothness, and with regards to dynamics, descriptors were used, such as *spectral centroid*, *spectral roll-off*, *spectral flux*, active speech level, integrated LUFS volume and LRA dynamics range. Prosodic characteristics included the average articulation rate, phoneme length variance, silence share, F_0 curve change range and rate, divergence from typical intonation patterns and energy envelope in the 2–20 Hz band. The comparison of values obtained for authentic and synthetic recordings was presented in Table 1.

The results indicate significant differences between deepfake recordings and authentic materials. The primary frequency outline in 32% of deepfake recordings showed flattening ($\Delta p = 0.22$, $PR = 1.7$), jitter and shimmer parameters were lowered in 29% of samples ($\Delta p = 0.20$, $PR = 1.7$), which suggests the lack of natural voice micro-fluctuations. The HNR indicated unnaturally clear voice in 28% of synthetic recordings ($\Delta p = 0.18$, $PR = 1.6$). In the range of cepstral and spectral characteristics, MFCC and LFCC distribution anomalies occurred in 34% of samples ($\Delta p = 0.25$, $PR = 1.8$), while the CQCC characteristics revealed non-physical high frequency energy distributions in 30% of recordings ($\Delta p = 0.21$, $PR = 1.7$). The analysis of F1–F3 revealed the shift of resonances in 27% of synthetic materials ($\Delta p = 0.17$, $PR = 1.6$), however the *spectral flatness* and *spectral slope* measures confirmed spectrum flattening in 26% of recordings ($\Delta p = 0.16$, $PR = 1.6$). Phase characteristics revealed anomalies in 22% of deepfakes ($\Delta p = 0.14$, $PR = 1.6$), while the analysis of energy and dynamics showed variability in centroid, *roll-off* and *flux* variation in 25% of samples ($\Delta p = 0.15$, $PR = 1.6$). The reduced range of LUFS/LRA dynamics was recorded in 21% of recordings ($\Delta p = 0.13$, $PR = 1.5$). Prosodic indicators showed an unnatural articulation rate and silence duration in 23% of synthetic materials ($\Delta p = 0.14$, $PR = 1.6$), while the energy envelope in the 2–20 Hz band indicated the lack of natural micromodulations in 20% of samples ($\Delta p = 0.12$, $PR = 1.5$). These results unambiguously prove that deepfake recordings are characterised by voice parameters smoothing, reduced spectral variation and disrupted dynamics, which enables distinguishing them from authentic recordings.

The characteristic robustness analysis showed that cepstral coefficients MFCC, LFCC and CQCC, as well as the set of tonal voice parameters, such as F_0 jitter and shimmer, maintain high differentiation effectiveness even after applying lossy compression. Phase characteristics and energy dynamics measures showed moderate sensitivity to the presence of background noise, however intonation and prosodic parameters were subject to phoneme segmentation errors and required recordings with proper time and articulation quality.

fazowe, dynamiczne oraz prozodyczne. Uwzględniono średnią i wariancję częstotliwości podstawowej (F_0), miary jittera (RAP, PPQ5) oraz shimmera (APQ3, APQ5), a także współczynnik harmoniczo-szumowy (HNR). W zakresie charakterystyki widmowej zastosowano współczynniki cepstralne MFCC z deltami i deltadeltami, LFCC, CQCC, wektory LPC, formanty F1–F3 i ich szerokości pasm, nachylenie widmowe powyżej 4 kHz oraz miarę *spectral flatness*. Analizę fazową oparto na zmodyfikowanym widmie opóźnienia grupowego, cepstrum fazowym i płynności częstotliwości chwilowej, a w zakresie dynamiki wykorzystano takie deskryptory jak *spectral centroid*, *spectral roll-off*, *spectral flux*, poziom mowy aktywnej ASL (ang. *active speech level*), zintegrowana głośność LUFS i zakres dynamiki LRA. Cechy prozodyczne obejmowały średnie tempo artykulacji, wariancję długości fonemów, udział ciszy, zakres i tempo zmian krzywej F_0 , dywergencję od typowych wzorców intonacyjnych oraz obwiednię energii w paśmie 2–20 Hz. Porównanie wartości uzyskanych dla nagrań autentycznych i syntetycznych przedstawiono w tabeli 1.

Wyniki wskazują na istotne różnice pomiędzy nagraniami typu deepfake a materiałami autentycznymi. Kontur częstotliwości podstawowej w 32% nagrań deepfake wykazywał wygładzenie ($\Delta p = 0,22$, $PR = 1,7$), a parametry jittera i shimmera były obniżone w 29% próbek ($\Delta p = 0,20$, $PR = 1,7$), co sugeruje brak naturalnych mikrofluktuacji głosu. Współczynnik HNR wskazywał na nienaturalnie czysty głos w 28% nagrań syntetycznych ($\Delta p = 0,18$, $PR = 1,6$). W zakresie cech cepstralnych i widmowych anomalie rozkładu współczynników MFCC i LFCC wystąpiły w 34% próbek ($\Delta p = 0,25$, $PR = 1,8$), a charakterystyka CQCC ujawniła niefizyczne rozkłady energii wysokoczęstotliwościowych w 30% nagrań ($\Delta p = 0,21$, $PR = 1,7$). Analiza formantów F1–F3 wykazała przesunięcia rezonansów w 27% materiałów syntetycznych ($\Delta p = 0,17$, $PR = 1,6$), natomiast miary *spectral flatness* (współczynnik płaskości widma) i *spectral slope* (współczynnik nachylenia widma amplitudowego) potwierdziły wygładzenie widma w 26% nagrań ($\Delta p = 0,16$, $PR = 1,6$). Cechy fazowe ujawniły anomalie w 22% deepfake ($\Delta p = 0,14$, $PR = 1,6$), a analiza energii i dynamiki wykazała spadek zmienności wskaźników centroid, *roll-off* oraz *flux* w 25% próbek ($\Delta p = 0,15$, $PR = 1,6$). Zmniejszony zakres dynamiki LUFS/LRA odnotowano w 21% nagrań ($\Delta p = 0,13$, $PR = 1,5$). Wskaźniki prozodyczne wykazały nienaturalne tempo artykulacji i długość okresów ciszy w 23% materiałów syntetycznych ($\Delta p = 0,14$, $PR = 1,6$), a obwiednia energii w paśmie 2–20 Hz wskazała na brak naturalnych mikromodulacji w 20% próbek ($\Delta p = 0,12$, $PR = 1,5$). Wyniki te jednoznacznie dowodzą, że nagrania typu deepfake charakteryzują się wygładzeniem parametrów głosu, zmniejszoną zmiennością spektralną oraz zaburzoną dynamiką, co pozwala odróżniać je od nagrań autentycznych.

Analiza odporności cech wykazała, że współczynniki cepstralne MFCC, LFCC oraz CQCC, a także zestaw tonalnych parametrów głosu, takich jak F_0 jitter i shimmer, zachowują wysoką skuteczność rozróżniania nawet po zastosowaniu stratnej kompresji. Cechy fazowe oraz miary dynamiki energetycznej wykazały umiarkowaną wrażliwość na obecność szumów tła, natomiast parametry intonacyjne i prozodyczne były podatne na błędy segmentacji fonemów i wymagały nagrań o odpowiedniej jakości czasowej i artykulacyjnej.

Table 1. Effectiveness and stability of acoustic speech descriptors in differentiating real and authentic recordings (DFRW set; values indicating the highest discriminatory force)

Tabela 1. Skuteczność i stabilność deskryptorów akustycznych mowy w różnicowaniu nagrań rzeczywistych i syntetycznych (zbiór DFRW; wartości wskazujące na największą siłę dyskryminacyjną)

Group of characteristics / descriptor / Grupa cech / deskryptor	p_df *[%]	p_real ** [%]	Δp ***	PR ****	Evaluation of stability and notes / Ocena stabilności i uwagi
MFCC / LFCC (cepstral characteristics) / MFCC / LFCC (cechy cepstralne)	55	30	0.25	1.80	Very stable, effective in different domains / Bardzo stabilne, skuteczne w różnych domenach
F0 (average / variability) / F0 (średnia / zmienność)	42	20	0.22	1.70	Stable, resistant to different speaking styles / Stabilne, odporne na różne style mówienia
CQCC (high frequency energy) / CQCC (energia wysokich częstotliwości)	51	30	0.21	1.70	Stable, good differentiation of synthesis / Stabilne, dobrze rozróżniające syntezę
Jitter / Shimmer	40	20	0.20	1.70	Stable, immune to lossy compression / Stabilne, niewrażliwe na kompresję stratną
HNR (harmonicity) / HNR (harmoniczność)	38	20	0.18	1.60	Stable, in particular for synthetic voices / Stabilne, szczególnie dla głosów syntetycznych
F1–F3 formants / Formanty F1–F3	37	20	0.17	1.60	Stable, requires precise analysis of formants / Stabilne, wymaga precyzyjnej analizy formantów
Spectral flatness / slope	36	20	0.16	1.60	Moderately stable, sensitive to noise / Umiarkowanie stabilne, wrażliwe na szumy
Centroid / roll-off / flux	35	20	0.15	1.60	Stable, differentiate smoothed spectra / Stabilne, różnicując wygładzone widma
Phase characteristics (group delay) / Cechy fazowe (grupowe opóźnienie)	34	20	0.14	1.60	Moderately stable / Umiarkowanie stabilne
Articulation rate and silence share / Tempo artykulacji i udział ciszy	34	20	0.14	1.60	Moderately stable, requires analysis of phonemes / Umiarkowanie stabilne, wymaga analizy fonemów
LUFS / LRA (speech dynamics) / LUFS / LRA (dynamika mowy)	33	20	0.13	1.50	Sensitive to distribution and compression / Wrażliwe na dystrybucję i kompresję
Energy envelope 2–20 Hz / Obwiednia energii 2–20 Hz	32	20	0.12	1.50	Sensitive to noise in recordings / Wrażliwe na zakłócenia nagrań

* p_df: percentage of deepfake samples showing anomaly (excess of θ threshold) / * p_df: odsetek próbek deepfake wykazujących anomalię (przekroczenie progu θ);

** p_real: percentage of real samples showing anomaly (*false positive rate* for the given characteristic) / ** p_real: odsetek próbek rzeczywistych wykazujących anomalię (*false positive rate* dla danej cechy);

*** Δp : frequency difference ($p_{df} - p_{real}$), absolute effect magnitude measure / *** Δp : różnica częstości ($p_{df} - p_{real}$), miara siły efektu bezwzględnego;

**** PR (Prevalence Ratio): prevalence coefficient (p_{df} / p_{real}), relative effect magnitude measure / **** PR (Prevalence Ratio): współczynnik przewagi (p_{df} / p_{real}), miara siły efektu względnego.

Values in bold designate the characteristic with the highest stability and effectiveness ($\Delta p \geq 0.22$) / Wartości pogrubione oznaczają cechy o najwyższej stabilności i skuteczności ($\Delta p \geq 0.22$)

Source: Own elaboration.

Źródło: Opracowanie własne.

Results for characteristics of synthetic speech artefacts

The analysis covered a set of acoustic descriptors, of which the purpose was to capture subtle properties typical of synthetically generated speech. Phase and vocoder characteristics, including modified group delay (MGD), phase cepstrum, index of phase coherence between harmonics and transient index based on short-time energy kurtosis were used. Harmonicity-noise measures, such as CPP (Cepstral Peak Prominence) with its variance and the HNR indicator in de Krom's version, were used as well. Modulation characteristics were modulated, including the Mel scale envelope modulation spectrum, modulation depth

Wyniki dla cech artefaktów mowy syntetycznej

Analiza objęła zestaw deskryptorów akustycznych, których celem było uchwycenie subtelnych właściwości charakterystycznych dla mowy generowanej syntetycznie. Wykorzystano cechy fazowe i wokoderowe, w tym zmodyfikowane widmo opóźnienia grupowego (MGD), cepstrum fazowe, indeks koherencji fazowej między harmonicznymi oraz wskaźnik transjentów oparty na kurtocie energii krótkoczasowej. Zastosowano także miary harmoniczności–szum, takie jak CPP (ang. *Cepstral Peak Prominence*) wraz z jego wariancją oraz wskaźnik HNR w wersji de Kroma. Oceniono cechy modulacyjne, obejmujące widmo modulacyjne

indicator and modulation correlation between bands and modulation inconsistency index. The study included prosodic characteristics, including the primary frequency change range and rate ($F0$), pause duration distribution and formant track smoothness, assessed based on the energy of the second derivative of $F1-F3$. The analysis was complemented by cepstral characteristics, represented by Constant Q Cepstral Coefficients (CQCC) and Linear Frequency Cepstral Coefficients (LFCC), reported in relation to phonetic segments. A comparison of the values of these descriptors between authentic recordings and synthetic recordings were presented in Table 5.1b.

The results obtained show that deepfake recordings are characterised by a series of typical anomalies that differentiate them from natural speech. Phase and vocoder properties represented by MGD and phase cepstrum revealed unnatural phase profiles in 33% of synthetic samples ($\Delta p = 0.20$, $PR = 1.5$), while the phase index showed a drop of synchronisation in 31% of such recordings ($\Delta p = 0.18$, $PR = 1.5$). The CPP indicator with its variance indicated disrupted harmonicity in 35% of cases ($\Delta p = 0.22$, $PR = 1.6$), while the HNR coefficient confirmed unnaturally clear voice in 30% of deepfakes ($\Delta p = 0.17$, $PR = 1.5$). The analysis of the modulation spectrum showed envelope smoothing in 36% of synthetic materials ($\Delta p = 0.23$, $PR = 1.7$), while modulation correlation between bands revealed non-physical shifts in 28% of cases ($\Delta p = 0.16$, $PR = 1.5$). Prosodic indicators confirmed restricted voice expression, which showed by reduced $F0$ change range and rate in 29% of deepfakes ($\Delta p = 0.17$, $PR = 1.5$) and unnatural pause distribution in 27% of such recordings ($\Delta p = 0.15$, $PR = 1.5$). In addition, formant track smoothness, indicating the lack of coarticulation, was identified as anomaly in 26% of samples ($\Delta p = 0.14$, $PR = 1.5$). Cepstral parameters CQCC and LFCC showed non-physical band filter characteristics in 32% of deepfake recordings ($\Delta p = 0.19$, $PR = 1.6$), while vocoder transient indicators identified the occurrence of typical clicks in 24% of samples ($\Delta p = 0.12$, $PR = 1.4$). These recordings confirm that synthetic speech is characterised by altered phase and harmonic structure, as well as distortions in the modulation and prosody range, which differentiates them from authentic recordings. The assessment of the robustness of characteristics showed that parameters, such as CPP, cepstral CQCC/LFCC sets and modulation spectrum, retain high effectiveness of differentiation even after lossy compression, which makes them particularly useful in low transmission quality conditions. Phase characteristics, including MGD and phase coherence, show moderate sensitivity to background noise and low signal to noise ratio, however vocoder transient indicators and pause rhythm characteristics are subject to errors arising from inaccurate phonetic segmentation, which reduces their application in materials with lower recording quality.

obwiedni w skalach Mel, wskaźnik głębokości modulacji, korelację modulacyjną między pasmami oraz indeks niespójności modulacyjnej. W badaniu uwzględniono cechy prozodyczne, w tym rozstęp i tempo zmian częstotliwości podstawowej ($F0$), rozkłady długości pauz oraz gładkość torów formantowych ocenianą na podstawie energii drugiej pochodnej $F1-F3$. Uzupełnieniem analizy były cechy cepstralne, reprezentowane przez Constant Q Cepstral Coefficients (CQCC) oraz Linear Frequency Cepstral Coefficients (LFCC), raportowane względem segmentów fonetycznych. Porównanie wartości tych deskryptorów pomiędzy nagraniami autentycznymi a syntetycznymi przedstawiono w tabeli 5.1b.

Uzyskane wyniki wskazują, że nagrania typu deepfake cechują się szeregiem charakterystycznych anomalii odróżniających je od mowy naturalnej. Właściwości fazowe i wokoderowe reprezentowane przez MGD oraz cepstrum fazowe ujawniły nienaturalne profile fazy w 33% próbek syntetycznych ($\Delta p = 0.20$, $PR = 1.5$), a indeks koherencji fazowej wykazał spadek spójności w 31% takich nagrań ($\Delta p = 0.18$, $PR = 1.5$). Wskaźnik CPP wraz z jego wariancją wskazał na zaburzoną harmoniczną w 35% przypadków ($\Delta p = 0.22$, $PR = 1.6$), zaś współczynnik HNR potwierdził nienaturalnie czysty głos w 30% deepfake ($\Delta p = 0.17$, $PR = 1.5$). Analiza widma modulacyjnego wykazała wygładzenie obwiedni w 36% materiałów syntetycznych ($\Delta p = 0.23$, $PR = 1.7$), a korelacja modulacyjna między pasmami ujawniła нефизyczne przesunięcia w 28% przypadków ($\Delta p = 0.16$, $PR = 1.5$). Wskaźniki prozodyczne potwierdziły ograniczoną ekspresję głosu, co przejawiało się zmniejszonym rozstępem i tempem zmian $F0$ w 29% deepfake ($\Delta p = 0.17$, $PR = 1.5$) oraz nienaturalnym rozkładem pauz w 27% takich nagrań ($\Delta p = 0.15$, $PR = 1.5$). Dodatkowo gładkość torów formantowych, wskazująca na brak koartykulacji, została zidentyfikowana jako anomalia w 26% próbek ($\Delta p = 0.14$, $PR = 1.5$). Parametry cepstralne CQCC i LFCC wykazały нефизyczne charakterystyki filtrów pasmowych w 32% nagrań deepfake ($\Delta p = 0.19$, $PR = 1.6$), a wskaźniki transjentów wokoderowych zidentyfikowały występowanie charakterystycznych kliknięć w 24% próbek ($\Delta p = 0.12$, $PR = 1.4$). Wyniki te potwierdzają, że mowa syntetyczna charakteryzuje się zarówno zmienioną strukturą fazową i harmoniczną, jak i zaburzeniami w zakresie modulacji i prozodii, co odróżnia ją od nagrań autentycznych. Ocena odporności cech wskazała, że parametry takie jak CPP, zestawy cepstralne CQCC/LFCC oraz widmo modulacyjne zachowują wysoką skuteczność rozróżniania nawet po zastosowaniu stratnej kompresji, co czyni je szczególnie przydatnymi w warunkach niskiej jakości transmisji. Cechy fazowe, w tym MGD i koherencja fazowa, wykazują umiarkowaną wrażliwość na szum tła i niski stosunek sygnału do szumu, natomiast wskaźniki transjentów wokoderowych oraz cechy rytmu pauz są podatne na błędy wynikające z niedokładnej segmentacji fonetycznej, co ogranicza ich zastosowanie w materiałach o niższej jakości nagrania.

Table 2. Effectiveness and stability of vocal and modulation artefact descriptors (characteristics with the highest resistance to quality degradations)
Tabela 2. Skuteczność i stabilność deskryptorów artefaktów wokalnych i modulacyjnych (cechy o najwyższej odporności na degradację jakościowe)

Characteristic / group of descriptors / Cecha / grupa deskryptorów	p_df *[%]	p_real [%]	Δp	PR	Notes on stability and operating usability / Uwagi o stabilności i przydatności operacyjnej
Modulation spectrum + depth / Widmo modulacyjne + głębokość	36	13	0.23	1.7	Very stable, sensitive to prosody smoothing / Bardzo stabilne, czułe na wygładzenie prozodyki
Cepstral Peak Prominence (CPP)	35	13	0.22	1.6	Stable, shows harmonicity anomalies / Stabilne, wskazuje anomalie harmonicznosci
MGD** + phase cepstrum / MGD** + cepstrum fazowe	33	13	0.20	1.5	Stable, good for clicks and phase discontinuities / Stabilne, dobre dla klików i nieciągłości fazy
CQCC / LFCC (band filters) / CQCC / LFCC (filtry pasmowe)	32	13	0.19	1.6	Very stable, resistant to compression / Bardzo stabilne, odporne na kompresję
Phase coherence index / Indeks koherencji fazowej	31	13	0.18	1.5	Moderately stable, sensitive to low SNR / Umiarkowanie stabilne, wrażliwe na niski SNR
F0 change range and rate / Rozstęp i tempo zmian F0	29	12	0.17	1.5	Stable, sensitive to restricted expression / Stabilne, czułe na ograniczoną ekspresję
HNR (source clarity) / HNR (czystość źródła)	30	13	0.17	1.5	Stable, good differentiation of vocoders / Stabilne, dobrze rozróżnia wokodery
Band modulation correlation / Korelacja modulacyjna pasm	28	12	0.16	1.5	Stable, shows band filtering anomalies / Stabilne, ujawnia anomalie filtracji pasmowej
Pause distributions (rhythmics) / Rozkłady pauz (rytmika)	27	12	0.15	1.5	Moderately stable, requires alignment tool / Umiarkowanie stabilne, wymaga narzędzia dopasowującego
Formant track smoothness / Gładkość torów formantowych	26	12	0.14	1.5	Stable, shows the lack of coarticulation / Stabilne, ujawnia brak koartykulacji
Vocoder transients / Transjenty wokoderowe	24	12	0.12	1.4	Sensitive to background noise / Wrażliwe na zakłócenia tła

*p_df, p_real, Δp , PR: definitions analogical to Table 1 / *p_df, p_real, Δp , PR: definicje analogiczne jak w Tabeli 1;

**MGD: *Modified Group Delay* / **MGD: *Modified Group Delay* (zmodyfikowane widmo opóźnienia grupowego);

***SNR: *Signal-to-Noise Ratio* / ***SNR: *Signal-to-Noise Ratio* (stosunek sygnału do szumu).

The values in bold indicate the characteristics recommended for the primary detection layer for the highest effectiveness parameters ($\Delta p \geq 0.22$) / Wartości pogrubione wskazują cechy rekomendowane do warstwy podstawowej detekcji ze względu na najwyższe parametry skuteczności ($\Delta p \geq 0.22$).

Source: Own elaboration.

Źródło: Opracowanie własne.

Table 3. Average effectiveness and stability indicators of groups of characteristics (p_df, p_real, Δp , PR) with variances and notes on their resistance to degradations

Tabela 3. Średnie wskaźniki skuteczności i stabilności grup cech (p_df, p_real, Δp , PR) wraz z wariancjami oraz uwagami dotyczącymi ich odporności na degradację

Group of characteristics / Grupa cech	Average p_df [%] / Średnie p_df [%]	Average p_real [%] / Średnie p_real [%]	Average Δp / Średnia Δp	Average PR / Średni PR	Variance p_df / Wariancja p_df	Variance p_real / Wariancja p_real	Variance Δp / Wariancja Δp	Variance PR / Wariancja PR	General notes on stability / Uwagi ogólne o stabilności
Results for sound characteristics / Wyniki dla cech dźwiękowych	38.92	21.67	0.17	1.62	47.91	13.89	0.0015	0.0069	Mostly stable; sensitivity: compression, noise / Głównie stabilne; wrażliwości: kompresja, szum
Results for characteristics of synthetic speech artefacts / Wyniki dla cech artefaktów mowy syntetycznej	30.09	12.55	0.18	1.53	12.81	0.25	0.0010	0.0056	Mostly stable; sensitivity: compression, SNR / Głównie stabilne; wrażliwości: kompresja, SNR

Source: Own elaboration.

Źródło: Opracowanie własne.

Process of selection of characteristics for the set

The selection of characteristics was conducted according to the methodology presented in the previous chapter, only based on the analysis of the frequency of deviations from the standard determined on the real recordings class, without using classifiers. For each characteristic, the effect direction was determined based on the median difference between authentic and synthetic recordings, while the anomaly threshold θ was determined in relation to the real class only. For characteristics overstated in deepfakes, $\theta = \text{median_real} + 2 \cdot \text{MAD_real}$ or $95.\text{percentile_real}$ was used, while for understated characteristics the threshold was set at the 5th percentile of the real class, ensuring the interpretability of thresholds as deviations from natural speech behaviour.

Sequential characteristics were aggregated to the recording level as the percentage of frames meeting the $f \geq \theta$ condition. A sample was considered as positive upon exceeding 10% of frames. For each characteristic, p_{df} and p_{real} values were determined and the differentiation capability was evaluated using $\Delta p = p_{df} - p_{real}$ and $PR = p_{df}/p_{real}$ with 95% CI, calculated using the percentile bootstrap method. The correction of multiple comparisons was conducted using the Benjamini–Hochberg procedure with $q < 5\%$ [84–85].

The characteristics that met jointly the validity requirements after FDR correction, $\Delta p \geq 0.15$ or $PR \geq 1.5$ and $p_{real} \leq 20\%$, were qualified to the set. These thresholds eliminate descriptors sensitive to typical platform degradations, while leaving characteristics with high differentiation force and low risk of false alarms. Characteristics with $p_{df} \geq 30\%$ and $p_{real} \leq 20\%$ were preferred. The application of this procedure enabled selecting the representative characteristics from the families defined in the previous chapter.

Complementarity benchmark

The purpose of the benchmark was to quantitatively check if the set of characteristics constitutes an independent evidence layer in channel degradation and distribution shift conditions and if it can support trained detectors by identifying stable anomalies. Trained detectors played the role of the decision layer, while the set was the role of the evidence layer with threshold defined based on the *real* class, which enables auditing and monitoring in continuous evaluation mode.

The comparisons were completed separately for three quality levels in DFRW. As reference point, RawNet2 and AASIST were assumed as *end to end* architecture and the WavLM model with MFA segmentation as representative of the self supervised approach. For the reference point, EER, pAUC with FPR $\leq 5\%$ and ECE after temperature calibration were reported. For the set, the pre-selection effectiveness was reported with the same FPR limitation and Δp and PR stability in qualitative sections.

The complementarity defined by error coverage of reference points with FPR = 5%. COV_FN is the percentage of the false negative decisions of the reference point marked by the set as anomalous, while COV_FP is the analogical percentage of false positive decisions. The results summarised in Table 4 show that with the increase of degradation, the effectiveness and calibration of the reference point deteriorate, while the set of characteristics retains relatively stable parameters. For RawNet2, pAUC drops

Proces selekcji cech do zbioru

Selekcję cech przeprowadzono zgodnie z metodyką przedstawioną w rozdziale wyżej, wyłącznie na podstawie analizy częstości odstępstw od normy wyznaczonej na klasie nagrań rzeczywistych, bez użycia klasyfikatorów. Dla każdej cechy określano kierunek efektu na podstawie różnicy median między nagraniami autentycznymi i syntetycznymi, a próg anomalii θ definiowano wyłącznie względem klasy real. Dla cech zawyżonych w deepfake stosowano $\theta = \text{mediana_real} + 2 \cdot \text{MAD_real}$ lub $95.\text{percentyl_real}$, natomiast dla cech zaniżonych próg ustalano na poziomie 5. percentyla klasy real, co zapewniało interpretowalność progów jako odchyień od zachowania mowy naturalnej.

Cechy sekwencyjne agregowano do poziomu nagrania jako odsetek klatek spełniających warunek $f \geq \theta$, uznając próbkę za pozytywną przy przekroczeniu 10% klatek. Dla każdej cechy wyznaczano p_{df} oraz p_{real} , a zdolność różnicowania oceniano za pomocą $\Delta p = p_{df} - p_{real}$ i $PR = p_{df}/p_{real}$ wraz z 95% CI obliczanymi metodą bootstrapu percentylowego. Korekcję wielokrotnych porównań realizowano procedurą Benjamini–Hochberg z $q < 5\%$ [84–85].

Do zbioru kwalifikowano cechy spełniające łącznie warunki istotności po korekcie FDR, $\Delta p \geq 0.15$ lub $PR \geq 1.5$ oraz $p_{real} \leq 20\%$. Progi te eliminują deskryptory wrażliwe na typowe degradacje platformowe, pozostawiając cechy o wysokiej sile różnicowania i niskim ryzyku fałszywych alarmów. Preferowano cechy o $p_{df} \geq 30\%$ i $p_{real} \leq 20\%$. Zastosowanie tej procedury pozwoliło wybrać reprezentatywne cechy spośród rodzin zdefiniowanych we wcześniejszym rozdziale.

Benchmark komplementarności

Celem benchmarku było ilościowe sprawdzenie, czy zbiór cech stanowi niezależną warstwę dowodową w warunkach degradacji kanałowych i przesunięć dystrybucji oraz czy może wspierać detektory uczone poprzez identyfikację stabilnych anomalii. Detektory uczone pełniły rolę warstwy decyzyjnej, natomiast zbiór rolę warstwy dowodowej z progami definiowanymi wyłącznie na klasie *real*, co umożliwia audytowalność i monitorowanie dryfu w trybie ewaluacji ciągłej.

Porównania przeprowadzono osobno dla trzech poziomów jakości w DFRW. Jako punkt odniesienia przyjęto RawNet2 i AASIST jako architektury *end to end* oraz model WavLM z segmentacją MFA jako reprezentanta podejścia self supervised. Dla punktu odniesienia raportowano EER, pAUC przy FPR $\leq 5\%$ oraz ECE po kalibracji temperaturowej. Dla zbioru raportowano skuteczność preselekcji przy tym samym ograniczeniu FPR oraz stabilność Δp i PR w przekrojach jakościowych.

Komplementarność zdefiniowano poprzez pokrycie błędów punktu odniesienia przy FPR = 5%. COV_FN oznacza odsetek fałszywie negatywnych decyzji punktu odniesienia oznaczonych przez zbiór jako anomalne, a COV_FP analogiczny odsetek dla fałszywie pozytywnych decyzji. Wyniki zestawione w tabeli 4 pokazują, że wraz ze wzrostem degradacji skuteczność i kalibracja punktu odniesienia ulegają pogorszeniu, podczas gdy zbiór cech zachowuje relatywnie stabilne parametry. Dla RawNet2

from 0.73 to 0.62 and ECE increases from 8.0% to 12.0%. For AASIST, pAUC drops from 0.76 to 0.65 and ECE increases from 7.0% to 11.0%. The WavLM+MFA model retains the highest effectiveness, but also deteriorates qualitatively, pAUC from 0.992 to 0.93 and ECE from 1.5% to 4.5%. Contrary, the set of characteristics retains stability in the entire quality range, pAUC from 0.85 to 0.81 and ECE from 2.2% to 2.8%, which confirms its predictability and usability in OOD scenarios.

pAUC spada z 0,73 do 0,62, a ECE rośnie z 8,0% do 12,0%. Dla AASIST obserwuje się spadek pAUC z 0,76 do 0,65 oraz wzrost ECE z 7,0% do 11,0%. Model WavLM+MFA utrzymuje najwyższą skuteczność, lecz także degradowa się jakościowo, pAUC z 0,992 do 0,93 oraz ECE z 1,5% do 4,5%. W przeciwieństwie do tego zbiór cech zachowuje stabilność w całym zakresie jakości, pAUC od 0,85 do 0,81 oraz ECE od 2,2% do 2,8%, co potwierdza jego przewidywalność i użyteczność w scenariuszach OOD.

Table 4. Comparison of the effectiveness of the reference point with the set of characteristics with FPR = 5%, using metrics EER, pAUC and ECE
Tabela 4. Porównanie skuteczności punktu odniesienia ze zbiorem cech przy FPR = 5%, z wykorzystaniem metryk EER, pAUC i ECE

Degradation level* / Poziom degradacji*	Model / Method / Model / Metoda	EER [%] ↓	pAUC (FPR < 5%) ↑	ECE [%] ↓	COVFN ** [%] ↑	COVFP [%] ↑
High quality / Wysoka jakość	RawNet2	24.0	0.73	8.0	28	32
	AASIST	22.0	0.76	7.0	30	33
	WavLM + MFA	3.2	0.992	1.5	18	40
	Set of characteristics (proposed) / Zbiór cech (proponowany)	14.5	0.85	2.2	—	—
Medium quality / Średnia jakość	RawNet2	29.0	0.68	10.0	42	38
	AASIST	26.0	0.71	9.0	44	39
	WavLM + MFA	5.2	0.975	2.6	26	46
	Set of characteristics (proposed) / Zbiór cech (proponowany)	15.2	0.84	2.4	—	—
High degradation / Wysoka degradacja	RawNet2	35.0	0.62	12.0	55	44
	AASIST	31.0	0.65	11.0	57	45
	WavLM + MFA	8.0	0.93	4.5	34	52
	Set of characteristics (proposed) / Zbiór cech (proponowany)	16.5	0.81	2.8	—	—

*The best results are in bold, while COV >50% values show a significant method complementarity / *Pogrubienie oznacza najlepsze wyniki, a wartości COV >50% wskazują na istotną komplementarność metod.

**COV_FN/FP indicators determine the percentage of reference points repaired by the set / **Wskaźniki COV_FN/FP określają odsetek błędów punktu odniesienia naprawionych przez zbiór.

Source: Own elaboration.

Źródło: Opracowanie własne.

At this point, the set provides effective coverage of reference point errors: for high degradation it is 49% for false negatives and 47% for positives (48% in total), while for high quality it is 25% and 35%, respectively (30% in total). A difficulty increase increases the role of the evidence layer, while reducing the effectiveness of classifiers. Figure 2 matches the pAUC drop of the reference point with stable pAUC, Δp and PR of the set. This discrepancy confirms complementarity: the set as interpretable evidence layer supports drift monitoring and continuous validation.

W tym punkcie zbiór skutecznie pokrywa błędy punktu odniesienia: dla wysokiej degradacji to 49% dla fałszywych negatywów i 47% dla pozytywów (łącznie 48%), a dla wysokiej jakości odpowiednio 25% i 35% (łącznie 30%). Wzrost trudności zwiększa rolę warstwy materiałów dowodowych przy spadku skuteczności klasyfikatorów. Na rycinie 2 zestawiono spadek pAUC punktu odniesienia ze stabilnym pAUC, Δp i PR zbioru. Ta rozbieżność potwierdza komplementarność: zbiór jako interpretowalna warstwa materiałów dowodowych wspiera monitorowanie dryfu i walidację ciągłą.

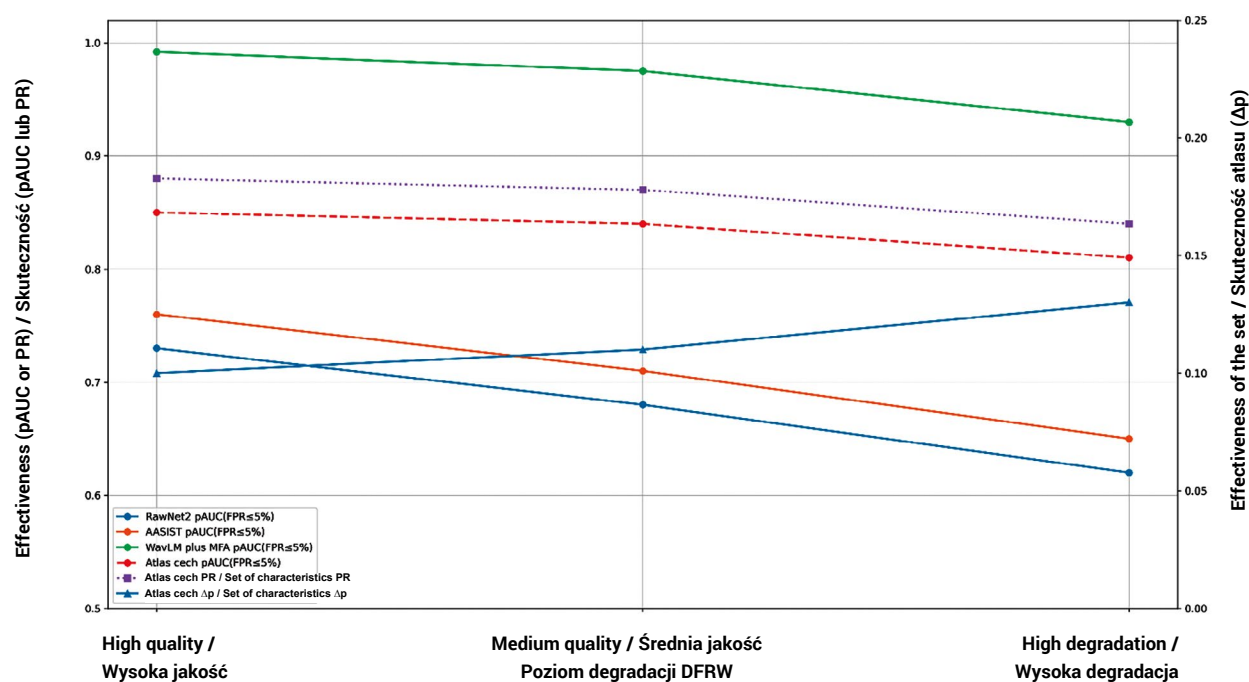


Figure 2. Drop in effectiveness of the reference point vs stability of the set of characteristics as a function of degradation
Rycina 2. Spadek skuteczności punktu odniesienia a stabilność zbioru cech w funkcji degradacji

Source: Own elaboration.

Źródło: Opracowanie własne.

Discussion and explanation of results

The results presented in this article confirm that synthetic speech shows systematic acoustic and prosodic deviations in relation to natural speech, of which a significant part is retained after platform degradations. The strongest differentiation signal comes from cepstral and spectral families and cepstral and modulation families, complemented by harmonicity and noise indicators and prosodic characteristics. The MFCC/LFCC and CQCC sets reach $p_{df} \approx 51$ –55% with $p_{real} \approx 30\%$ and Δp up to 0.25, however the modulation spectrum and CPP reach $\Delta p \approx 0.22$ –0.23 with $PR \approx 1.6$ –1.7. The decreased jitter and shimmer and the increased HNR imply excessive regularity of the voice source, leading to a consistent image of smoothing of the synthetic signal including the reduction of microfluctuations, increased harmonicity, impoverishment of prosody and more frequent phase anomalies.

From the security engineering perspective, the compromise between effectiveness and stability is crucial. Cepstral and modulation characteristics are characterised by low sensitivity for compression and recoding, which favours operational applications in KYC, AML and content moderation. Phase characteristics effectively show vocoder artefacts, but they are moderately sensitive to low SNR. Prosodic characteristics remain informative, however their power depends on segmentation quality and speech length, which supports a multi-family merger and over modelling of uncertainty instead of decisions based on single descriptors.

The observations obtained are consistent with literature and benchmarks of TTS/VC detection. The stability of LFCC and CQCC

Dyskusja i omówienie wyników

Wyniki przedstawione w niniejszym artykule potwierdzają, że mowa syntetyczna wykazuje systematyczne odchylenia akustyczne i prozodyczne względem mowy naturalnej, z których istotna część utrzymuje się po degradacjach platformowych. Najsilniejszy sygnał różnicujący pochodzi z rodzin cepstralnych i widmowych oraz cepstralno-modulacyjnych, uzupełnionych wskaźnikami harmoniczności–szum i cechami prozodycznymi. Zestawy MFCC/LFCC i CQCC osiągają $p_{df} \approx 51$ –55% przy $p_{real} \approx 30\%$ i Δp do 0,25, natomiast widmo modulacyjne i CPP uzyskują $\Delta p \approx 0,22$ –0,23 przy $PR \approx 1,6$ –1,7. Obniżone jitter i shimmer oraz podwyższony HNR wskazują na nadmierną regularność źródła głosowego, prowadząc do spójnego obrazu wygładzenia sygnału syntetycznego obejmującego redukcję mikrofluktuacji, wzrost harmoniczności, zubożenie prozodii i częstsze anomalie fazowe.

Z punktu widzenia inżynierii bezpieczeństwa kluczowy jest kompromis skuteczności i stabilności. Cechy cepstralne i modulacyjne cechują się niską wrażliwością na kompresję i rekodowanie, co sprzyja zastosowaniom operacyjnym w KYC, AML i moderacji treści. Cechy fazowe skutecznie ujawniają artefakty wokoderowe, lecz są umiarkowanie wrażliwe na niski SNR. Cechy prozodyczne pozostają informatywne, jednak ich moc zależy od jakości segmentacji i długości wypowiedzi, co przemawia za fuzją wielorodzinną i jawnym modelowaniem niepewności zamiast decyzji opartych na pojedynczych deskryptorach.

Uzyskane obserwacje są spójne z literaturą i benchmarkami wykrywania TTS/VC. Stabilność LFCC i CQCC po degradacjach

after degradations and their sensitivity to non-physical high frequency energy distributions correspond to ASVspoof results and the works of Todisco and Sahidullah [28], [70-71]. The lowered jitter and shimmer and the increased HNR confirm classic observations of excess source regularity in voice synthesis and conversion [65-67]. The dependency of phase characteristics from SNR and sensitivity of prosodic characteristics to temporal alignment and speech length correspond to the reports on OOD scenarios and platform chains [21], [36]. At the same time, the inclusion of metrics LSE-C and LSE-D confirms the usefulness of audio-video synchrony criteria in detecting *audio-driven* materials and secondary recording, as recommended by AV hybrids in forensics [21].

Lower Δp and PR averages for clear phase characteristics in DFRW, compared to laboratory conditions, most probably from the higher heterogeneity of the set and more intensive telecommunication degradations and cascade recordings. This justifies *in the wild* curation and combining the phase with cepstrum and modulation characteristics. The analysis of stability indicates that cepstra LFCC and CQCC and selected MFCC statistics remain relatively resistant to CRF 18–32 and MP4/WebM container changes, modulation indicators retain distinguishability in application filters and AR, however phase characteristics are the most useful in high quality and should play a role in supporting the merger.

These conclusions reinforce the need for OOD validation. Evaluation based on laboratory sets only can overstate the usability of phase and prosodic characteristics, while in real distribution cepstra and modulation ensure higher predictability. In operational terms, it means reporting pAUC with low FPR and regular revalidation in continuous evaluation mode. The combination of LSE-C and LSE-D with acoustic characteristics enable separating non-physical anomalies of the voice signal and articulation and phoneme inconsistencies, thus increasing the resistance to adaptive attacks targeting a single modality, which is completed in operation with 77% of audio samples in DFRW.

Based on the results, hybrid architecture is recommended, including the primary layer of LFCC+CQCC+MFCC with HNR and CPP, the complementary layer based on modulation spectrum and restricted set of phase characteristics, the multi-modal layer with LSE-C and LSE-D, and merger of the rating with weight depending on channel quality and temperature calibration or *Platt scaling*. The operating threshold should be tuned to the risk profile with $FPR \leq 5\%$ for pre-selection, lower FPR and full reporting of uncertainty in forensic tracks.

The analysis of sensitivity to anti-forensics indicates the complementarity of the families of characteristics. Temporal manipulations weaken prosodic characteristics, but do not fully mask the cepstra LFCC/CQCC and modulation spectrum, while noise and dither deteriorate phase characteristics and microdetails, with limited impact on metrics AV LSE-C and LSE-D. This confirms the validity of defence by diversification, combining independent evidence sources and attack transferability validation in OOD protocols [40].

The applied selection method based on exceeding the θ thresholds determined for the real class and the reporting of Δp and PR facilitate forensic interpretation and reporting, in particular

oraz ich czułość na niefizyczne rozkłady energii wysokoczęstotliwościowej odpowiada wynikom ASVspoof i pracom Todisco oraz Sahidullah [28], [70-71]. Obniżony jitter i shimmer oraz podwyższony HNR potwierdzają klasyczne obserwacje nadmiernej regularności źródła w syntezie i konwersji głosu [65-67]. Zależność cech fazowych od SNR oraz wrażliwość cech prozodycznych na dopasowanie czasowe i długość wypowiedzi są zgodne z doniesieniami dotyczącymi scenariuszy OOD i łańcuchów platformowych [21], [36]. Jednocześnie włączenie metryk LSE-C i LSE-D potwierdza przydatność kryteriów synchronii audio-wideo w wykrywaniu materiałów *audio-driven* i wtórnej rejestracji, zgodnie z rekomendacjami hybryd AV w forensyce [21].

Niższe średnie Δp i PR dla czystych cech fazowych w DFRW w porównaniu z warunkami laboratoryjnymi wynikają najprawdopodobniej z większej heterogeniczności zbioru oraz intensywniejszych degradacji telekomunikacyjnych i kaskadowych rekodowań. Uzasadnia to kurację *in the wild* oraz łączenie fazy z cepstrum i cechami modulacyjnymi. Analiza stabilności wskazuje, że cepstra LFCC i CQCC oraz wybrane statystyki MFCC pozostają relatywnie odporne na CRF 18–32 i zmiany kontenera MP4/WebM, wskaźniki modulacyjne zachowują rozróżnialność przy filtrach aplikacyjnych i AR, natomiast cechy fazowe są najbardziej użyteczne w wysokiej jakości i powinny pełnić rolę wspomagającą fuzję.

Wnioski te wzmacniają potrzebę walidacji OOD. Ocena wyłącznie na zbiorach laboratoryjnych może zawyżać użyteczność cech fazowych i prozodycznych, podczas gdy w dystrybucji rzeczywistej większą przewidywalność zapewniają cepstra i modulacja. Operacyjnie oznacza to raportowanie pAUC przy niskich FPR oraz regularną rewalidację w trybie ewaluacji ciągłej. Połączenie LSE-C i LSE-D z cechami akustycznymi umożliwia separację anomalii niefizyczności sygnału głosu oraz niespójności artykulacji i fonemów, zwiększając odporność na ataki adaptacyjne ukierunkowane na pojedynczą modalność, co jest wykonalne operacyjnie przy 77% próbek z audio w DFRW.

Na podstawie wyników rekomendowana jest architektura hybrydowa obejmująca warstwę podstawową LFCC+CQCC+MFCC z HNR i CPP, warstwę uzupełniającą opartą o widmo modulacyjne i ograniczony zestaw cech fazowych, warstwę multimodalną z LSE-C i LSE-D oraz fuzję punktacji z ważeniem zależnym od jakości kanału i kalibracją temperaturową lub *Platt scaling*. Próg operacyjny należy dostrajać do profilu ryzyka, przy $FPR \leq 5\%$ dla preselekcji oraz niższym FPR i pełnym raportowaniu niepewności w ścieżkach forensycznych.

Analiza podatności na antyforensykę wskazuje na komplementarność rodzin cech. Manipulacje temporalne osłabiają cechy prozodyczne, lecz nie maskują w pełni cepstrów LFCC/CQCC i widma modulacyjnego, natomiast szum i dither degradują cechy fazowe i mikrodetale, przy ograniczonym wpływie na metryki AV LSE-C i LSE-D. Potwierdza to zasadność obrony przez dywersyfikację, łączenia niezależnych źródeł dowodowych i walidacji transferowalności ataków w protokołach OOD [40].

Zastosowana metodyka selekcji oparta na przekroczeniach progów θ wyznaczonych na klasie real oraz raportowanie Δp i PR ułatwiają interpretację i raportowanie forensyczne, zwłaszcza w połączeniu z wizualizacjami spektrogramów, map

combined with spectrograph visualisations, modulation maps and $F0$ outlines [10], [37]. In accordance with XAI recommendations, it is required to add uncertainty calibration and interpretation limitations, in particular for low SNR and short speeches [38–39].

The limitations cover 23% of samples without audio, sensitivity of θ thresholds to domain drift, which requires continuous validation, and the dependency of some prosodic characteristics on segmentation quality. The systematic analysis does not include generative attacks optimised for specific characteristics of the set, which remains the direction for further studies. In practice, pre-selection based on LFCC, CQCC, MFCC, CPP, HNR and modulation characteristics with ECE reporting, supplementation with LSE-C and LSE-D in AV analysis and continuous Δp and PR drift monitoring with θ updates and tests of robustness.

The priority is to expand DFRW to DFRWv2 with a greater share of diffusion models and telecommunication degradations and development of set characteristic merger methods with light trained models, while retaining interpretability and uncertainty control. The DFRW analysis shows that the set is based on LFCC, CQCC, HNR, modulation spectrum and selected phase and prosodic characteristics enables credible differentiation of synthetic contents in real distribution. A key advantage of the approach is separation of the decision layer and the evidence layer, which provides auditability, predictability and mergeability with any trained detector as independent evidence layer in OOD scenarios.

Summary and conclusions

The purpose of the study was to develop an empirically verified set of descriptors for synthetic speech detection, considering in particular TTS and VC artefacts. Using the author's characteristic selection framework and the DFRW, it was demonstrated that cepstral descriptors LFCC and CQCC are the most stable component of detection ($\Delta p \approx 0.25$), while retaining resistance to platform degradations. Source (HNR, CPP) and modulation indicators effectively show algorithmic regularity and prosody smoothing, while phase characteristics precisely identify vocoder inconsistencies, which in turn demonstrates sensitivity to noise. It was confirmed that integrating acoustics with audio-video synchronisation metrics (LSE-C/D) significantly increases the resistance to attacks targeting a single modality. The implications for security engineering include the proposition of layer-based characteristic application, need for OOD (Out-of-Distribution) validation and requirement to base decisions on interpretable excesses of statistic thresholds. From the system maintenance perspective, it is crucial to use cyclic revalidation in the continuous evaluation model is crucial for mitigating technological drift and to use XAI reporting. The future work directions assume expanding the database to the scale of 500,000 clips (DFRWv2), developing hybrid methods and tests of resistance to adaptive attacks. To conclude, the multi-family merger of characteristics, combined with uncertainty calibration, constitutes the foundation for building transparent and robust forensic tools.

modulacyjnych i konturów $F0$ [10], [37]. Zgodnie z zaleceniami XAI wymagane jest dołączanie kalibracji niepewności i ograniczeń interpretacyjnych, szczególnie przy niskim SNR i krótkich wypowiedziach [38–39].

Ograniczenia obejmują 23% próbek bez audio, wrażliwość progów θ na dryf domenowy wymagającą ciągłej walidacji oraz zależność części cech prozodycznych od jakości segmentacji. Nie analizowano systematycznie ataków generatywnych optymalizowanych pod konkretne cechy zbioru, co pozostaje kierunkiem dalszych badań. W praktyce zaleca się preselekcję opartą o LFCC, CQCC, MFCC, CPP, HNR i cechy modulacyjne z raportowaniem ECE, uzupełnienie o LSE-C i LSE-D w analizie AV oraz ciągły monitoring dryfu Δp i PR z aktualizacją θ i testami odporności.

Priorytetem jest rozszerzenie DFRW do DFRWv2 z większym udziałem modeli dyfuzyjnych i degradacji telekomunikacyjnych oraz rozwój metod fuzji cech zbioru z lekkimi modelami uczonymi przy zachowaniu interpretowalności i kontroli niepewności. Analiza DFRW pokazuje, że zbiór oparty na LFCC, CQCC, HNR, widmie modulacyjnym oraz wybranych cechach fazowych i prozodycznych umożliwia wiarygodne rozróżnianie treści syntetycznych w dystrybucji rzeczywistej. Kluczową przewagą podejścia jest rozdzielenie warstwy decyzyjnej od warstwy dowodowej, co zapewnia audytowalność, przewidywalność i możliwość fuzji z dowolnym detektorem uczonym jako niezależną warstwą materiałów dowodowych w scenariuszach OOD.

Podsumowanie i wnioski

Celem pracy było opracowanie empirycznie zweryfikowanego zbioru deskryptorów do detekcji mowy syntetycznej, ze szczególnym uwzględnieniem artefaktów TTS i VC. Wykorzystując autorskie ramy selekcji cech oraz zbiór DFRW, wykazano, że deskryptory cepstralne LFCC i CQCC stanowią najstabilniejszy komponent detekcji ($\Delta p \approx 0.25$), zachowując odporność na degradację platformowe. Wskaźniki źródłowe (HNR, CPP) oraz modulacyjne skutecznie ujawniają algorytmiczną regularność i wygładzenie prozodii, podczas gdy cechy fazowe precyzyjnie identyfikują nieciągłości wokoderowe, wykazując jednak wrażliwość na szum. Potwierdzono, że integracja akustyki z metrykami spójności audio-wideo (LSE-C/D) istotnie zwiększa odporność na ataki ukierunkowane na pojedynczą modalność. Implikacje dla inżynierii bezpieczeństwa obejmują postulat warstwowego stosowania cech, konieczność walidacji OOD (ang. *Out-of-Distribution*) oraz wymóg oparcia decyzji na interpretowalnych przekroczeniach progów statystycznych. Z perspektywy utrzymania systemów kluczowa jest cykliczna rewalidacja w modelu ewaluacji ciągłej w celu mitygacji dryfu technologicznego oraz stosowanie raportowania XAI. Przyszłe kierunki prac zakładają rozbudowę bazy danych do skali 500 tys. klipów (DFRWv2), rozwój metod hybrydowych oraz testy odporności na ataki adaptacyjne. Podsumowując, wielorodzinna fuzja cech połączona z kalibracją niepewności stanowi fundament budowy transparentnych i odpornych narzędzi forensycznych.

Source of funding

The publication was created as part of the project entitled: "Opracowanie interpretowanego algorytmu detekcji deepfake z wykorzystaniem atlasu cech deepfake" (Development of an interpretable deepfake detection algorithm using a deepfake feature atlas), funded by the GZM Metropolis under the Metropolitan Science Support Fund Programme.

Źródło finansowania

Publikacja powstała w ramach projektu pt.: „Opracowanie interpretowanego algorytmu detekcji deepfake z wykorzystaniem atlasu cech deepfake”, finansowanego ze środków Górnośląsko-Zagłębiowskiej Metropolii w ramach Programu Metropolitalny Fundusz Wspierania Nauki.

Abbreviations and definitions / Skróty i definicje

95% CI	Confidence interval 95%, i.e. the range of values with high probability of including the true parameter value / Przedział ufności 95%, czyli zakres wartości, w którym z wysokim prawdopodobieństwem znajduje się prawdziwa wartość parametru
AASIST	Network detector of fake speech, designed for resistance to different types of attacks / Sieciowy detektor fałszerstw mowy, projektowany pod kątem odporności na różne typy ataków
APQ3, APQ5	Variants of amplitude irregularity measures, used to describe the shimmer / Warianty miar nieregularności amplitudy, stosowane do opisu shimmer
ASVspoof	International set of tests and data for evaluation of fake speech detection methods / Międzynarodowy zestaw testów i danych do oceny metod wykrywania fałszerstw mowy
BRISQUE	The image quality measure without reference image is based on natural image statistics / Miara jakości obrazu bez obrazu wzorcowego, oparta na statystyce naturalnych obrazów
CEO fraud	CEO fraud method / Oszustwo „na prezesa”
CQCC	Coefficients based on fixed relative resolution in frequency, sensitive to artefacts of synthesis / Współczynniki oparte na stałej rozdzielczości względnej w częstotliwości, wrażliwe na artefakty syntezy
CRF	The video compression quality parameter, in which the higher value usually means stronger compression / Parametr jakości kompresji wideo, gdzie większa wartość zwykle oznacza silniejszą kompresję
De Krom	The harmonicity measure calculation methodology, used in HNR analysis / Metodyka obliczania miar harmoniczności, używana w analizie HNR
EBU R128	The volume measurement and normalisation standard, used to standardise recordings / Norma pomiaru i normalizacji głośności, stosowana do ujednolicania nagrań
Intonation outline entropy / Entropia konturu intonacyjnego	The measure of speech melody change complexity, higher for natural expression / Miara złożoności zmian melodii mowy, wyższa dla naturalnej ekspresji
EXIF	Image or video file metadata, described by recording and device parameters / Metadane pliku obrazu lub wideo, opisujące parametry rejestracji i urządzenia
F0	Primary frequency, corresponding to voice pitch / Częstotliwość podstawowa, odpowiadająca wysokości głosu
FastSpeech	Quick speech synthesis method, designed for short generation time / Szybka metoda syntezy mowy, projektowana z myślą o krótkim czasie generacji
FDR	Control of the percentage of false discoveries, i.e. the procedure limiting the number of wrong conclusions with multiple statistic tests / Kontrola odsetka fałszywych odkryć, czyli procedura ograniczająca liczbę błędnych wniosków przy wielu testach statystycznych
Mobile filters and AR / Filtry mobilne i AR	Automatic image effects applied by mobile applications, including extended image components that change the face and background appearance / Automatyczne efekty obrazu nakładane przez aplikacje mobilne, w tym elementy rozszerzonego obrazu, które zmieniają wygląd twarzy i tła
F1, F2, F3 formants / Formanty F1, F2, F3	First three resonances of the voice track, important for articulation quality / Pierwsze trzy rezonanse toru głosowego, ważne dla jakości artykulacji

FPS	Number of frames per second, i.e. the video image refresh rate / Liczba klatek na sekundę, czyli częstotliwość odświeżania obrazu wideo
GAN	Generation model based on competition between two networks, one generating the data and other evaluating their authenticity / Model generatywny oparty na rywalizacji dwóch sieci, jednej generującej dane i drugiej oceniającej ich autentyczność
GOP	Group of images in video compression, determining the distribution of full and expected frames / Grupa obrazów w kompresji wideo, struktura określająca rozmieszczenie klatek pełnych i przewidywanych
H.264 AVC	Standard video compression commonly used in the Internet / Standard kompresji wideo powszechnie stosowany w internecie
H.265 HEVC	Newer video compression standard, with higher effectiveness / Nowszy standard kompresji wideo o wyższej efektywności
HNR	Ratio of harmonic components to noise, measure of “clarity” phonation / Stosunek składowych harmoniczných do szumu, miara „czystości” fonacji
IQR	The inter-quartile range, i.e. the difference between quartile 75% and 25%, describing the typical data range / Rozstęp międzykwartylowy, czyli różnica między kwartylem 75% i 25%, opisująca typowy rozrzut danych
ITU R BS.1770	Volume calculation method, including hearing perception / Metoda obliczania głośności z uwzględnieniem percepcji słuchowej
ITU T P.56	Standard for determining the active speech level / Norma wyznaczania poziomu mowy aktywnej
Jitter	Primary period vibrations, i.e. small irregularities of the vocal fold vibration time / Drgania okresu podstawowego, czyli drobne nieregularności czasu drgań fałdów głosowych
DCT quantisation / Kwantyzacja DCT	Simplification of cosine transformation coefficients in compression, being the source of typical lossy artefacts / Uproszczenie współczynników transformacji kosinusowej w kompresji, będące źródłem typowych artefaktów stratnych
LFCC	Coefficients describing the spectrum on a linear scale, useful for fake detection / Współczynniki opisujące widmo na skali liniowej, użyteczne w detekcji fałszerstw
LPC	The model describing the voice track by adjusting the filtering, used for formant estimation / Model opisujący tor głosowy przez dopasowanie filtracji, wykorzystywany do estymacji formantów
LPIPS	The measure of perception similarity based on neural network representations / Miara podobieństwa percepcyjnego oparta na reprezentacjach sieci neuronowych
LRA	Range of volume variation in the recording / Zakres zmienności głośności w nagraniu
LSE C (Lip Sync Error Confidence)	Indicator of certainty of lips movement synchronisation with speech / Wskaźnik pewności dopasowania ruchu ust do mowy
LSE D (Lip Sync Error Distance)	Indicator of error magnitude of lips movement synchronisation with speech / Wskaźnik wielkości błędu dopasowania ruchu ust do mowy
LUFS	Standardised measure of volume perceived by a human / Znormalizowana miara głośności odczuwanej przez człowieka
Lip sync methods / Metody lip sync	Methods of synchronisation of lip movements with speech sound, making the image look like talking / Metody dopasowania ruchu ust do dźwięku mowy, aby obraz wyglądał jak mówiący
Reenactment methods / Metody reenactment	Methods of replication of face movements and mimics based on another source of control, for example recording or sound / Metody odtwarzania ruchów twarzy i mimiki na podstawie innego źródła sterowania, na przykład nagrania lub dźwięku
MFCC (Mel-Frequency Cepstral Coefficients)	Coefficients describing the speech spectrum shape on a frequency scale similar to human hearing / Współczynniki opisujące kształt widma mowy na skali częstotliwości zbliżonej do słuchu człowieka
Pitch	Head pitch up or down, i.e. vertical rotation / Odchylenie głowy w górę lub w dół, czyli obrót pionowy
Platt scaling	The classifier results calibration method consisting in matching the logistic function with raw decision results. In Polish literature, this method is sometimes referred to as Platt's scaling / Metoda kalibracji wyników klasyfikatora polegająca na dopasowaniu funkcji logistycznej do surowych wyników decyzyjnych. W polskiej literaturze metoda ta bywa określana jako skalowanie Platta

PR	The frequency prevalence ratio, i.e. the quotient of phenomenon frequency in the synthetic class to frequency in the authentic class / Współczynnik przewagi częstości, czyli iloraz częstości zjawiska w klasie syntetycznej do częstości w klasie autentycznej
Pre-emphasis of 0.97 / Preemfaza 0,97	Amplification of high frequency components before analysis, to show articulation details better / Wzmocnienie składowych wysokoczęstotliwościowych przed analizą, aby lepiej uwidocznili szczegóły artykulacyjne
PSNR	The measure of difference between image and standard, based on error mean square / Miara różnicy między obrazem a wzorcem, oparta na błędzie średniokwadratowym
Frame I / Ramka I	Independent coded full frame, being the reference point for other frames in the GOP group / Klatka pełna kodowana niezależnie, będąca punktem odniesienia dla innych klatek w grupie GOP
RAP, PPQ5	Variants of period irregularity measures, used to describe the jitter / Warianty miar nieregularności okresu, stosowane do opisu jitter
RawNet2	Network detector trained directly from speech signal, used as the comparison method / Sieciowy detektor uczony bezpośrednio z sygnału mowy, używany jako metoda porównawcza
Shimmer	Amplitude vibrations, i.e. small volume irregularities in subsequent volume periods / Drgania amplitudy, czyli drobne nieregularności głośności kolejnych okresów głosu
Mel scale / Skala Mel	Frequency scale adjusted to human hearing sensitivity / Skala częstotliwości dopasowana do wrażliwości słuchu człowieka
SSIM	Measure of structural similarity of images, including the perception / Miara podobieństwa strukturalnego obrazów, uwzględniająca percepcję
TNO simulations / Symulacje TNO	Analyses completed by the Netherlands Organisation for Applied Scientific Research, usually in the phenomenon effects modelling form / Analizy wykonywane przez Niderlandzką Organizację Badań Stosowanych, zwykle w formie modelowania skutków zjawisk
pHash signature / Sygnatura pHash	Short content "print" calculated so that similar materials have a similar signature, used to detect copies / Krótki „odcisk” treści, obliczany tak, aby podobne materiały miały podobny podpis, używany do wykrywania kopii
Tacotron 2	Speech synthesis model converting text into acoustic representation and then sound / Model syntezy mowy przekształcający tekst w reprezentację akustyczną, a następnie w dźwięk
TTS	Text to speech synthesis, i.e. automatic generation of voice recording based on written text / Synteza mowy z tekstu, czyli automatyczne wytwarzanie nagrania głosu na podstawie zapisanego tekstu
VMAF	Measure of video quality combining several perception components / Miara jakości wideo łącząca kilka składowych percepcyjnych
VP9	Video compression standard developed for Internet distribution / Standard kompresji wideo rozwijany dla dystrybucji internetowej
WAV	Sound file format storing signal without compression losses / Format pliku dźwiękowego przechowujący sygnał bez strat kompresji
wav2vec 2.0	Model learning speech representation from recordings without labels, often used as detection database / Model uczący reprezentacji mowy z nagrań bez etykiet, często używany jako baza do detekcji
WaveNet	Family of speech synthesizers based on neural networks, generating sound sampled in time / Rodzina metod syntezy mowy oparta na sieciach neuronowych, wytwarzająca dźwięk próbkowany w czasie
WavLM	Model learning speech representation from large sets, applied to robustness tasks / Model uczący reprezentacji mowy z dużych zbiorów, stosowany do zadań odpornościowych
XAI	Methods of explaining artificial intelligence algorithms, of which the purpose is to show, why the model made the given decision / Metody wyjaśniania działania algorytmów sztucznej inteligencji, których celem jest pokazanie, dlaczego model podjął daną decyzję
Yaw	Head yaw left or right in relation to the vertical axis, i.e. horizontal rotation / Odchylenie głowy w lewo lub w prawo względem osi pionowej, czyli obrót poziomy
YIN	Method of voice height determination from speech signal / Metoda wyznaczania wysokości głosu z sygnału mowy

AI Use Statement

The author declares that artificial intelligence tools were used in the preparation of this article only within the scope indicated below:

- language and stylistic verification of the manuscript.

The author takes full responsibility for the content of the publication, including the scientific accuracy, interpretation of results, and final editing of the manuscript. Artificial intelligence tools were used solely as supporting instruments.

The journal's editorial policy prohibits the uncritical copying of AI-generated content and its inclusion in a publication without proper critical analysis, verification, and revision by the author.

Oświadczenie dotyczące wykorzystania AI

Autor oświadcza, że w procesie przygotowania niniejszego artykułu wykorzystano narzędzia oparte na sztucznej inteligencji wyłącznie w zakresie wskazanym poniżej:

- weryfikacja językowa i stylistyczna tekstu.

Autor ponosi pełną odpowiedzialność za treść publikacji, w tym za poprawność merytoryczną, interpretację wyników oraz ostateczną redakcję tekstu. Narzędzia sztucznej inteligencji były wykorzystywane wyłącznie jako narzędzia pomocnicze. Polityka redakcyjna czasopisma zabrania bezrefleksyjnego kopiowania treści wygenerowanych przez narzędzia AI oraz pozostawiania ich w publikacji bez krytycznej analizy, weryfikacji i redakcji przez autora.

Literature / Literatura

- [1] Amodei D., Hernandez D., *AI and Compute*, OpenAI, 2018.
- [2] Kaplan J., McCandlish S., Henighan T. et al., *Scaling Laws for Neural Language Models*, arXiv:2001.08361, 2020.
- [3] Brown T.B., Mann B., Ryder N. et al., *Language Models Are Few-Shot Learners*, "Advances in Neural Information Processing Systems" 2020, 33, 1877–1901.
- [4] Achiam J., Adler S., Agarwal S. et al., *GPT-4 Technical Report*, arXiv:2303.08774, 2023.
- [5] Chesney R., Citron D.K., *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, "California Law Review" 2019, 107, 1753–1819, <https://doi.org/10.15779/Z38RV0D15J>.
- [6] Verdoliva L., *Media Forensics and Deepfakes: An Overview*, "IEEE Journal of Selected Topics in Signal Processing" 2020, 14(5), 910–932, <https://doi.org/10.1109/JSTSP.2020.3002101>.
- [7] Wang C., Chen S., Wu Y., Zhang Z., Zhou L., Liu S., Wei F., *Neural Codec Language Models Are Zero-Shot Text-to-Speech Synthesizers*, arXiv:2301.02111, 2023.
- [8] Ren Y., Hu C., Tan X., Qin T., Zhao S., Zhao Z., Liu T.Y., *Fast-Speech 2: Fast and High-Quality End-to-End Text to Speech*, arXiv:2006.04558, 2020.
- [9] Korshunov P., Marcel S., *Vulnerability of Face Recognition to Deep Morphing*, w: *ICB Workshops*, 2019.
- [10] Nautsch A., Wang X., Todisco M. et al., *ASVspoof 2019: A Large-Scale Public Database of Synthesized, Converted and Replayed Speech*, "Computer Speech & Language" 2022, 72, 101309, <https://doi.org/10.1016/j.csl.2021.101309>.
- [11] Sumsb, *Identity Fraud Report 2023: Trends and Forecasts*, Sumsb, 2023 [dok. elektr.], <https://sumsub.com/blog/guides-reports/identity-fraud-report-2023/> [dostęp: 01.12.2024].
- [12] Regula Forensics, *Deepfake Trends 2024: Business Identity Fraud Survey*, 2024 [dok. elektr.], <https://regulaforensics.com/resources/deepfake-trends-2024-report/> [dostęp: 01.12.2024].
- [13] Matern F., Riess C., Stammeringer M., *Exploiting Visual Artifacts to Expose Deepfakes and Face Manipulations*, w: *WACV Workshops*, 2019.
- [14] Guarnera L., Giudice O., Battiato S., *DeepFake Detection by Analyzing Convolutional Traces*, w: *CVPR Workshops*, 2020.
- [15] Mittal T., Bhattacharya U., Chandra R., Bera A., Manocha D., *Emotions Don't Lie: An Audio-Visual Deepfake Detection Method Using Affective Cues*, w: *Proceedings of the 28th ACM International Conference on Multimedia*, 2020, 2823–2832, <https://doi.org/10.1145/3394171.3413530>.
- [16] Frank J., Schönherr L., *WaveFake: A Data Set to Facilitate Audio Deepfake Detection*, arXiv:2111.02813, 2021.
- [17] Kumar S.V., Reddy S.T.A., Kalyani V., *Deepfake Detection on Social Media*, "International Journal of Communication Networks and Information Security" 2024, 16(5), 776–782.
- [18] DiResta R., *The Supply of Disinformation Will Soon Be Infinite*, The Atlantic 2020.
- [19] Europol, *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement*, Spotlight Report, 2024 [dok. elektr.].
- [20] TNO, *Generative AI and the Information Domain: Scenario-Based Analysis*, 2023 [dok. elektr.].
- [21] Haliassos A., Vougioukas K., Petridis S., Pantic M., *Lips Don't Lie: A Generalisable and Robust Approach to Face Forgery Detection*, w: *CVPR*, 2021, 5039–5049, <https://doi.org/10.1109/CVPR46437.2021.00500>.
- [22] Li M., Ahmadiadli Y., Zhang X.P., *A Survey on Speech Deepfake Detection*, *ACM Computing Surveys* 2025, 57(7), 1–38, <https://doi.org/10.1145/3657424>.
- [23] Dolhansky B., Howes R., Pflaum B. et al., *The DeepFake Detection Challenge (DFDC) Dataset*, arXiv:2006.07397, 2020.
- [24] Rössler A., Cozzolino D., Verdoliva L., Riess C., Thies J., Nießner M., *FaceForensics++: Learning to Detect Manipulated Facial Images*, w: *ICCV*, 2019, <https://doi.org/10.1109/ICCV.2019.00076>.
- [25] Jiang L., Li R., Wu W. et al., *DeeperForensics-1.0: A Large-Scale Dataset for Real-World Face Forgery Detection*, w: *CVPR*, 2020, <https://doi.org/10.1109/CVPR42600.2020.00288>.
- [26] Li Y., Yang X., Sun P., Qi H., Lyu S., *Celeb-DF: A Large-Scale Challenging Dataset for DeepFake Forensics*, w: *CVPR*, 2020, <https://doi.org/10.1109/CVPR42600.2020.00327>.
- [27] Kinnunen T., Sahidullah M., Delgado H. et al., *The ASVspoof*

- 2017 Challenge, w: *Interspeech*, 2017, <https://doi.org/10.21437/Interspeech.2017-1111>.
- [28] Todisco M., Wang X., Vestman V. et al., *ASVspoof 2019: Future Horizons in Spoofed and Fake Audio Detection*, arXiv:1904.05441, 2019.
- [29] Wu Z., Yamagishi J., Kinnunen T. et al., *ASVspoof: The Automatic Speaker Verification Spoofing and Countermeasures Challenge*, *IEEE Journal of Selected Topics in Signal Processing* 2017, 11(4), 588–604, <https://doi.org/10.1109/JSTSP.2017.2739166>.
- [30] Eom J., Lee J., Kim H. et al., *AASIST: Audio Anti-Spoofing Using Integrated Spectro-Temporal Graph Attention Networks*, w: *INTERSPEECH* 2022, 2398–2402, <https://doi.org/10.21437/Interspeech.2022-11067>.
- [31] Baevski A., Zhou Y., Mohamed A., Auli M., *wav2vec 2.0: A Framework for Self-Supervised Learning of Speech Representations*, *NeurIPS* 2020, 33, 12449–12460.
- [32] Durall R., Keuper M., Keuper J., *Watch Your Up-Convolution: CNN-Based Generative Deep Neural Networks Are Failing to Reproduce Spectral Distributions*, w: *CVPR*, 2020, <https://doi.org/10.1109/CVPR42600.2020.00795>.
- [33] Guo C., Pleiss G., Sun Y., Weinberger K.Q., *On Calibration of Modern Neural Networks*, w: *ICML*, 2017, 1321–1330.
- [34] Lu Y., Luo R., Ebrahimi T., *Improving Deepfake Detectors against Real-World Perturbations*, *Applications of Digital Image Processing XLVI*, *SPIE* 2023, <https://doi.org/10.1117/12.2676695>.
- [35] Carlini N., Tramer F., Wallace E. et al., *Poisoning Web-Scale Training Datasets Is Practical*, arXiv:2302.10149, 2023.
- [36] Qian Y., Yin G., Sheng L., Chen Z., Shao J., *Thinking in Frequency: Face Forgery Detection by Mining Frequency-Aware Clues*, w: *ECCV*, 2020, 86–103, https://doi.org/10.1007/978-3-030-58577-8_6.
- [37] Doshi-Velez F., Kim B., *Towards a Rigorous Science of Interpretable Machine Learning*, arXiv:1702.08608, 2017.
- [38] Wang T., Liao X., Chow K.P., Lin X., Wang Y., *Deepfake Detection: A Comprehensive Survey from the Reliability Perspective*, arXiv:2211.10881, 2022.
- [39] Selvaraju R.R., Cogswell M., Das A. et al., *Grad-CAM: Visual Explanations from Deep Networks via Gradient-Based Localization*, w: *ICCV*, 2017, <https://doi.org/10.1109/ICCV.2017.74>.
- [40] Neves J.C., Tolosana R., Vera-Rodriguez R. et al., *GANprintR: Improved Fakes and Evaluation of the State of the Art in Face Manipulation Detection*, *IEEE Journal of Selected Topics in Signal Processing* 2020, 14(5), 1038–1048, <https://doi.org/10.1109/JSTSP.2020.2999165>.
- [41] Paullada A., Raji I.D., Bender E.M., Denton E., Hanna A., *Data and Its (Dis)Contents*, *Patterns* 2021, 2(11), 100336, <https://doi.org/10.1016/j.patter.2021.100336>.
- [42] Gebu T., Morgenstern J., Vecchione B. et al., *Datasheets for Datasets*, *Communications of the ACM* 2021, 64(12), 86–92, <https://doi.org/10.1145/3458723>.
- [43] Ho J., Jain A., Abbeel P., *Denoising Diffusion Probabilistic Models*, *NeurIPS* 2020, 33, 6840–6851.
- [44] Mittal T., Sinha R., Swaminathan V., Collomosse J., Manocha D., *Video Manipulations Beyond Faces*, w: “WACV” 2023, 643–652, <https://doi.org/10.1109/WACV56688.2023.00073>.
- [45] Mittal A., Soundararajan R., Bovik A.C., *Making a “Completely Blind” Image Quality Analyzer*, *IEEE Signal Processing Letters* 2013, 20(3), 209–212, <https://doi.org/10.1109/LSP.2012.2227726>.
- [46] Zhang R., Isola P., Efros A.A., Shechtman E., Wang O., *The Unreasonable Effectiveness of Deep Features as a Perceptual Metric*, w: “CVPR” 2018, 586–595, <https://doi.org/10.1109/CVPR.2018.00068>.
- [47] Tu Z., Wang Y., Birkbeck N., Adsumilli B., Bovik A.C., *UGC-VQA*, *IEEE Transactions on Image Processing* 2021, 30, 4449–4464, <https://doi.org/10.1109/TIP.2021.3070508>.
- [48] Teed Z., Deng J., *RAFT: Recurrent All-Pairs Field Transforms for Optical Flow*, w: “ECCV” 2020, https://doi.org/10.1007/978-3-030-58536-5_24.
- [49] Khalid H., Tariq S., Kim M., Woo S.S., *FakeAVCeleb*, arXiv:2108.05080, 2021.
- [50] Chung J.S., Zisserman A., *Out of Time: Automated Lip Sync in the Wild*, “ACCV” 2016, 251–263, https://doi.org/10.1007/978-3-319-54184-6_16.
- [51] Prajwal K.R., Mukhopadhyay R., Namboodiri V.P., Jawahar C.V., *A Lip Sync Expert Is All You Need*, *ACM Multimedia* 2020, 484–492, <https://doi.org/10.1145/3394171.3413532>.
- [52] Baltrušaitis T., Zadeh A., Lim Y.C., Morency L-P., *OpenFace 2.0*, “IEEE FG” 2018, <https://doi.org/10.1109/FG.2018.00019>.
- [53] Frank J., Eisenhofer T., Schönherr L. et al., *Leveraging Frequency Analysis for Deep Fake Image Recognition*, “ICML” 2020, 3247–3258.
- [54] Tolosana R., Vera-Rodriguez R., Fierrez J., Morales A., Ortega-Garcia J., *Deepfakes and Beyond*, *Information Fusion* 2020, 64, 131–148, <https://doi.org/10.1016/j.inffus.2020.06.014>.
- [55] Cohen J., *A Coefficient of Agreement for Nominal Scales*, *Educational and Psychological Measurement* 1960, 20(1), 37–46, <https://doi.org/10.1177/001316446002000104>.
- [56] Krippendorff K., *Content Analysis: An Introduction to Its Methodology*, 4th ed., SAGE, 2019.
- [57] Artstein R., Poesio M., *Inter-Coder Agreement for Computational Linguistics*, *Computational Linguistics* 2008, 34(4), 555–596, <https://doi.org/10.1162/coli.07-034-R2>.
- [58] Northcutt C.G., Athalye A., Mueller J., *Pervasive Label Errors in Test Sets Destabilize Machine Learning Benchmarks*, arXiv:2103.14749, 2021.
- [59] Güera D., Delp E.J., *Deepfake Video Detection Using Recurrent Neural Networks*, “AVSS” 2018, <https://doi.org/10.1109/AVSS.2018.8639163>.
- [60] EBU, *R 128: Loudness Normalisation and Permitted Maximum Level of Audio Signals*, European Broadcasting Union, 2014.
- [61] ITU-R, *BS.1770-4: Algorithms to Measure Audio Programme Loudness and True-Peak Audio Level*, ITU, 2015.
- [62] ITU-T, *P.56: Objective Measurement of Active Speech Level*, ITU, 2011.
- [63] Bianchi T., Piva A., *Image Forgery Localization via Block-Grained Analysis of JPEG Artifacts*, *IEEE Transactions on Information Forensics and Security* 2012, 7(3), 1003–1017, <https://doi.org/10.1109/TIFS.2012.2187516>.

- [64] de Cheveigné A., Kawahara H., *YIN: A Fundamental Frequency Estimator for Speech and Music*, "Journal of the Acoustical Society of America" 2002, 111(4), 1917–1930, <https://doi.org/10.1121/1.1458024>.
- [65] Titze I.R., *Principles of Voice Production*, Prentice Hall, 1994.
- [66] Boersma P., *Accurate Short-Term Analysis of the Fundamental Frequency*, "Proceedings of the Institute of Phonetic Sciences" 1993, 17, 97–110.
- [67] Krom G.D., *A Cepstrum-Based Technique for Determining a Harmonics-to-Noise Ratio*, "Journal of Speech and Hearing Research" 1993, 36(2), 254–266, <https://doi.org/10.1044/jshr.3602.254>.
- [68] De Leon P.L., Stewart B., Yamagishi J., *Synthetic Speech Discrimination Using Pitch Pattern Statistics*, w: *Interspeech*, 2012.
- [69] Muda L., Begam M., Elamvazuthi I., *Voice Recognition Algorithms Using MFCC and DTW*, arXiv:1003.4083, 2010.
- [70] Sahidullah M., Kinnunen T., Hanilçi C., *A Comparison of Features for Synthetic Speech Detection*, w: *Interspeech*, 2015.
- [71] Todisco M., Delgado H., Evans N., *Constant Q Cepstral Coefficients*, "Computer Speech & Language" 2017, 45, 516–535, <https://doi.org/10.1016/j.csl.2017.01.001>.
- [72] Markel J.D., Gray A.J., *Linear Prediction of Speech*, Springer, 2013.
- [73] Rabiner L., Schafer R., *Theory and Applications of Digital Speech Processing*, Prentice Hall, 2010.
- [74] Peeters G., *A Large Set of Audio Features for Sound Description*, CUIDADO IST Project Report, 2004.
- [75] Murthy H.A., Yegnanarayana B., *Formant Extraction from Group Delay Function*, "Speech Communication" 1991, 10(3), 209–221, [https://doi.org/10.1016/0167-6393\(91\)90008-K](https://doi.org/10.1016/0167-6393(91)90008-K).
- [76] McAuliffe M., Socolof M., Mihuc S. et al., *Montreal Forced Aligner*, w: *Interspeech*, 2017, 498–502, <https://doi.org/10.21437/Interspeech.2017-1386>.
- [77] Patel Y., Tanwar S., Gupta R. et al., *Deepfake Generation and Detection*, IEEE Access 2023, 11, 143296–143323, <https://doi.org/10.1109/ACCESS.2023.3342844>.
- [78] Shen J., Pang R., Weiss R.J. et al., *Natural TTS Synthesis by Conditioning WaveNet*, w: *ICASSP*, 2018, 4779–4783, <https://doi.org/10.1109/ICASSP.2018.8461368>.
- [79] Kim J., Kong J., Son J., *Conditional Variational Autoencoder with Adversarial Learning*, w: *ICML*, 2021, 5530–5540.
- [80] Jędrasiak K., *Audio Stream Analysis for Deep Fake Threat Identification*, Civitas et Lex 2024, 41(1), 21–35.
- [81] Elliott T.M., Theunissen F.E., *The Modulation Transfer Function for Speech Intelligibility*, "PLoS Computational Biology" 2009, 5(3), e1000302, <https://doi.org/10.1371/journal.pcbi.1000302>.
- [82] Houtgast T., Steeneken H.J., *A Review of the MTF Concept*, "Journal of the Acoustical Society of America" 1985, 77(3), 1069–1077, <https://doi.org/10.1121/1.392224>.
- [83] Hillenbrand J., Houde R.A., *Acoustic Correlates of Breathiness Vocal Quality*, "Journal of Speech, Language, and Hearing Research" 1996, 39(2), 311–321, <https://doi.org/10.1044/jshr.3902.311>.
- [84] Benjamini Y., Hochberg Y., *Controlling the False Discovery Rate*, Journal of the Royal Statistical Society B 1995, 57(1), 289–300, <https://doi.org/10.1111/j.2517-6161.1995.tb02031.x>.
- [85] Efron B., Tibshirani R.J., *An Introduction to the Bootstrap*, Chapman & Hall/CRC, 1994.
- [86] Tomashenko N., Wang X., Vincent E. et al., *Supplementary Material to the Paper "The VoicePrivacy 2020 Challenge"* 2022.

KAROL JĘDRASIAK, PH.D. ENG. – academic teacher, didactician and manager, author of over 88 scientific publications, including 3 scientific monographs with high citability. The author's scientific experience includes participation in 26 research and development projects, also as a manager. Active participant in more than 30 scientific conferences and symposia. Expert of the WSL2014-2020 ROP, member of the Steering Committee of the Game INN Sector Program and the Society for Image Processing. As a result of his previous work and cooperation with industry, he participated in the development of 32 claims of intellectual property rights (6 granted patents, 8 patent applications, 18 design registration rights). Specialist in computer vision, computer graphics, artificial intelligence tools, computer, database and sensor system development. Since 2008, he has held management positions in private companies. For many years he was CEO of VR Technology, a company developing algorithms in the area of data analysis, commercializing innovative solutions in virtual reality technology and simulation as well as coaching systems. In 2024, he was awarded the Medal of the National Education Commission and a certificate of appreciation for his exceptional contribution to the successful implementation of the "e-Instructor Certification Programme" by NATO Assistant Secretary General for Operations Tom Goffus.

DR INŻ. KAROL JĘDRASIAK – nauczyciel akademicki, dydaktyk i menadżer, autor ponad 88 publikacji naukowych, w tym trzech monografii naukowych, o wysokiej cytowalności. Jego doświadczenie naukowe obejmuje udział w 26 projektach badawczo-rozwojowych, w tym w charakterze kierownika projektu. Aktywny uczestnik w ponad 30 konferencjach i sympozjach. Ekspert RPO WSL/POIR, członek Komitetu Sterującego Programu Sektorowego GameINN, członkiem Towarzystwa Przetwarzania Obrazów. W rezultacie dotychczasowej pracy oraz współpracy z przemysłem powstało 32 zastrzeżeń prawa własności intelektualnej (6 przyznanych patentów, 8 zgł. patentowych, 18 praw z rejestracji wzoru przemysłowego). Specjalista w zakresie wizji komputerowej, wirtualnej rzeczywistości, narzędzi sztucznej inteligencji, wytwarzania systemów informatycznych, bazodanowych i sensorycznych. Od 2008 piastował stanowiska kierownicze w przedsiębiorstwach prywatnych. Przez wiele lat był Prezesem Zarządu spółki VR-Technology zajmującej się opracowywaniem algorytmów z zakresu analizy danych oraz komercjalizacją innowacyjnych rozwiązań z zakresu technologii wirtualnej rzeczywistości oraz profesjonalnych systemów symulacyjnych i trenażerowych. W 2024 został uhonorowany Medalem Komisji Edukacji Narodowej oraz certyfikatem uznania za wyjątkowy wkład w pomyślną realizację „Programu Certyfikacji e-Instruktorów”, nadanym przez Asystenta Sekretarza Generalnego NATO ds. Operacji Toma Goffusa.



CNBOP-PIB

SFT

SAFETY & FIRE TECHNOLOGY



MONOGRAFIE



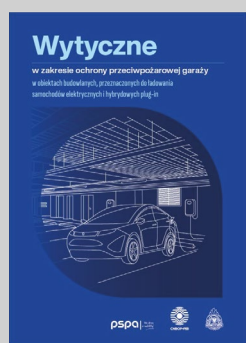
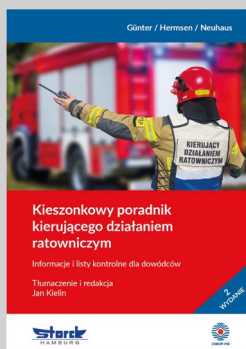
WYTYCZNE



STANDARDY

PORADNIKI

CZASOPISMO
NAUKOWE



DYSCYPLINY
według MNiSW

inżynieria chemiczna
inżynieria materiałowa
inżynieria środowiska, górnictwo i energetyka
nauki o bezpieczeństwie

ZAKRES TEMATYCZNY

- teoria i modelowanie rozwoju pożaru
- metody i środki zapobiegania pożarom oraz ograniczania ich skutków
- dochodzenia popożarowe i analiza ryzyka pożaru
- taktyka, technika i bezpieczeństwo w działaniach ratowniczo-gaśniczych
- aspekty prawne i edukacja w ochronie przeciwpożarowej
- bezpieczeństwo i ochrona ludności
- zagrożenia i ochrona środowiska
- materiały w ochronie środowiska i zagrożeniach pożarowych
- nowoczesne technologie w ochronie przeciwpożarowej i ochronie środowiska



80 pkt MNiSW



BazTech
EBSCO

DOAJ
DIRECTORY OF
OPEN ACCESS
JOURNALS

INDEX
COPERNICUS
INTERNATIONAL

CENTRUM NAUKOWO-BADAWCZE
OCHRONY PRZECIWOPOŻAROWEJ
im. Józefa Tuliszkowskiego
PAŃSTWOWY INSTYTUT BADAWCZY
ul. Nadwiślańska 213
05-420 Józefów k. Otwocka

TWÓJ PARTNER
w **BEZPIECZEŃSTWIE**

Karol Łyziński, Arkadiusz Trzos

Jagiellonian University Medical College, Department of Anaesthesiology and Intensive Care, Department of Disaster and Emergency Medicine / Uniwersytet Jagielloński Collegium Medicum, Wydział Lekarski, Katedra Anestezjologii i Intensywnej Terapii, Zakład Medycyny Katastrof i Pomocy Doraźnej

Jagiellonian University Medical College, Department of Anaesthesiology and Intensive Care / Uniwersytet Jagielloński Collegium Medicum, Wydział Lekarski, Katedra Anestezjologii i Intensywnej Terapii, Atmed, Bielsko Biała

Corresponding author / Autor korespondencyjny: karol.lyzinski@uj.edu.pl

A New Medical Doctrine for CBRNE Threats: a Framework for Developing Poland's Emergency Medical Services, Civil Protection and Civil Defence

Nowa doktryna medyczna wobec zagrożeń CBRNE – kierunek rozwoju systemu ratownictwa medycznego, ochrony ludności i obrony cywilnej w Polsce

ABSTRACT

Purpose: The purpose of the article is to present the proposition of a modern medical doctrine for chemical, biological, radiation, nuclear and explosive (CBRNE) threats for Poland, focused on the emergency medical services and their connections with health protection, civil protection and civil defence. The proposed doctrine arranges priorities and compromises in relation to activities under the conditions of uncertainty, time pressure and limited resources.

Introduction: From a medical perspective, the primary task is to quickly identify the consequences of an incident and to initiate protection and treatment activities even if the cause of the incident is yet to be clearly determined. The course of care is influenced by: the need for personal protection equipment, the decontamination process and the risk of secondary exposure. The effectiveness of system response is in addition limited by information pressure (including contradictory reports, misinformation and communication overload), as well as disruption of infrastructure and communication (which may destabilise health protection operations regardless of the number of victims). In that perspective, the article presents emergency medical services as an integral part of the public safety, civil protection and civil defence system that requires interoperability and coordinated cooperation with the national rescue and firefighting system and other CBRNE crisis response entities.

Methodology: The article is conceptual in nature and based on a focused narrative review with thematic synthesis. The starting point was the analysis of literature and expert materials in a work repository comprising 308 items from 2020–2025. Following a multi-stage selection, sources of highest operational and medical usability and credibility were included in the qualitative analysis and synthesis. The publications covered medical rescue and hospital operations under CBRNE threats, mass incidents and patient care organisation and coordination. Works unrelated to the medical or operational dimension were excluded. On that basis, thematic categorisation was conducted and ten pillars were introduced as areas of critical capabilities determining the feasibility of medical operations.

Conclusions: The proposed doctrine consists of ten pillars of feasibility of medical operations for CBRNE incidents, related to risk identification, personnel safety, operational effectiveness, coordination, information and detection, care continuity, logistics, cooperation, education, risk communication and social resilience. This framework is a starting point for the development of strategies, minimum performance standards and readiness criteria and then their testing and further validation.

Keywords: emergency medical services, medical doctrine, CBRNE threats, state readiness, crisis response, civil protection and civil defence, crisis management.

Type of article: review article

Received: 04.02.2026; Reviewed: 13.02.2026; Accepted: 02.03.2026;

Authors' ORCID IDs: K. Łyziński - 0000-0003-3292-2459; A. Trzos - 0000-0002-4390-0901;

Percentage contribution: K. Łyziński – 75%; A. Trzos – 25%;

Please cite as: Safety & Fire Technology 2026, 1, 86–105, <https://doi.org/10.12845/sft.67.1.2026.4>;

This is an open access article under the CC BY-SA 4.0 license (<https://creativecommons.org/licenses/by-sa/4.0/>).

ABSTRAKT

Cel: Celem artykułu jest przedstawienie propozycji nowoczesnej doktryny medycznej wobec zagrożeń chemicznych, biologicznych, radiacyjnych, nuklearnych i wybuchowych (CBRNE) dla Polski, ukierunkowanej na system ratownictwa medycznego oraz jego powiązania z ochroną zdrowia, ochroną ludności i obroną cywilną. Proponowana doktryna porządkuje priorytety i kompromisy w odniesieniu do działań w warunkach niepewności, presji czasu i ograniczonych zasobów.

Wprowadzenie: Z perspektywy medycznej nadrzędnym zadaniem jest szybkie rozpoznanie skutków zdarzenia oraz uruchomienie działań ochronnych i leczniczych, nawet jeśli źródło incydentu nie zostało jeszcze jednoznacznie ustalone. Na przebieg opieki wpływają: konieczność pracy w środkach ochrony indywidualnej, prowadzenie dekontaminacji oraz ryzyko wtórnej ekspozycji. Skuteczność odpowiedzi systemowej dodatkowo ograniczają presja informacyjna (obejmująca sprzeczne raporty, dezinformację i przeciążenie komunikacji), a także zakłócenia infrastruktury oraz łączności (które mogą destabilizować funkcjonowanie ochrony zdrowia niezależnie od liczby poszkodowanych). W tym ujęciu artykuł przedstawia ratownictwo medyczne jako integralny element systemu bezpieczeństwa, ochrony ludności i obrony cywilnej, wymagający interoperacyjności oraz skoordynowanego współdziałania z krajowym systemem ratowniczo-gaśniczym i innymi podmiotami reagowania kryzysowego w zdarzeniach CBRNE.

Metodologia: Artykuł ma charakter koncepcyjny i opiera się na ukierunkowanym przeglądzie narracyjnym z syntezą tematyczną. Punktem wyjścia była analiza piśmiennictwa i materiałów eksperckich ujętych w repozytorium roboczym obejmującym 308 pozycji z lat 2020–2025. Po selekcji etapowej do analizy jakościowej i syntezy włączono źródła o najwyższej przydatności operacyjno-medycznej i wiarygodności. Uwzględniano publikacje dotyczące działań ratowniczo-medycznych i szpitalnych podczas zagrożeń CBRNE, zdarzeń masowych oraz organizacji i koordynacji opieki nad pacjentem. Wyłączano prace niezwiązane z wymiarem medycznym lub operacyjnym. Na tej podstawie przeprowadzono kategoryzację tematyczną i wyprowadzono dziesięć filarów jako obszary krytycznych zdolności warunkujących wykonalność działań medycznych.

Wnioski: Zaproponowana doktryna obejmuje dziesięć filarów wykonalności działań medycznych w zdarzeniach CBRNE, odnoszących się do rozpoznania ryzyka, bezpieczeństwa personelu, sprawności operacyjnej, koordynacji, informacji i detekcji, ciągłości opieki, logistyki, współdziałania, edukacji oraz komunikacji ryzyka i odporności społecznej. Rama ta stanowi punkt wyjścia do opracowania strategii, minimalnych standardów wykonawczych i kryteriów gotowości, a następnie ich sprawdzenia w ćwiczeniach oraz dalszej walidacji.

Słowa kluczowe: ratownictwo medyczne, doktryna medyczna, zagrożenia CBRNE, gotowość państwa, reagowanie kryzysowe, ochrona ludności i obrona cywilna, zarządzanie kryzysowe

Typ artykułu: artykuł przeglądowy

Przyjęty: 04.02.2026; **Zrecenzowany:** 13.02.2026; **Zaakceptowany:** 02.03.2026;

Identyfikatory ORCID autorów: K. Łyziński - 0000-0003-3292-2459; A. Trzos - 0000-0002-4390-0901;

Procentowy wkład merytoryczny: K. Łyziński – 75%; A. Trzos – 25%;

Proszę cytować: Safety & Fire Technology 2026, 1, 86–105, <https://doi.org/10.12845/sft.67.1.2026.4>;

Artykuł udostępniany na licencji CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>).

Introduction

Any changes in the structure and funding principles of emergency medical services and health protection in the area of civil protection and civil defence require prior definition of a coherent response concept. This applies in particular to changes in response to evolving chemical, biological, radiation, nuclear and explosive (CBRNE) threats. This concept may be formulated as a doctrine, which is an organised reference for the decision-makers responsible for system development and adaptation.

The doctrine is a systematic set of assumptions, principles and priorities that direct the institution under the conditions of uncertainty, time pressure and limited resources. It is not a catalogue of procedures, but a framework that defines primary purposes, organises the understanding of threats and states the compromises acceptable in extreme situations [1]. From the systemic perspective, the doctrine forms a common language for many entities, which enables coherent planning, training and cooperation [1–2].

A medical doctrine is a special form of doctrine, which focuses on life and health protection and healthcare organisation. In disaster medicine, it organises the relationships between clinical priorities and operational constraints: it defines the framework for medical operations under the conditions of resources shortage, defines the acceptable risk limits for personnel and defines the principles of integration of pre-hospital operations with the capacity of hospitals and the entire health protection system in a long-term perspective [2–3].

CBRNE threats are a particular challenge for the medical doctrine. The operating conditions, including the need for personal protection equipment (PPE), decontamination processes and

Wstęp

Wszelkie zmiany w strukturze i zasadach funkcjonowania systemu ratownictwa medycznego oraz ochrony zdrowia w obszarze ochrony ludności i obrony cywilnej (OLiOC) wymagają uprzedniego określenia spójnej koncepcji reagowania. Dotyczy to w szczególności zmian podejmowanych w odpowiedzi na zmieniające się zagrożenia chemiczne, biologiczne, radiacyjne, nuklearne i wybuchowe (CBRNE). Koncepcję tę można ująć w formie doktryny, która stanowi uporządkowany punkt odniesienia dla decydentów odpowiedzialnych za rozwój i dostosowanie systemu.

Doktryna jest usystematyzowanym zbiorem założeń, zasad i priorytetów, które ukierunkowują działanie instytucji w warunkach niepewności, presji czasu i ograniczonych zasobów. Nie jest katalogiem procedur, lecz ramą, która definiuje cele nadrzędne, porządkuje sposób rozumienia zagrożeń oraz wskazuje dopuszczalne kompromisy w sytuacjach skrajnych [1]. W ujęciu systemowym doktryna tworzy wspólny język dla wielu podmiotów, umożliwiając spójne planowanie, szkolenie i współdziałanie [1–2].

Doktryna medyczna jest szczególną postacią doktryny, skoncentrowaną na ochronie życia i zdrowia oraz organizacji opieki medycznej. W medycynie katastrof porządkuje relacje między priorytetami klinicznymi a ograniczeniami operacyjnymi: definiuje ramy działań medycznych w warunkach niedoboru zasobów, określa granice akceptowalnego ryzyka personelu oraz zasady integracji działań przedszpitalnych z możliwościami szpitali i całego systemu ochrony zdrowia w perspektywie długoterminowej [2–3].

Szczególnym wyzwaniem dla doktryny medycznej są zagrożenia CBRNE. Warunki prowadzenia działań, w tym konieczność pracy w środkach ochrony indywidualnej (ŚOI), procesy

the risk of secondary exposure, directly determine the course of care and clinical decisions [4]. In parallel, information pressure covering the uncertainty and conflict of reports, misinformation and the overload of communication and information exchange between services and health protection entities impedes the decision-making and coordination of operations [5]. In addition, the risk of the disruption of operating continuity of health protection components has a direct impact on system response effectiveness [5]. The experience of the COVID-19 pandemic in Europe showed that a biological incident may impose long-term constraints on the operational capability of the system by facility overloads, essential resources (e.g. PPE) shortages and information and misinformation pressures [6]. In Polish reality, the inconsistency of preparation and the uneven development of competences, resources and interoperational capabilities persist. In addition, under hybrid threat conditions, including i.a. disruption of infrastructure and communication, cyberattacks and information and misinformation pressures, the probability of occurrence of complex and long-term scenarios is increased [7–9].

The response to CBRNE incidents is operational and systemic in nature and it requires close cooperation of emergency medical services, broadly understood as pre-hospital and hospital operations, with the national rescue and firefighting system and other civil protection and public administration entities by means appropriate coordination mechanisms. From this perspective, emergency medical services are an integral part of civil safety and crisis response, which directly conditions the feasibility of medical operations: it integrates clinical decisions with rescue personnel safety, zone organisation, logistics and organised cooperation of services.

In addition, tasks arising from the national framework of civil protection and civil defence constitute essential context. Broadly understood emergency medical services and healthcare are entities responsible for civil protection and civil defence tasks, which implies obligation to prepare for operation in case of crisis situations, including CBRNE incidents [10]. In the current safety situation of the Republic of Poland, this responsibility is particularly relevant, as medical readiness becomes a component of state resilience and continuous operation of essential public services [5], [7].

Poland lacks a coherent doctrine focused on emergency medical services to organise operating compromises (safety – effectiveness – continuity) and integrate emergency medical services with the national rescue and firefighting system and civil protection and civil defence in the context of CBRNE threats. The purpose of this article is to present a proposition of such medical doctrine and its integration with health protection, the national rescue and firefighting system and civil protection and civil defence. This doctrine is formulated as ten pillars defining the priorities and requirements for preparing and conducting medical operations. The article is conceptual in nature and constitutes a starting point for further staged works: from deriving minimum performance standards and training assumptions, through testing them in exercises and simulations, to refining them based on expert assessment and case studies, as well as mapping pillars on real incidents. The relationships between the pillars are presented in Figure 1.

dekontaminacji i ryzyko wtórnej ekspozycji, bezpośrednio kształtują przebieg opieki i decyzje kliniczne [4]. Równolegle presja informacyjna obejmująca niepewność i sprzeczność raportów, dezinformację oraz przeciążenie komunikacji i obiegu informacji między służbami i podmiotami ochrony zdrowia utrudnia podejmowanie decyzji i koordynację działań [5]. Dodatkowo ryzyko zakłócenia ciągłości działania elementów ochrony zdrowia bezpośrednio wpływa na skuteczność odpowiedzi systemowej [5]. Doświadczenia z pandemii COVID-19 w Europie pokazały, że zdarzenie biologiczne może długotrwale ograniczać zdolność systemu do działania poprzez przeciążenie placówek, braki w kluczowych zasobach (np. ŚOI) oraz presję informacyjną i dezinformację [6]. W polskich realiach nadal utrzymuje się nieśpójność przygotowania oraz nierównomierny rozwój kompetencji, zasobów i zdolności interoperacyjnych. Dodatkowo w warunkach zagrożeń hybrydowych, obejmujących m.in. zakłócenia infrastruktury i łączności, cyberataki oraz presję informacyjną i dezinformację, zwiększa się prawdopodobieństwo wystąpienia scenariuszy złożonych i długotrwałych [7–9].

Reagowanie na zdarzenia CBRNE ma charakter operacyjno-systemowy i wymaga ścisłego współdziałania systemu ratownictwa medycznego – rozumianego szeroko jako działania przedszpitalne i szpitalne – z krajowym systemem ratowniczo-gaśniczym oraz innymi podmiotami ochrony ludności i administracji publicznej, przy wykorzystaniu odpowiednich mechanizmów koordynacji. W tym ujęciu ratownictwo medyczne stanowi integralny element bezpieczeństwa cywilnego i reagowania kryzysowego, ponieważ bezpośrednio warunkuje wykonalność działań medycznych: łączy decyzje kliniczne z bezpieczeństwem ratowników, organizacją stref, logistyką oraz uporządkowanym współdziałaniem służb.

Dodatkowy, istotny kontekst stanowią zadania wynikające z krajowych ram ochrony ludności i obrony cywilnej. Szeroko rozumiane ratownictwo medyczne oraz ochrona zdrowia są podmiotami realizującymi zadania OLiOC, co implikuje obowiązek przygotowania do działania w sytuacjach kryzysowych, w tym w zdarzeniach CBRNE [10]. W aktualnym środowisku bezpieczeństwa Rzeczypospolitej Polskiej obowiązek ten nabiera szczególnego znaczenia, ponieważ gotowość medyczna staje się elementem odporności państwa i ciągłości funkcjonowania kluczowych usług publicznych [5], [7].

W polskich realiach brakuje spójnej doktryny ukierunkowanej na ratownictwo, która porządkowałaby kompromisy działania (bezpieczeństwo – skuteczność – ciągłość) i integrowała system ratownictwa medycznego z KSRG oraz ramami OLiOC w kontekście zagrożeń CBRNE. Celem niniejszego artykułu jest przedstawienie propozycji takiej doktryny medycznej oraz powiązania jej z ochroną zdrowia, KSRG i OLiOC. Doktryna ta została ujęta jako dziesięć filarów wyznaczających priorytety i wymagania dla przygotowania oraz prowadzenia działań medycznych. Artykuł ma charakter koncepcyjny i stanowi punkt wyjścia do dalszych prac prowadzonych etapowo: od wyprowadzenia minimalnych standardów wykonawczych i założeń szkoleniowych, przez ich sprawdzenie w ćwiczeniach i symulacjach, po doprecyzowanie w oparciu o ocenę ekspercką, analizę przypadków i mapowanie filarów na realne incydenty. Zależności między filarami przedstawiono na rycinie 1.

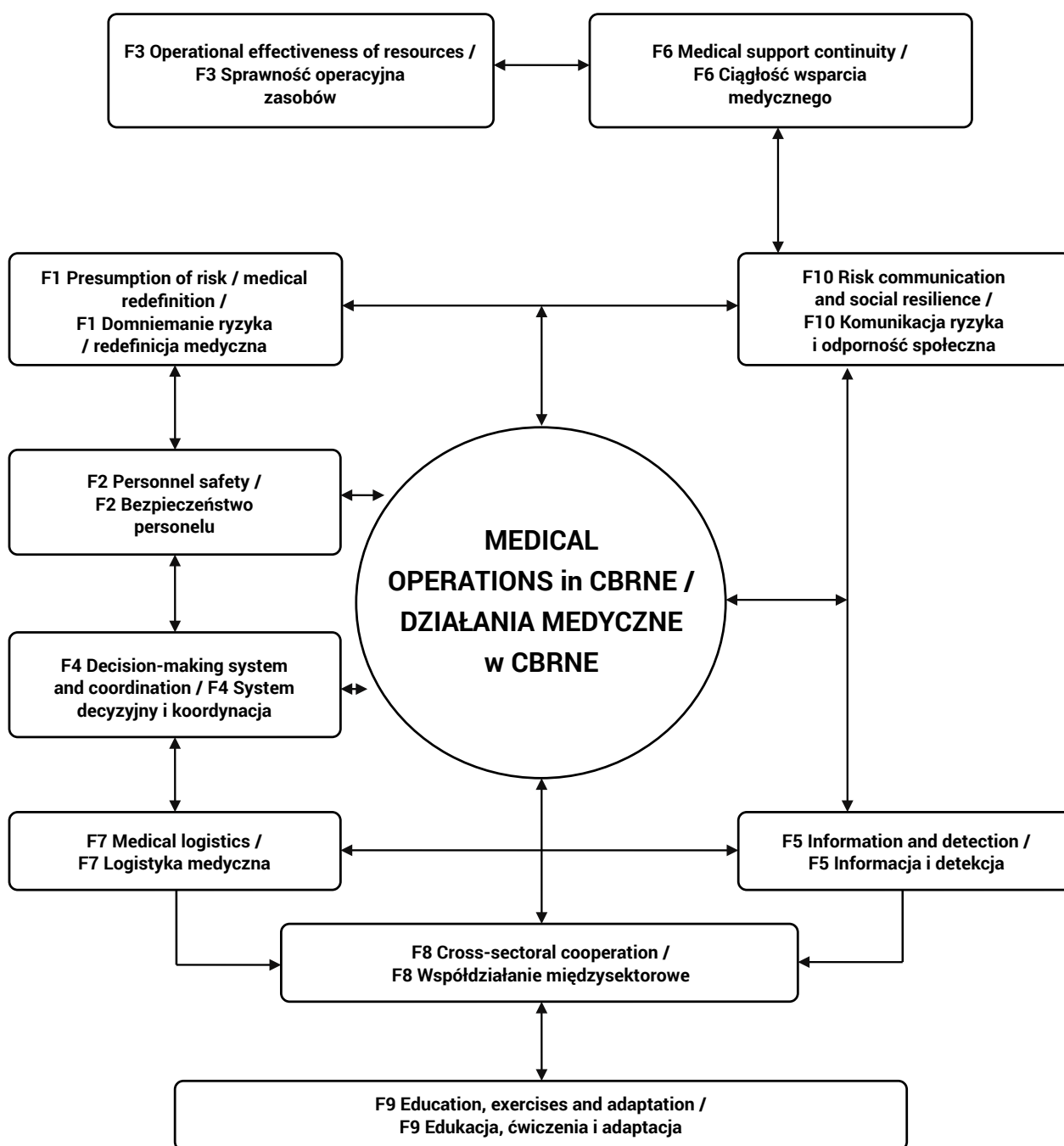


Figure 1. Map of medical doctrine pillars in view of CBRNE threats
Rycina 1. Mapa filarów doktryny medycznej wobec zagrożeń CBRNE

Source: Own elaboration.

Źródło: Opracowanie własne.

Methodology

The article is conceptual in nature and based on a focused narrative review with thematic synthesis. Its purpose was to organise the key domains conditioning the feasibility of medical operations for CBRNE incidents. The starting point was the analysis of literature and expert materials in a work repository comprising 308 items from 2020-2025 (scientific articles, book

Metodologia

Artykuł ma charakter koncepcyjny i opiera się na ukierunkowanym przeglądzie narracyjnym z syntezą tematyczną, którego celem było uporządkowanie kluczowych domen zdolności warunkujących wykonalność działań medycznych w zdarzeniach CBRNE. Punktem wyjścia była analiza piśmiennictwa i materiałów eksperckich ujętych w repozytorium roboczym obejmującym

chapters, conference papers and institutional documents: guidelines, reports and standards).

Following a multi-stage selection, 43 sources of highest operational and medical usability and credibility were included in the qualitative analysis and thematic synthesis. The materials were identified by searching in literature databases (e.g. PubMed, Scopus/Web of Science, Google Scholar) and by reviewing publications and institutional documents, using a combination of keywords related to: CBRNE/HAZMAT, disaster medicine, pre-hospital and hospital rescue (first contact units), mass incidents, decontamination, personnel safety (PPE and collective protection), medical logistics, coordination and command, decision-making support and risk communication. A supplementary literature review in key publications was conducted to include essential institutional documents (guidelines, norms, standards). The search and selection of materials was conducted in the 06/2025–12/2025 period. The identification and selection process was conducted in stages.

The selection was conducted in two steps: the first step was a pre-selection based on the title and abstract, the second step was the assessment of full texts for inclusion/exclusion criteria and operational and medical usability. The publications selected for the analysis were directly related to rescue and medical operations and the functioning of health protection in case of CBRNE incidents, to mass incidents and to the organisation and coordination of patient care. The works rejected were strictly technological, engineering or military in nature, without relevance for clinical decisions, organisation and medical logistics. The quality and credibility of sources was assessed pragmatically, according to the conceptual nature of the work and heterogeneity of the material (studies, reviews, guidelines, standards). Priority was given to reviewed publications and documents with clearly identified institutional authorship and transparent material basis. Works with low transparency of sources or opinion-forming in nature, without literature basis, were considered as auxiliary material and not used as basis for key conclusions. Due to the purpose of the work (conceptual synthesis and derivation of doctrine framework), no formal systematic review procedure (PRISMA) or evidence quality evaluation tools (GRADE) were used. Selection focused on operational usability and coherence with disaster medicine practice. The review was designed according to reliability and transparency principles for narrative articles (SANRA, scale for the assessment of narrative review articles). The synthesis was conducted by thematic categorisation of conclusions into the areas of system capabilities (i.e. personnel safety, decontamination, segregation, care continuity, logistics, coordination and command, information/detection, cooperation and risk communication), followed by consolidation of these areas into ten pillars of the doctrine as critical domains conditioning the feasibility of medical operations in case of CBRNE incidents. The next stage of works is validating pillars by means of exercises, simulations, case studies and expert process

308 pozycji z lat 2020–2025 (artykuły naukowe, rozdziały książek, publikacje konferencyjne oraz dokumenty instytucjonalne: wytyczne, raporty i normy).

Po selekcji etapowej do analizy jakościowej i syntezy tematycznej włączono 43 źródła o najwyższej przydatności operacyjno-medycznej i wiarygodności. Materiały identyfikowano poprzez przeszukiwanie baz literaturowych (m.in. PubMed, Scopus/Web of Science, Google Scholar) oraz przegląd publikacji i dokumentów instytucjonalnych, z wykorzystaniem kombinacji słów kluczowych odnoszących się do: CBRNE/HAZMAT, medycyny katastrof, ratownictwa przedszpitalnego i szpitalnego (jednostki pierwszego kontaktu), zdarzeń masowych, dekontaminacji, bezpieczeństwa personelu (ŚOI i ochrona zbiorowa), logistyki medycznej, koordynacji i dowodzenia, wsparcia decyzji oraz komunikacji ryzyka. Uzupełniając przeprowadzono przegląd bibliografii w publikacjach kluczowych oraz włączono istotne dokumenty instytucjonalne (wytyczne, normy, standardy). Wyszukiwanie i dobór materiałów przeprowadzono w okresie 06.2025–12.2025. Proces identyfikacji i selekcji prowadzono etapowo.

Selekcję realizowano w dwóch krokach: pierwszym był wstępny odsiew na podstawie tytułu i streszczenia, drugim zaś ocena pełnych tekstów pod kątem kryteriów włączenia/wyłączenia i przydatności operacyjno-medycznej. Do analizy wybierano publikacje odnoszące się bezpośrednio do działań ratowniczo-medycznych i funkcjonowania ochrony zdrowia w zdarzeniach CBRNE, zdarzeń masowych oraz organizacji i koordynacji opieki nad pacjentem. Odrzucano prace o charakterze wyłącznie technologicznym, inżynierskim lub militarnym, które nie przekładały się na decyzje kliniczne, organizacyjne ani logistykę medyczną. Jakość i wiarygodność źródeł oceniano pragmatycznie, adekwatnie do koncepcyjnego charakteru pracy i heterogeniczności materiału (badania, przeglądy, wytyczne, normy). Priorytet nadawano publikacjom recenzowanym oraz dokumentom o jasno określonym autorstwie instytucjonalnym i przejrzystych podstawach merytorycznych. Prace o niskiej przejrzystości źródeł lub o charakterze opiniotwórczym, bez oparcia w literaturze, traktowano jako materiał pomocniczy i nie wykorzystywano ich jako podstawy kluczowych wniosków. Ze względu na cel pracy (synteza koncepcyjna i wyprowadzenie ram doktrynalnych) nie używano formalnej procedury przeglądu systematycznego (PRISMA) ani narzędzi oceny jakości dowodów (GRADE). Zastosowano selekcję ukierunkowaną na użyteczność operacyjną i spójność z praktyką medycyny katastrof. Przegląd opracowano z uwzględnieniem zasad rzetelności i transparentności właściwych dla przeglądów narracyjnych (ang. *scale for the assessment of narrative review articles*, SANRA). Syntezę przeprowadzono poprzez kategoryzację tematyczną wniosków w obszary zdolności systemu (m.in. bezpieczeństwo personelu, dekontaminacja, segregacja, ciągłość opieki, logistyka, koordynacja i dowodzenie, informacja/detekcja, współdziałanie oraz komunikacja ryzyka), a następnie konsolidację tych obszarów do dziesięciu filarów doktryny jako domen krytycznych warunkujących wykonalność działań medycznych w zdarzeniach CBRNE. Walidacja filarów w ćwiczeniach, symulacjach, analizach przypadków oraz w procesie eksperckim stanowi kolejny etap prac.

Medical doctrine pillars in view of CBRNE threats

Pillar 1. Medical redefinition of CBRNE threats and presumption of risk principle

The starting point of the doctrine is redefinition of CBRNE threats from the medical perspective. In classical terms, CBRNE is connected above all with weapons of mass destruction (military use) or incidents of terrorist nature [11]. From the perspective of medical operations, the type of incident, its nature and the use of agent remain relevant, however at the initial stage, they do not determine key clinical and organisational decisions. It arises from the fact that the CBRNE component can be overt, covert or presumed. In the medical rescue system, the incident consequences understood as the required personnel protection level, the risk of secondary exposure, the necessity, scope and type of decontamination, the adjustment of medical segregation, the course of treatment and the impact on the continuous operation of health protection infrastructure [4], [12].

In the framework of medical redefinition, the principle of presumption of risk is adopted, according to which any incident with unclear aetiology or component of hazardous substances and materials (HAZMAT) should be initially considered as potential CBRNE incident, until credibly excluded. This approach limits decision-making delays and reduces the time until implementation of safeguards and proper mode of rescue and medical operations [12].

The redefinition also includes indirect factors, which may initiate or modify CBRNE incidents, including the disruptions of rescue and medical infrastructure (e.g. power outages), cyberattacks, information and misinformation pressures, as well as environmental and climatic factors, which may contribute to the escalation of incidents and facilitate the spreading of effects, including the release of hazardous materials and secondary medical consequences [13–14]. These conditions form a common denominator for operations in non-permissive environment, which constitutes a permanent background for medical operations, in which standard rescue and medical procedures are subject to significant restrictions [4].

As a consequence, the doctrine assumes a broad view of CBRNE threats, focusing on early identification and risk reduction, assuming that operations will be conducted under the conditions of risk, which cannot be fully eliminated.

Pillar 2. Safety of medical personnel with conscious risk acceptance

By definition, emergency medical services work under the conditions of threat. In case of CBRNE incidents, risk is multi-dimensional and includes the exposure of personnel, secondary contamination of patients, equipment and infrastructure, short-term and long-term health consequences and the risk of the loss of operating capability caused by exclusion of people and key components of the rescue and medical system. This pillar allows taking an increased risk following a conscious threat assessment and implementing operations to reduce exposure and contamination, so that the risk level remain proportional to the expected clinical benefit, while not causing the system to lose the capability for further operation.

Filary doktryny medycznej wobec zagrożeń CBRNE

Filar 1. Medyczna redefinicja zagrożeń CBRNE i zasada domniemanie ryzyka

Punktem wyjścia doktryny jest redefinicja zagrożeń CBRNE z perspektywy medycznej. W ujęciu klasycznym CBRNE jest związane przede wszystkim z bronią masowego rażenia (użycie militarne) lub zdarzeniami o charakterze terrorystycznym [11]. Z perspektywy działań medycznych rodzaj zdarzenia, jego charakter oraz sposób użycia czynnika pozostają istotne, jednak w fazie wstępnej nie przesądzają o kluczowych decyzjach klinicznych i organizacyjnych. Wynika to z tego, że komponent CBRNE może być jawny, ukryty albo domniemany. W systemie ratownictwa medycznego rozstrzygające są konsekwencje zdarzenia rozumiane jako wymagany poziom zabezpieczenia personelu, ryzyko wtórnej ekspozycji, konieczność oraz zakres i rodzaj dekontaminacji, dostosowanie segregacji medycznej, sposób prowadzenia leczenia oraz wpływ na ciągłość funkcjonowania infrastruktury ochrony zdrowia [4], [12].

W ramach redefinicji medycznej przyjmuje się zasadę domniemanie ryzyka, zgodnie z którą zdarzenie o niejasnej etiologii lub z komponentem substancji i materiałów niebezpiecznych (HAZMAT) należy wstępnie traktować jako potencjalnie CBRNE, dopóki nie zostanie to wiarygodnie wykluczone. Takie podejście ogranicza opóźnienia decyzyjne i skraca czas do wdrożenia zabezpieczeń oraz właściwego trybu działań ratowniczo-medycznych [12].

Redefinicja uwzględnia również czynniki pośrednie, które mogą inicjować lub modyfikować zdarzenia CBRNE, w tym zakłócenia infrastruktury ratowniczo-medycznej (np. przerwy w dostawach energii), cyberataki, presję informacyjną i dezinformację oraz czynniki środowiskowe i klimatyczne, które mogą sprzyjać eskalacji zdarzeń i ułatwiać rozprzestrzenianie skutków, w tym uwolnień materiałów niebezpiecznych i wtórnych następstw medycznych [13–14]. Uwarunkowania te tworzą wspólny mianownik działań w środowisku nieprzyjawnym (ang. *non-permissive*), stanowiącym trwałe tło działań medycznych, w którym standardowe procedury ratowniczo-medyczne ulegają istotnym ograniczeniom [4].

W konsekwencji doktryna przyjmuje szerokie ujęcie zagrożeń CBRNE, kładąc nacisk na wczesne rozpoznanie i ograniczenie ryzyka, przy założeniu, że działania będą prowadzone w warunkach ryzyka, którego nie da się całkowicie wyeliminować.

Filar 2. Bezpieczeństwo personelu medycznego przy świadomej akceptacji ryzyka

Ratownictwo medyczne z definicji działa w warunkach zagrożenia. W zdarzeniach CBRNE ryzyko jest wielowymiarowe i obejmuje ekspozycję personelu, wtórne skażenie pacjentów, sprzętu oraz infrastruktury, następstwa zdrowotne wczesne i odległe oraz ryzyko utraty zdolności operacyjnej wskutek wyłączenia ludzi i kluczowych elementów systemu ratowniczo-medycznego. Filar ten dopuszcza podejmowanie podwyższonego ryzyka po świadomej ocenie zagrożenia i wdrożeniu działań ograniczających ekspozycję i skażenie, tak aby poziom ryzyka pozostawał proporcjonalny do spodziewanej korzyści klinicznej, a system nie tracił zdolności do dalszego działania.

The most important component of the pillar is the availability and readiness of resources that enable safe medical operations, including the selection and availability of PPE, the activation of response procedures for CBRNE incidents and the adjustment of infrastructure operation. It also includes collective protection, understood as organisational and technical preparation of facilities, at which the personnel works, to reduce the exposure and risk of secondary contamination (e.g. separation of zones and passageways, isolation, ventilation and decontamination solutions). A practical reference point can be the infectious diseases unit, where safety is ensured not only by the equipment of personnel, but also by the zoning regime and isolation and transmission control support infrastructure.

The doctrine emphasises that the development of this segment is a pre-requisite of operational effectiveness. Personal protection must enable rescue and medical procedures, not only isolate the medical personnel. In a majority of realistic scenarios, the protection level corresponding to level C¹ will be sufficient for medical operations, however selected hospital emergency departments and trauma centres and hospital specialised departments should be prepared to work at higher protection levels (B, A) if required by the conditions and clinical purpose [4], [15].

Personnel safety is ensured by the implementation of collective protection principles, organisation of operation zones, entry and exit principles, requirements for medical infrastructure and safe and responsible operation standards. It also includes operation interruption and termination criteria and procedures after personnel exposure to a hazardous agent. In non-permissive environment, the identification of the feasibility limit for rescue and medical operations under risk conditions and such risk management that prevents losing the system capability to help subsequent patients become prominent. Another component of the pillar is psychological preparation and post-incident support mechanisms, because operations under CBRNE are connected with high psychological stress and potential for long-term consequences [4], [16]. The post-2022 experiences of Ukraine show that high stress levels, long duties, sleep disorders and burnout risk in personnel may become an equally significant systemic constraint as equipment shortages. In case of resources shortage and time pressure, the need for prioritisation in providing medical assistance additionally increases the psychological stress in medical teams. From the doctrine perspective, it justifies considering psychological resilience as a component of operation safety. The standard should also include rotation and regeneration of resources, quick support interventions (e.g. first psychological

Najważniejszym elementem filaru jest dostępność i gotowość zasobów umożliwiających bezpieczne prowadzenie działań medycznych, w tym dobór i dostępność ŚOI, uruchomienie procedur reagowania na zdarzenia CBRNE oraz dostosowanie sposobu funkcjonowania infrastruktury. Obejmuje to również ochronę zbiorową, rozumianą jako organizacyjne i techniczne przygotowanie obiektów, w których pracuje personel, tak aby ograniczać ekspozycję i ryzyko wtórnego skażenia (np. wydzielenie stref i ciągów komunikacyjnych, rozwiązania izolacyjne, wentylacyjne i dekontaminacyjne). Praktycznym punktem odniesienia może być oddział zakaźny, gdzie bezpieczeństwo zapewnia nie tylko wyposażenie personelu, ale także reżim strefowy i infrastruktura wspierająca izolację oraz kontrolę transmisji.

Doktryna podkreśla, że rozwój tego segmentu jest warunkiem skuteczności działań. Zabezpieczenie indywidualne musi umożliwiać wykonywanie procedur ratunkowych i medycznych, a nie jedynie izolować personel medyczny. W większości realistycznych scenariuszy poziom ochrony odpowiadający zabezpieczeniu poziomowi C¹ będzie wystarczający do prowadzenia działań medycznych, jednak wybrane szpitalne oddziały ratunkowe (SOR) i centra urazowe (CU) oraz szpitalne oddziały specjalistyczne powinny być przygotowane do pracy w wyższych poziomach zabezpieczenia (B, A), jeżeli warunki i cel kliniczny tego wymagają [4], [15].

Bezpieczeństwo personelu zapewnia się poprzez wdrożenie zasad ochrony zbiorowej, organizacji stref działań, reguł wejścia i wyjścia, wymagań dotyczących infrastruktury medycznej oraz standardów bezpiecznego i odpowiedzialnego wykonywania czynności. Obejmuje ono także kryteria przerwania i zakończenia działań oraz procedury postępowania po ekspozycji personelu na czynnik niebezpieczny. W środowisku nieprzyjawnym szczególnego znaczenia nabiera rozpoznanie granicy wykonalności działań ratowniczo-medycznych w warunkach ryzyka i takie zarządzanie ryzykiem, aby nie doprowadzić do utraty zdolności systemu do udzielania pomocy kolejnym pacjentom. Elementem filaru jest również przygotowanie psychologiczne oraz mechanizmy wsparcia po zdarzeniu, ponieważ działania w CBRNE wiążą się z wysokim obciążeniem psychicznym i możliwością konsekwencji długofalowych [4], [16]. Doświadczenia Ukrainy po 2022 r. pokazują, że wysoki poziom stresu, długie dyżury, zaburzenia snu oraz ryzyko wypalenia personelu mogą stać się ograniczeniem systemowym równie istotnym jak braki sprzętowe. W sytuacjach niedoboru zasobów i presji czasu konieczność podejmowania decyzji o priorytetach udzielania pomocy dodatkowo zwiększa obciążenie psychiczne zespołów medycznych.

1 Level D – routine protection clothing used in everyday pre-hospital and hospital practice, extended by respiratory protection equipment in the form of half-masks with P3 filter, disposable gloves and eye protection (e.g.: glasses, face shield, goggles). This level is applicable to everyday medical practice.

Level C – protective suit, minimum type 3, with full-face mask with attached filter unit or suit with special hood with panoramic visor cooperating with filtering and ventilation unit with attached filter units.

Level B – non-gas-tight suit, minimum type 3, with breathing apparatus on the back outside the suit or with air line connected to the breathing apparatus. The protection level is used in a situation, which requires full isolation of the respiratory tract, without requiring full isolation of the skin (gas-tight suit).

Level A – gas-tight suit with air apparatus on the rescuer's back inside the suit or air line connected to the suit. This is applicable, when the threat caused by hazardous material in the environment is particularly high.

1 Poziom D – rutynowe ubranie ochronne wykorzystywane w codziennej praktyce przedszpitalnej i szpitalnej wzbogacone o środki ochrony dróg oddechowych w postaci półmasek z filtrem P3 oraz rękawiczki jednorazowe i osłonę oczu (np.: okulary, przyłbica, gogle). Poziom ten ma zastosowanie w codziennej praktyce medycznej.

Poziom C – kombinezon ochronny, minimum typ. 3., z maską pełnotwarzową z dołączonym filtropochłaniaczem lub kombinezon ze specjalnym kapturem wyposażonym w wizjer panoramiczny współpracujący z urządzeniem filtrowentylującym z dołączonymi filtropochłaniaczami.

Poziom B – kombinezon niegazoszczelny, minimum typ. 3., z aparatem powietrznym umieszczonym na plecach na zewnątrz kombinezonu lub linią powietrzną doprowadzoną do aparatu powietrznego. Poziom zabezpieczenia wykorzystywany jest w sytuacji, w której zachodzi konieczność pełnej izolacji dróg oddechowych bez konieczności pełnej izolacji skóry (gazoszczelności kombinezonu).

Poziom A – kombinezon gazoszczelny z aparatem powietrznym umieszczonym na plecach ratownika wewnątrz kombinezonu lub z doprowadzoną do kombinezonu linią powietrzną. Ma on zastosowanie w sytuacji, gdy zagrożenie ze strony materiału niebezpiecznego znajdującego się w środowisku jest szczególnie wysokie.

aid for personnel) and clear overload reduction rules. Similar conclusions were described after the Hamas attack on Israel (2023), when the incident scale and time pressure increased the risk of personnel overload [17–18].

Pillar 3. Operational effectiveness of medical resources: mobility, modularity and quick operational reinforcement capability

In CBRNE incidents, advantage is also obtained by systems capable of quick resource activation under the conditions of uncertainty and restrictions [4], [19–20]. The third doctrine pillar assumes that the operational effectiveness of resources implies the capacity of quick expansion of medical operations and relocation and deployment of forces and resources (e.g. teams, equipment, medical facilities) in response to situation changes. It also includes operation in the modular mode, using the components that could be matched and increased depending on the circumstances. The purpose was to maintain real response capabilities and capability to quickly increase them in case of a larger incident scale.

The effectiveness of resources in terms of equipment means above all easy and immediate access to PPE, basic decontamination sets, equipment for initial detection and identification of hazardous agents for medical purposes, as well as to necessary medicines, medical products and dressing materials [7], [9]. The organisational dimension includes quick activation of resources, the capability for increasing the medical response scale and the capability for creating and reinforcing medical points in the field, so that medicine is present at the place of incident, not restricted to accepting the effects at the hospital.

In practice, the doctrine assumes maintaining the capabilities to respond to CBRNE incidents in first line structures (medical rescue teams, dispatch centres, rescue units), because these units make first decisions take actions that determine the safety and course of further medical operations.

As a result, the point of gravity is shifted from the possession of resources in itself to the capability for their quick use and reinforcement in the place and time, in which the medical need actually arises.

Pillar 4. Decision-making system and coordination of medical operations

CBRNE incidents require decisions made quickly, often based on incomplete and quickly changing information [21]. The proposed doctrine assumes that the decision-making system should shorten the decision-making path, i.e. clearly define the roles and rights of officers, organise the horizontal and vertical information flow and define the criteria for increasing the scale of medical response.

In practice, it means forming an integrated medical decision-making system at incident level, from the place of incident, through dispatch centres, rescue units and coordination structures, to specialised treatment units. This system is based on

Z perspektywy doktryny uzasadnia to traktowanie odporności psychicznej jako elementu bezpieczeństwa działań. Standard powinien obejmować rotację i regenerację zespołów, szybkie interwencje wsparcia (np. pierwszą pomoc psychologiczną dla personelu) oraz jasne reguły ograniczające przeciążenie. Podobne wnioski opisywano po ataku Hamasu na Izrael (2023), gdy skala zdarzenia i presja czasu zwiększały ryzyko przeciążenia personelu [17–18].

Filar 3. Sprawność operacyjna zasobów medycznych: mobilność, modułowość i zdolność do szybkiego wzmocnienia działań

W zdarzeniach CBRNE przewagę zyskują systemy zdolne do szybkiego uruchomienia zasobów w warunkach niepewności i ograniczeń [4], [19–20]. Trzeci filar doktryny przyjmuje, że sprawność operacyjna zasobów oznacza zdolność do szybkiego rozwinięcia działań medycznych oraz przemieszczania i rozdysponowania sił i środków (np. zespołów, sprzętu, punktów medycznych) w odpowiedzi na zmianę sytuacji. Obejmuje także pracę w trybie modułowym, z wykorzystaniem elementów, które można zestawiać i zwiększać zależnie od rozwoju zdarzenia. Celem jest utrzymanie realnych zdolności reagowania oraz możliwość szybkiego ich zwiększenia w przypadku większej skali zdarzenia.

Sprawność zasobów w wymiarze sprzętowym oznacza przede wszystkim łatwy i natychmiastowy dostęp do ŚOI, podstawowych zestawów dekontaminacyjnych, sprzętu do wstępnej detekcji i identyfikacji czynników niebezpiecznych na potrzeby medyczne, a także do niezbędnych leków, wyrobów medycznych i materiałów opatrunkowych [7], [9]. Wymiar organizacyjny obejmuje szybkie uruchamianie zasobów, możliwość zwiększania skali odpowiedzi medycznej oraz możliwość tworzenia i wzmocniania punktów medycznych w terenie, tak aby medycyna była obecna na miejscu zdarzenia, a nie ograniczała się do przyjęcia skutków w szpitalu.

W praktyce doktryna zakłada utrzymywanie zdolności reagowania na zdarzenia CBRNE w strukturach pierwszej linii (zespoły ratownictwa medycznego, dyspozytornie, oddziały ratunkowe), ponieważ w tych jednostkach podejmowane są pierwsze decyzje i działania determinujące bezpieczeństwo i przebieg dalszych działań medycznych.

W efekcie filar ten przesuwą punkt ciężkości z samego posiadania zasobów na zdolność ich szybkiego użycia i wzmocnienia w miejscu oraz czasie, w którym realnie powstaje potrzeba medyczna.

Filar 4. System decyzyjny i koordynacja działań medycznych

Zdarzenia CBRNE wymagają decyzji podejmowanych szybko, często przy niepełnej i dynamicznie zmieniającej się informacji [21]. Proponowana doktryna zakłada, że system podejmowania decyzji powinien skracać ścieżkę decyzyjną, czyli jasno określać role i uprawnienia osób funkcyjnych, porządkować przepływ informacji w płaszczyźnie poziomej i pionowej oraz definiować kryteria zwiększania skali odpowiedzi medycznej.

W praktyce oznacza to utworzenie zintegrowanego układu koordynacji decyzji medycznych w zdarzeniu, od miejsca zdarzenia, przez dyspozytornie, oddziały ratunkowe i struktury koordynacyjne, aż po specjalistyczne jednostki leczenia. Układ ten opiera się na zasadzie jednolitości dowodzenia i kontroli

the principle of uniform command and control: critical decisions have a clear owner and their implementation is monitored in real time. The support consist of command and decision support tools (SWD), including analytics, situation awareness building and AI-powered solutions, used to aggregate data and organise the situation view [21–23]. From a medical operation perspective, this process could be described as a cycle: information and data collection, clinical interpretation, decision, implementation and assessment of effects, repeated in short intervals as subsequent information arrives, which correspond to the (observe – orient – decide – act) decision loop [24].

Key decisions are related to the personnel protection level, designation and organisation of medical zones, implementation of segregation, performance of initial life-saving interventions, decontamination, selection transport routes and target hospitals, activation of additional resources and relocation of patients between facilities. The doctrine assumes that a significant portion of decisions should be made at the lowest possible decision level to ensure quick and effective performance, i.e. at the level with appropriate rights, current situation awareness and resources necessary to perform the resolution with active SWD support. The criteria for increasing the scale of response should be clear and practical to enable quick transition from identification to operation. Multi-level acceptance extends the response time and could generate unfavourable clinical and operational effects.

In non-permissive environment, “medical command” must remain resistance to communication disruptions, information chaos and misinformation, as well as system overload. The doctrine assumes designing a decision process to remain executable in degradation mode, i.e. with limited communication, incomplete data and temporary decrease in resource availability. In practice, it means using alternative communication channels, redundancy of communication channels and information sources, using minimum data sets for critical decisions and clear criteria of interruption of operations upon exceeding the acceptable risk.

Pillar 5. Information and CBRNE agent detection and identification for medical purposes

Information is a critical resource, however its value depends on the capability of the system for quick collection, verification and conversion into decisions and operations [25]. This pillar assumes that the medical rescue system should effectively collect and receive information, integrate it from multiple sources and ensure coherent interpretation in the entire response chain – from dispatch centres and medical rescue units to hospitals and the national rescue and firefighting system, as well as cooperating services and inspections (e.g. State Sanitary Inspection, PIS).

The purpose is to reduce the situations, in which data is available, however it does not reach the decision-makers or it is subject to incoherent interpretation. For medical operations, key information influences clinical and organisational decisions, in particular related to decontamination needs, selection of personnel protection, risk of secondary exposure, implementation of treatment and rules and modes of patient reference.

wykonania (ang. *command and control*): decyzje krytyczne mają jednoznacznego właściciela, a ich wdrożenie jest monitorowane w czasie rzeczywistym. Wsparciem są narzędzia wspomaganie dowodzenia i decyzji (SWD), w tym analityka, budowanie świadomości sytuacyjnej oraz rozwiązania wykorzystujące AI, służące agregacji danych i porządkowaniu obrazu sytuacji [21–23]. W ujęciu operacyjno-medycznym proces ten można opisać jako cykl: zebranie informacji i danych, interpretacja kliniczna, decyzja, wdrożenie i ocena skutków, powtarzany w krótkich interwałach wraz z napływem kolejnych informacji, co odpowiada pętli decyzyjnej OODA (ang. *observe – orient – decide – act*) [24].

Kluczowe decyzje dotyczą poziomu zabezpieczenia personelu, wyznaczenia i organizacji stref medycznych, wdrożenia segregacji, wykonania wstępnych interwencji ratujących życie, dekontaminacji, wyboru tras transportu i szpitali docelowych, uruchomienia dodatkowych zasobów oraz relokacji pacjentów pomiędzy placówki. Doktryna przyjmuje, że znaczna część decyzji powinna zapadać na możliwie najniższym poziomie decyzyjnym zapewniającym ich bezpieczne i skuteczne wykonanie, tj. na poziomie dysponującym odpowiednimi uprawnieniami, bieżącą świadomością sytuacyjną oraz zasobami niezbędnymi do realizacji rozstrzygnięcia, przy aktywnym wsparciu SWD. Kryteria zwiększania skali odpowiedzi powinny być jednoznaczne i praktyczne, aby umożliwiały szybkie przejście od rozpoznania do działania. Wielostopniowa akceptacja wydłuża czas reakcji i może generować niekorzystne skutki kliniczne oraz operacyjne.

W środowisku nieprzyjawnym „dowodzenie medyczne” musi pozostawać odporne na zakłócenia komunikacji, chaos informacyjny i dezinformację oraz przeciążenie systemu. Doktryna zakłada projektowanie procesu decyzyjnego tak, aby był wykonalny również w trybie degradacji, czyli przy ograniczonej łączności, niepełnych danych i czasowym spadku dostępności zasobów. W praktyce oznacza to stosowanie zastępczych kanałów komunikacji, zdublowanie kanałów łączności i źródeł informacji, posługiwanie się minimalnymi zestawami danych do decyzji krytycznych oraz jasne kryteria przerywania działań w sytuacji przekroczenia dopuszczalnego ryzyka.

Filar 5. Informacja oraz detekcja i identyfikacja czynników CBRNE na potrzeby medyczne

Informacja jest zasobem krytycznym, jednak jej wartość zależy od tego, czy system potrafi ją szybko pozyskać, zweryfikować i przekształcić w decyzje oraz działania [25]. Filar ten zakłada, że system ratownictwa medycznego powinien sprawnie gromadzić i odbierać informacje, integrować je z wielu źródeł oraz zapewniać ich spójną interpretację w całym łańcuchu reagowania – od dyspozytorni i zespołów ratownictwa medycznego po szpitale oraz KSRR i służby oraz inspekcje współdziałające (np. Państwową Inspekcję Sanitarną, PIS).

Celem jest ograniczenie sytuacji, w której dane są dostępne, lecz nie trafiają do osób podejmujących decyzje albo są interpretowane w sposób niespójny. Dla działań medycznych kluczowe są informacje wpływające na decyzje kliniczne i organizacyjne, w szczególności dotyczące potrzeby dekontaminacji, doboru zabezpieczenia personelu, ryzyka wtórnej ekspozycji, wdrożenia leczenia oraz zasad i trybu kierowania pacjentów.

The doctrine assumes the development of capabilities for detection and initial identification of hazardous agents for medical purposes in first line structures, i.e. based on the CBRNE POCT (point-of-care testing) approach, designed to provide adequate information for quick clinical and organisational decisions [26]. Agent confirmation may require using reference laboratories, however initial decisions should be preferably made without undue delay.

The information pillar also includes the capability for operation under the conditions of time pressure and information overload. In practice, it means using decision-making support tools for segregation, logistics and distribution of resources, while retaining the priority for clinical evaluation and medical personnel responsibility. A practical measure of quality of the information pillar is whether key decision-making data reaches the appropriate decision level in time and undergoes coherent interpretation to enable quick implementation of operations.

Pillar 6. Medical support continuity: from place of incident to long-term consequences

Medical patient care in a CBRNE incident is a continuous process. The treatment starts in the place of incident, but clinical and organisational effects may show and accrue over time, thus generating health protection overloads over weeks and months. As a consequence, the medical rescue system should be designed as care path initiator – from first contact, through transport and emergency department to specialised departments, as well as outpatient care and public health operations if needed [3–4], [19].

A particular challenge are mixed incidents, in which mechanical injuries coexist with exposure to a hazardous agent. In such scenarios, trauma care, decontamination and personnel protection should progress in parallel with simultaneous prevention of secondary contamination of rescue and hospital infrastructure. The lack of coherence between the pre-hospital and hospital stages could then result in delays of life-saving interventions or unacceptable risk for personnel and patients, as well as destabilisation of hospital emergency department and other department operations.

Care continuity also includes continuity of information on exposure, clinical condition dynamics and therapeutic interventions implemented. The information on suspected hazardous agent presence, possible exposure path, observed symptoms and performed operations should be transferred at least with the patient, optimally before their arrival, because some CBRNE consequences may reveal late [4].

Pillar 7. Medical logistics as feasibility condition

In CBRNE incidents, logistics determines the response effectiveness. A simple practical rule is applicable here: logistics is not everything, but everything is nothing without logistics. It means that CBRNE medical response planning should consider the actual logistics capabilities in first line units and the reinforcement mechanism of entities affected by incident effects [11], [20].

Doktryna zakłada rozwój zdolności detekcyjnych i wstępnej identyfikacji czynników niebezpiecznych na potrzeby medyczne w strukturach pierwszej linii, m.in. w oparciu o podejście POCT CBRNE (ang. *point-of-care testing*), które ma dostarczać informacji wystarczających do szybkich decyzji klinicznych i organizacyjnych [26]. Potwierdzenie czynnika może wymagać wykorzystania laboratoriów referencyjnych, jednak warto, aby decyzje wstępne zapadały bez zbędnej zwłoki.

Filar informacyjny obejmuje także zdolność działania w warunkach presji czasowej i przeciążenia informacyjnego. W praktyce oznacza to stosowanie narzędzi wspomagających podejmowanie decyzji w zakresie segregacji, logistyki i dystrybucji zasobów, przy zachowaniu nadrzędności oceny klinicznej i odpowiedzialności personelu medycznego. Praktycznym miernikiem jakości filaru informacyjnego jest to, czy kluczowe dane decyzyjne docierają na czas do właściwego poziomu decyzyjnego i są interpretowane spójnie, tak aby umożliwić szybkie wdrożenie działań.

Filar 6. Ciągłość wsparcia medycznego: od miejsca zdarzenia do konsekwencji długoterminowych

Opieka medyczna nad pacjentem w zdarzeniu CBRNE jest procesem ciągłym. Leczenie zaczyna się na miejscu zdarzenia, ale skutki kliniczne i organizacyjne mogą ujawniać się i narastać w czasie, generując obciążenia ochrony zdrowia również w perspektywie tygodni i miesięcy. W konsekwencji system ratownictwa medycznego powinien być projektowany jako inicjator ścieżki opieki – od pierwszego kontaktu, przez transport i SOR, po oddziały specjalistyczne, a w razie potrzeby także opiekę ambulatoryjną i działania zdrowia publicznego [3–4], [19].

Szczególnym wyzwaniem są zdarzenia mieszane, w których obrażenia mechaniczne współistnieją z narażeniem na czynnik niebezpieczny. W takich scenariuszach zaopatrzenie urazów, dekontaminacja oraz ochrona personelu powinny przebiegać równolegle, przy jednoczesnym zapobieganiu wtórnemu skażeniu infrastruktury ratowniczej i szpitalnej. Brak spójności między etapem przedszpitalnym i szpitalnym może wówczas skutkować opóźnieniem interwencji ratujących życie albo nieakceptowalnym ryzykiem dla personelu i pacjentów, a także destabilizacją funkcjonowania SOR i kolejnych oddziałów.

Ciągłość opieki obejmuje także ciągłość informacji o ekspozycji, dynamice stanu klinicznego oraz wdrożonych interwencjach terapeutycznych. Informacje o podejrzeniu obecności czynnika niebezpiecznego, możliwej drodze narażenia, obserwowanych objawach i dotychczasowych działaniach powinny być przekazywane co najmniej wraz z pacjentem, a optymalnie przed jego przybyciem, ponieważ część następstw CBRNE może ujawniać się z opóźnieniem [4].

Filar 7. Logistyka medyczna jako warunek wykonalności

W zdarzeniach CBRNE logistyka determinuje skuteczność odpowiedzi. Obowiązuje tu prosta zasada praktyczna: logistyka nie jest wszystkim, ale wszystko bez logistyki jest niczym. Oznacza to, że planowanie odpowiedzi medycznej na zagrożenia CBRNE powinno obejmować realne zdolności logistyczne w jednostkach pierwszej linii oraz mechanizmy wzmacniania podmiotów dotkniętych skutkami zdarzenia [11], [20].

The priority resource categories include PPE, decontamination solutions (including variants that enable quick operations in the field and medical decontamination), pre-diagnostics and patient monitoring equipment, hazardous agent detection and initial identification tools, as well as exposure-specific critical medical products, including select antidotes. Merely having the resources “in stock” is not sufficient. Distribution, rotation, real-time availability and capability for quick replenishment and transport of resources under the conditions of system overload are essential.

Logistic resilience should also include the capability for resource replenishment under crisis conditions. In practice, it means the development and maintenance of national and regional production capabilities for key PPE, pieces of decontamination equipment and select categories of medical equipment and materials necessary for operation in CBRNE environment. In parallel, it is necessary to ensure the availability of critical medicinal products, including select antidotes and medicines used after exposure to CBRNE agents, through strategic reserves, delivery contracting and, if justified, capabilities for quick production or packaging.

Another significant component of this resilience is the regulatory field. Some products and technologies used in CBRNE preparation and response could be subject to trade controls as dual use goods, which could influence the resource availability and acquisition rate in some scenarios [27]. From the perspective of feasibility of operations, it is justified to review and rationalise formal restrictions on select resources necessary for medical operations, in particular in terms of dual-use classification. The purpose is not to weaken the trade security for these products, but to prevent regulations from forming barriers that impede quick provision of the medical rescue and health protection system with equipment necessary for personnel and patient protection in a crisis situation [4], [7].

In addition, logistics in CBRNE incidents includes maintaining the continuity of operation of critical components, such as: dispatch centres, rescue units and reference facilities, understood as designated facilities and laboratories for confirmation diagnostics and specialised treatment in CBRNE context. In a hybrid environment, provisions should be made for power and communication disruptions, which could restrict the operation capabilities regardless of the number of victims. For that reason, the doctrine assumes planning broadly understood infrastructural and logistic health protection as part of readiness for CBRNE incidents [28].

Pillar 8. Cross-sectoral cooperation with local level priority

By definition, CBRNE incidents require cooperation of many entities: medical rescue system, the national rescue and firefighting system, Polish Armed Forces, Police, inspections and public administration. The doctrine assumes a cross-sectoral approach, but also formulates an overarching principle: the civilian system should have its own response capabilities, while military support

Do priorytetowych kategorii zasobów należą ŚOI, rozwiązania dekontaminacyjne (w tym warianty umożliwiające szybkie działania w terenie i prowadzenie dekontaminacji medycznej), wyposażenie do wstępnej diagnostyki i monitorowania pacjentów, narzędzia detekcji i wstępnej identyfikacji czynników niebezpiecznych, a także produkty medyczne o znaczeniu krytycznym w określonych ekspozycjach, w tym wybrane odtrutki. Samo posiadanie zasobów „na stanie” nie jest wystarczające. Kluczowe znaczenie mają dystrybucja, rotacja, dostępność w czasie rzeczywistym oraz możliwość szybkiego uzupełniania i przemieszczania zasobów w warunkach przeciążenia systemu.

Odporność logistyczna powinna obejmować także zdolność do odtwarzania zasobów w warunkach kryzysu. W praktyce oznacza to rozwijanie i utrzymywanie krajowych lub regionalnych zdolności produkcyjnych w zakresie kluczowych ŚOI, elementów wyposażenia dekontaminacyjnego oraz wybranych kategorii sprzętu i materiałów medycznych niezbędnych do działań w środowisku CBRNE. Równolegle konieczne jest zapewnienie dostępności produktów leczniczych o znaczeniu krytycznym, w tym wybranych antidotów i leków stosowanych po narażeniu na czynniki CBRNE, poprzez rezerwy strategiczne, kontraktowanie dostaw oraz tam, gdzie jest to uzasadnione zdolność do szybkiej produkcji lub konfekcjonowania.

Istotnym elementem tej odporności jest również wymiar regulacyjny. Część wyrobów i technologii używanych w przygotowaniu i reagowaniu na CBRNE może podlegać reżimowi kontroli obrotu jako produkty podwójnego zastosowania, co w określonych scenariuszach może wpływać na dostępność i tempo pozyskania zasobów [27]. Z perspektywy wykonalności działań zasadne jest dokonanie przeglądu i racjonalizacji ograniczeń formalnych dotyczących wybranych zasobów niezbędnych do prowadzenia działań medycznych, w szczególności w zakresie klasyfikacji *dual-use*. Celem nie jest osłabienie bezpieczeństwa obrotu tymi produktami, lecz zapewnienie, aby regulacje nie tworzyły barier utrudniających szybkie wyposażenie systemu ratownictwa medycznego i ochrony zdrowia w środki konieczne do ochrony personelu i pacjentów w sytuacji kryzysowej [4], [7].

Logistyka w zdarzeniach CBRNE obejmuje ponadto utrzymanie ciągłości funkcjonowania elementów krytycznych, takich jak: dyspozytornie, oddziały ratunkowe oraz ośrodki referencyjne, rozumiane jako wyznaczone placówki i pracownice zapewniające diagnostykę potwierdzającą oraz leczenie specjalistyczne w CBRNE. W środowisku hybrydowym należy liczyć się z zakłóceniami zasilania i łączności, które mogą ograniczać możliwości działania niezależnie od liczby poszkodowanych. Z tego względu doktryna zakłada planowanie szeroko rozumianej odporności infrastrukturalnej i logistycznej ochrony zdrowia jako elementu gotowości na zdarzenia CBRNE [28].

Filar 8. Współdziałanie międzysektorowe z priorytetem poziomu lokalnego

Zdarzenia CBRNE z definicji wymagają współdziałania wielu podmiotów: systemu ratownictwa medycznego, KSRG, Sił Zbrojnych RP, Policji, inspekcji oraz administracji publicznej. Doktryna przyjmuje podejście międzysektorowe, ale jednocześnie formułuje zasadę nadrzędną: system cywilny powinien posiadać

should be considered as supplement, not foundation of medical safety. This results both from operational needs in first hours of the incident and the military crisis reality, in which military resources may be limited, unavailable or subordinate to defence priorities [8–9], [29–30].

The pillar of cooperation is focused on practical interoperability. Before solutions are finished at the national level, the response effectiveness is often determined by the capability of local entities for cooperation: agreement of communication channels, joint exercises, elementary standardisation of notification procedures and initial division of roles. In this arrangement, the local level is essential, because at this level first decisions are made and resources and patients are initially allocated. The experiences of the Israeli medical rescue system (Magen David Adom) of 2023 showed that in practice interoperability is based on multiple components of feasibility: centralised coordination of pre-hospital resources, quickly deployed medical points, agile evacuation management and resistant communication and information exchange channels. In turn, the experiences of Ukraine after 2022 show that under the conditions of degradations of infrastructure and communication, the following become essential: clear division of roles, simple criteria for increasing the scale of response, compatible communication channels and capabilities for reallocation of resources and distribution of patients.

From the perspective of this doctrine, the conclusion is practical: the cooperation of the medical rescues system with the national rescue and firefighting system and administration should be designed as a permanent operating mechanism (joint situation awareness, agreed criteria for activating additional forces and measures and reallocation of resources, cyclic exercises), not as a solution to be activated only in crisis situation [18], [31–32].

Cooperation also includes preparation of hospitals, protection of hospital infrastructure and coherent integration of pre-hospital decisions with the capabilities of hospital rescue departments and other departments. In practice, it means that the medical rescue system cannot operate in isolation from hospital planning or broader solutions in the field of civil protection and civil defence.

Pillar 9. Spiral education, exercises and capability for quick adaptation

The capability for responding to CBRNE incidents is a function of competence, not declaration. The analyses of medical personnel competences show educational gaps and the lack of standardisation of teaching programmes, which results in uneven readiness to respond and limited operational confidence in CBRNE incident scenarios [8], [24], [33–34]. The experiences of Ukraine after 2022 show that under the conditions of long-term crisis, it is possible to quickly implement modular training programmes for pre-hospital and hospital personnel, focused on specific competence gaps and real operational constraints. From the doctrine perspective it means that training should be conducted in short cycles and regularly updated based on conclusions from operations, while its scope should include not only

własne zdolności reagowania, natomiast wsparcie wojskowe należy traktować jako uzupełnienie, a nie fundament bezpieczeństwa medycznego. Wynika to zarówno z potrzeb operacyjnych w pierwszych godzinach zdarzenia, jak i z realiów kryzysu militarnego, w którym zasoby wojskowe mogą być ograniczone, niedostępne lub podporządkowane priorytetom obronnym [8–9], [29–30].

Filar współdziałania akcentuje praktyczny wymiar interoperacyjności. Zanim rozwiązania zostaną domknięte formalnie na poziomie krajowym, o skuteczności odpowiedzi często decyduje zdolność podmiotów lokalnych do wspólnego działania: uzgodnienia kanałów komunikacji, prowadzenia wspólnych ćwiczeń, elementarnej standaryzacji procedur powiadamiania oraz wstępnego podziału ról. Poziom lokalny ma w tym układzie znaczenie kluczowe, ponieważ to tam zapadają pierwsze decyzje oraz następuje wstępna alokacja zasobów i pacjentów. Doświadczenia izraelskiego systemu ratownictwa medycznego (Magen David Adom) z wydarzeń 2023 r. pokazują, że interoperacyjność w praktyce opiera się na kilku elementach wykonalności: scentralizowanej koordynacji zasobów przedszpitalnych, szybko uruchamianych punktach medycznych, sprawnym zarządzaniu ewakuacją oraz odpornych kanałach łączności i wymiany informacji. Z kolei doświadczenia Ukrainy po 2022 r. wskazują, że w warunkach degradacji infrastruktury i łączności kluczowe stają się: jasny podział ról, proste kryteria zwiększania skali odpowiedzi, kompatybilne kanały komunikacji oraz zdolność do relokacji zasobów i dystrybucji pacjentów.

Z perspektywy niniejszej doktryny wniosek jest praktyczny: współdziałanie systemu ratownictwa medycznego z KSRG i administracją powinno być projektowane jako stały mechanizm działania (wspólna świadomość sytuacyjna, uzgodnione kryteria uruchamiania dodatkowych sił i środków oraz relokacji zasobów, cykliczne ćwiczenia), a nie jako rozwiązanie uruchamiane dopiero w sytuacji kryzysowej [18], [31–32].

Współdziałanie obejmuje również przygotowanie szpitali, ochronę infrastruktury szpitalnej oraz spójne powiązanie decyzji przedszpitalnych z możliwościami oddziałów ratunkowych i pozostałych oddziałów szpitalnych. W praktyce oznacza to, że system ratownictwa medycznego nie może funkcjonować w izolacji od planowania szpitalnego ani od szerszych rozwiązań w obszarze ochrony ludności i obrony cywilnej.

Filar 9. Edukacja spiralna, ćwiczenia i zdolność szybkiej adaptacji

Zdolność reagowania na zdarzenia CBRNE jest funkcją kompetencji, a nie deklaracji. Analizy dotyczące kompetencji personelu medycznego wskazują na luki edukacyjne i brak standaryzacji programów nauczania, co przekłada się na nierównomierną gotowość do reagowania oraz ograniczoną pewność działania w scenariuszach zdarzeń CBRNE [8], [24], [33–34]. Doświadczenia Ukrainy po 2022 r. pokazują, że w warunkach długotrwałego kryzysu możliwe jest szybkie wdrażanie modułowych programów szkoleniowych dla personelu przedszpitalnego i szpitalnego, ukierunkowanych na konkretne luki kompetencyjne oraz realne ograniczenia operacyjne. Z perspektywy doktryny wynika z tego, że szkolenie powinno być prowadzone w krótkich cyklach i regularnie aktualizowane na podstawie wniosków z działań, a jego

clinical procedures, but also work organisation under the conditions of limited communication, system overload and resources shortage [35–36].

In response to this problem, the doctrine proposes adopting a spiral teaching model and returning to CBRNE contents (in medical context) at subsequent stages of professional development, with increasing difficulty level and according to the professional role.

Training includes practical components, including work using personal protection equipment, organisation of medical care, medical segregation under the conditions of contamination or suspected contamination, basics of medical decontamination, life-saving interventions, as well as communication and transmission of information in the system. The exercises should include different scenarios, including mixed scenarios (injury and exposure), because they are the best to test the coherence of the decision and logistics process [37].

The core of pillar of education is formation of the capability for quick adaptation, understood as adjustment of clinical decisions and work organisation to the changing threat and operational constraints. In CBRNE incidents, the changeability of conditions means i.a. uncertainty in relation to the agent, change of the exposure risk level, need to use personal protection equipment, disruptions of communication and resources availability and dynamically increasing system overload. Thus, pre-graduate and post-graduate education should develop competences and capability for independent operation in medical personnel to form capability for making decisions under dynamic conditions, ongoing updates to the action plan and with the arrival of new information and for maintaining treatment priorities despite environmental, organisational and social pressures.

Pillar 10. Risk communication and building social resilience

The proposed assumptions also include a social dimension, because human behaviours directly translate to burden on the medical rescue and health protection system. In CBRNE incidents, the risk of system destabilisation arises not only from the exposure itself, but also from social responses, such as increased sense of threat, panic, avoidance of collaboration or refusal to participate in operations, mass migrations, uncontrolled inflow of people to rescue departments, as well as information chaos, media pressure and misinformation [38–42]. In a hybrid environment, understood as simultaneous impact of physical threats and operations in the information domain (including deliberate influence, manipulation and communication disturbance operations), such phenomena could be deliberately reinforced and used for crisis escalation [5], [13], [25].

Crisis communication is a component of health security [4], [39]. In the context of this article, it means an organised and coordinated process of communication of threat information and recommended protections to the public and medical personnel, based on credible data and coherent with system capabilities [40–42]. It includes preparation of communication scenarios and templates, agreement on communication contents between institutions and clear integration of information communicated to the public with medical and organisational operations.

zakres powinien obejmować nie tylko procedury kliniczne, ale także organizację pracy w warunkach ograniczonej łączności, przeciążenia systemu i niedoboru zasobów [35–36].

W odpowiedzi na ten problem doktryna proponuje przyjęcie spiralnego modelu nauczania i powracanie do treści CBRNE (w kontekście medycznym) na kolejnych etapach rozwoju zawodowego, z rosnącym poziomem trudności i adekwatnością do roli zawodowej.

Szkolenie zakłada elementy praktyczne, w tym pracę w środkach ochrony indywidualnej, organizację opieki medycznej, segregację medyczną w warunkach skażenia lub podejrzenia skażenia, podstawy dekontaminacji medycznej, interwencje ratujące życie, a także komunikację i przekazywanie informacji w systemie. Ćwiczenia powinny obejmować różne scenariusze, w tym scenariusze mieszane (uraz i ekspozycja), ponieważ to one najlepiej testują spójność procesu decyzyjnego i logistycznego [37].

Rdzeniem filaru edukacyjnego jest kształtowanie zdolności do szybkiej adaptacji, rozumianej jako dostosowywanie decyzji klinicznych i organizacji pracy do zmieniającego się zagrożenia oraz ograniczeń operacyjnych. W zdarzeniach CBRNE zmienność warunków oznacza m.in. niepewność co do rodzaju czynnika, zmianę poziomu ryzyka ekspozycji, konieczność pracy w środkach ochrony indywidualnej, zakłócenia łączności i dostępności zasobów oraz dynamicznie narastające przeciążenie systemu. Dlatego kształcenie przeddyplomowe i podyplomowe powinno rozwijać kompetencje oraz umiejętność samodzielnego działania personelu medycznego tak, aby był on zdolny do podejmowania decyzji w warunkach dynamicznych, bieżącego aktualizowania planu postępowania wraz z napływem nowych informacji oraz utrzymania priorytetów leczniczych mimo presji środowiskowej, organizacyjnej i społecznej.

Filar 10. Komunikacja ryzyka i budowanie odporności społecznej

Proponowane założenia obejmują również wymiar społeczny, ponieważ zachowania ludności bezpośrednio przekładają się na obciążenie systemu ratownictwa medycznego i ochrony zdrowia. W zdarzeniach CBRNE ryzyko destabilizacji systemu wynika nie tylko z samej ekspozycji, ale także z reakcji społecznych, takich jak nasilone poczucie zagrożenia, panika, unikanie współpracy lub odmowa uczestnictwa w działaniach, masowe przemieszczanie się, niekontrolowany napływ osób do oddziałów ratunkowych, a także chaos informacyjny, presja medialna i dezinformacja [38–42]. W środowisku hybrydowym, rozumianym jako równoczesne oddziaływanie zagrożeń fizycznych i działań w dziedzinie informacyjnej (w tym celowych operacji wpływu, manipulacji i zakłóceń komunikacji), zjawiska te mogą być świadomie wzmacniane i wykorzystywane do eskalacji kryzysu [5], [13], [25].

Komunikacja ryzyka jest elementem bezpieczeństwa zdrowotnego [4], [39]. W kontekście niniejszego artykułu oznacza ona zorganizowany, koordynowany proces przekazywania społeczeństwu i personelowi medycznemu informacji o zagrożeniu oraz o zalecanych działaniach ochronnych, oparty na wiarygodnych danych i spójny z możliwościami systemu [40–42]. Obejmuje przygotowanie scenariuszy i schematów przekazu, uzgodnienie treści komunikatów między instytucjami oraz jasne powiązanie

Communication should decrease chaos, not magnify it, show specific behaviours, justify the implemented restrictions and build the predictability of system operations [40–41]. In operational terms, risk communication is a system capability that reduces the behaviours that increase exposure and secondarily overload the medical rescue and health protection system [42–43].

In practice, it means aiming for the principle of a single coherent source of communication agreed on between key stakeholders (health protection, public administration, the national rescue and firefighting system and services and inspections), while distinguishing communication for the public and for the personnel [40–41]. The effectiveness of communication is increased by the formulation of messages as short instructions of behaviour (what to do / what not to do / where to report), integrated with actual system capabilities (e.g. indicating the patient admission paths and decontamination points) [40–42]. An important tool is proactive communication, which consists in prior explanation of typical false narratives and expected collective behaviours before they begin to shape social decisions [42–43]. In mass inflow scenarios, it is particularly important to activate “information triage” channels (e.g. helplines, crisis contacts, dispatch centres), which direct people without urgent indications to appropriate points and reduce fear-driven reporting [40], [42]. It should be complemented by the capability for ongoing monitoring of the information circulation and frequently asked questions and false message and then updating messages in short cycles to maintain the coherence of information across the response chain [41–43].

Building social resilience also includes operations prior to the incident, including educating citizens on basic safety principles, reinforcing trust in institutions and preparing the public for cooperation with the civil protection and civil defence system [40–41]. Social resilience is a system resource, because it translates to behaviours that reduce the exposure and the number of people that require medical intervention, reduce the percentage of reports without clinical justification and streamlines referring patients to appropriate care points [40], [42]. As a result, it influences the rate of seeking help and the capability of maintaining the continuity of operation of health protection under the conditions of overload, in particular under information pressure and misinformation risk [41–43].

Discussion

The proposed medical doctrine for CBRNE threats is prospective in nature – it does not describe the current condition, but indicates a direction of development for the medical rescue system and its integrations with civil protection and civil defence. It is justified based on systemic analyses that recur in literature and the consistent long-term observations of the authors, indicating that modern threats are complex and dynamic in nature, systemic preparation and coherence remain inadequate and the effects

informacji kierowanych do społeczeństwa z działaniami medycznymi i organizacyjnymi. Komunikacja powinna zmniejszać chaos, a nie go potęgować, wskazywać konkretne zachowania, uzasadniać wprowadzane ograniczenia i budować przewidywalność działań systemu [40–41]. W ujęciu operacyjnym komunikacja ryzyka stanowi zdolność systemową ograniczającą zachowania, które zwiększają ekspozycję oraz wtórnie przeciążają system ratownictwa medycznego i ochrony zdrowia [42–43].

W praktyce oznacza to dążenie do zasady jednego, spójnego źródła komunikatów uzgadnianych między kluczowymi interesariuszami (ochrona zdrowia, administracja publiczna, KSRG oraz służby i inspekcje), przy rozróżnieniu komunikatów dla społeczeństwa i dla personelu [40–41]. Skuteczność przekazu zwiększa formułowanie komunikatów jako krótkich instrukcji zachowania (co robić / czego nie robić / gdzie się zgłaszać), powiązanych z realnymi możliwościami systemu (np. wskazanie ścieżek przyjęcia pacjenta i punktów dekontaminacji) [40–42]. Istotnym narzędziem jest komunikacja wyprzedzająca, polegająca na uprzednim wyjaśnianiu typowych fałszywych narracji i oczekiwanych zachowań zbiorowych, zanim zaczną one kształtować decyzje społeczne [42–43]. W scenariuszach masowego napływu szczególne znaczenie ma uruchomienie kanałów „triage’u informacyjnego” (np. infolinie, komunikaty kryzysowe, dyspozytornie), które kierują osoby bez wskazań pilnych do właściwych punktów i ograniczają zgłaszanie napędzane lękiem [40], [42]. Uzupełnieniem powinna być zdolność bieżącego monitorowania obiegu informacji i najczęściej pojawiających się pytań oraz fałszywych przekazów, a następnie aktualizowania komunikatów w krótkich cyklach, aby utrzymać spójność informacji w całym łańcuchu reagowania [41–43].

Budowanie odporności społecznej obejmuje także działania prowadzone przed zdarzeniem, w tym edukację obywateli w zakresie podstawowych zasad bezpieczeństwa, wzmacnianie zaufania do instytucji oraz przygotowanie społeczności do współpracy z systemem ochrony ludności i obrony cywilnej [40–41]. Odporność społeczna jest zasobem systemowym, ponieważ przekłada się na zachowania ograniczające ekspozycję i liczbę osób wymagających interwencji medycznej, zmniejsza odsetek zgłoszeń nieuzasadnionych klinicznie oraz usprawnia kierowanie pacjentów do właściwych punktów opieki [40], [42]. W efekcie wpływa na tempo zgłaszania się po pomoc i na możliwość utrzymania ciągłości działania ochrony zdrowia w warunkach przeciążenia, szczególnie w sytuacji presji informacyjnej i ryzyka dezinformacji [41–43].

Dyskusja

Proponowana doktryna medyczna wobec zagrożeń CBRNE ma charakter perspektywny – nie opisuje stanu obecnego, lecz wyznacza kierunek rozwoju systemu ratownictwa medycznego oraz jego powiązań z ochroną ludności i obroną cywilną. Jej uzasadnienie wynika z powtarzających się w literaturze analiz systemowych oraz zgodnych z nimi wieloletnich obserwacji autorów, wskazujących, że współczesne zagrożenia mają charakter złożony i dynamiczny, przygotowanie i spójność systemowa

of CBRNE incidents could be long-term and extend beyond the pre-hospital stage [8–9], [19], [29], [37–38], [44–45]. From this perspective, the doctrine is a framework that organises operational priorities and compromises.

The implementation of the proposed pillars requires real financial and organisational conditions, because some of the capabilities generates fixed costs of maintaining readiness, including rotation and replenishment of stocks, service and periodical replacement of equipment, as well as cyclic training sessions and exercises. The greatest costs are related to maintaining the availability of PPE, decontamination solutions, resilience of infrastructure, medical logistics and material and medicinal reserves with limited shelf life. In practice, a significant limitation is the unevenness of equipment and readiness in PPE and decontamination solutions between the medical rescue and health protection system and the national rescue and firefighting system, which may obstruct interoperability in the first stage of incident [7], [46–47].

From the feasibility perspective, staged implementation is justified: first, minimum standards for the “first line” (emergency response teams, dispatch centres, hospital emergency departments) and clear rules for sharing resources in incident, then reinforcing select reference facilities and medical logistics mechanisms. In this context, it is worth considering the possibility of using the reserves maintained at the national and regional level as buffer for the initial phase, and support from the European level if needed, while maintaining the operational availability, rotation, agile distribution and clear rules of activation for medical operation purposes [47–48].

The proposed doctrine is framework in nature and does not substitute any operational standards or procedures. Its implementation requires converting the pillars into organisational, training and logistics solutions adjusted to the local level. The potential limitation of the approach is the risk of inconsistent interpretation of the pillars between entities if minimum standards and common operational criteria are not prepared. An additional limitation is the dependency on the availability of personnel and the capability to maintain readiness in the long term, in particular under the conditions of system overload and disruptions in the supply chain [46–47]. For that reason, it is essential to implement solutions in stages, test them in exercises and correct them based on conclusions from operation [49–50].

The presented doctrine is framework and conceptual in nature, so its operational usefulness requires further validation. It is worth conducting the validation in stages: first, by translating the pillars into minimum performance standards and readiness criteria, then by pilot implementations and decision-making and practical exercises, followed by expert assessment, analysis of consistency with conclusions from real incidents and further improvement of solutions [47], [49–50]. Only after that stage would it be justified to gradually transfer validated components of the doctrine to further systemic implementation. Under the conditions of peace, the implementation of permanent systemic solutions in medical rescue usually takes several years, while achieving full organisational maturity and permanent reinforcement of changes more often requires a 5–10 years longer

pozostają niewystarczające, a skutki zdarzeń CBRNE mogą być długotrwałe i wykraczać poza fazę przedszpitalną [8–9], [19], [29], [37–38], [44–45]. W tym ujęciu doktryna pełni rolę ramy porządkującej priorytety i kompromisy działania.

Wdrożenie proponowanych filarów wymaga uwzględnienia realnych uwarunkowań finansowych i organizacyjnych, ponieważ część zdolności generuje koszty stałe związane z utrzymaniem gotowości, w tym rotacją i odtwarzaniem zapasów, serwisowaniem oraz okresową wymianą wyposażenia, a także cyklicznymi szkoleniami i ćwiczeniami. Największe obciążenia dotyczą utrzymania dostępności ŚOI, rozwiązań dekontaminacyjnych, odporności infrastrukturalnej, logistyki medycznej oraz rezerw materiałowych i lekowych o ograniczonym terminie przydatności. Istotnym ograniczeniem w praktyce jest nierównomierność wyposażenia i gotowości w obszarze ŚOI oraz rozwiązań dekontaminacyjnych pomiędzy systemem ratownictwa medycznego i ochroną zdrowia a podmiotami KSRG, co może utrudniać interoperacyjność w pierwszej fazie zdarzenia [7], [46–47].

Z perspektywy wykonalności zasadne jest etapowanie wdrożenia: w pierwszej kolejności minimalne standardy dla „pierwszej linii” (ZRM, dyspozytornie, SOR) oraz jasne zasady współdzielenia zasobów w zdarzeniu, następnie wzmocnienie wybranych ośrodków referencyjnych i mechanizmów logistyki medycznej. W tym kontekście warto uwzględnić możliwość wykorzystania rezerw utrzymywanych na poziomie krajowym i regionalnym jako bufora dla fazy początkowej, a w razie potrzeby także wsparcia z poziomu europejskiego, przy jednoczesnym zapewnieniu ich dostępności operacyjnej, rotacji, sprawnej dystrybucji oraz jasnych zasad uruchamiania na potrzeby działań medycznych [47–48].

Proponowana doktryna ma charakter ramowy i nie zastępuje standardów operacyjnych ani procedur. Jej wdrożenie wymaga przełożenia filarów na rozwiązania organizacyjne, szkoleniowe i logistyczne dostosowane do poziomu lokalnego. Potencjalnym ograniczeniem podejścia jest ryzyko rozbieżnej interpretacji filarów między podmiotami, jeżeli nie zostaną opracowane minimalne standardy i wspólne kryteria działania. Dodatkowym ograniczeniem jest zależność od dostępności kadr i zdolności do utrzymania gotowości w długim okresie, zwłaszcza w warunkach przeciążenia systemu i zakłóceń łańcuchów dostaw [46–47]. Z tego względu kluczowe znaczenie ma etapowe wdrażanie rozwiązań, ich testowanie w ćwiczeniach oraz korygowanie na podstawie wniosków z działań [49–50].

Przedstawiona doktryna ma charakter ramowy i koncepcyjny, dlatego jej operacyjna użyteczność wymaga dalszej walidacji. Walidację warto prowadzić etapowo: najpierw poprzez przełożenie filarów na minimalne standardy wykonawcze i kryteria gotowości, później przez pilotażowe wdrożenia oraz ćwiczenia decyzyjne i praktyczne, a następnie przez ocenę ekspercką, analizę zgodności z wnioskami z realnych incydentów i dalsze doskonalenie rozwiązań [47], [49–50]. Dopiero po takim etapie zasadne byłoby stopniowe przenoszenie sprawdzonych elementów doktryny do szerszego wdrożenia systemowego. W warunkach pokoju wdrożenie trwałych rozwiązań systemowych w ratownictwie medycznym zwykle zajmuje kilka lat, natomiast osiągnięcie pełnej dojrzałości organizacyjnej i trwałego utrwalenia zmian części wymaga perspektywy 5–10 lat lub dłuższej. W warunkach

perspective. Under the conditions of armed conflict, this process could be accelerated by operational pressure, which shortens decision-making paths, forces reorganisation of resources and favours quicker implementation of solutions considered as indispensable for maintaining the continuity of services. The Ukrainian experiences show, however, that this acceleration is mostly adaptive in nature, not fully transformational – organisational, logistics and training changes are implemented quicker, but their permanent rooting requires further institutionalisation, standardisation, stable funding and reconstruction of systemic capabilities [51–52], [55–56]. For that reason, a realistic perspective for the implementation and validation of the doctrine on a national scale seems to be a long-term process, pursued in stages and subject to cyclic evaluation.

The proposed pillars of the doctrine are the authorial synthesis based on the review of literature and normative documents and long-term observations of the medical rescue system operation and readiness in Poland, while referring to international frameworks and adapting them to national conditions. The doctrine refers to select international frameworks and standards (NATO, WHO, EU civil protection mechanisms), approaches based on incident management exercises and standards cycle, regarded as point of reference, not as solutions adequate or feasible for direct transfer to the Polish system [21–22], [48–50]. In that sense, the doctrine emphasises flexibility and capability for quick adaptation: the pillars are intended to organise priorities and compromises, but their implementation must be adjusted to local resource, organisational and infrastructural conditions.

For medical operations in CBRNE incidents, it is crucial to identify the effects and activate adequate protection and treatment operations, rather than to identify the nature and source of the incident. It means that it is necessary to simultaneously consider the safety of the personnel and medical infrastructure, need for decontamination, segregation, treatment and proper allocation of patients, often under the conditions of incomplete information, disrupted communication, limited resources and information pressure [4], [12–13], [45], [59]. The effectiveness of the response depends on the coherent operation of multiple critical capabilities at the same time: safety of medical operations, information, logistics, coordination, care continuity and interoperability at the local level. From this perspective, the doctrine does not boil down to individual procedures, but it organises the dependencies between these components and indicates that the lack of any of them quickly limits the feasibility of operations. Hence, own readiness and practical local agreements are particularly important, because at the initial stage of incident external support may be limited, delayed or subject to other priorities [2], [9], [28], [32], [46], [57–58].

The doctrine translates the complexity of modern CBRNE threats into a coherent set of capabilities that determine the feasibility of medical operations under the conditions of uncertainty, disruptions and limited resources. This shows that the effectiveness of the response is determined by proper management of personnel safety, operational effectiveness and logistics, a clearly defined decision-making system and exchange of information relevant for medical decisions. The command and decision support

konfliktu zbrojnego proces ten może ulec przyspieszeniu pod wpływem presji operacyjnej, która skraca ścieżki decyzyjne, wymusza reorganizację zasobów i sprzyja szybkiemu wdrażaniu rozwiązań uznanych za niezbędne dla utrzymania ciągłości świadczeń. Doświadczenia ukraińskie wskazują jednak, że przyspieszenie to ma najczęściej charakter adaptacyjny, a nie w pełni transformacyjny – szybciej wdrażane są zmiany organizacyjne, logistyczne i szkoleniowe, lecz ich trwałe zakorzenienie wymaga późniejszej instytucjonalizacji, standaryzacji, stabilnego finansowania i odbudowy zdolności systemowych [51–52], [55–56]. Z tego względu realistycznym horyzontem dla wdrożenia i walidacji doktryny w skali krajowej wydaje się proces wieloletni, realizowany etapami i poddawany cyklicznej ocenie.

Proponowane filary doktryny stanowią autorską syntezę opartą na przeglądzie piśmiennictwa i dokumentów normatywnych oraz na wieloletnich obserwacjach funkcjonowania systemu ratownictwa medycznego i gotowości w Polsce, przy jednoczesnym odniesieniu do ram międzynarodowych i ich adaptacji do warunków krajowych. Doktryna odwołuje się do wybranych ram i standardów międzynarodowych (NATO, WHO, mechanizmów ochrony ludności UE), podejść opartych na cyklu ćwiczeń oraz standardów zarządzania incydemem, traktując je jako punkt odniesienia, a nie jako rozwiązania wystarczające lub możliwe do bezpośredniego przeniesienia do polskiego systemu [21–22], [48–50]. W tym sensie doktryna kładzie nacisk na elastyczność i zdolność szybkiej adaptacji: filary mają porządkować priorytety i kompromisy, ale ich wdrożenie musi uwzględniać lokalne uwarunkowania zasobowe, organizacyjne i infrastrukturalne.

Dla działań medycznych w zdarzeniach CBRNE kluczowe jest nie tyle ustalenie charakteru i źródła zdarzenia, ile szybkie rozpoznanie jego skutków i uruchomienie adekwatnych działań ochronnych i leczniczych. Oznacza to konieczność jednoczesnego uwzględnienia bezpieczeństwa personelu i infrastruktury medycznej, potrzeby dekontaminacji, segregacji, leczenia oraz właściwej alokacji pacjentów, często w warunkach niepełnej informacji, zakłóconej łączności, ograniczonych zasobów i presji informacyjnej [4], [12–13], [45], [59]. Skuteczność odpowiedzi zależy od spójnego działania kilku krytycznych zdolności jednocześnie: bezpieczeństwa działań medycznych, informacji, logistyki, koordynacji, ciągłości opieki oraz interoperacyjności na poziomie lokalnym. W tym ujęciu doktryna nie sprowadza się do pojedynczych procedur, lecz porządkuje zależności między tymi elementami i wskazuje, że brak któregoś z nich szybko ogranicza wykonalność działań. Szczególne znaczenie ma przy tym gotowość własna i praktyczne uzgodnienia lokalne, ponieważ w fazie początkowej zdarzenia wsparcie zewnętrzne może być ograniczone, opóźnione lub podporządkowane innym priorytetom [2], [9], [28], [32], [46], [57–58].

Doktryna przekłada złożoność współczesnych zagrożeń CBRNE na spójny zestaw zdolności, które decydują o wykonalności działań medycznych w warunkach niepewności, zakłóceń i ograniczonych zasobów. Pokazuje, że o skuteczności odpowiedzi decydują właściwe zarządzanie bezpieczeństwem personelu, sprawność operacyjna i logistyka, jasno zdefiniowany system decyzyjny oraz przepływ informacji istotnej dla decyzji medycznych. Narzędzia wsparcia dowodzenia i podejmowania

tools and situation awareness building solutions may reinforce that process by aggregating data from multiple sources and organising the view of the situation for decision-makers. The view of medical care as continuum and interoperability based on local readiness reinforce system resilience and reduce the risk that the response will be only limited to reactive acceptance of the effects of the incident.

Conclusions

The proposed medical doctrine for CBRNE threats is a framework that organises the preparation and response of the medical rescue system and its integrations with health protection, the national rescue and firefighting system, civil protection and civil defence. Its fundamental value, however, consists in shifting the point of gravity from the identification of the type of threat in itself to the feasibility conditions for medical operations in the environment of uncertainty, disruptions and limited resources. The proposed ten pillars define a coherent direction for the development of medical readiness, but their practical value will depend on conversion into minimum performance standards, readiness criteria, exercises and further validation in national conditions. In the current security environment of Poland, the development of such approach should not be regarded as a development option, but as a component of building of state resilience.

Definitions

Feasibility of medical operations – the capability of maintaining basic medical functions (e.g. medical segregation, patient stabilisation, life-saving interventions, initial treatment) and organisational functions (e.g. decontamination, patient transport, care continuity and coordination) under limited resources, time pressure and infrastructural impediments, while retaining an acceptable safety level of personnel and patients.

Non-permissive environment – an operational situation, in which the actual or suspected contamination/exposures, instability or direct threat for teams and operational constraints (including infrastructural and informational) jointly impede or prevent standard rescue and medical procedures.

Conscious risk acceptance – justified undertaking of operations despite the risk that cannot be fully eliminated, after implementing the available measures to reduce that risk (e.g. PPE, zone organisation, decontamination, safety procedures) and while maintaining the agreed rules of coordination and responsibility for decisions.

Medical readiness – capability of the system to quickly initiate and maintain operations in CBRNE incidents, arising from prepared resources (e.g. personnel, equipment, medicines), procedures and training sessions, interoperability, effective coordination and communication and solutions to ensure the continuity of operation.

decyzji oraz rozwiązania budujące świadomość sytuacyjną mogą ten proces wzmacniać przez agregację danych z wielu źródeł i porządkowanie obrazu sytuacji dla decydentów. Ujęcie opieki medycznej jako kontinuum oraz interoperacyjność oparta na lokalnej gotowości wzmacniają odporność systemu i ograniczają ryzyko, że odpowiedź zostanie sprowadzona do wyłącznie reaktywnego przyjmowania skutków zdarzenia.

Wnioski

Proponowana doktryna medyczna wobec zagrożeń CBRNE stanowi ramę porządkującą przygotowanie i reagowanie systemu ratownictwa medycznego oraz jego powiązania z ochroną zdrowia, KSRG, ochroną ludności i obroną cywilną. Jej zasadniczą wartością jest przesunięcie punktu ciężkości z samego rozpoznania rodzaju zagrożenia na warunki wykonalności działań medycznych w środowisku niepewności, zakłóceń i ograniczonych zasobów. Dziesięć zaproponowanych filarów wyznacza spójny kierunek rozwoju gotowości medycznej, ale ich praktyczna wartość będzie zależała od przełożenia na minimalne standardy wykonawcze, kryteria gotowości, ćwiczenia oraz dalszą walidację w warunkach krajowych. W aktualnym środowisku bezpieczeństwa Polski opracowanie takiego podejścia należy traktować nie jako opcję rozwojową, lecz jako element budowania odporności państwa.

Definicje

Wykonalność działań medycznych – zdolność do utrzymania podstawowych funkcji medycznych (np. segregacja medyczna, stabilizacja pacjenta, interwencje ratujące życie, wstępne postępowanie lecznicze) oraz organizacyjnych (np. dekontaminacja, transport pacjentów, ciągłość opieki oraz koordynacja) przy ograniczonych zasobach, presji czasu i utrudnieniach infrastrukturalnych, z zachowaniem akceptowalnego poziomu bezpieczeństwa personelu i pacjentów.

Środowisko nieprzyjazne (ang. *non-permissive*) – sytuacja operacyjna, w której rzeczywiste lub podejrzewane skażenie/ekspozycje, niestabilność sytuacji lub bezpośrednie zagrożenie dla zespołów oraz ograniczenia operacyjne (w tym infrastrukturalne i informacyjne) łącznie utrudniają lub uniemożliwiają prowadzenie standardowych procedur ratowniczo-medycznych.

Świadoma akceptacja ryzyka – uzasadnione podejmowanie działań mimo ryzyka, którego nie da się całkowicie wyeliminować, po wdrożeniu dostępnych środków ograniczania tego ryzyka (np. ŚOI, organizacja stref, dekontaminacja, procedury bezpieczeństwa) oraz przy zachowaniu uzgodnionych zasad koordynacji i odpowiedzialności za decyzje.

Gotowość medyczna – zdolność systemu do szybkiego uruchomienia i utrzymania działań w zdarzeniach CBRNE, wynikająca z przygotowanych zasobów (np. kadry, sprzęt, leki), procedur i szkoleń, interoperacyjności, sprawnej koordynacji i łączności oraz rozwiązań zapewniających ciągłość działania.

AI Use Statement

The authors declare that artificial intelligence tools were used in the preparation of this article only within the scope indicated below:

- language and stylistic verification of the manuscript (ChatGPT – OpenAI),
- searching for and identifying potential bibliographic sources (SciSpace i ChatGPT),
- support in developing the structure of the manuscript (ChatGPT – OpenAI).

The authors take full responsibility for the content of the publication, including the scientific accuracy, interpretation of results, and final editing of the manuscript. Artificial intelligence tools were used solely as supporting instruments.

The journal's editorial policy prohibits the uncritical copying of AI-generated content and its inclusion in a publication without proper critical analysis, verification, and revision by the authors.

Oświadczenie dotyczące wykorzystania AI

Autorzy oświadczają, że w procesie przygotowania niniejszego artykułu wykorzystano narzędzia oparte na sztucznej inteligencji wyłącznie w zakresie wskazanym poniżej:

- weryfikacja językowa i stylistyczna tekstu (ChatGPT – OpenAI),
- wyszukiwanie i identyfikacja potencjalnych źródeł bibliograficznych (SciSpace i ChatGPT),
- wsparcie w opracowaniu struktury pracy (ChatGPT – OpenAI).

Autorzy ponoszą pełną odpowiedzialność za treść publikacji, w tym za poprawność merytoryczną, interpretację wyników oraz ostateczną redakcję tekstu. Narzędzia sztucznej inteligencji były wykorzystywane wyłącznie jako narzędzia pomocnicze.

Polityka redakcyjna czasopisma zabrania bezrefleksyjnego kopiowania treści wygenerowanych przez narzędzia AI oraz pozostawiania ich w publikacji bez krytycznej analizy, weryfikacji i redakcji przez autorów.

Literature / Literatura

- [1] Nisser J., *Implementing military doctrine: A theoretical model*, "Comparative Strategy" 2021, 40(3), 273–289, <https://doi.org/10.1080/01495933.2021.1912514>.
- [2] Kocaki H. et al., *The Science of Disaster Medicine: From Response to Risk Reduction*, "Medeni Medical Journal" 2021, 36(4), 281–288, <https://doi.org/10.4274/MMJ.galenos.2021.50375>.
- [3] Hick J.L. et al., *Allocating Scarce Resources in Disasters: Emergency Department Principles*, "Annals of Emergency Medicine" 2012, 59(3), 177–187, <https://doi.org/10.1016/j.annemergmed.2011.06.012>.
- [4] Mugavero R., Shin H., *Safety and Emergency Medical Care in CBRN*, CEMEC Handbook Series 3, 2025, <https://doi.org/10.23810/CEMEC-4>.
- [5] Tin D. et al., *Hybrid warfare and counter-terrorism medicine*, "European Journal of Trauma and Emergency Surgery" 2023, 49(5), 1987–1996, <https://doi.org/10.1007/s00068-023-02230-y>.
- [6] Beishuizen B.H.H. et al., *A systematic literature review on public health and healthcare resources for pandemic preparedness planning*, "BMC Public Health" 2024, 24, art. 3114, <https://doi.org/10.1186/s12889-024-20629-z>.
- [7] *Bezpieczni w czasie kryzysu: jak zadbać o zdrowie obywateli i żołnierzy, kiedy świat się chwieje?*, WIM-PIB, Warszawa 2025, <https://wim.mil.pl/wp-content/uploads/2025/08/raport-bezpieczni-w-czasie-kryzysu.pdf> [dostęp: 6.01.2026].
- [8] Piekarski M., *Możliwe scenariusze zagrożeń terrorystycznych na terytorium Rzeczypospolitej Polskiej w kontekście zagrożeń hybrydowych*, "Terroryzm – studia, analizy, prewencja" 2022, 2(2), 71–92, <https://doi.org/10.4467/27204383TER.22.019.16339>.
- [9] Trzos A., Łyziński K., *The potential of emergency medical response to CBRNE threats in the context of military-civilian cooperation*, "Safety & Fire Technology" 2024, 64(2), 158–174, <https://doi.org/10.12845/sft.64.2.2024.10>.
- [10] Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907).
- [11] Barbee G. i in., *Chemical, Biological, Radiological and Nuclear (CBRN) Injury Part I: Initial Response to CBRN Agents (CPG ID: 69)*, Joint Trauma System Clinical Practice Guideline, 2018.
- [12] Kippnich M. et al., *Managing CBRN mass casualty incidents at hospitals – Find a simple solution for a complex problem: A pilot study*, "American Journal of Disaster Medicine" 2024, 19(1), 45–53, <https://doi.org/10.5055/ajdm.0471>.
- [13] Granholm F. et al., *The Complexities of Hybrid Warfare and the Impact on Tactical Emergency Medical Support*, "Health Security" 2023, 21(2), 140–147, <https://doi.org/10.1089/hs.2022.0161>.
- [14] Smith M., Weir A.G.A., *CBRNE3 medicine in the austere environment: the challenges*, "BMJ Military Health" 2022, 168(6), 474–478, <https://doi.org/10.1136/military-2022-002259>.
- [15] Łyziński K., Trzos A., *Środki ochrony indywidualnej w praktyce personelu medycznego*, „Stany Nagłe po Dyplomie” 2025, 9(1), 1–8, <https://podyplomie.pl/stany-nagle-podyplomie/41311,środki-ochrony-indywidualnej-w-praktyce-personelu-medycznego> [dostęp: 4.07.2025].
- [16] Naushad V.A. et al., *A Systematic Review of the Impact of Disaster on the Mental Health of Medical Responders*, "Pre-hospital and Disaster Medicine" 2019, 34(6), 632–643, <https://doi.org/10.1017/S1049023X19004874>.
- [17] Deac A.A. et al., *Ukrainian healthcare providers under siege*

- during the first year of war: challenges and adaptations, "BJPsych International" 2024, 21(2), 35–37, <https://doi.org/10.1192/bji.2023.43>.
- [18] Jaffe E. et al., *Managing a Mega Mass Casualty Event by a Civilian Emergency Medical Services Agency*, "International Journal of Public Health" 2024, 69, art. 1606907, <https://doi.org/10.3389/ijph.2024.1606907>.
- [19] Binkley J.M., Kemp K.M., *Mobilization of Resources and Emergency Response on the National Scale*, "Surgical Clinics of North America" 2022, 102(1), 1–12, <https://doi.org/10.1016/j.suc.2021.09.014>.
- [20] Nazari S. et al., *Structural elements and requirements in forming prehospital health response teams*, "Disaster Medicine and Public Health Preparedness" 2023, 17, art. e300, 1–8, <https://doi.org/10.1017/dmp.2022.259>.
- [21] European Committee for Standardization (CEN), CWA 17974:2023: *Basic CBRN training curriculum*, CEN, Brussels 2023, <https://civil-protection-knowledge-network.europa.eu/system/files/2025-04/cwa-on-eu-training-curriculum.PDF> [dostęp: 6.02.2026].
- [22] NATO Civil Emergency Planning, *The International CBRN Training Curriculum*, 2013, <https://civil-protection-knowledge-network.europa.eu/media/international-cbrn-training-curriculum> [dostęp: 5.02.2026].
- [23] Elfahim O. et al., *Artificial Intelligence in Prehospital Emergency Care*, "Big Data and Cognitive Computing" 2025, 9(9), art. 219, <https://doi.org/10.3390/bdcc9090219>.
- [24] Tanui D.J., *Application of Boyd's OODA loop to emergency response*, "Journal of Emergency Management" 2021, 19(5), 461–468, <https://doi.org/10.5055/jem.0564>.
- [25] Costigan S.S. et al., *Hybrid Threats and Hybrid Warfare Reference Curriculum*, Brussels 2022, <https://nato.int/content/dam/nato/webready/documents/deep/Hybrid-threats-and-hybrid-warfare-ENGLISH.pdf> [dostęp: 5.02.2026].
- [26] Trzos A., Łyziński K., *Proponowane kierunki rozwoju ratownictwa medycznego...*, w: *Epidemiologia i bezpieczeństwo CBRNE*, t. 4, Zielonka 2025, 143–166.
- [27] Regulation (EU) 2021/821..., "Official Journal of the European Union" 2021, L206, 1–461, <https://eur-lex.europa.eu/eli/reg/2021/821/oj/eng> [dostęp: 5.02.2026].
- [28] Granholm F. et al., *Not war, not terrorism*, "American Journal of Emergency Medicine" 2022, 60, 178–183, <https://doi.org/10.1016/j.ajem.2022.10.021>.
- [29] Tsagarliotis I. et al., *Assessing the Role of Military Units*, "Military Medicine" 2025, 190(1–2), e1–e10, <https://doi.org/10.1093/milmed/usaf548>.
- [30] Kalkman J.P., *Military crisis responses to COVID-19*, "Journal of Contingencies and Crisis Management" 2021, 29(1), 99–103, <https://doi.org/10.1111/1468-5973.12328>.
- [31] Jaffe E. et al., *Prehospital Care Under Fire*, "Prehospital and Disaster Medicine" 2024, 39(3), 275–278, <https://doi.org/10.1017/S1049023X24000438>.
- [32] Quinn J. et al., *Prehospital Lessons From the War in Ukraine*, "Military Medicine" 2024, 189(1–2), 17–29, <https://doi.org/10.1093/milmed/usad253>.
- [33] Kako M. et al., *CBRN Education and Training*, "Prehospital and Disaster Medicine" 2018, 33(1), 100–107, <https://doi.org/10.1017/S1049023X18000043>.
- [34] Długosz K. et al., *CBRNE education and training for Polish health professionals*, "Folia Medica Cracoviensia" 2025, 65(2), 113–125, <https://doi.org/10.24425/fmc.2025.156129>.
- [35] Bury G. et al., *Ukraine Trauma Project*, "BMJ Open" 2023, 13(11), art. e077895, <https://doi.org/10.1136/bmjopen-2023-077895>.
- [36] Dzhemiliev A. et al., *Enhancing trauma care in Ukraine*, "World Journal of Surgery" 2024, 48(11), 2716–2727, <https://doi.org/10.1002/wjs.12362>.
- [37] Baetzner A.S. et al., *Preparing medical first responders*, "Scandinavian Journal of Trauma, Resuscitation and Emergency Medicine" 2022, 30, art. 56, <https://doi.org/10.1186/s13049-022-01056-8>.
- [38] Ranse J. et al., *Strengthening emergency department response*, "Australasian Emergency Care" 2024, 27(4), 100–108, <https://doi.org/10.1016/j.auec.2024.09.003>.
- [39] World Health Organization, *Hospital Safety Index*, Geneva 2015, <https://iris.who.int/handle/10665/258966> [dostęp: 2.02.2026].
- [40] World Health Organization, *Risk communication and community engagement*, Geneva 2020, <https://iris.who.int/bitstream/handle/10665/331513/WHO-2019-nCoV-RCCE-2020-2-eng.pdf> [dostęp: 4.03.2026].
- [41] European Centre for Disease Prevention and Control, *Recommendations for preparedness planning*, Stockholm 2025, <https://www.ecdc.europa.eu/en/publications-data/recommendations-preparedness-planning-public-health-threats> [dostęp: 4.03.2026].
- [42] Khan S. et al., *Risk communication and community engagement during COVID-19*, "International Journal of Disaster Risk Reduction" 2022, 74, art. 102903, <https://doi.org/10.1016/j.ijdrr.2022.102903>.
- [43] do Nascimento I.J.B. et al., *Infodemics and health misinformation*, "Bulletin of the World Health Organization" 2022, 100(9), 544–561, <https://doi.org/10.2471/BLT.21.287654>.
- [44] Goniewicz K. et al., *The importance of pre-training gap analyses*, "BMC Public Health" 2021, 21, art. 114, <https://doi.org/10.1186/s12889-021-10165-5>.
- [45] NATO Standardization Office, AMedP-7.1, 2018, https://coemed.org/files/stanags/03_AMEDP/AMedP-7.1_EDA_V1_E_2461.pdf [dostęp: 5.02.2026].
- [46] Konieczny M., *Cooperation and interoperability...*, "Acta Iuris Stetinensis" 2024, 47(1), 9–25, <https://doi.org/10.18276/ais.2023.47-01>.
- [47] Farhat H. et al., *Preparedness and emergency response strategies*, "Journal of Contingencies and Crisis Management" 2024, 32(2), 215–227, <https://doi.org/10.1111/1468-5973.12592>.
- [48] European Commission, *EU Civil Protection Mechanism*, https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_en [dostęp: 01.03.2026].
- [49] International Organization for Standardization, *ISO 22398:2013*, Geneva 2013, <https://www.iso.org/standard/50294.html> [dostęp: 5.03.2026].
- [50] U.S. Department of Homeland Security, *HSEEP Doctrine*, Washington DC 2020 [dostęp: 5.03.2026].

- [51] Lawry L.L. i in., *Health System Organization and Logistics of Trauma Care*, "Inquiry" 2025, 62, art. 469580251333327, <https://doi.org/10.1177/00469580251333327>.
- [52] Walravens S. et al., *Characteristics of Medical Evacuation by Train*, "JAMA Network Open" 2023, 6(6), art. e2319726, <https://doi.org/10.1001/jamanetworkopen.2023.19726>.
- [53] Erickson T.B. et al., *Evaluation of CBRNE Knowledge Change*, "Disaster Medicine and Public Health Preparedness" 2023, 17, art. e387, <https://doi.org/10.1017/dmp.2023.52>.
- [54] Kivlehan S.M. et al., *Evaluation of change in emergency care knowledge*, "BMJ Open" 2022, 12(6), art. e050871, <https://doi.org/10.1136/bmjopen-2021-050871>.
- [55] Truppa C. et al., *Health systems resilience*, "Conflict and Health" 2024, 18, art. 2, <https://doi.org/10.1186/s13031-023-00560-7>.
- [56] WHO Regional Office for Europe, *Health financing in Ukraine*, Copenhagen 2022, <https://iris.who.int/bitstream/handle/10665/361645/WHO-EURO-2022-5882-45647-65535-eng.pdf> [dostęp: 9.03.2026].
- [57] Christiaens W. et al., *Organisation des soins médicaux...*, Brussels 2023, <https://doi.org/10.57598/R374BS>.
- [58] Del Pinto M. et al., *The National and Local Dimension...*, Bristol 2024, 204–221, <https://doi.org/10.46692/9781529226775.013>.
- [59] Morton H., Johnson C., *Chemical, biological, radiological and nuclear major incidents*, "Surgey (Oxford)" 2021, 39(8), 500–507, <https://doi.org/10.1016/j.mpsur.2021.05.005>.

KAROL ŁYZIŃSKI, PH.D. – senior lecturer and employee of the Jagiellonian University Medical College, Department of Anaesthesiology and Intensive Care, Department of Disaster and Emergency Medicine. His scientific work is focused on the organisation and completion of emergency medical operations in CBRNE incidents, including the preparation of medical rescue teams and hospital rescue departments for detection, decontamination and safe victim handling operations. He is the co-author of publications on emergency medical services in CBRNE incidents. He combines his scientific and didactic experience with pre-hospital practice in emergency medical services. He was the assistant director of the CBRNE project at the Jagiellonian University Medical College – "Reinforcement of CBRNE safety – coordination and standardisation" (pursued in 2021–2024).

ARKADIUSZ TRZOS, PH.D. – employee of the Jagiellonian University Medical College, at present linked with the Department of Anaesthesiology and Intensive Care, UJ CM. His scientific and didactic work is focused on the organisation and management of medical operations in mass incidents and disasters. He was the manager of the CBRNE project at the Jagiellonian University Medical College – "Reinforcement of CBRNE safety – coordination and standardisation" (pursued in 2021–2024). At present, he is developing the Mobile Medical Module (MMM) project; its preparation involved i.a. underwater for test applications in simulated microgravity environments.

DR N. O ZDR. KAROL ŁYZIŃSKI – starszy wykładowca oraz pracownik Uniwersytetu Jagiellońskiego – Collegium Medicum w Katedrze Anestezjologii i Intensywnej Terapii, Zakładzie Medycyny Katastrof i Pomocy Doraźnej. W swojej pracy naukowej zajmuje się organizacją i realizacją medycznych działań ratunkowych w zdarzeniach CBRNE, w tym przygotowaniem zespołów ratownictwa medycznego i szpitalnych oddziałów ratunkowych do działań związanych z detekcją, dekontaminacją oraz bezpiecznym postępowaniem z poszkodowanymi. Jest współautorem publikacji dotyczących ratownictwa medycznego w incydentach CBRNE. Doświadczenie naukowe i dydaktyczne łączy z praktyką przedszpitalną w pogotowiu ratunkowym. Pełnił funkcję zastępcy dyrektora projektu CBRNE na UJ CM – „Wzmocnienie bezpieczeństwa w zakresie CBRNE – koordynacja i standaryzacja” (realizowanego w latach 2021–2024).

DR ARKADIUSZ TRZOS – pracownik Uniwersytetu Jagiellońskiego – Collegium Medicum, obecnie związany z Katedrą Anestezjologii i Intensywnej Terapii UJ CM. W pracy naukowej i dydaktycznej koncentruje się na organizacji i zarządzaniu działaniami medycznymi w zdarzeniach masowych oraz katastrofach. Pełnił funkcję kierownika projektu na UJ CM – „Wzmocnienie bezpieczeństwa w zakresie CBRNE – koordynacja i standaryzacja”. Aktualnie rozwija projekt Mobile Medical Module (MMM); w ramach jego przygotowania prowadzono m.in. testy podwodne do zastosowań w środowisku symulowanej mikrogravitacji.

Jan Kielin, Jacek Zboina, Paweł Janik, Damian Bąk

Scientific and Research Centre for Fire Protection – National Research Institute / Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy
Corresponding author / Autor korespondencyjny: jkielin@cnbop.pl

Threats Related to the Operation of Energy Storage Systems, Preventative Measures and Impact Mitigation Methods

Zagrożenia związane z eksploatacją magazynów energii elektrycznej, środki zapobiegania ich wystąpieniu oraz sposoby ograniczania skutków

ABSTRACT

Purpose: The purpose of the article is identification and practical presentation of real threats that could occur during the operation of energy storage systems. The article is in particular focused on a material and practical description of threats and technical measures, especially dedicated to fire protection, which may effectively prevent or mitigate the impact of these threats for people, property and the environment.

Introduction: The themes of safety of energy storage systems, including fire safety, is extremely relevant in the context of the ongoing energy transition of our country. The need for a reliable discussion of this subject is indicated for example by the fact that in the context of the actual threat of using energy storage systems, in which lithium-ion batteries are used, dramatically different positions appear. The authors hope that the content of this article will be contribute to redirecting the discussion of the fire safety of energy storage systems to a field dominated by arguments based on objective empirical evidence.

Methodology: The article is based on the analysis of literature of the subject, including legal regulations and international standards, scientific research results, as well as own results of full-scale empirical research on energy storage systems, in which emergency conditions were generated by varied scenarios.

Conclusions: The improvement of the fire safety of energy storage systems requires strengthening the test, certification and regulation system for lithium-ion batteries. It is necessary to develop national technical regulations and detailed industry guidelines, including insurance matters, to refine the principles for the design, operation and fire protection of energy storage systems. The authors also see the need for extensive research on threats and safety measure effectiveness, as well as for publishing a guide for the facility users and rescue services, including practical guidelines for the design of such facilities, as well as for the response to incidents in facilities with a battery energy storage system (BESS).

Keywords: fire safety, fire protection, energy storage, batteries, rechargeable batteries

Type of article: review article

Received: 31.10.2025; **Reviewed:** 16.01.2026; **Accepted:** 30.01.2026;

Authors' ORCID IDs: J. Kielin – 0000-0002-3506-5424; J. Zboina – 0000-0002-9436-5830, P. Janik – 0000-0003-4498-7575; D. Bąk - 0000-0002-2549-3855;

Percentage contribution: J. Kielin – 40%; J. Zboina – 30%, P. Janik – 15%; D. Bąk – 15%;

Please cite as: Safety & Fire Technology 2026, 1, 106–133, <https://doi.org/10.12845/sft.67.1.2026.5>;

This is an open access article under the CC BY-SA 4.0 license (<https://creativecommons.org/licenses/by-sa/4.0/>).

ABSTRAKT

Cel: Celem artykułu jest identyfikacja i praktyczne przedstawienie rzeczywistych zagrożeń, jakie mogą zaistnieć podczas eksploatacji systemów magazynowania energii elektrycznej. W artykule szczególną uwagę poświęcono rzeczowemu i praktycznemu opisaniu zagrożeń oraz środków technicznych, zwłaszcza tych dedykowanych ochronie przeciwpożarowej, które mogą tym zagrożeniom skutecznie przeciwdziałać lub ograniczać ich skutki w odniesieniu do ludzi, mienia oraz środowiska.

Wprowadzenie: Tematyka dotycząca bezpieczeństwa systemów magazynowania energii elektrycznej, w tym bezpieczeństwa pożarowego, jest niezwykle aktualna w kontekście dokonującej się aktualnie w naszym kraju transformacji energetycznej. Na potrzebę przeprowadzenia rzetelnej dyskusji w tym zakresie wskazuje chociażby to, że w kontekście faktycznego zagrożenia, jakie niesie ze sobą stosowanie magazynów energii, w których wykorzystuje się baterie litowo-jonowe, pojawiają się skrajnie różne stanowiska. Autorzy wyrażają nadzieję, że treści zawarte w niniejszym artykule będą stanowiły przyczynek do przekierowania dyskusji w obszarze bezpieczeństwa pożarowego magazynów energii na płaszczyznę, na której dominują argumenty oparte na obiektywnych dowodach empirycznych.

Metodologia: Artykuł opracowano na podstawie analizy literatury przedmiotu, w tym regulacji prawnych i standardów międzynarodowych, wyników badań naukowych, także własnych wyników z pełnoskalowych badań empirycznych magazynów energii, w których w różnych scenariuszach doprowadzono do stanów awaryjnych.

Wnioski: Poprawa bezpieczeństwa pożarowego magazynów energii elektrycznej wymaga wzmocnienia systemu badań, certyfikacji i regulacji dotyczących baterii litowo-jonowych. Wskazane jest opracowanie krajowych przepisów technicznych oraz szczegółowych wytycznych branżowych, w tym dotyczących kwestii ubezpieczeniowych, które doprecyzowałyby zasady projektowania, eksploatacji i ochrony przeciwpożarowej magazynów energii. Autorzy widzą także potrzebę przeprowadzenia szerokich badań nad zagrożeniami oraz skutecznością zabezpieczeń, jak również publikacji poradnika dla użytkowników obiektów i służb ratowniczych z praktycznymi wskazówkami na temat projektowania takich systemów, a także reagowania na incydenty w obiektach zawierających akumulatorowy system magazynowania energii elektrycznej (ASMEE).

Słowa kluczowe: bezpieczeństwo pożarowe, ochrona przeciwpożarowa, magazynowanie energii, baterie, akumulatory

Typ artykułu: artykuł przeglądowy

Przyjęty: 31.10.2025; **Zrecenzowany:** 16.01.2026; **Zaakceptowany:** 30.01.2026;

Identyfikatory ORCID autorów: J. Kielin – 0000-0002-3506-5424; J. Zboina – 0000-0002-9436-5830, P. Janik – 0000-0003-4498-7575; D. Bąk – 0000-0002-2549-3855;

Procentowy wkład merytoryczny: J. Kielin – 40%; J. Zboina – 30%, P. Janik – 15%; D. Bąk – 15%;

Proszę cytować: Safety & Fire Technology 2026, 1, 106–133, <https://doi.org/10.12845/sft.67.1.2026.5>;

Artykuł udostępniany na licencji CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>).

Introduction

Until recently, energy storage in batteries was a marginal subject, regarded as promising, but expensive and unused technology. In recent years, however, it has reached the status of an important development area, in which all primary public service companies, project developers, banks and investors try to participate. These projects are driven by the increasing capability of individual countries to supply their energy demands from renewable energy sources. In many cases, sources such as solar and wind energy are characterised by high variability of generated energy volume depending on the atmospheric conditions, time of the day and season of the year. By using batteries capable of storing energy in overproduction periods and “returning” it to the grid in increased demand periods, distribution grid operators may maintain stable supply. The progress of the energy storage industry is also favoured by the progress in the physical chemistry of the batteries themselves and their equipment, including software. In addition, proper financing systems are a major stimulant in the context of growth of the subject sector of the market.

The development of every industry and new technologies is almost always accompanied by the emergence of new and unknown threats, as well as the evolution of already identified threats. This article, based on research, addresses the problems of threats that could occur during the operation of stationary battery energy storage systems (BESS). These are the most common currently used energy storage methods based on lithium-ion batteries. This technology is currently prevailing due to its numerous advantages, primarily related to energy efficiency. It should be kept in mind, however, that the use of the BESS may also be connected with threats for facility users, the natural environment and infrastructure. Attempts were made to identify and characterise the subject threats. In addition, possible measures were also identified, which reduce reducing the probability of occurrence and spreading to an acceptable risk level.

Since the BESS are commonly used, it is necessary to expand the knowledge required to implement effective fire protection

Wprowadzenie

Magazynowanie energii w bateriach do niedawna było w branży energetycznej tematem marginalnym, postrzeganym w kategoriach obiecującej, ale drogiej i niewykorzystanej technologii. Od kilku lat zyskuje ono jednak rangę ważnego obszaru rozwojowego, w którym starają się uczestniczyć wszystkie główne przedsiębiorstwa świadczące usługi publiczne, deweloperzy projektów, banki i inwestorzy. Projekty te napędzane są przez rosnącą zdolność poszczególnych krajów do zaspokajania potrzeb energetycznych ze źródeł odnawialnych. W wielu przypadkach źródła takie jak energia słoneczna, wiatrowa cechują się dużą zmiennością objętości produkowanej energii w zależności od warunków atmosferycznych oraz pory dnia i roku. Dzięki zastosowaniu akumulatorów zdolnych do zmagazynowania energii w okresach nadprodukcji oraz „oddania” jej do sieci w okresach wzmożonego zapotrzebowania operatorzy sieci dystrybucji mogą utrzymać stabilność zasilania. Progrewowi branży magazynowania energii sprzyja również postęp dokonujący się w zakresie fizykochemii samych baterii oraz ich osprzętu, w tym oprogramowania. Ponadto dużą rolę stymulującą w kontekście wzrostu omawianego sektora rynku odgrywają odpowiednie systemy finansowania.

Rozwojowi każdej branży i nowych technologii niemal zawsze towarzyszy powstawanie nowych, dotychczas nieznanych rodzajów zagrożeń, a także ewolucja tych już zidentyfikowanych. W niniejszym artykule – na podstawie badań – przybliżono problematykę zagrożeń, jakie mogą wystąpić podczas eksploatacji stacjonarnych akumulatorowych systemów magazynowania energii elektrycznej (ASMEE). Są to najpowszechniej aktualnie stosowane metody magazynowania energii, oparte na bateriach litowo-jonowych. Technologia ta dominuje obecnie ze względu na swoje liczne zalety, głównie dotyczące efektywności energetycznej. Należy jednak pamiętać, że użytkowanie ASMEE może wiązać się także z zagrożeniami dla użytkowników obiektów, środowiska naturalnego i infrastruktury. Wspomniane zagrożenia starano się zidentyfikować i scharakteryzować. Wskazano ponadto możliwe środki służące ograniczaniu tych zagrożeń,

solutions for these technologies. It is also confirmed by the analysis of test results, including specialised real tests of different scenarios of storage system emergency and fully developed fires conducted by the Scientific and Research Centre for Fire Protection (CNBOP-PIB) [2]. For more than 10 years, the institute has conducted for the purposes of approval of the batteries used in electric vehicles. To test energy storage systems, it uses the experience and knowledge arising from collaboration with the manufacturers of the subject batteries.

Further grounds for the necessity to develop knowledge in this area is provided by the analysis of the available data on fire incidents involving energy storage equipment. The examples are as follows:

1. Explosion and deflagration of batteries in a container-based BESS (2.16 MWh) in Arizona on 19 April 2019; 8 firefighters were severely injured during fire service operations [3].
2. Fire during the tests of a 13-ton LIB (lithium-ion battery) system in a Tesla battery storage in the state of Victoria, Australia, on 30 July 2021; it took 4 days to extinguish [4].
3. Fire and explosion in a 25 MWh energy storage, consisting of LiFePO_4 cells and located next to a photovoltaic (PV) plant on a commercial building in Beijing on 16 April 2021; 2 firefighters died in the incident [5].

Similar incidents also occurred in Poland. The batteries located in the infrastructure were the cause of the occurrence and spreading of fire.

1. On 23 April 2024, on a company site in Trzebinia (Chrzanów District), a warehouse container adapted for energy storage system caught fire; the cause of the fire was an explosion of a Li-Ion battery; one person was injured in the incident [6].
2. On 5 November 2024 in Choczniak near Wadowice, a container with Li-Ion batteries (on a private property) caught fire; an explosion occurred during fire service operations, in which one firefighter was injured [7].
3. On 22 September 2025 in Chodzież (at Wielkopolskie Centrum Pulmonologii i Torakochirurgii, Greater Poland Centre for Pulmonology and Thoracic Surgery), a Pv-panel supplied energy storage system caught fire; the fire occurred in a battery cabinet, used to collect and store the energy generated by the PV plant; no people injured [8].

On the night of 24 August 2024, a tenement house in Poznań tragically caught fire; two explosions occurred in the cellar during the fire. Many batteries were found there. During the rescue operations, an explosion occurred, which injured 11 firefighters and 3 civilians; sadly, 2 firefighters died [9].

The tragic consequences of the above-mentioned incidents highlight the importance of the fire safety of energy storage systems and the urgent need to develop methods of identifying hazards and implementing effective protection measures. It is essential that these methods consider the needs of all stakeholders and be clear to them. Energy storage is the area of works and interests of above all the energy industry (e.g. battery suppliers and manufacturers, energy equipment), the fire protection industry and the broader energy infrastructure and equipment safety

poprzez sprowadzanie prawdopodobieństwa ich powstania i rozprzestrzeniania do poziomu ryzyka akceptowalnego.

W związku z tym, że ASMEE są powszechnie stosowane, konieczne jest poszerzanie wiedzy niezbędnej do wdrażania skutecznych rozwiązań służących ochronie przeciwpożarowej tych technologii. Potwierdza to również analiza wyników badań, w tym specjalistycznych badań rzeczywistych dla różnych scenariuszy stanów awaryjnych magazynów i ich pełnoekranowych pożarów prowadzonych w Centrum Naukowo-Badawczym Ochrony Przeciwpowodzi – Państwowym Instytucie Badawczym (CNBOP-PIB) [2]. Instytut ten od ponad dziesięciu lat prowadzi badania na potrzeby homologacji baterii stosowanych w pojazdach elektrycznych. W badaniach magazynów energii korzysta z doświadczeń i wiedzy wynikających ze współpracy z producentami tych baterii.

Kolejną przesłanką wskazującą na konieczność rozwijania wiedzy w tym obszarze są analizy dostępnych danych dotyczących zdarzeń pożarowych z udziałem urządzeń do magazynowania energii. Poniżej wymieniono ich przykłady:

1. Eksplozja akumulatorów i deflagacja w kontenerowym ASMEE (2,16 MWh) w Arizonie 19 kwietnia 2019 r.; w trakcie działań straży pożarnych ciężko rannych zostało ośmiu strażaków [3].
2. Pożar podczas testowania 13-tonowego systemu LIB (lithium-ionowego) w magazynie baterii firmy Tesla w australijskim stanie Wiktorii 30 lipca 2021 r.; jego ugaszenie zajęło cztery dni [4].
3. Pożar i eksplozja w magazynie energii o pojemności 25 MWh, składającym się z ogniw LiFePO_4 i zlokalizowanym przy instalacji fotowoltaicznej (PV) na budynku komercyjnym, w dniu 16 kwietnia 2021 r. w Pekinie; w zdarzeniu zmarło dwóch strażaków [5].

Podobne zdarzenia miały miejsce również w Polsce. Zlokalizowane w infrastrukturze baterie były przyczyną powstania oraz rozprzestrzeniania się pożaru.

1. W dniu 23 kwietnia 2024 r. na terenie jednej z firm w miejscowości Trzebinia (pow. chrzanowski) doszło do pożaru kontenera magazynowego adaptowanego na magazyn energii; pożar był spowodowany wybuchem akumulatora Li-Ion; w wyniku zdarzenia została poszkodowana jedna osoba [6].
2. W dniu 5 listopada 2024 r. w miejscowości Choczniak k. Wadowic miał miejsce pożar kontenera z akumulatorami Li-Ion (na prywatnej posesji); podczas działań straży pożarnych doszło do wybuchu, w wyniku którego poszkodowany został jeden ze strażaków [7].
3. W dniu 22 września 2025 r. w Chodzieży (na terenie Wielkopolskiego Centrum Pulmonologii i Torakochirurgii) zapalił się magazyn energii zasilany panelami PV; ogień pojawił się w jednej z szaf akumulatorowych, które służą do gromadzenia i przechowywania prądu wytwarzanego przez instalację PV; nie było osób poszkodowanych [8].

W nocy z 24 na 25 sierpnia 2024 r. doszło do tragicznego pożaru kamienicy w Poznaniu; w jego trakcie nastąpiły dwie eksplozje w piwnicy. Znalaziono tam wiele baterii i akumulatorów. Podczas akcji ratowniczej doszło do wybuchu, w wyniku którego obrażenia odniosło jedenastu strażaków oraz trzy osoby cywilne; niestety dwóch strażaków straciło życie [9].

industry. In addition, the collaborating entities, initiating and supplying knowledge, information, test results and solutions includes industry associations, research units and the national insurer. It is the effective collaboration of these entities that contributes to the development of solutions for BESS design, production and operation practices (e.g. the expert panel *The role and place of fire protection in the implementation of energy transition* during the "Fire Safety Forum" organised by PZU LAB in Aleksandrów Łódzki on 11/06/2024). Thus, the works to create the subject methods require the participation of experts representing various fields of knowledge and industries. Such initiative was undertaken at CNBOP-PI, in collaboration with two industry associations operating in the field of energy storage, i.e. Polskie Stowarzyszenie Magazynowania Energii (PSME, Polish Energy Storage Association), Polska Izba Magazynowania Energii (PIME, Polish Chamber of Energy Storage) and Stowarzyszenie Inżynierów i Techników Pożarnictwa (SITP, The Association of Fire Engineers and Technicians) [10]. The subject initiative is supported by experts of the Headquarters of the State Fire Service and the Fire University.

Considering the dynamic development of BESS nationwide, both in large scale and household (prosumer) applications, it should be assumed that without proper prevention of the fire hazards directly connected with the common use of lithium-ion batteries the intensity and diversity of incidents involving the two types of energy storage systems are expected to increase. According to the literature of the subject, the risk of occurrence and spreading of fire and explosion in facilities with battery energy storage systems may result from the occurrence of specific risk factors:

- electric, such as: battery failures, overcharge, quick discharge, loss of remote monitoring systems, internal short-circuits, overheating, water penetration, lightning strike (leading to thermal runaway),
- chemical, such as: inherent risks related to stored hazardous goods, transformer oil/fuel oil leaks, cooling gas/coolant leaks, chemical reactions,
- related to the ventilation gases ignition hazard,
- related to the risk of fire spreading due to the proximity of batteries, containers/enclosures to one another, infrastructure in place and vegetation (including screening vegetation),
- related to the risk of mechanical damage to batteries, containers/enclosures, caused by vehicle crashing,
- landscape, such as adjacent forest/grass fire caused by fire on site or external site infrastructure ignition caused by glow, thermal radiation and flame impact [15].

Problems and concerns related to the need to ensure proper fire safety also arise from unclear legal regulations and normative requirements for fire protection in relation to the construction and operation of such storage systems – both at the European level and at the national level. In many countries of the European Union, national regulations and normative requirements have already been implemented for the design, installation and operation of energy storage systems. In these countries, key fire safety hazards are identified in an essentially consistent manner, by defining restrictions, technical requirements and location

Tragiczne skutki przywołanych powyżej zdarzeń wskazują na ważność problematyki bezpieczeństwa pożarowego magazynów energii oraz pilną potrzebę opracowania metodologii identyfikacji zagrożeń oraz wdrażania skutecznych środków ochrony przed nimi. Istotne jest, aby metodyka ta uwzględniała potrzeby wszystkich interesariuszy oraz była dla nich zrozumiała. Magazynowanie energii to obszar prac i zainteresowań przede wszystkim branży energetycznej (np. dostawców i producentów akumulatorów, urządzeń energetycznych), branży przeciwpożarowej oraz branży zajmującej się bezpieczeństwem infrastruktury i urządzeń elektroenergetycznych w szerszym zakresie. Wśród podmiotów współpracujących, inicjujących i dostarczających wiedzy, informacji, wyników badań, a także rozwiązań należy ponadto wymienić stowarzyszenia branżowe, jednostki naukowe i krajowego ubezpieczyciela. To właśnie efektywna współpraca tych podmiotów przyczynia się do wypracowywania rozwiązań dla praktyki projektowania, wykonania i eksploatacji ASMEE (np. panel ekspercki pt. *Rola i miejsce ochrony pożarowej we wdrażaniu transformacji energetycznej* podczas „Forum Bezpieczeństwa Pożarowego” organizowanego przez PZUlab w Aleksandrowie Łódzkim, w dniu 11.06.2024 roku). Z tego względu w pracach nad stworzeniem omawianej metodyki konieczna jest partycypacja ekspertów reprezentujących różne obszary wiedzy oraz branże. Taką inicjatywę podjęto w CNBOP-PIB we współpracy z dwoma stowarzyszeniami branżowymi prowadzącymi działalność w obszarze magazynowania energii, tj. Polskim Stowarzyszeniem Magazynowania Energii (PSME), Stowarzyszeniem Polska Izba Magazynowania Energii (PIME) oraz Stowarzyszeniem Inżynierów i Techników Pożarnictwa (SITP) [10]. Przedmiotową inicjatywę wspierają eksperci z Komendy Głównej Państwowej Straży Pożarnej oraz Akademii Pożarniczej.

Ze względu na dynamiczny rozwój ASMEE w kraju – zarówno w zastosowaniach wielkoskalowych, jak i domowych (prosumenckich) – należy przyjąć, iż bez odpowiedniego przeciwdziałania zagrożeniom pożarowym bezpośrednio związanym z powszechnym stosowaniem akumulatorów litowo-jonowych można spodziewać się nasilenia i różnorodności incydentów z udziałem obu typów magazynów energii. Według literatury przedmiotu ryzyko powstania i rozprzestrzeniania się pożaru oraz wybuchu w obiektach z akumulatorowymi systemami magazynowania energii może wynikać z występowania określonych czynników ryzyka:

- elektrycznych, takich jak: usterki akumulatora, przeładowanie, szybkie rozładowanie, utrata systemów zdalnego monitorowania, wewnętrzne zwarcia, przegrzanie, przedostanie się wody, uderzenie pioruna (prowadzące do niestabilności termicznej),
- chemicznych, takich jak: nieodłączne zagrożenia związane z przechowywanymi towarami niebezpiecznymi, wycieki oleju transformatorowego/oleju napędowego, gazu chłodniczego/chłodziwa, chemiczne reakcje,
- związanych z groźbą zapłonu gazów wentylacyjnych,
- związanych z groźbą rozprzestrzeniania się ognia ze względu na bliskość akumulatorów, pojemników/obudów względem siebie, infrastruktury na miejscu i roślinności (w tym roślinności ekranującej),
- związanych z groźbą uszkodzenia mechanicznego akumulatorów, pojemników/obudów spowodowane uderzeniem pojazdu,

requirements. Suitable regulations in Poland are still being developed and should be introduced in the coming years (counting from 2026). During these works, certain concerns arise, e.g. connected to the lack of sufficient and credible research on the fire safety of the lithium-ion batteries located in civil structures or in their direct vicinity. They are above all related to the impact of these devices on fire development or direct initiation. All these matters, essential for fire safety, are presented as synthetically and accessibly as possible in the following sections of this article, which address in turn: energy storage technologies, battery-based electric energy storage systems operation hazards and their prevention and mitigation methods. At this occasion, requirements and standards are reviewed in the context of the fire safety of the subject technologies and final conclusions and recommendations are formulated.

- krajobrazowych, takich jak pożar sąsiadującego lasu / pożar trawy spowodowany pożarem w obiekcie lub zewnętrzny zapłon infrastruktury obiektu spowodowany żarem, promieniowaniem cieplnym i oddziaływaniem płomieni [15].

Problemy i wątpliwości związane z koniecznością zapewnienia właściwego bezpieczeństwa pożarowego wynikają również z nadal niewystarczających i niejednoznacznych regulacji prawnych i wymagań normatywnych w zakresie ochrony przeciwpożarowej w odniesieniu do budowy i eksploatacji takich magazynów – zarówno na poziomie europejskim, jak i krajowym. W wielu państwach Unii Europejskiej wdrożono już krajowe przepisy i wymagania normatywne dotyczące projektowania, instalowania i eksploatacji magazynów energii. W państwach tych w zasadniczo zgodny sposób zidentyfikowano kluczowe zagrożenia w zakresie bezpieczeństwa pożarowego, określając ograniczenia, wymagania techniczne i te dotyczące lokalizacji. Odpowiednie przepisy w Polsce są nadal opracowywane i w najbliższych latach (licząc od 2026 roku) powinny zostać wdrożone. W trakcie tych prac pojawiają się pewne wątpliwości, m.in. związane z brakiem wystarczających i wiarygodnych badań w zakresie bezpieczeństwa pożarowego baterii litowo-jonowych lokalizowanych w obiektach budowlanych lub w bezpośrednim ich sąsiedztwie. Dotyczą one przede wszystkim wpływu tych urządzeń na rozwój pożaru lub jego bezpośrednie inicjowanie. Wszystkie te kluczowe dla bezpieczeństwa pożarowego kwestie w możliwie syntetyczny i przystępny sposób zostały przedstawione w kolejnych częściach niniejszego artykułu, poświęconych odpowiednio: technologiom magazynowania energii, zagrożeniom związanym z eksploatacją akumulatorowych systemów magazynowania energii elektrycznej oraz sposobom zapobiegania im i ich ograniczania. Przy tej okazji dokonano przeglądu wymagań i standardów w kontekście zapewnienia bezpieczeństwa pożarowego omawianych technologii oraz sformułowano wnioski końcowe i rekomendacje.

Currently used energy storage technologies

In the technological context, energy storage is necessary to ensure the stability of energy grids, development of renewable energy sources and transport. Batteries already are an inherent part of the devices and infrastructure essential for our technology-based societies.

There are many divisions and classifications of energy storage systems. From the fire safety perspective, it is essential to divide them according to the storage technology in use. On its basis, the primary types of the currently used energy storage systems include:

- mechanical energy storage systems – using physical processes to accumulate and release energy; the most popular of them include pumped storage power plants, flywheel systems and compressed air storage systems;
- electrochemical electric energy storage systems – also referred to as rechargeable batteries or batteries, which are devices that store electric energy in chemical form and then release it when necessary; they use chemical

Aktualnie stosowane technologie magazynowania energii

W kontekście technologicznym magazynowanie energii jest niezbędne dla zapewnienia stabilności sieci energetycznych, rozwoju odnawialnych źródeł energii i transportu. Akumulatory są już nieodzowną częścią urządzeń oraz infrastruktury kluczowej dla naszych społeczeństw opartych na technologii.

Istnieją liczne podziały i klasyfikacje magazynów energii. Kluczowym z perspektywy bezpieczeństwa pożarowego kryterium jest ich rozróżnienie ze względu na zastosowaną technologię magazynowania. Opierając się na nim, wśród głównych rodzajów wykorzystywanych aktualnie magazynów energii można wymienić:

- mechaniczne magazyny energii elektrycznej – wykorzystujące procesy fizyczne do gromadzenia i uwalniania energii; do najpopularniejszych z nich należą elektrownie szczytowo-pompowe, systemy z kołami zamachowymi (ang. *flywheels*) oraz magazyny sprężonego powietrza;
- elektrochemiczne magazyny energii elektrycznej – zwane również akumulatorami lub bateriami, będące urządzeniami, które przechowują energię elektryczną w postaci

reactions to accumulate and release electric energy;

- chemical electric energy storage systems – systems, in which electric energy is converted into chemical energy (by electrochemical reactions) and then converted back into electric energy;
- electric energy storage systems – equipment used to store electric energy for later use; operating by accumulating energy (e.g. from photovoltaic panels) in batteries or other technologies and releasing it when necessary; they can be used on a different scale, from household photovoltaic systems to larger systems in the energy grid.

In this article, considering the analysed hazards and fire safety conditions, the authors focused on electrochemical electric energy storage systems (batteries and rechargeable batteries). They store energy in cells using chemical reactions, which then may be converted into electric energy. It should be emphasised that at present it is the most common method of electric energy storage, in particular in mobile and household applications, but also in the currently designed large scale and industrial storage systems. With regards to the technologically available solutions used in electrochemical energy storage systems, several types of batteries are distinguished, among which the most popular are:

- lithium-ion batteries – commonly used in smartphones, notebooks, electric vehicles and household energy storage systems for energy obtained from photovoltaic panels; characterised by high energy density; the lithium-ion battery chemistry, generally related to cell cathode chemistry, is the core technology of the battery system; cell chemistry is one of primary parameters, which determine if a battery is suitable for the given application; the key differentiators of batteries are: energy density¹, safety², price³ and available C⁴ coefficient [1];
- acid-lead batteries – legacy type, still widely used in the automotive industry (e.g. car batteries) and as emergency power sources;
- redox-flow batteries – they store energy in liquids (electrolytes) flowing through cells; characterised by scalability and suitability for long-term storage, making them attractive for large stationary systems;
- supercapacitors – they provide very fast charge and discharge and long life, but they store much less energy than batteries; used where short and intense power pulses are required; used for many years in e.g. trams, electric locomotives [1].

Mankind has been using different forms for centuries. At present lithium-ion battery (LIB)-based BESS are particularly

chemicznej, a następnie uwalniają ją, gdy jest potrzebna; wykorzystują one reakcje chemiczne do gromadzenia i oddawania energii elektrycznej;

- chemiczne magazyny energii elektrycznej – systemy, w których energia elektryczna jest przekształcana w energię chemiczną (poprzez reakcje elektrochemiczne), a następnie może być ponownie zamieniona na energię elektryczną;
- elektryczne magazyny energii – urządzenia służące do przechowywania energii elektrycznej w celu jej późniejszego wykorzystania; działające poprzez akumulowanie energii (np. z paneli fotowoltaicznych) w bateriach lub innych technologiach i oddawanie jej, gdy jest to potrzebne; mogą być stosowane w różnych skalach, od domowych instalacji fotowoltaicznych po większe systemy w sieci energetycznej.

W niniejszym artykule, z uwagi na analizowane zagrożenia i warunki bezpieczeństwa pożarowego, autorzy skupili swoją uwagę na elektrochemicznych magazynach energii elektrycznej (baterie i akumulatory). Energia jest w nich przechowywana w ogniwach z wykorzystaniem reakcji chemicznych, które można następnie przekształcać w energię elektryczną. Podkreślenia wymaga, iż jest to obecnie najbardziej powszechna metoda magazynowania energii elektrycznej, szczególnie w zastosowaniach mobilnych i domowych, ale także w projektowanych obecnie magazynach wielkoskalowych i przemysłowych. W zakresie dostępnych technologicznie rozwiązań stosowanych w elektrochemicznych magazynach energii wyróżniamy kilka rodzajów akumulatorów, z których najpopularniejsze to:

- akumulatory litowo-jonowe – stosowane powszechnie w smartfonach, laptopach, pojazdach elektrycznych i domowych systemach magazynowania energii pozyskiwanej z paneli fotowoltaicznych; charakteryzują się wysoką gęstością energii; chemia akumulatora litowo-jonowego, która ogólnie odnosi się do chemii katody ogniwa, to technologia stanowiąca serce systemu akumulatorowego; chemia ogniwa jest jednym z głównych parametrów, które decydują o tym, czy akumulator nadaje się do danego zastosowania; kluczowymi czynnikami różnicującymi akumulatory są: ich gęstość energetyczna¹, bezpieczeństwo², cena³ i dostępny współczynnik C⁴ [1];
- akumulatory kwasowo-ołowiowe – starszy typ, wciąż szeroko stosowany w motoryzacji (np. akumulatory samochodowe) oraz jako awaryjne źródła zasilania;
- akumulatory przepływowe (ang. *redox-flow batteries*) – magazynują energię w cieczach (elektrolitach) przepływających przez ogniwa; charakteryzują się skalowalnością

¹ Gęstość energetyczna jest miarą tego, ile energii można zgromadzić w danej masie ogniwa. Zazwyczaj jest wyrażana w Wh/kg.

² Głównym czynnikiem zagrożenia dla bezpieczeństwa w przypadku stanów awaryjnych akumulatorów litowo-jonowych jest możliwość wystąpienia niestabilności termicznej, określanej także jako „ucieczka termiczna” lub „rozbieganie termiczne”.

³ Cena jest jednym z kluczowych czynników wpływających na podaż akumulatorów.

⁴ Współczynnik C to bardzo ważny czynnik wpływający na jakość akumulatora. Jest miarą szybkości, z jaką energia może być pobierana lub wprowadzana do ogniwa podczas ładowania. Wysokie współczynniki C (0,5 C lub wyższe) wskazują, że ogniwo można szybko ładować lub rozładowywać, podczas gdy niższe współczynniki C (poniżej 0,5 C) oznaczają, że ogniwo musi być ładowane lub rozładowywane wolniej. Można także powiedzieć, że ogniwa umożliwiające wysokie współczynniki C (zwykle 0,5 C lub wyższe) to ogniwa dużej mocy, a te, które umożliwiają niższe współczynniki C (zwykle 0,25 C i niższe), to ogniwa wysokoenergetyczne.

¹ Energy density is the measure of the energy volume that may be accumulated in the given cell mass. It is usually expressed in Wh/kg.

² The main safety hazard factor in lithium-ion battery emergencies is the potential occurrence of thermal runaway.

³ Price is a key factor affecting the battery supply.

⁴ The C coefficient is a very important factor affecting the battery quality. It is a measure of the rate, at which energy may be drawn from or introduced to cells while charging. High C coefficient values (0.5 C or higher) indicate that the cell may be quickly charged or discharged, while lower C coefficient values (below 0.5 C) mean that the cell must be charged or discharged slower. It may be said that cells that enable high C coefficient values (usually 0.5 C or higher) are high power cells and the cells that enable lower C coefficient values (usually 0.25 C or lower) are high energy cells.

popular, compared to other battery-based technologies, as they offer higher energy and power values, long life and acceptable costs. However, the combination of high energy materials and inflammable electrolytes significantly increases the risk of specific emergencies, including fire. Fire safety hazards related to BESS operation are presented in the remainder of the article.

Battery energy storage systems (BESS) operation hazards

LIB-based BESS, compared to other above-discussed storage technologies, due to the design, operating principle and fire load, are characterised by the greatest potential fire hazard. Therefore, the knowledge of different types of lithium-ion battery cells (both in terms of chemical composition of the electrolyte and geometry) and their behaviour in case of fire is essential for the design of effective fire protection measures. Due to the earlier development of electromobility and the approval requirements applicable to that area, previous research on LIB cell behaviour and fire-fighting was mostly conducted above all in the automotive sector (including the already referred to approval tests for electric vehicle batteries conducted for more than 10 years by CNBOP-PIB). However, sufficient and reliable research is still missing as basis for conclusions and evidence of effectiveness of solutions and fire protections for using LIB to store energy in civil structures or in their vicinity. This applies to location at distances that could have an impact on the subject civil structures in the context of fire safety, including with regards to threats to the life and health of facility users, rescuers, as well as property and the environment. The prior research conducted at CNBOP-PIB in this regard enable formulating the following conclusions that the authors consider significant.

The battery cells in electric vehicles and BESS (intended for use as large scale, industrial and household energy storage) are principally different products in terms of properties and hazards. All batteries used in the automotive industry are approved, which means that in a detailed compliance evaluation process, an independent certifying unit confirmed their properties, as well as protection functionalities. For BESS, due to the lack of an obligatory process of safety parameter evaluation by notified test laboratories and certifying units, such confirmations are most often absent. Thus, in this case the declared properties and utility features cannot be fully trusted, also with regards to their stability

- i możliwością długoterminowego przechowywania, co czyni je atrakcyjnymi dla dużych systemów stacjonarnych;
- superkondensatory – zapewniają bardzo szybkie ładowanie i rozładowywanie oraz długą żywotność, ale magazynują znacznie mniej energii niż baterie; stosowane tam, gdzie potrzebne są krótkie, intensywne impulsy mocy; są od wielu lat stosowane np. w tramwajach, elektrobusach [1].

Różne formy magazynowania energii były stosowane przez człowieka od wieków. Szczególnym zainteresowaniem aktualnie cieszą się ASMEE wykorzystujące baterie litowo-jonowe (LIB), które – w porównaniu z innymi technologiami akumulatorowymi – oferują wyższą energię i moc, długą żywotność oraz akceptowalne koszty. Jednak połączenie wysokoenergetycznych materiałów z łatwopalnymi elektrolitami zwiększa istotnie ryzyko określonych stanów awaryjnych, w tym pożaru. Zagrożenia w zakresie bezpieczeństwa pożarowego związane z eksploatacją ASMEE przedstawiono w kolejnej części artykułu.

Zagrożenia związane z eksploatacją akumulatorowych systemów magazynowania energii elektrycznej (ASMEE)

ASMEE, w których wykorzystuje się LIB, na tle innych omówionych powyżej technologii magazynowania – z uwagi na ich budowę, zasadę działania oraz występujące obciążenie ogniowe – cechują się największym potencjalnym zagrożeniem pożarowym. Dlatego znajomość różnych typów ogniw LIB (zarówno pod względem składu chemicznego elektrolitu, jak i geometrii) oraz ich zachowania w warunkach pożaru jest kluczowa w kontekście projektowania skutecznych środków ochrony przeciwpożarowej. Wcześniejszy rozwój elektromobilności oraz obowiązujące w tym obszarze wymagania homologacyjne sprawiły, że większość dotychczasowych badań nad zachowaniem i gaszeniem pożarów ogniw LIB prowadzono przede wszystkim w sektorze motoryzacyjnym (w tym przywoływane już badania homologacyjne baterii pojazdów elektrycznych prowadzone od ponad 10 lat przez CNBOP-PIB). Brak natomiast nadal wystarczających i wiarygodnych badań dających podstawy co do wnioskowania i dowodów skuteczności rozwiązań i zabezpieczeń przeciwpożarowych dla stosowania LIB do magazynowania energii w obiektach budowlanych lub w ich pobliżu. Mowa o lokalizacji w odległościach mogących mieć wpływ na wspomniane obiekty budowlane w kontekście ich bezpieczeństwa pożarowego, w tym w wymiarze zagrożenia dla życia i zdrowia użytkowników takich obiektów, ratowników, a także mienia i środowiska. Dotychczasowe badania prowadzone w CNBOP-PIB w tym zakresie pozwalają na sformułowanie poniższych, istotnych według autorów wniosków.

Ogniwa baterii w pojazdach elektrycznych oraz te w ASMEE (o zamierzonym zastosowaniu jako wielkoskalowe, przemysłowe i domowe magazyny energii) to zasadniczo różne wyroby co do właściwości i zagrożeń. Wszystkie baterie stosowane w przemyśle motoryzacyjnym są homologowane, co oznacza, że w szczegółowym procesie oceny zgodności niezależna jednostka certyfikacyjna potwierdziła ich właściwości, a także funkcjonalności ochronne. W przypadku ASMEE, ze względu na brak obligatoryjnego udziału

and repeatability in relation to the subsequent batches introduced to the market. This is a very important difference between BESS and approved batteries in electric vehicles. Unfortunately, it is still not always noticed and understood in market practice.

Meanwhile, specific properties, such as the above-mentioned accumulated energy density, high efficiency, life and depth of discharge range, determined the common use of storage systems with lithium-ion batteries (LIB): LFP – lithium iron phosphate, NMC – lithium nickel manganese cobalt oxide or LTO – lithium titanate oxide.

LIB batteries, due to the combustible chemical composition of the electrolytes used, may be a fire and explosion hazard, while the decisive factor for maintaining safety during their operation is keeping the individual cells in stable operating conditions – in a specific range of voltage, temperature and internal pressure. The causes of hazards from LIB may be due to the impact of external and/or internal factors, such as: mechanical damage, thermal effects, electric phenomena in cell (i.e. overload, over-voltage, short-circuit, overcharge, excess discharge), change of useful properties of manufacture materials with time, ageing or incorrect operation, internal manufacture defects [10–14]. A particular concern is due to the latter of the listed factors, which should be regarded as non-validated risk due to the above-mentioned lack of implementation of a suitable market supervision system that would involve competent bodies and independent entities for compliance evaluation to guarantee the marketing of products with confirmed properties, including in terms of stability, both in a specific product life cycle and subsequent specimens of the given type. This matter is addressed in detail in the remainder of the article.

Lithium-ion battery systems are large masses of electrochemical materials intended to store a specific energy volume. During normal operation, the current flow in individual circuits is controlled, which enables charging and discharging the batteries as programmed in the system control unit. However, there are possible cases (emergencies), in which the operation stability of batteries may be disrupted. A consequence of these disruptions, under the most unfavourable circumstances, could be an abrupt release of a specific energy volume, previously accumulated in the given storage system (the increased energy demand results in an increase of battery capacity and thus the energy accumulated in energy storage systems). If the battery operation supervision system becomes unable to limit the electric current from and to a cell, short-circuit occurs, leading to a quick discharge of stored energy and abrupt heating of the cell or cells affected by the subject failure. Then, an uncontrolled temperature increase may occur, up to 400°C. In such conditions, combustible gases may be released within a cell, such as hydrogen, hydrocarbons, hydrogen fluoride, hydrogen chloride, hydrogen cyanide and carbon monoxide [1]. This process, commonly referred to as thermal runaway may spread in a chain reaction, increasing the temperature of adjacent cells and modules to the level, at which they cannot be cooled from the outside.

The impact of the above-mentioned sources of hazard from LIB may lead to increased temperature in a single cell or in a given LIB module and, by consequence, initiate the failure propagation

w procesie oceny parametrów bezpieczeństwa notyfikowanych laboratoriów badawczych oraz jednostek certyfikujących, takich potwierżeń najczęściej brakuje. W związku z powyższym, w tym przypadku nie można mówić o pełnym zaufaniu do deklarowanych właściwości i cech użytkowych, a także o ich stałości oraz powtarzalności w odniesieniu do kolejnych partii wprowadzanych do obrotu wyrobów. To bardzo ważna różnica pomiędzy ASMEE i homologowanymi bateriami w pojazdach elektrycznych – niestety nadal nie zawsze dostrzegana i rozumiana w praktyce rynkowej.

Tymczasem specyficzne cechy, takie jak wspomniana już wcześniej duża gęstość gromadzonej energii, wysoka sprawność, żywotność i zakres głębokości rozładowania, zdecydowały o powszechności wykorzystywania magazynów z bateriami wykonanymi w technologii litowo-jonowej (LIB): LFP – litowo-żelazowo-fosforowej (ang. *lithium iron phosphate*), NMC – litowo-niklowo-manganowo-kobaltowej (ang. *lithium nickel manganese cobalt oxide*), lub LTO – litowo-tytanowej (ang. *lithium titanate oxide*).

Baterie LIB, ze względu na palną kompozycję chemiczną stosowanych w nich elektrolitów, mogą stanowić zagrożenie pożarowe i wybuchowe, zaś czynnikiem decydującym dla zachowania bezpieczeństwa w trakcie ich eksploatacji jest utrzymanie poszczególnych ogniw w stabilnych warunkach pracy – w określonym przedziale napięcia, temperatury i ciśnienia wewnętrznego. Przyczyny zagrożeń ze strony baterii LIB mogą być spowodowane oddziaływaniem czynników zewnętrznych i/lub wewnętrznych, m.in. takich jak: uszkodzenia mechaniczne, oddziaływanie termiczne, zjawiska elektryczne w ogniwie (tj. przeciążenie, przepięcie, zwarcie, przeładowanie, nadmierne rozładowanie), zmiana właściwości użytkowych materiałów konstrukcyjnych pod wpływem czasu, starzenia ich lub niewłaściwej eksploatacji, wewnętrzne wady produkcyjne [10–14]. Szczególny niepokój budzi ostatni z wymienionych czynników, który należy postrzegać w kategoriach ryzyka niezwalidowanego, ze względu na wspomniany już wcześniej brak wdrożenia, odpowiedniego systemu nadzoru rynku, który poprzez udział w nim odpowiednich organów oraz niezależnych podmiotów oceny zgodności, dawałby rękojmię wprowadzania na rynek wyrobów o potwierdzonych właściwościach, w tym w kontekście ich stałości, zarówno w cyklu życia danego wyrobu, jak i kolejnych egzemplarzy danego typu. Zagadnienie to zostało uszczegółowione w dalszej części artykułu.

Systemy baterii litowo-jonowych to duże masy materiałów elektrochemicznych, które są przeznaczone do magazynowania określonej ilości energii. Podczas normalnej eksploatacji przepływ prądu w poszczególnych układach odbywa się w sposób kontrolowany, dzięki czemu baterie mogą się ładować i rozładowywać w sposób zaprogramowany w module sterowania systemu. Istnieje jednak kilka możliwych przypadków (stany awaryjne), w których stabilność pracy akumulatorów może zostać zakłócona. Konsekwencją wystąpienia tych zakłóceń, w najbardziej niepożądanych okolicznościach może być gwałtowne uwalnianie określonej ilości energii, która została wcześniej zgromadzona w danym magazynie (wzrost zapotrzebowania na energię skutkuje wzrostem pojemności akumulatorów i tym samym ilości energii gromadzonej przez magazyny energii). Jeśli system nadzorowania pracy baterii nie jest już w stanie ograniczyć prądu elektrycznego płynącego do i z celi, dochodzi do zwarcia,

process. As a result of battery cell overheating, the chemical components within begin to react with one another or decompose, thus releasing heat and increasing pressure. As a result, the degassing process may occur, during which the accumulated, pressurised and evaporated inflammable electrolyte is released from the battery through enclosure components with special reduced resistance or design relief valves. The impact of harmful external and internal factors may also lead to an internal short-circuit in the battery cell, resulting in an uncontrolled and quick discharge, leading to a further abrupt temperature increase. Exceeding the thermal resistance of the manufacture materials of the battery cell results in the decomposition and release of combustible aerosol, constituting a mixture of different above-listed gases. The released inflammable gases, sparking and high temperatures may cause fire or, in extreme cases, explosion [10], [14]. To conclude, the characteristic symptoms of battery operation failure are in turn: temperature increase, degassing, release of combustible aerosol in characteristic white colour and then fire emergence. The accumulating gases, if not discharged properly, increase the risk of explosion.

Figure 1 shows the most common causes of thermal runaway in battery cells and/or modules, including:

- mechanical damage, in which the cell is physically deformed in a way that causes a short-circuit, by crushing or perforation;
- electric damage, in which a short-circuit develops within a cell. This may occur under normal operation conditions or if a cell is overcharged or unevenly discharged;
- excess heating, in which a cell is heated up to extreme temperatures.

co prowadzi do szybkiego rozładowania zmagazynowanej energii i gwałtownego podgrzania ogniwa lub ogniw dotkniętych przedmiotową awarią. Wówczas może dojść do niekontrolowanego wzrostu temperatury, nawet do 400°C. W takich warunkach wewnątrz celi mogą uwalniać się gazy palne, takie jak wodór, węglowodory, fluorowodór, chlorowodór, cyjanowodór oraz tlenek węgla [1]. Proces ten, powszechnie określany niestabilnością termiczną, może rozprzestrzeniać się jako reakcja łańcuchowa, podnosząc temperaturę sąsiednich ogniw, modułów do poziomu, w którym nie można ich już schłodzić od zewnątrz.

Oddziaływanie wymienionych wcześniej źródeł zagrożeń ze strony baterii LIB może doprowadzić do wzrostu temperatury w pojedynczym ogniwie lub danym module baterii LIB i – w konsekwencji – zapoczątkować proces propagacji awarii. W wyniku przegrzania ogniwa baterii składniki chemiczne w nim występujące zaczynają ze sobą reagować lub ulegają rozkładowi, uwalniając ciepło i powodując wzrost ciśnienia. W efekcie może dojść do procesu odgazowania, w trakcie którego nagromadzony pod ciśnieniem odparowany łatwopalny elektrolit znajduje ujście z baterii przez części obudowy o specjalnie obniżonej odporności lub konstrukcyjne zawory nadmiarowe. Oddziaływanie szkodliwych czynników zewnętrznych i wewnętrznych może doprowadzić także do wewnętrznego zwarcia w ogniwie baterii, w wyniku którego następuje niekontrolowane i szybkie jego rozładowanie prowadzące do gwałtownego dalszego wzrostu temperatury. Przekroczenie wytrzymałości termicznej materiałów konstrukcyjnych ogniwa baterii powoduje ich rozkład, wydzielanie palnego aerosolu, stanowiącego mieszaninę różnych, wymienionych wcześniej gazów. Wydobywające się łatwopalne gazy, iskrzenie i wysokie temperatury mogą być przyczyną pożaru lub w skrajnych przypadkach wybuchu [10], [14]. Podsumowując, w następstwie stanu awaryjnego pracy baterii charakterystycznymi objawami są kolejno: wzrost temperatury, odgazowanie, wydzielanie palnego aerosolu o charakterystycznej białej barwie, a następnie pojawienie się ognia. Gromadzące się gazy, jeśli nie zostaną prawidłowo odprowadzone, zwiększają ryzyko wybuchu.

Rycina 1 przedstawia najczęstsze przyczyny niestabilności termicznej w ogniwach i/lub modułach baterii, w tym:

- uszkodzenie mechaniczne, w którym ogniwo jest fizycznie odkształcane w sposób powodujący zwarcie, przez zmiażdżenie albo perforację;
- uszkodzenie elektryczne, w którym wewnątrz ogniwa rozwija się zwarcie. Może się to zdarzyć w normalnych warunkach pracy lub jeśli ogniwo jest przeładowane albo nadmiernie rozładowane;
- nadmierne nagrzewanie, w którym ogniwo jest podgrzewane do ekstremalnych temperatur.

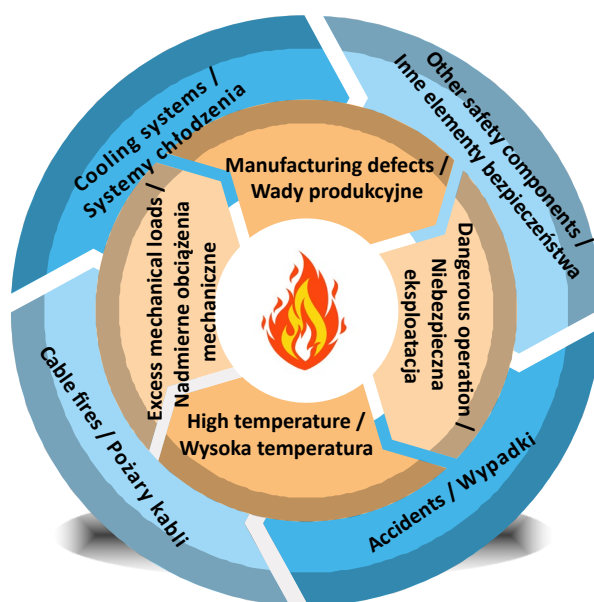


Figure 1. BESS fires caused by battery and BOS (battery operating system)
Rycina 1. Pożary ASMEE powodowane przez akumulator i BOS (ang. *battery operating system*)

Source: Own elaboration based on [1].

Źródło: Opracowanie własne na podstawie [1].

Organic solvents in electrolyte are highly ignitable inflammable components. Lithium salt is subject to thermal decomposition, which results in toxic products.

The analysis of the safety hazard related to LIB leads to very important conclusions, included i.a. in a publication entitled *A Cell to Grid Guide to Utility-scale Battery Energy Storage Systems* [1]. It stated that components other than the battery cause safety incidents more often than the battery itself. The research results on BESS incidents were published in May 2024 by the Electric Power Research Institute (EPRI). The institution demonstrated based on its database that more than 65% incidents could be attributed to the systems and devices integrated with the BESS, compared to 11% caused directly by battery cells and modules. According to that source, the integration of systems and their components with the BESS, including fire detection system sensors and control and firefighting systems, causes much more incidents and emergencies. It may be assumed that the above-mentioned incidents were caused by improper selection of the above-mentioned fire protection equipment [1].

The risk of using improper fire protection equipment is also a problem noted by CNBOP-PIB. Thus, in the opinion of the authors, the fire protection equipment used in energy storage systems, such as fire signalling systems or fixed firefighting equipment, should be subject to prior additional tests to confirm the correctness (effectiveness) of operation in the subject applications. Meanwhile, in Poland such tests have not been conducted in practice, despite their availability at various units, not only the research institute of the State Fire Service. Analogical tests to confirm the declared functionalities are required for the BMS used in the BESS.

Problems related to the manufacture of battery cells and modules still exist, e.g. when mixing electrode materials, coiling cells or welding connections at the module level. As original

Rozpuszczalniki organiczne w elektrolicie są składnikami łatwopalnymi o wysokiej podatności na zapłon. Sól litowa ulega rozkładowi termicznemu, prowadząc do powstawania toksycznych produktów.

Analiza zagrożeń dotyczących bezpieczeństwa związanych z akumulatorami LIB prowadzi do bardzo ważnych wniosków, które zawarto m.in. w publikacji pt. *A Cell to Grid Guide to Utility-scale Battery Energy Storage Systems* [1]. Stwierdzono w niej, że elementy niebędące akumulatorem częściej powodują incydenty związane z bezpieczeństwem niż sam akumulator. Wyniki badań dotyczących incydentów z ASMEE opublikował w maju 2024 roku Electric Power Research Institute (EPRI). Instytucja ta wykazała na podstawie prowadzonej przez siebie bazy, że ponad 65% zdarzeń można przypisać zintegrowanym z ASMEE systemom i urządzeniom, w porównaniu do 11% spowodowanych bezpośrednio przez ogniwa i moduły akumulatorowe. Integracja z ASMEE systemów i ich elementów, takich jak czujniki będące częścią systemów detekcji pożaru oraz systemów do kontroli i gaszenia, według tego źródła, przysparza zdecydowanie więcej incydentów i stanów awaryjnych. Można domniemywać, że wspomniane incydenty powstawały ze względu na zły dobór wymienionych urządzeń przeciwpożarowych [1].

Ryzyko zastosowania niewłaściwych urządzeń przeciwpożarowych jest również problemem dostrzeganym w CNBOP-PIB. Z tego względu autorzy wyrażają pogląd, że urządzenia przeciwpożarowe stosowane w magazynach energii, takie jak systemy sygnalizacji pożarowej czy stałe urządzenia gaśnicze, powinny wcześniej być poddane dodatkowym badaniom, pozwalającym potwierdzić prawidłowość (skuteczność) ich działania w omawianych zastosowaniach. Tymczasem w Polsce takich testów dotychczas w praktyce nie prowadzono, pomimo ich dostępności w ofercie różnych jednostek – nie tylko instytutu badawczego Państwowej Straży Pożarnej. Analogicznych badań w zakresie

equipment manufacturers (OEM) accelerate the manufacturing, manufacturing lines become vulnerable to quality problems, despite a high level of automation. Factory audits and quality controls remain an essential component that guarantees safe operation of the BESS, but still insufficient, as already demonstrated multiple times.

To continue the considerations, it is worth noting the solutions used in the United States. It should be emphasised that in the process of analysis of the fire hazards related to the operation of large scale battery electric energy storage systems most of the regulations applicable in the United States assume that the entire BESS container may be exposed to an uncontrolled temperature increase caused by the fire of individual cells. Therefore, in case of danger or LIB failure, the recommended safety practices for rescuers are reduced to leaving the container to burn out without attempting to enter or save equipment, in order to prioritise the safety of the rescuers and site personnel. When developing assumptions and fire protection requirements, it is assumed that losses be limited to one object, the container. Thus, preventing the heat transfer from one container to another and controlling the accumulation of explosive gases are particularly emphasised [1].

The first of the above-mentioned aspects is usually considered already at the stage of container design and verified by destructive tests by the manufacturers. The second requirement is met by fitting the container with venting equipment and/or deflagration panels that open to reduce the pressure inside the container.

Of course, the above-mentioned fire protection strategies cannot be used for industrial and household storage systems, which are mostly located within or in direct vicinity of civil structures. The solutions used in relation to them are discussed in the following section of this article.

Prevention and mitigation of electric energy storage systems operation hazards

As a rule, preventing the subject hazards consists in eliminating the unfavourable conditions that could lead to emergencies. Preventing includes considering the actual and identified fire safety hazards and implementing effective measures to reduce or eliminate them already at the design stage, at the cell, module, rack and container level. Another important part is using “multi-layered” monitoring and automatic control systems that maintain the BESS in the proper operation range. In prevention and mitigation of the fire hazards related to operation of electric energy storage systems, the following are essential:

potwierdzenia deklarowanych funkcjonalności wymagają BMS-y stosowane w ASMEE.

Problemy związane z produkcją ogniw i modułów akumulatorowych wciąż występują, m.in. podczas mieszania materiału elektrod, nawijania ogniw czy spawania połączeń na poziomie modułu. W miarę jak producenci oryginalnego wyposażenia (POW) przyspieszają produkcję, linie produkcyjne stają się podatne na problemy jakościowe, mimo wysokiego poziomu automatyzacji. Audyty fabryczne oraz kontrole jakości pozostają kluczowym elementem gwarantującym bezpieczną pracę ASMEE, ale – jak już kilkakrotnie wykazano – nadal niewystarczającym.

Kontynuując rozważania w tym zakresie, warto zwrócić uwagę na rozwiązania stosowane w USA. Należy podkreślić, iż w procesie analizy zagrożeń pożarowych związanych z eksploatacją wielkoskalowych akumulatorowych systemów magazynowania energii elektrycznej większość obowiązujących tam przepisów zakłada, że cały kontener ASMEE może być narażony na niekontrolowany wzrost temperatury w wyniku pożaru pojedynczych ogniw. Dlatego w przypadku zagrożenia czy stanu awaryjnego LIB rekomendowane praktyki bezpieczeństwa dla ratowników sprowadzają się do pozostawienia kontenera do wypalenia bez podejmowania prób wejścia do środka lub ratowania sprzętu, aby na pierwszym miejscu postawić bezpieczeństwo ratowników i personelu obiektu. Przy tworzeniu założeń i warunków ochrony przeciwpożarowej zakłada się przy tym ograniczenie strat do jednego obiektu – kontenera. W związku z tym szczególny nacisk kładzie się na zapobieganie przenoszeniu się ciepła z jednego kontenera do drugiego oraz na kontrolę gromadzenia się gazów wybuchowych [1].

Pierwszy z wyżej wymienionych aspektów jest zwykle uwzględniany już na etapie projektowania kontenera i weryfikowany poprzez testy niszczące przeprowadzane przez producentów. Drugi wymóg realizowany jest poprzez zastosowanie w kontenerze urządzeń odpowietrzających oraz/lub paneli deflagacyjnych, które otwierają się w celu obniżenia ciśnienia wewnątrz kontenera.

Oczywiście ww. strategii ochrony przeciwpożarowej nie można stosować w przypadku magazynów przemysłowych i domowych, które w większości przypadków zlokalizowane są wewnątrz lub w bezpośredniej bliskości obiektów budowlanych. W odniesieniu do nich stosowane są rozwiązania omówione w kolejnym rozdziale niniejszego artykułu.

Zapobieganie i ograniczanie zagrożeń związanych z eksploatacją magazynów energii elektrycznej

Co do zasady zapobieganie omawianym zagrożeniom polega na eliminacji niekorzystnych warunków, które mogą prowadzić do stanów awaryjnych. Zapobieganie obejmuje uwzględnianie rzeczywistych, zidentyfikowanych zagrożeń w zakresie bezpieczeństwa pożarowego i wdrażanie skutecznych środków ich ograniczania lub eliminacji już na etapie projektowania – zarówno na poziomie ogniw, modułu, stojaka, jak i kontenera. Ponadto istotnym elementem jest stosowanie „wielowarstwowego” monitorowania oraz automatycznych systemów kontroli, które utrzymują ASMEE w pożądanym zakresie działania. W zapobieganiu

- energy storage system properties confirmed in the compliance test and evaluation process,
- functionalities and properties of the battery operation monitoring BMS confirmed in the test and evaluation process,
- electric protections automatic circuit disconnection capability according to the assumed BMS safety algorithms,
- properly selected, designed and dedicated as necessary passive and active fire protections,
- use of appropriate technical protections and broadly understood fire protection equipment.

In addition, in the context of the fire safety of these plants, technical requirements and application guidelines are important (e.g. location, room ventilation, line routing), as well as requirements for the design and installation works and maintenance and operation requirements.

Despite using many, possibly best prevention methods, battery failures may still occur, which unless properly mitigated may lead to severe incidents, both health and life-threatening and causing damage to property and the environment. The specifics of the subject risk arises from the above-described possibility of occurrence of thermal runaway. In almost every case, there is a short period between the emergence of the first symptoms of battery failure (release of gases, white smoke) and the moment, when the process of abrupt temperature increase, degassing and thermal runaway becomes irreversible.

i ograniczeniu zagrożeń pożarowych związanych z eksploatacją magazynów energii elektrycznej kluczowe są:

- potwierdzone w procesie badań i oceny zgodności właściwości magazynów energii,
- potwierdzone w procesie badań i oceny zgodności funkcjonalności i właściwości BMS-ów monitorujących pracę baterii,
- zabezpieczenia elektryczne i zdolność do automatycznego rozłączania obwodów według przyjętych algorytmów bezpieczeństwa BMS-ów,
- właściwie dobrane, zaprojektowane i według potrzeb dedykowane bierne i czynne zabezpieczenia przeciwpożarowe,
- stosowanie odpowiednich zabezpieczeń technicznych i szeroko rozumianych urządzeń służących ochronie przeciwpożarowej.

Ponadto w kontekście bezpieczeństwa pożarowego tych instalacji istotne są warunki techniczne i wytyczne stosowania (np. lokalizacji, wentylacji pomieszczeń, prowadzenia przewodów), a także wymagania w zakresie projektowania i prac instalacyjnych oraz warunki konserwacji i eksploatacji.

Pomimo stosowania licznych, możliwie najlepszych metod zapobiegania, wciąż mogą występować awarie baterii, które – jeśli nie zostaną odpowiednio ograniczone – mogą prowadzić do poważnych incydentów zagrażających zarówno zdrowiu i życiu osób, jak i wywołujących szkody w mieniu i środowisku. Specyfika omawianego ryzyka wynika, z opisanych powyżej możliwości zaistnienia niestabilności termicznej. W niemal każdym przypadku istnieje krótki okres pomiędzy pojawieniem się pierwszych oznak awarii baterii (wydzielenie gazów, białego dymu) a momentem, w którym proces gwałtownego wzrostu temperatury, odgazowania i niestabilności termicznej baterii staje się nieodwracalny.

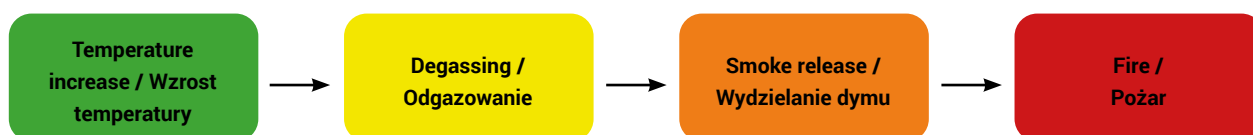


Figure 2. Cykl rozwoju awarii ogniwa baterii litowo-jonowej
Rycina 2. Lithium-ion battery cell failure development cycle

Source: Own elaboration based on [10].

Źródło: Opracowanie własne na podstawie [10].

Monitoring cell voltage and temperature (including the increase), using dedicated high sensitivity smoke and gas sensors and protection redundancy, disconnecting the power supply upon detection of incorrect cell activity and automatic reporting of the potential incidents to the fire service, as well as using automatically activated control and firefighting systems are the energy storage fire hazard prevention measures used in civil structures or in their direct vicinity.

Here, it should be emphasised that if the preventative measures prove insufficient, then it is only possible to undertake efforts to reduce the impact. At this stage, action is taken to minimise the fire impact on the people nearby, property and the environment and

Monitorowanie napięć i temperatury ogniw (w tym jej przyrostu), stosowanie dedykowanych czujników dymu i gazów o wysokiej czułości oraz redundancji zabezpieczeń, odłączanie zasilania w przypadku wykrycia nieprawidłowej aktywności ogniw i automatyczne powiadamianie straży pożarnej o potencjalnych incydentach, a także stosowanie automatycznie aktywowanych systemów kontroli i gaszenia to środki zapobiegania zagrożeniom pożarowym magazynów energii stosowanych w obiektach budowlanych lub w bezpośrednim ich sąsiedztwie.

Podkreślić przy tym należy, że jeśli podjęte środki prewencyjne okażą się niewystarczające, możliwe jest już tylko podejmowanie wysiłków na rzecz ograniczania jego skutków. Na tym

to prevent the spreading of fire to other parts of the battery system and to reduce the potential impact and spreading of the fire in the given civil structure and to other structures nearby. For this purpose, the Polish fire service uses standard procedures, designed considering the safety measures and rescuer protection measures, as well as rescue experience and practices.

The risk of occurrence of the equipment defects, system failures or operator errors always exists. Implementing appropriate prevention, detection, warning and mitigation activities minimises the potential losses related to these failures and increases the safety of rescuers if an incident occurs.

Ensuring the fire safety of batteries is connected with the necessity of using appropriate protection devices. Of course, designing fire safe installations and planning dedicated fire protection measures requires additional time, resources and funds. However, in case of safety incidents, the potential costs related to human health and life hazards, property losses and environmental damage are very high. Thus, the “safety above all” approach, understood as rationalisation of fire protection based on balancing the actual hazard level with the implemented protective measures level, including insurance protection matters, is justified from the social, ethical and economic perspective.

The remainder of the article discusses the possible methods of designing products, developing solutions and building and maintaining systems to effectively reduce the risk to life, property and the environment, while keeping the use of batteries and supervision systems and their protection economical. In BESS battery protection, BMS plays the role of first protection – it monitors and signalises irregularities in the voltage, current and temperature at the cell level. The capability to signal irregularities in battery operation and disconnect at the electrical protections level are important and essential components of the safety system. BMS functionalities and parameters are an important matter. The BMS requirements and their confirmation by testing these products are essential for building the trust in these devices, guaranteed parameters or declared functionalities.

In addition to standard monitoring and control at the BESS level, some OEM use additional solutions to reduce the battery overheating risk. An example are the local control and firefighting systems activated upon detection of thermal incident, temperature increase (according to the authors, it would be even better to control for an unnatural temperature increase). The installed firefighting automatic activation systems may feed water or other dedicated cooling/extinguishing agents directly to the module, in which an emergency was identified, and to adjacent module in order to reduce their temperature, in particular for NMC or NCA cells.

To protect battery packs, sprinkler systems are also used, dedicated for local or standard protection, designed for room protection. Here it is important that all these firefighting systems consider the additional hazards resulting from the use of LIB (fire load, combustion process specifics, including its duration, continuation even under oxygen supply from the outside etc.) and be capable of controlling and/or firefighting. The firefighting effectiveness should be confirmed by proper control tests.

Some manufacturers of large scale, container-based storage systems assume, however, that a complete loss of the container

etapie prowadzi się działania mające na celu zminimalizowanie wpływu pożaru na osoby znajdujące się w pobliżu oraz na mienie i środowisko, a także zapobieganie rozprzestrzenianiu się pożaru na pozostałe części systemu baterii i ograniczenie możliwości oddziaływania, rozprzestrzeniania się pożaru w danym obiekcie budowlanym oraz na obiekty sąsiednie. Polska straż pożarna w tym zakresie stosuje standardowe zasady postępowania opracowywane z uwzględnieniem środków bezpieczeństwa i ochrony ratowników, a także doświadczeń i praktyki ratowniczej.

Ryzyko wystąpienia wad urządzeń, awarii systemu lub błędów popełnianych przez operatorów istnieje zawsze. Wdrożenie odpowiednich działań w zakresie zapobiegania, wykrywania, ostrzegania oraz ograniczania skutków pozwala zminimalizować potencjalne straty związane z tymi awariami, a także zwiększa bezpieczeństwo ratowników w przypadku wystąpienia incydentu.

Zapewnienie bezpieczeństwa pożarowego akumulatorów wiąże się z koniecznością stosowania odpowiednich urządzeń zabezpieczających. Oczywiście, projektowanie bezpiecznych pożarowo instalacji oraz planowanie dedykowanych środków ochrony przeciwpożarowej wymaga dodatkowego czasu, zasobów i nakładów finansowych. Jednak w przypadku wystąpienia incydentów bezpieczeństwa potencjalne koszty związane z zagrożeniem dla zdrowia i życia ludzi, stratami materialnymi oraz szkodami dla środowiska są bardzo wysokie. Dlatego podejście „bezpieczeństwo przede wszystkim” – rozumiane jako racjonalizacja ochrony przeciwpożarowej oparta na zbilansowaniu rzeczywistego poziomu zagrożenia z poziomem wdrożonych środków ochronnych, włączając w to kwestie ochrony ubezpieczeniowej, jest uzasadnione zarówno z perspektywy społecznej, etycznej, jak ekonomicznej.

W dalszej części artykułu omówiono, w jaki sposób można projektować produkty, opracowywać rozwiązania oraz budować i utrzymywać systemy w sposób, który pozwala skutecznie ograniczyć ryzyko dla życia, mienia oraz środowiska, przy jednoczesnym zachowaniu ekonomii stosowania akumulatorów i systemów nadzoru oraz ich ochrony. BMS pełni rolę pierwszego zabezpieczenia w ochronie baterii ASMEE. Monitoruje – on i sygnalizuje nieprawidłowości w zakresie napięcia, natężenia prądu oraz temperatury na poziomie ogniwa. Zdolność do sygnalizacji nieprawidłowości pracy baterii i rozłączanie na poziomie zabezpieczeń elektrycznych to ważne, podstawowe elementy systemu zabezpieczeń. Funkcjonalności BMS i jego parametry są istotnym zagadaniem. Wymagania dla BMS i ich potwierdzenie przez badania tych wyrobów są kluczowe dla budowania zaufania do tych urządzeń, gwarantowanych parametrów, czy deklarowanych funkcjonalności.

Poza standardowym monitorowaniem i kontrolą na poziomie ASMEE, niektórzy producenci POW stosują dodatkowe rozwiązania ograniczające ryzyko przegrzania baterii. Przykładem są miejscowe systemy kontroli i gaszenia aktywowane w przypadku wykrycia zdarzenia termicznego – wzrostu temperatury (według autorów jeszcze lepszym rozwiązaniem byłoby kontrolowanie nienaturalnego przyrostu temperatury). Zainstalowane systemy automatycznego aktywowania gaszenia mogą podawać wodę lub inne dedykowane środki chłodzące/gaśnicze bezpośrednio do modułu, w którym zidentyfikowano stan awaryjny, oraz do sąsiednich modułów w celu obniżenia ich temperatury – szczególnie w przypadku ogniwn NMC lub NCA.

is nearly certain if an uncontrolled thermal incident occurs in any cell or module. In such cases, the priority is to prevent the accumulation of explosive gases and to stop the incident from spreading to the adjacent containers. To further reduce the escalation risk, modules may be physically separated from one another or equipped with fire partitions.

Some energy storage systems are also equipped with additional fire protection measures, intended to control or extinguish LIB fires using conventional methods, such as inert gas or aerosol. Unfortunately, in this case it should be noted that the above-mentioned extinguishing agents do not cause a cooling effect. Thus, activating them cannot prevent thermal runaway if it occurs. Thus, based on the fire test results available in the literature of the subject, this type of devices are not recommended to protect energy storage systems [16]. In large scale container storage systems, most manufacturers use fire detection systems, most often using smoke and gas detectors, acoustic and optical signalers, FACP and control panels for that purpose. Systems are also designed to transmit fire alarms to the fire service. Fire and gas detection systems, like other fire protection equipment used for the fire protection of battery packs, require confirming the effectiveness in detecting fire phenomena and other emergencies in the subject application.

Designing multiple levels of technical protections and fire protection forms in large scale container-based storage systems, only partially mentioned above, has significant advantages compared to the solutions currently used in storage systems with significantly smaller capacities, industrial and household. As a rule, active and passive fire protections are used. Active protections in these detection and firefighting systems using various extinguishing agents were partially mentioned. Passive protections were not discussed, of which the essence consists in using solutions to separate a specific zone, space and thus limit the potential of uncontrolled spreading of fire. Analogically, relief and ventilation systems were not discussed.

In practice, the protection of the latter is reduced to ensuring proper design and monitoring operation by BMS. However, the matters of fire safety protections include in particular the matters of storage system location, including the maintenance of proper distances or fire separations from other structures, devices or combustible materials and between individual modules, the provision of ventilation and fire protection equipment required to install in the given type of civil structure (e.g. indoor and outdoor hydrants and fire extinguishers).

In turn, in industrial storage systems, most often installed in suitable enclosures, the so-called cabinet enclosures, in addition to the protections discussed in the previous paragraph, solutions are found that provide for using detection devices and autonomous fixed firefighting devices, in particular gas-powered. It is also not rare to fit this type of storage systems with semi-fixed devices that enable the coming rescue teams to connect their fire hoses and feed extinguishing water inside the storage system.

BESS should be designed considering specific measures necessary to meet the basic safety requirements. Thus, a series of factors should be analysed and evaluated, in particular related to:

Do zabezpieczenia zestawów baterii stosowane są również systemy tryskaczowe dedykowane do ochrony miejscowej lub standardowej – projektowane do ochrony pomieszczeń. Ważne jest przy tym, aby wszystkie te systemy gaszenia uwzględniały dodatkowe zagrożenia wynikające ze stosowania LIB (obciążenie ogniowe, specyfika procesu spalania, w tym jego długotrwałość, kontynuacja nawet w warunkach dostępu tlenu z zewnątrz itp.) i były zdolne do ich kontroli i/lub gaszenia. Skuteczność gaszenia powinna być potwierdzona w drodze odpowiednich badań kontrolnych.

Część producentów wielkoskalowych, kontenerowych magazynów przyjmuje natomiast założenie, zgodnie z którym całkowita utrata kontenera jest niemal pewna, jeśli w którymkolwiek ogniwie lub module wystąpi niekontrolowane zdarzenie termiczne. W takich przypadkach priorytetem jest zapobieganie gromadzeniu się gazów wybuchowych oraz powstrzymanie rozprzestrzeniania się incydentu na sąsiednie kontenery. Aby dodatkowo ograniczyć ryzyko eskalacji, moduły mogą być fizycznie odseparowane od siebie lub wyposażone w oddzielenia przeciwpożarowe.

Niektóre magazyny energii wyposażane są również w dodatkowe środki ochrony przeciwpożarowej, przeznaczone do kontroli lub gaszenia pożarów LIB przy użyciu konwencjonalnych metod, takich jak gaz obojętny lub aerosol. Niestety, w tym przypadku należy mieć świadomość, że wymienione środki gaśnicze nie wywołują efektu chłodzącego. Tym samym ich zadziałanie nie jest w stanie powstrzymać niestabilności termicznej, jeśli do niej dojdzie. W związku z powyższym na podstawie dostępnych w literaturze przedmiotu wyników testów pożarowych nie rekomenduje się stosowania tego rodzaju urządzeń do zabezpieczania magazynów energii [16]. Większość producentów w wielkoskalowych magazynach kontenerowych stosuje systemy detekcji pożaru, najczęściej wykorzystując do tego celu czujki dymu i gazów, sygnalizatory akustyczne i optyczne, CSP, panele sterowania. Projektowane są również systemy transmisji alarmów pożarowych do straży pożarnej. Systemy detekcji pożaru i gazów – podobnie jak inne urządzenia przeciwpożarowe stosowane do ochrony przeciwpożarowej zestawów baterii – wymagają potwierdzenia skuteczności do wykrywania zjawisk pożarowych i innych stanów awaryjnych w omawianym zastosowaniu.

Projektowanie w wielkoskalowych magazynach kontenerowych wielu poziomów zabezpieczeń technicznych oraz form ochrony przeciwpożarowej, o której tylko w części wspomniano powyżej, ma istotne zalety w porównaniu do rozwiązań, jakie obecnie stosuje się w magazynach o znacząco mniejszych pojemnościach – przemysłowych i domowych. Co do zasady stosowane są czynne i bierne zabezpieczenia przeciwpożarowe. O czynnych zabezpieczeniach, w tym systemach detekcji i gaszenia wykorzystujących różne środki gaśnicze po części wspomniano. Nie omawiano biernych zabezpieczeń, których istota sprowadza się do stosowania rozwiązań mających na celu wydzielenie go w określonej strefie, przestrzeni, ograniczenie możliwości niekontrolowanego rozprzestrzeniania się pożaru. Analogicznie nie omawiano systemów odciążania i wentylacji.

Ochrona tych ostatnich w praktyce sprowadza się do zapewnienia odpowiedniej konstrukcji i monitorowania ich pracy przez BMS-y. Natomiast kwestie zabezpieczeń przeciwpożarowych uwzględniają w szczególności kwestie lokalizacji magazynu,

- 1) battery properties,
- 2) application condition and guidelines and design and installation works requirements,
- 3) operation and maintenance,
- 4) application of suitable technical protections and fire protections.

Ad. 1) In this context, it should be evaluated that the currently applicable regulations at the level of EU countries [17] do not guarantee proper supervision over the course of the battery safety compliance evaluation process they provide for. This state of affairs generates the risk of marketing and use of products with unconfirmed properties and, even worse, products of unknown origin. They are products offered on the market, in relation to which there are no clear declarations and documents of origin, manufacturer and manufacturer's responsibility for the product. They are most often available at attractive prices, but no entity assumes responsibility for them. They also leave significant concerns regarding their declared parameters and legality of marketing.

Ad. 2) It is also worth noting that a vast majority of countries uses national regulations, industry guidelines and insurer-specified requirements in that area. However, in Poland the legal framework development process in the subject area has only begun (legislation works on the amendment to the construction law and regulation on the technical conditions which must be fulfilled by buildings and their location).

In addition, the above-mentioned works on the creation of fire protection guidelines for energy storage systems are pursued in collaboration with: KG PSP, SITP, PIME and PSME. The completion of the above-mentioned works, within several coming months, with active involvement of the insurance companies operating on the Polish market, seems to be necessary in view of the currently accelerating processes related to the energy transition of our country, including the just initiated design works on the construction of major large scale storage systems in the energy sector.

Ad. 3) As already mentioned above, the vast majority of lithium-ion storage system failures is caused by improper use and failure to ensure proper operating conditions. Thus, to reduce the risk of occurrence and development of fire as much as possible, care should be taken in particular to place the subject equipment in well-ventilated rooms (preferably: dedicated for that application), in which temperature is maintained in appropriate range, away from heat sources and inflammable substances. It is also necessary to provide for solutions to protect the batteries from the potential mechanical damage. In the considered context, both during the delivery and in the place of use, an essential role is played by equipment for: monitoring battery operation parameters (BMS), detecting fire incidents and emergencies, preventing fire propagation to further cells and modules, as well as further fire spreading [10].

Ad. 4) As mentioned in the previous section, it is important to use BMS with parameters and functionalities confirmed in tests and compliance evaluation. BMS functionalities combined with electric technical protections determine the efficiency and effectiveness of the electric protections in use, including the capability to effectively disconnect batteries in case of emergency.

w tym zapewnienie odpowiednich odległości lub oddzieleni przeciwpożarowych od innych obiektów, urządzeń, czy materiałów palnych oraz pomiędzy poszczególnymi modułami, zapewnienie wentylacji oraz urządzeń przeciwpożarowych wymaganych do zainstalowania w danym rodzaju obiektu budowlanego (np. hydranty wewnętrzne i zewnętrzne, gaśnice).

Z kolei w magazynach przemysłowych, najczęściej montowanych w odpowiednich obudowach, tzw. szafowych, oprócz zabezpieczeń omówionych w poprzednim akapicie spotyka się rozwiązania przewidujące stosowanie urządzeń detekcyjnych oraz autonomicznych stałych urządzeń gaśniczych, w szczególności gazowych. Nierzadko tego rodzaju magazyny wyposaża się również w półstałe urządzenia, pozwalające przybyłym ekipom ratowniczym na podłączenie węży pożarniczych oraz podanie wody gaśniczej do wnętrza magazynu.

ASMEE powinny być projektowane z uwzględnieniem określonych środków niezbędnych do zapewnienia podstawowych wymagań bezpieczeństwa. Mając to na uwadze, analizie i ocenie należy poddać szereg czynników, w szczególności dotyczących:

- 1) właściwości baterii,
- 2) warunków i wytycznych stosowania oraz wymagań dla projektowania i prac instalacyjnych,
- 3) eksploatacji i konserwacji,
- 4) stosowania odpowiednich zabezpieczeń technicznych i przeciwpożarowych.

Ad. 1) W tym kontekście należy ocenić, że stosowane obecnie regulacje na poziomie państw UE [17] nie gwarantują odpowiedniego nadzoru nad przebiegiem przewidzianego w nich procesu oceny zgodności baterii pod względem bezpieczeństwa. Ten stan rzeczy generuje ryzyko wprowadzania do obrotu i użytkowania wyrobów o niepotwierdzonych właściwościach, co gorsza również wyrobów niewiadomego pochodzenia. Są to oferowane na rynku wyroby, w stosunku do których brak jednoznacznych deklaracji i dokumentów dotyczących ich pochodzenia, producenta i jego odpowiedzialności za wyrób. Najczęściej są one atrakcyjne cenowo, ale nikt nie bierze za nie odpowiedzialności. Pozostają również istotne wątpliwości co do ich deklarowanych parametrów i legalności wprowadzania do obrotu.

Ad. 2) Podkreślenia wymaga fakt, iż zdecydowana większość państw stosuje w tym zakresie regulacje krajowe, wytyczne branżowe oraz wymagania określone przez ubezpieczycieli. Natomiast w Polsce dopiero rozpoczęto proces tworzenia ram prawnych w omawianym obszarze (prace legislacyjne nad nowelizacją prawa budowlanego oraz rozporządzenia w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie).

Kontynuowane są również wspomniane już wcześniej prace nad stworzeniem wytycznych dotyczących ochrony przeciwpożarowej magazynów energii we współpracy z: KG PSP, SITP, PIME oraz PSME. Dokończenie powyższych prac, w perspektywie kilku lub kilkunastu najbliższych miesięcy, przy aktywnym włączeniu się w ten proces działających na polskim rynku zakładów ubezpieczeń, jawi się jako konieczność, w obliczu przyspieszających obecnie procesów związanych z transformacją energetyczną naszego kraju, w tym rozpoczętych właśnie prac projektowych dotyczących budowy dużych magazynów wielkoskalowych w sektorze energetycznym.

Apart from the energy storage system product properties and technical protections in use, in the context of fire protection, it is essential to place energy storage systems at appropriate distance from other structures or to separate them using components with proper fire rating. At present, the most commonly used fire protections dedicated for energy storage systems include fire phenomena detection systems, room ventilation, fire separation and fixed and semi-fixed firefighting equipment, used to control or extinguish fires.

In the design of energy storage system fire protection, one should not forget the need to provide operating conditions for fire service teams. In this context, the particularly important aspects include the access (fire routes), water sources for external firefighting, including protection from fire propagation to adjacent storage systems and other structures.

Ad. 3) Jak nadmieniono już wcześniej, za zdecydowaną większość awarii magazynów litowo-jonowych odpowiedzialne jest ich niewłaściwe użytkowanie i brak dbałości o odpowiednie warunki pracy. W związku z powyższym, aby w możliwie największym stopniu ograniczyć ryzyko powstania i rozwoju pożaru magazynu energii, należy w szczególności zadbać o umieszczanie omawianych urządzeń w pomieszczeniach dobrze wentylowanych (najlepiej dedykowanych temu zastosowaniu), w których temperatura utrzymywana jest w odpowiednich zakresach, z dala od źródeł ciepła i łatwopalnych substancji. Konieczne jest również przewidzenie rozwiązań zabezpieczających baterie przed możliwymi uszkodzeniami mechanicznymi. Zarówno w trakcie ich dostawy, jak i w miejscu użytkowania niezmiennie istotną rolę w rozpatrywanym kontekście stanowią również urządzenia służące: monitorowaniu parametrów pracy akumulatora (BMS), detekcji zdarzeń pożarowych, stanów awaryjnych, zapobieganiu propagacji pożaru na kolejne ogniwa i moduły, a także dalszego rozprzestrzenienia się pożaru [10].

Ad. 4) Zgodnie z tym co powiedziano w poprzednim punkcie, ważne jest stosowanie BMS-ów o potwierdzonych w badaniach oraz procesie oceny zgodności parametrach i funkcjonalnościach. Funkcjonalności BMS-ów w powiązaniu z elektrycznymi zabezpieczeniami technicznymi decydują o sprawności i skuteczności zastosowanych zabezpieczeń elektrycznych, w tym zdolności do skutecznego rozłączania baterii w przypadku ich stanów awaryjnych. Poza właściwościami wyrobu – magazynu energii, stosowanymi zabezpieczeniami technicznymi, w kontekście zapewnienia bezpieczeństwa pożarowego kluczowa jest lokalizacja magazynów energii, w odpowiedniej odległości od innych obiektów lub od tych obiektów oddzielona elementami o odpowiedniej klasie odporności ogniowej. Wśród najpowszechniej aktualnie stosowanych zabezpieczeń przeciwpożarowych dedykowanych do ochrony magazynów energii wskazać należy systemy służące detekcji zjawisk pożarowych, wentylację pomieszczeń, stosowanie oddzieliń przeciwpożarowych oraz stałe i półstałe urządzenia gaśnicze, służące kontroli pożaru lub jego ugaszeniu.

Projektując zabezpieczenia przeciwpożarowe magazynów energii, nie można również zapominać o potrzebie zapewnienia warunków prowadzenia działań przez zastępy straży pożarnych. W tym kontekście szczególnie istotne są kwestie dostępu (drog pożarowych), zapewnienia źródeł wody do zewnętrznego gaszenia, w tym obrony przed przeniesieniem się pożaru na sąsiednie magazyny lub inne obiekty.

Review of requirements and standards in the context of safe operation of battery electric energy storage systems

In relation to the already mentioned deficits in national legal regulations and still incomplete works on industry guidelines, it is justified to refer to the technical principles defined in international standards. Selected standards developed by NFPA (National Fire Protection Association) and standards by UL (Underwriters Laboratories) created for the American market in relation to stationary BESS are presented below. These standards are applied in many

Przegląd wymagań i standardów w kontekście zapewnienia bezpieczeństwa eksploatacji akumulatorowych systemów magazynowania energii elektrycznej

Wobec występowania wspomnianych już deficytów w zakresie krajowych regulacji prawnych oraz niesfinalizowanych jeszcze prac nad wytycznymi branżowymi, zasadne jest sięganie po zasady wiedzy technicznej określone w standardach międzynarodowych. Poniżej przedstawiono wybrane standardy opracowane przez NFPA (ang. National Fire Protection Association) oraz normy UL (ang. Underwriters Laboratories) stworzone na potrzeby rynku

countries not only in relation to energy storage, but also broadly understood fire protection. Although introducing these requirements directly in Polish conditions is not always possible, after proper adaptation to the reality of our countries a lion's share of these requirements may be successfully considered as recognised resource of technical knowledge.

As introduction, it should be noted that safety requirements and standards are designed for stationary battery systems, including large scale BESS installations. These regulations are based on pre-existing electric safety standards and experience from BESS fires in the United States in recent years. In the United States, specific guidelines are already applicable in this regard, however Polish BESS regulations are currently in development.

Standard UL 9540 – Energy Storage Systems and Equipment, 2023 Edition

UL 9540 is a safety standard for entire energy storage systems – it includes not only the battery, but also the storage system, power conversion, control and protection circuits [18]. The standard defines i.a. the following requirements:

- electrical – including insulation strength, fire protection, component selection,
- mechanical and environmental – resistance to vibration, temperature and mechanical impact,
- fire/thermal – explosion control, thermal runaway reduction, protection from fire propagation in battery systems.

The standard also defines storage system capacity limits for some types of installation, e.g. for electrochemical systems: the maximum system capacity cannot exceed 20 kWh (72 MJ) in residential structures and 50 kWh (180 MJ) in non-residential structures, unless specific tests are completed as per UL 9540A.

NFPA 855 standard – Standard for the Installation of Stationary Energy Storage Systems, 2026 Edition

NFPA 855 is the recently updated standard for stationary energy storage system installations [19]. It defines the minimum safety requirements for separation distances, fire protection, operation and training and emergency response for BESS in residential, commercial and industrial environments [20]. It is a set of requirements that is connected with the requirements of other NFPA standards and standards, such as:

- NFPA 69 – *Standard on Explosion Protection by Deflagration Venting, 2024 Edition* on explosion protection,
- NFPA 68 – *Standard on Explosion Protection by Deflagration Venting, 2023 Edition* on explosion protection by deflagration venting,
- NFPA 72 – *National Fire Alarm and Signaling Code®, 2025 Edition* on alarm and monitoring systems,
- NFPA 13 – *Standard for the Installation of Sprinkler Systems* on sprinkler systems.

In the latest edition of this standard, published in October 2025, in response to international incidents related to fires of energy storage systems, requirements were introduced or revised for fire detection and suppression, explosion control, ventilation, gas detection and thermal failures. In addition, requirements were refined for fire and explosion tests (large scale fire tests).

amerykańskiego w odniesieniu do stacjonarnych ASMEE. Standardy te są stosowane w wielu państwach nie tylko w odniesieniu do magazynowania energii, ale również szeroko pojętej ochrony przeciwpożarowej. Co prawda, wdrożenie tych wymagań w warunkach polskich nie zawsze jest możliwe wprost, niemniej po dokonaniu odpowiedniej ich adaptacji do realiów występujących w naszym kraju, gros z tych wymagań może być z powodzeniem stosowane jako uznany zasób wiedzy technicznej.

Na wstępie należy zaznaczyć, iż wymagania i normy bezpieczeństwa opracowane zostały dla stacjonarnych systemów akumulatorowych, w tym instalacji ASMEE na dużą skalę. Regulacje te bazują na wcześniej istniejących normach bezpieczeństwa elektrycznego oraz doświadczeniach zdobytych w wyniku pożarów ASMEE w USA z ostatnich lat. W Stanach Zjednoczonych obowiązują już szczegółowe wytyczne w tym zakresie, natomiast polskie regulacje dotyczące ASMEE są obecnie wciąż w trakcie opracowywania.

Norma UL 9540 – Energy Storage Systems and Equipment, 2023 Edition

UL 9540 to norma bezpieczeństwa dotycząca całego systemu magazynowania energii – obejmuje nie tylko baterię, ale także układ magazynowania, konwersję mocy, sterowanie, obwody zabezpieczeń [18]. Norma określa m.in. wymagania:

- elektryczne – w tym wytrzymałość izolacji, zabezpieczenia przeciwporażeniowe, dobór elementów,
- mechaniczne i środowiskowe – odporność na wibracje, temperatury, oddziaływania mechaniczne,
- pożarowe/termiczne – kontrolę wybuchów, ograniczenie niestabilności termicznej (ang. *thermal runaway*), ochrony przed propagacją pożaru w systemach baterii.

Norma określa także limity pojemności magazynów dla niektórych typów instalacji – np. dla systemów elektrochemicznych: maksymalna pojemność dla instalacji w obiektach mieszkalnych nie może przekroczyć 20 kWh (72 MJ), a dla obiektów niemieszkalnych 50 kWh (180 MJ), chyba że spełniono określone testy zgodne z UL 9540A.

Norma NFPA 855 – Standard for the Installation of Stationary Energy Storage Systems, 2026 Edition

NFPA 855 to ostatnio zaktualizowana norma dotycząca instalacji stacjonarnych systemów magazynowania energii [19]. Określa ona minimalne wymagania bezpieczeństwa dotyczące odległości separacyjnych, ochrony przeciwpożarowej, eksploatacji i szkoleń oraz reagowania w sytuacjach awaryjnych dla ASMEE w środowiskach mieszkalnych, komercyjnych i przemysłowych [20]. Jest to zbiór wymagań, który powiązano z wymaganiami innych norm NFPA i standardów, takich jak:

- NFPA 69 – *Standard on Explosion Protection by Deflagration Venting, 2024 Edition* na temat zapobiegania wybuchom,
- NFPA 68 – *Standard on Explosion Protection by Deflagration Venting, 2023 Edition* na temat zapobiegania wybuchom poprzez odpowietrzanie deflagracyjne,
- NFPA 72 – *National Fire Alarm and Signaling Code®, 2025 Edition* dot. systemów alarmowych i monitorujących,
- NFPA 13 – *Standard for the Installation of Sprinkler Systems* dot. systemów zraszaczy.

The standard also includes the assumptions that uncontrolled heat spreading will progress within a single battery enclosure and the most effective method of managing this process is to allow it to burn out, while preventing the accumulation of explosive gases. Thus, the standard is in particular focused on explosion protection and drainage of combustible gases.

At the stage of obtaining permits and building the BESS, it is required to submit detailed planning documents for acceptance of fire safety conditions. This documentation includes the location and layout of the place of BESS, manufacturer's specifications and evaluations, details of fire protection, detection, control and firefighting, ventilation and relief. The installation and start-up requirements are to a large extent based on manufacturer's guidelines, however additional requirements and restrictions may be applicable.

The requirements of NFPA 855 constitute a solid basis for the implementation of BESS application and operation principles. This standard also includes useful information attachments. They are the source of information, which may be helpful in the context of application of standard requirements at the stage of BESS design and operation. The most important are:

1. Attachment B, which addresses hazards specific to battery energy storage systems. Safety control and hazard mitigation must also include the inherent hazards related to these systems, which may differ depending on battery technology. BESS operation may involve fire and explosion hazards, chemical and electrical hazards, accumulated or stored energy hazards and physical hazards. Different hazards will occur in normal operating conditions and in emergency and non-typical conditions;
2. Attachment C, which provides firefighting solutions adjusted to the BESS installation. This attachment also includes information that firefighters and rescue service members should know to enable an effective response to energy storage system incidents.
The fire service should have a developed action plan for fire, explosion and other emergencies related to the BESS installation, which should include the following components:
 - procedures described in the site operation plan and emergency response plan,
 - identification of the types of BESS technologies in use, potential hazards and method of responding to fires and incidents related to a specific BESS system,
 - identification of the location of all electric disconnectors in the building and understanding that it is not always possible to remove or isolate the electric energy accumulated in BESS equipment,
 - procedures of power shutdown and disconnection or device isolation to reduce the risk of fire, electric shock and injury,
 - application of procedures of handling damaged BESS equipment after fire, including:
 - considering that electric energy remains in batteries and other battery energy storage systems (BESS) damaged by the fire could cause re-ignition long after the fire is initially extinguished.

W najnowszym wydaniu tej normy, opublikowanym w październiku 2025 r., w reakcji na międzynarodowe incydenty związane z pożarami magazynów energii, wprowadzono lub zrewidowano wymagania dotyczące wykrywania i tłumienia pożaru, kontroli wybuchów, wentylacji, detekcji gazów oraz awarii termicznych. Ponadto doprecyzowano wymagania odnośnie badań ogniowych i wybuchowych (testy ogniowe w dużej skali). Norma zawiera także założenia, iż niekontrolowane rozprzestrzenianie się ciepła będzie postępować w obrębie pojedynczej obudowy baterii, a najskuteczniejszym sposobem zarządzania tym procesem jest pozwolenie na jego wypalenie, przy jednoczesnym zapobieganiu gromadzeniu się gazów wybuchowych. Z tego powodu norma kładzie szczególny nacisk na ochronę przed wybuchami oraz odprowadzanie gazów palnych.

W fazie uzyskiwania pozwoleń i budowy ASMEE wymaga się przedłożenia szczegółowych dokumentów planistycznych w celu akceptacji warunków bezpieczeństwa pożarowego. Dokumentacja ta obejmuje lokalizację i układ miejsca, w którym znajduje się ASMEE, specyfikacje i oceny producenta, szczegóły dotyczące zabezpieczeń przeciwpożarowych detekcji kontroli i gaszenia, wentylacji i odciążeń. Wymagania dotyczące instalacji i uruchomienia w dużej mierze opierają się na wytycznych producenta, chociaż mogą być stosowane dodatkowe wymagania i ograniczenia.

Wymagania zawarte w normie NFPA 855 stanowią solidne podstawy do wdrażania zasad stosowania i eksploatacji ASMEE. Norma ta zawiera także przydatne załączniki informacyjne. Są one źródłem szczegółowych informacji, które mogą być pomocne w kontekście stosowania wymagań normy w fazie projektowania i eksploatacji ASMEE. Najważniejsze z nich to:

1. Załącznik B, który omawia zagrożenia specyficzne dla systemów magazynowania energii w akumulatorach. Kontrola bezpieczeństwa i ograniczanie zagrożeń muszą uwzględniać nieodłączne zagrożenia związane z tymi systemami, które mogą się różnić w zależności od technologii baterii. Podczas eksploatacji ASMEE mogą pojawić się zagrożenia pożarowe i wybuchowe, chemiczne, elektryczne, zagrożenia związane z energią zgromadzoną lub zmagazynowaną oraz zagrożenia fizyczne. Inne zagrożenia wystąpią w normalnych warunkach eksploatacji, a inne w czasie awarii i w warunkach nietypowych;
2. Załącznik C, który proponuje rozwiązania dotyczące zwalczania pożarów dostosowane do instalacji ASMEE. Załącznik ten zawiera informacje, które strażacy i przedstawiciele służb ratowniczych powinni znać, aby móc skutecznie reagować na zdarzenia związane z systemami magazynowania energii.
Straż pożarna powinna mieć opracowany plan działania na wypadek pożaru, wybuchu i innych sytuacji awaryjnych związanych z instalacją ASMEE, który powinien zawierać następujące elementy:
 - procedury zawarte w opisie planu działania obiektu i planu reagowania kryzysowego,
 - określenie rodzajów stosowanych technologii ASMEE, potencjalnych zagrożeń oraz metod reagowania na pożary i zdarzenia związane z konkretnym systemem ASMEE,

- ordering contact with qualified personnel to safely remove the damaged BESS equipment from the site (contact details should be in the site operation plan and the emergency response plan) [21].
3. Attachment D – including a review of energy storage systems technologies;
 4. Attachment F – with a historical perspective on battery energy storage systems;
 5. Attachment G – lithium-ion battery (LIB) energy storage systems (BESS) firefighting and safety guidelines. It also includes information for the designers, users law enforcement administration bodies, i.e. entities involved in the process of planning, approval and operation of LIB-based BESS installations. The content of the attachment is focused on hazard identification and evaluation, firefighting, fire protection and fire and gas detection. It includes information on LIB properties and features, minimum safety, maintenance and operation requirement implementation guidelines and other information, which may be used to spread the knowledge and technical conditions and safety principles for LIB installations.

At present, this standard is a standard that constitutes a source of the latest technical knowledge on electric energy storage.

- określenie lokalizacji wszystkich rozłączników elektrycznych w budynku i zrozumienie, że energia elektryczna zgromadzona w urządzeniach ASMEE nie zawsze może zostać usunięta lub odizolowana,
- procedury wyłączania i odłączania zasilania lub izolowania urządzeń w celu zmniejszenia ryzyka pożaru, porażenia prądem elektrycznym i obrażeń ciała,
- stosowanie procedur postępowania z uszkodzonymi urządzeniami ASMEE po pożarze, w tym:
 - uwzględniających, że energia elektryczna pozostała w akumulatorach i innych systemach magazynowania energii (ASMEE) uszkodzonych w wyniku pożaru może spowodować ponowne zapalenie się długo po wstępnym ugaszeniu pożaru,
 - nakazujących kontakt z wykwalifikowanym personelem, który bezpiecznie usunie uszkodzony sprzęt ASMEE z obiektu (dane kontaktowe powinny znajdować się w planie działania obiektu i planie reagowania na sytuacje awaryjne) [21].

3. Załącznik D – zawierający przegląd technologii systemów magazynowania energii;
4. Załącznik F – z historyczną perspektywą dotyczącą akumulatorowych systemów magazynowania energii;
5. Załącznik G – wytyczne dotyczące gaszenia pożaru i bezpieczeństwa systemów magazynowania energii (ASMEE) z akumulatorami litowo-jonowymi (LIB). Zawiera też informacje dla projektantów, użytkowników i organów administracji egzekwujących prawo, tj. podmiotów, które uczestniczą w procesie planowania, zatwierdzania oraz eksploatacji instalacji ASMEE opartych na LIB. Treść załącznika koncentruje się na identyfikacji i ocenie zagrożeń, gaszeniu pożarów, ochronie przeciwpożarowej oraz wykrywaniu pożarów i gazów. Zawiera informacje na temat właściwości i cech LIB, wytyczne dotyczące wdrażania minimalnych wymagań bezpieczeństwa, konserwacji i eksploatacji systemów ochrony przeciwpożarowej oraz inne informacje, które mogą być wykorzystane do upowszechniania wiedzy i warunków technicznych i zasad bezpieczeństwa dla instalacji LIB.

Niniejsza norma aktualnie jawi się jako standard, który stanowi zasób najnowszej wiedzy technicznej dotyczącej magazynowania energii elektrycznej.

NFPA 68 and 69 standards

The NFPA 68 standard addresses the design, location, installation, operation and maintenance of equipment and systems used to discharge the gases and pressures generated by deflagration within rooms or enclosures. In turn, the NFPA 69 standard addresses explosion prevention systems in rooms or facilities, in which a combustible mixture of gases, vapours, mists, dusts or hybrid mixtures (e.g. dust and gas) may occur.

Considering the hazards caused by BESS, explosion prevention is an essential component of the safety design of those systems. The NFPA 855 standard defines the explosion prevention requirements by installation of protection systems. In that

Normy NFPA 68 i 69

Norma NFPA odnosi się do projektowania, lokalizacji, instalacji, eksploatacji oraz utrzymania urządzeń i systemów służących do odprowadzenia gazów i ciśnień powstałych w wyniku deflagracji wewnątrz pomieszczeń lub obudów. Z kolei norma NFPA 69 dotyczy systemów zapobiegania wybuchom w pomieszczeniach lub urządzeniach, w których może wystąpić palna mieszanina gazów, par, mgieł, pyłów albo hybrydowych mieszanek (np. pyłu i gazu).

Uwzględniając zagrożenia stwarzane przez ASMEE, zapobieganie wybuchom stanowi jeden z kluczowych elementów projektowania bezpieczeństwa tych systemów. Norma NFPA 855 określa wymagania zapobiegania wybuchom poprzez instalację systemów

respect, it refers to NFPA 68 – *Standard for Explosion Prevention by Deflagration Venting* [22] or NFPA 69 – *Standard for Explosion Prevention Systems*. The NFPA 69 standard [223] is more general and applicable to any type of explosion prevention, while the NFPA 68 standard is focused on a single explosion control method, i.e. deflagration venting design. It means specifically venting explosive gases and/or using special panels designed to subside in case of explosion. The deflagration panels are designed to subside (provide structure relief) in case of explosion, as shown in Figure 3.

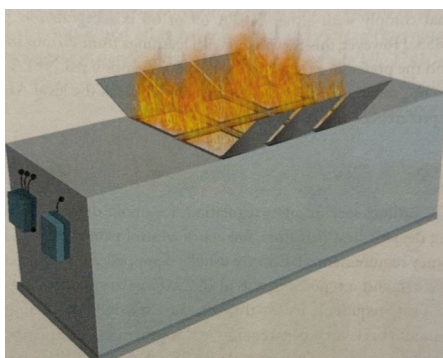


Figure 3. Illustration of the deflagration panel function in a BESS container
Rycina 3. Ilustracja funkcji panelu deflagracji w kontenerze ASMEE

Source: Own elaboration based on [1].

Źródło: Opracowanie własne na podstawie [1].

However, not all battery enclosures are equipped with deflagration panels. The designer may opt to use different protection methods, as agreed on with the fire protection expert.

The NFPA 68 and NFPA 69 standards jointly include the requirements for gas detection, ventilation and mitigation protection systems, designed to minimise the risk related to BESS functioning. NFPA 69 requires the concentration of combustible substances in the enclosure not to exceed 25% of the lower explosion limit, which is the lowest concentrations, at which the given gas may ignite under specific temperature and pressure conditions. This standard requires using more active protection measures, including (not limited to) gas sensors, smoke sensors and exhaust ventilation, which must be designed and installed in enclosures. NFPA 68 recommends designing “passive” deflagration openings or adding them to the enclosure. They should open upon the increase of pressure caused by the accumulation of gases to enable discharging them before reaching the combustion limits [1].

NFPA 72

The NFPA 72 standard defines detailed safety requirements for smoke and heat sensors, alarm signallers, fire control and signalling panels, as well as redundancy requirements in the design of fire detection systems [24]. BESS are usually equipped with smoke and gas detection and fire signalling systems. This standard also includes the requirements for effective operation

ochronnych. Powołuje się w tym zakresie na normę NFPA 68 – *Standard for Explosion Prevention by Deflagration Venting* [22] lub NFPA 69 – *Standard for Explosion Prevention Systems*. Norma NFPA 69 [223] jest bardziej ogólna i dotyczy zapobiegania wybuchom dowolnego rodzaju, podczas gdy NFPA 68 koncentruje się na jednej metodzie ograniczania wybuchów – projektowaniu odpowietrzania deflagracji. Oznacza to konkretnie odpowietrzanie gazów wybuchowych i/lub zastosowanie specjalistycznych paneli przeznaczonych do ustąpienia w przypadku wybuchu. Panele deflagacyjne są projektowane tak, aby ustąpiły (stanowiły odciążenie konstrukcji) w przypadku wybuchu, co przedstawia rycina 3.

Jednak nie wszystkie obudowy akumulatorów wyposażone są w panele deflagacyjne – projektanci mogą zdecydować się na zastosowanie innych metod ochrony, w uzgodnieniu z rzeczoznawcą do spraw zabezpieczeń przeciwpożarowych.

NFPA 68 i NFPA 69 łącznie obejmują wymagania dotyczące systemów wykrywania gazu, wentylacji oraz ograniczania wybuchów, mające na celu minimalizację ryzyka związanego z funkcjonowaniem ASMEE. NFPA 69 wymaga, aby stężenie substancji palnych w obudowie nie przekraczało 25% dolnej granicy wybuchowości, która jest najniższym stężeniem, przy którym dany gaz może ulec zapłonowi w określonych warunkach temperatury i ciśnienia. Norma ta nakłada konieczność stosowania bardziej aktywnych środków ochrony, w tym (ale nie wyłącznie) czujników gazu, czujników dymu oraz wentylacji wyciągowej, które muszą być zaprojektowane i zainstalowane w obudowach. NFPA 68 zaleca projektowanie „pasywnych” otworów deflagacyjnych lub ich dodanie w obudowie. Powinny one otwierać się pod wpływem wzrostu ciśnienia spowodowanego nagromadzeniem gazów, umożliwiając ich odprowadzenie przed osiągnięciem granic palności [1].

NFPA 72

Norma NFPA 72 określa szczegółowe wymagania bezpieczeństwa dotyczące czujników dymu i ciepła, sygnalizatorów alarmowych, central i paneli sygnalizacji pożaru, a także wymagań dotyczących redundancji w projektowaniu systemów detekcji pożaru [24]. ASMEE są zwykle wyposażane w systemy detekcji dymu i gazów i sygnalizacji pożaru. Norma ta zawiera również wymagania

of the fire signalling system and its emergency power supply. In relation to large scale BESS located in a wide area, the standard sets additional requirements to use a rescue operations management centre with all individual control/alarm panels in containers connected to it. This centre is an information point for rescuers, who arrive first to the place of incident. The BESS operator must provide continuous remote monitoring of the system to enable immediate reporting to the local fire service. External monitoring companies may fulfil that function as well, using automatic dialling to the fire service command centre [1].

NFPA 550

The NFPA 550 standard is *Guide to the Fire Safety Concepts Tree*, [25]. Its purpose is to provide a structured tool to enable the analysis and better understanding of the fire safety strategy. The Fire Safety Concepts Tree is a logical graphical structure that presents all possible strategies and measures that could be used to prevent fires or minimise their impact.

The NFPA 550 standard does not directly define requirements for the design or installation of fire protection systems, but provides guidance and methodology to support fire safety activities, in particular in:

- understanding the relationships between different fire protection measures – it explains how different components (e.g. detection, firefighting, smoke control, evacuation, ignition prevention) contribute to the achievement of fire safety;
- analysing codes and standards – it helps the users in accurate and effective analysis of the related codes and standards, while showing the placement of specific requirements in the system.
- identifying gaps and redundancy in strategies – it enables identifying the possible deficiencies (gaps) or unnecessary repetitions (redundancy) in the fire protection plan for the purposes of strategic optimisation;
- supporting performance-based projects – as a very extensive tool for engineers and designers, who create fire safety solutions based on achieving specific performance targets, not just meeting “rigid” regulations;
- promoting better decision-making – by identification of gaps and redundancy areas in fire protection strategies, the standard supports more informed and effective decisions.
- communicating fire safety concepts – the guide provides tools that help specialists to clearly communicate fire safety concepts to other stakeholders (architects, building owners, public officers).

The NFPA 550 standard is intended for a broad group of fire safety specialists, including: designers and architects, engineers, in particular fire safety engineers, safety consultants, public officers responsible for enforcing construction regulations and supervising structure safety. It does not define detailed technical requirements, but provides guidelines and methodology, coherent conceptual frameworks to facilitate logical and comprehensive design and evaluation of fire safety strategies.

dotyczące skutecznego działania systemu sygnalizacji pożaru oraz jego zasilania awaryjnego. W odniesieniu do wielkoskalowych ASMEE rozlokowanych na dużym terenie norma nakłada dodatkowe obowiązki stosowania centrum zarządzania działaniami ratowniczymi, do którego podłączone są wszystkie poszczególne centrale/ panele alarmowe w kontenerach. Centrum to pełni rolę punktu informacyjnego dla ratowników, którzy jako pierwsi przybyli na miejsce zdarzenia. Operator ASMEE musi zapewnić ciągły zdalny monitoring systemu, aby móc w razie potrzeby natychmiastowo powiadomić lokalną straż pożarną. Zewnętrzne firmy monitorujące mogą również pełnić tę funkcję, wykorzystując automatyczne wybieranie numeru do centrum dowodzenia strażą pożarną [1].

NFPA 550

Norma NFPA 550 to *Przewodnik po strukturze koncepcji bezpieczeństwa pożarowego* [25]. Jego celem jest dostarczenie ustrukturyzowanego narzędzia umożliwiającego analizę oraz lepsze zrozumienie strategii bezpieczeństwa pożarowego. Struktura koncepcji bezpieczeństwa pożarowego to logiczna struktura graficzna przedstawiająca wszystkie możliwe strategie i środki, które mogą być zastosowane w celu zapobiegania pożarom lub minimalizowania ich skutków.

Norma NFPA 550 nie określa bezpośrednio wymagań w zakresie projektowania ani instalacji systemów ochrony przeciwpożarowej, stanowi raczej przewodnik oraz metodologię, która wspiera działania w zakresie bezpieczeństwa pożarowego, w szczególności w:

- zrozumieniu relacji między różnymi środkami ochrony przeciwpożarowej – wyjaśnia, jak różne elementy (np. detekcja, gaszenie, kontrola dymu, ewakuacja, zapobieganie zapłonowi) współpracują ze sobą, aby osiągnąć cel, jakim jest bezpieczeństwo pożarowe;
- analizie kodów i standardów – pomaga użytkownikom w dokładnej i efektywnej analizie powiązanych kodów i standardów, pokazując, gdzie w systemie mieszczą się konkretne wymagania.
- identyfikacji luk i nadmiarowości w strategiach – umożliwia zidentyfikowanie, gdzie w planie ochrony przeciwpożarowej mogą występować braki (luki) lub niepotrzebne powtórzenia (nadmiarowości), co pozwala na optymalizację strategii;
- wspieraniu projektów opartych na wydajności – jako bardzo rozbudowane narzędzie dla inżynierów i projektantów, którzy tworzą rozwiązania bezpieczeństwa pożarowego oparte na osiąganiu konkretnych celów wydajnościowych, a nie tylko na spełnianiu „sztywnych” przepisów;
- promowaniu lepszego podejmowania decyzji – poprzez identyfikację luk i nadmiarowych obszarów w strategiach ochrony przeciwpożarowej, norma wspiera bardziej świadome i efektywne decyzje.
- komunikowaniu koncepcji bezpieczeństwa pożarowego – przewodnik dostarcza narzędzi, które pomagają specjalistom w jasnym przekazywaniu koncepcji bezpieczeństwa pożarowego innym zainteresowanym stronom (architektom, właścicielom budynków, urzędnikom).

NFPA 551

The NFPA 551 standard is a methodological guide. Its primary purpose is to support the evaluation process and interpretation of fire risk evaluation [26].

The purpose of NFPA 551 is to provide guidelines above all to bodies with jurisdiction over fire protection and to other stakeholders, such as: insurance company representatives, building owners, fire safety engineers, with regards to:

- the assessment of adequacy and correctness of the fire risk assessment for the given fire safety problem;
- the support of risk-based decision-making to improve the fire safety.

This standard does not impose any specific methods of risk assessment or risk acceptance criteria. Instead, it is focused on the technical review process and the required documentation necessary for reliable evaluation of hazards. It includes a detailed explanation of different aspects of the fire risk assessment process, including:

1. The bases for fire risk assessment;
 - the definitions of key terms, such as risk, hazard, probability and consequences;
 - the importance of risk analysis for informed decision-making on fire safety.
2. Methods of fire risk assessment:
 - **qualitative** – for risk assessment based on expert opinions and general principles (e.g. checklists);
 - **semi-quantitative, criteria-based** – using a combination of qualitative assessment and partial quantifications (e.g. point scales);
 - **semi-quantitative, consequence-based** – focused on fire consequences;
 - **quantitative** – using advanced mathematical and statistical models to calculate probabilities and consequences (e.g. incident tree analysis, fire simulations);
 - **cost and benefit analyses** – including the economic aspect in risk assessment.
3. Risk assessment procedure components and characteristics:
 - **selection of fire scenarios** – guidelines for identification and selection of realistic and challenging fire scenarios for analysis;
 - **identification of hazards** – help in the identification of potential fire hazards;
 - **probability analysis** – guidelines for fire occurrence probability assessment;

Norma NFPA 550 jest skierowana do szerokiego grona specjalistów związanych z bezpieczeństwem pożarowym, w tym: projektantów i architektów, inżynierów, w szczególności inżynierów bezpieczeństwa pożarowego, konsultantów ds. bezpieczeństwa, urzędników odpowiedzialnych za egzekwowanie przepisów budowlanych i nadzór nad bezpieczeństwem obiektów. Nie definiuje ona szczegółowych wymagań technicznych, lecz stanowi wytyczne i metodologię, dostarcza spójnych ram pojęciowych, ułatwiających logiczne oraz kompleksowe projektowanie i ocenę strategii bezpieczeństwa pożarowego.

NFPA 551

Norma NFPA 551 pełni funkcję przewodnika metodologicznego. Jej głównym celem jest wspieranie procesu oceny i interpretacji ocen ryzyka pożarowego [26].

NFPA 551 ma na celu dostarczenie wytycznych przede wszystkim organom posiadającym jurysdykcję w zakresie ochrony przeciwpożarowej, a także innym zainteresowanym stronom, takim jak: przedstawiciele firm ubezpieczeniowych, właściciele budynków, inżynierowie bezpieczeństwa pożarowego, w zakresie:

- oceny adekwatności i prawidłowości wykonania oceny ryzyka pożarowego dla danego problemu bezpieczeństwa pożarowego;
- wspierania podejmowania decyzji opartych na ryzyku w celu poprawy bezpieczeństwa pożarowego.

Norma ta nie narzuca konkretnych metod przeprowadzania ocen ryzyka ani nie ustala kryteriów akceptacji ryzyka. Zamiast tego, koncentruje się na procesie przeglądu technicznego i wymaganej dokumentacji niezbędnej do rzetelnej oceny zagrożeń. Szczegółowo omawia różne aspekty oceny ryzyka pożarowego, w tym:

1. Podstawy oceny ryzyka pożarowego:
 - definicje kluczowych pojęć, takich jak ryzyko, zagrożenie, prawdopodobieństwo, konsekwencje;
 - znaczenie analizy ryzyka dla podejmowania świadomych decyzji dotyczących bezpieczeństwa pożarowego.
2. Metody oceny ryzyka pożarowego:
 - **jakościowe** – oceniające ryzyko na podstawie opinii ekspertów i ogólnych zasad (np. listy kontrolne);
 - **półilościowe** oparte na kryteriach – wykorzystujące kombinację oceny jakościowej i częściowej kwantyfikacji (np. skale punktowe);
 - **półilościowe oparte na konsekwencjach** – skupiające się na skutkach pożaru;
 - **ilościowe** – stosujące zaawansowane modele matematyczne i statystyczne do obliczania prawdopodobieństwa i konsekwencji (np. analiza drzewa zdarzeń, symulacje pożarów);
 - **analizy kosztów i korzyści** – uwzględniające aspekt ekonomiczny w ocenie ryzyka.
3. Elementy składowe i charakterystyka procedur oceny ryzyka:
 - **wyбір scenariuszy pożarowych** – wytyczne dotyczące identyfikacji i wyboru realistycznych i stanowiących wyzwanie scenariuszy pożarowych do analizy;

- **consequences analysis** – assessment of potential consequences of fire (e.g. for human life, property and the environment).
- 4. Information and documentation requirements:
 - the scope of information is necessary to conduct a reliable risk assessment;
 - the need for comprehensive risk assessment project documentation;
 - importance of the operation and maintenance manual as component supporting the risk assessment.
- 5. Addressing uncertainty:
 - considering and handling uncertainty in the fire risk assessment process, which is an inherent component of such analyses.
- 6. Qualifications of risk assessment personnel:
 - the importance of adequate qualifications and experience of the personnel responsible for conducting and analysing fire risk assessments.

To conclude, NFPA 551 is not a set of strict regulations, but a guide that standardises the approach to the evaluation and verification of fire risk assessments. This is a useful tool for anyone, who evaluates or approves fire safety solutions based on risk analysis. It offers support in conducting risk assessments in a reliable, comprehensive and comprehensible manner, which by consequence contributes to the improvement of the overall level of fire safety.

In the summary of the requirements and standards review, due to the scope of the subject, it is only possible to refer to selected examples of requirements and standards, which are used in that area in other countries. They include e.g. the United Kingdom, PAS 63100:2024 *Electrical installations – Protection against fire of battery energy storage systems for use in dwellings – Specification*, or Sweden, *Detta dokument är en bilaga till RISE Report 2023:117, Guidelines for the fire protection of battery energy storage systems*.

Summary and conclusions

In the view of the above considerations, it is justified to formulate the following final conclusions that the authors regard as contribution to indicating proper activities aimed at improving fire safety in the design, construction and operation of electric energy storage systems in Poland:

1. **Testing and certification of energy storage systems**
Building trust⁵ in the declared BESS and LIB battery parameters, as well as their repeatability, by application of the

⁵ The trust in LIB battery energy storage systems, like in other products, can be built based on test evidence. Their declared parameters and repeatability of batteries in mass usage may be confirmed by testing and certification.

- **identyfikacja zagrożeń** – pomoc w rozpoznawaniu potencjalnych zagrożeń pożarowych;
- **analiza prawdopodobieństwa** – wskazówki dotyczące oceny prawdopodobieństwa wystąpienia pożaru;
- **analiza konsekwencji** – ocena potencjalnych skutków pożaru (np. dla życia ludzi, mienia, środowiska).

4. Wymagania dotyczące informacji i dokumentacji:
 - jakie informacje są niezbędne do przeprowadzenia rzetelnej oceny ryzyka;
 - konieczność sporządzania kompleksowej dokumentacji projektu oceny ryzyka;
 - znaczenie instrukcji eksploatacji i konserwacji jako elementu wspierającego ocenę ryzyka.
5. Adresowanie niepewności:
 - jak uwzględniać i radzić sobie z niepewnością w procesie oceny ryzyka pożarowego, która jest nieodłącznym elementem takich analiz.
6. Kwalifikacje osób przeprowadzających oceny ryzyka:
 - znaczenie odpowiednich kwalifikacji i doświadczenia personelu odpowiedzialnego za przeprowadzanie i analizowanie ocen ryzyka pożarowego.

Reasumując, NFPA 551 nie jest zbiorem ścisłych przepisów, lecz przewodnikiem, który standaryzuje podejście do oceny i weryfikacji ocen ryzyka pożarowego. Jest to użyteczne narzędzie dla każdego, kto zajmuje się oceną lub zatwierdzaniem rozwiązań z zakresu bezpieczeństwa pożarowego opartych na analizie ryzyka. Stanowi wsparcie w przeprowadzaniu ocen ryzyka w sposób rzetelny, kompleksowy i zrozumiały, co w konsekwencji przyczynia się do poprawy ogólnego poziomu bezpieczeństwa pożarowego.

W podsumowaniu przeglądu wymagań i standardów, z uwagi na obszerność tematyki, możliwe jest przywołanie jedynie wybranych przykładów wymagań i standardów, które są w tym zakresie stosowane w innych państwach. Należą do nich m.in. brytyjski – PAS 63100:2024 *Electrical installations – Protection against fire of battery energy storage systems for use in dwellings – Specification*, czy szwedzki – *Detta dokument är en bilaga till RISE Report 2023:117, Guidelines for the fire protection of battery energy storage systems*.

Podsumowanie i wnioski

W świetle powyższych rozważań zasadne jest sformułowanie następujących wniosków końcowych, które w ocenie autorów stanowią przyczynek do wskazania właściwych działań służących poprawie bezpieczeństwa pożarowego w zakresie projektowania, budowy i eksploatacji magazynów energii elektrycznej w Polsce:

1. **Badania i certyfikacja magazynów energii**
Zbudowanie zaufania⁵ do deklarowanych parametrów

⁵ Zaufanie do magazynów energii z bateriami LIB – podobnie jak w przypadku innych wyrobów – można zbudować, opierając się na dowodach z badań. Ich deklarowane parametry, a także powtarzalność masowo stosowanych baterii mogą potwierdzić testy i certyfikacja.

requirements of the relevant European regulations [14] or by introduction of additional national safety requirements, similar to other EU countries.

2. National regulations for safe application of BESS

The development and implementation of national regulations on the technical conditions⁶ of application and operation of large scale, industrial and household energy storage systems.

3. Research on hazards and effective mitigation measures

The intensification of scientific, qualification and experimental and empirical research on the safety of⁷ energy storage systems and effectiveness of the technical protections in use, both electric and dedicated to fire protection.

4. Detailed requirements and guidelines for safe application and operation

The development and implementation of national industry and insurance guidelines⁸ for the design, manufacture and operation of large scale, industrial and household energy storage systems, which will refine the legal requirements based on research and technical knowledge.

5. Guide to BESS incidents for rescue services

The preparation and implementation for application of the guide for electric energy storage systems operating personnel and rescue services. Such document should include guidelines for first aid personnel in incidents involving battery energy storage systems (BESS). It should also include recommendations for planning and response to fire incidents [29].

ASMEE i baterii LIB, a także ich powtarzalności poprzez stosowanie wymagań obowiązujących w tym zakresie regulacji europejskich [14] lub wdrożenie podobnie jak inne państwa UE, dodatkowych wymagań krajowych w zakresie ich bezpieczeństwa.

2. Przepisy krajowe dotyczące bezpieczeństwa stosowania ASMEE

Opracowanie i wdrożenie krajowych regulacji w zakresie warunków technicznych⁶ stosowania i eksploatacji magazynów energii wielkoskalowych, przemysłowych i domowych.

3. Badania dotyczące zagrożeń i skutecznych środków ich ograniczania

Intensyfikacja badań naukowych, kwalifikacyjnych i doświadczalnych oraz empirycznych w zakresie bezpieczeństwa⁷ magazynów energii i skuteczności stosowanych zabezpieczeń technicznych, zarówno elektrycznych, jak i dedykowanych ochronie przeciwpożarowej.

4. Szczegółowe wymagania i wytyczne w zakresie bezpieczeństwa stosowania i eksploatacji

Opracowanie i wdrożenie krajowych wytycznych branżowych i ubezpieczeniowych⁸ w zakresie projektowania, wykonywania i eksploatacji magazynów energii wielkoskalowych, przemysłowych i domowych, które na podstawie badań i wiedzy technicznej uszczegółowią wymagania przepisów prawa.

5. Poradnik dla służb ratowniczych dotyczący zdarzeń związanych z ASMEE

Opracowanie i wdrożenie do stosowania poradnika dla osób obsługujących systemy magazynowania energii elektrycznej i służb ratowniczych. Dokument taki powinien zawierać wytyczne dla osób udzielających pierwszej pomocy w przypadku incydentów z udziałem systemów magazynowania energii (ASMEE). Powinien również zawierać zalecenia dotyczące planowania i reagowania na zdarzenia pożarowe [29].

⁶ The need for technical conditions is related i.a. to the location itself, battery capacity, BMS properties, application of other technical protections and fire protections.

⁷ Developing regulations, requirements and guidelines requires knowledge based on research and evidence. Too radical reliance on expert opinions may result both in excessive underestimation of fire risks and the other extreme, i.e. overestimation.

⁸ This is an ongoing process that is disrupted and restricted by the above-mentioned lack of research and evidence of effectiveness of the adopted solutions.

⁶ Potrzeba warunków technicznych odnosi się między innymi do samej, lokalizacji, pojemności baterii, właściwości BMS, stosowanych innych zabezpieczeń technicznych i przeciwpożarowych.

⁷ Do opracowania regulacji, wymagań i wytycznych niezbędna jest wiedza oparta o badania i dowody. Zbyt radykalne w tym zakresie oparcie się tylko na osądach eksperckich może skutkować zarówno nadmiernym niedoszacowaniem ryzyk pożarowych jak i drugiej skrajności czyli ich przeszacowania.

⁸ Jest to proces, który trwa, ale który jest zakłócany i ograniczany wspomnianym powyżej brakiem badań i dowodów skuteczności przyjmowanych rozwiązań.

Abbreviations and definitions

BESS	battery energy storage system
ATP	adenosine triphosphate
BMS	battery management system – electronic system for managing a battery or battery pack. Its tasks include: cell voltage and temperature control, overload and discharge protection, cell balancing, battery health monitoring (SoC, SoH).
DoD	depth of discharge of battery
Mobile BESS	mobile battery energy storage system
HV	high voltage
IDLH	immediately dangerous to life or health
IFC	International Fire Code
KG PSP	Komenda Główna Państwowej Straży Pożarnej (Headquarters of the State Fire Service)
LIB	lithium-ion battery
NFPA	National Fire Protection Association (in the United States)
OSHA	Occupational Safety and Health Administration (in the United States)
HVAC	heating, ventilation, and air conditioning
PIME	Polska Izba Magazynowania Energii (Polish Chamber of Energy Storage)
OEM	original equipment manufacturer
PPE	personal protective equipment
ERP	energy response plan (referred to as “emergency operations plan” in NFPA 855)
PSME	Polskie Stowarzyszenie Magazynowania Energii (Polish Energy Storage Association)
RTE	sound trip efficiency
SCADA	supervisory control and data acquisition
SIPS	system integration and protection system
SITP	Stowarzyszenie Inżynierów i Techników Pożarnictwa (The Association of Fire Engineers and Technicians)
BCS	battery control system
BOS	battery operating system
SOC	state of charge of battery
SOH	state of health
BMS	battery management system
ECS	energy control system ECS
MPT	mains power transformer
UPS	uninterruptible power supply

Skróty i definicje

ASMEE	akumulatorowy system magazynowania energii elektrycznej.
ATP	adenozynotrifosforan
BMS	układ elektroniczny zarządzający baterią lub pakietem akumulatorów. Jego zadania to m.in. kontrola napięcia i temperatury ogniw, ochrona przed przeładowaniem lub rozładowaniem, balansowanie ogniw, monitorowanie stanu baterii (SoC, SoH).
GR	głębokość rozładowania akumulatora (ang. <i>depth of discharge</i>)
H-ASMEE	mobilny akumulatorowy system magazynowania energii elektrycznej
WN	wysokie napięcie
IDLH	bezpośrednie zagrożenie dla życia lub zdrowia
IFC	Międzynarodowy Kodeks Przeciwpowarowej
KG PSP	Komenda Główna Państwowej Straży Pożarnej
LIB	bateria litowo-jonowa
NFPA	Krajowe Stowarzyszenie Ochrony Przeciwpowarowej (w Stanach Zjednoczonych)
OSHA	Amerykańska Agencja Bezpieczeństwa i Higieny Pracy
OWK	ogrzewanie, wentylacja, klimatyzacja (ang. <i>heating, ventilation, and air conditioning</i> , HVAC)
PIME	Polska Izba Magazynowania Energii
POW	producent oryginalnego wyposażenia (ang. <i>original equipment manufacturer</i> , OEM)
PPE	środki ochrony indywidualnej
PRA	plan reagowania awaryjnego (określony w normie NFPA 855 jako „plan działań kryzysowych”)
PSME	Polskie Stowarzyszenie Magazynowania Energii
RTE	sprawność w obiegu zamkniętym
SCADA	nadzór, kontrola i gromadzenie danych
SIPS	system integracji i ochrony systemu
SITP	Stowarzyszenie Inżynierów i Techników Pożarnictwa
SNA	system nadzoru akumulatora (ang. <i>battery control system</i> , BCS)
SOB	system operacyjny baterii (ang. <i>battery operating system</i> , BOS)
SOC	stan naładowania akumulatora
SZ	stopień zużycia (ang. <i>state of health</i> , SOH)
SZA	system zarządzania akumulatorem (ang. <i>battery management system</i> , BMS)
SZE	system zarządzania energią (ang. <i>energy control system</i> , ECS)
TM	transformator mocy (ang. <i>main power transformer</i>)
UPS	system zasilania awaryjnego

AI Use Statement

The authors declare that artificial intelligence tools were used in the preparation of this article only within the scope indicated below:

- language and stylistic verification of the manuscript (ChatGPT – OpenAI),
- searching for and identifying potential bibliographic sources (SciSpace i ChatGPT),
- support in developing the structure of the manuscript (ChatGPT – OpenAI).

The authors take full responsibility for the content of the publication, including the scientific accuracy, interpretation of results, and final editing of the manuscript. Artificial intelligence tools were used solely as supporting instruments.

The journal's editorial policy prohibits the uncritical copying of AI-generated content and its inclusion in a publication without proper critical analysis, verification, and revision by the authors.

Oświadczenie dotyczące wykorzystania AI

Autorzy oświadczają, że w procesie przygotowania niniejszego artykułu wykorzystano narzędzia oparte na sztucznej inteligencji wyłącznie w zakresie wskazanym poniżej:

- weryfikacja językowa i stylistyczna tekstu (ChatGPT – OpenAI),
- wyszukiwanie i identyfikacja potencjalnych źródeł bibliograficznych (SciSpace i ChatGPT),
- wsparcie w opracowaniu struktury pracy (ChatGPT – OpenAI).

Autorzy ponoszą pełną odpowiedzialność za treść publikacji, w tym za poprawność merytoryczną, interpretację wyników oraz ostateczną redakcję tekstu. Narzędzia sztucznej inteligencji były wykorzystywane wyłącznie jako narzędzia pomocnicze.

Polityka redakcyjna czasopisma zabrania bezrefleksyjnego kopiowania treści wygenerowanych przez narzędzia AI oraz pozostawiania ich w publikacji bez krytycznej analizy, weryfikacji i redakcji przez autorów.

Literature / Literatura

- [1] Lebowitz D., Daly S., Sundaram S., *A Cell to Grid Guide to Utility-scale Battery Energy Storage Systems*, The BESS Book, 2024.
- [2] Kłapsa W., *Badania magazynów energii w zakresie bezpieczeństwa pożarowego, wstępny raport z badań Instytutu*, w: *Raport z IV Międzynarodowej Konferencji Naukowej pt. Bezpieczeństwo Nowych Technologii*, Zboina J., Pietrzak M., CNBOP-PIB, Józefów 2025.
- [3] The Federal Emergency Management Agency (FEMA), *Emerging Hazards of Battery Energy Storage System Fires*, <https://www.fema.gov/case-study/emerging-hazards-battery-energy-storage-system-fires> [dostęp: październik 2025].
- [4] Green-news.pl, *Pali się magazyn energii Tesli w Australii. Mieszkańcy zostaną bez prądu?*, <https://www.green-news.pl/1994-strazacy-walczą-z-ogniem-który-zajął-część-magazynu-energii-tesli-w-australii-czy-mieszkańcy-zostaną-bez-prądu> [dostęp: październik 2025].
- [5] CTIF – *Fire and Explosion in Beijing Energy Storage Power Station (2021)* – raport CTIF – International Fire and Rescue Services.
- [6] Komenda Powiatowa Państwowej Straży Pożarnej w Chrzanowie, *Pożar kontenera z akumulatorami w Trzebini*, <https://www.gov.pl/web/kppsp-chrzanow/pozar-kontenera-z-akumulatorami> [dostęp: październik 2025].
- [7] Portal Wirtualna Polska, *Wybuch kontenera z bateriami. Akcja w Małopolsce*, <https://wiadomosci.wp.pl/wybuch-kontenera-z-bateriami-akcja-w-malopolsce-7089523445000960> [dostęp: październik 2025].
- [8] Portal WRC, *Groźny pożar magazynu energii. Akcja strażaków trwała kilka godzin*, <https://www.portalwrc.pl/wielkopolska/wielkopolska/20784-groźny-pożar-magazynu-energii-akcja-strazakov-trwała-kilka-godzin> [dostęp: październik 2025].
- [9] Serwis wakcji.pl, *Tragiczny pożar kamienicy w Poznaniu: dwóch strażaków straciło życie*, <https://wakcji.pl/tragiczny-pożar-kamienicy-w-poznaniu-dwóch-strazakov-straciło-życie> [dostęp: październik 2025].
- [10] Janik P., Tępiński J., *Bezpieczeństwo pożarowe magazynów litowo-jonowych – wyzwania i dylematy*, SFT Vol. 61 Issue 1, 2025, 98–107, <https://doi.org/10.12845/sft.65.1.2025.8>.
- [11] *Guidance on Integrated fire protection solutions for Lithium-Ion batteries*, V1.0-EN, Euralarm, Switzerland, 2022.
- [12] Babiński K., Gemra A., Janik P. et al., *Wytyczne w zakresie ochrony przeciwpożarowej garaży w obiektach budowlanych, przeznaczonych do ładowania samochodów elektrycznych i hybrydowych plug-in*, Wydawnictwo CNBOP-PIB, 2024, <https://doi.org/10.17381/2024.2>.
- [13] Kielin J., Kołodziejczyk T., Majka I., Tępiński J., Zboina J., *Prowadzenie działań ratowniczych podczas zdarzeń z udziałem pojazdów z napędem elektrycznym*, CNBOP-PIB, Józefów 2023.
- [14] Tępiński J., *Bezpieczeństwo pożarowe garaży przeznaczonych do przechowywania i ładowania samochodów z napędem elektrycznym – zasady wiedzy technicznej*, Bezpieczna i Cyfrowa Chemia. Raport Polskiej Izby Przemysłu Chemicznego, Warszawa 2024.
- [15] Design Guidelines and Model Requirements Renewable Energy Facilities v4 CFA – Stan Victoria (Wytyczne projektowe i wymagania modelowe dla obiektów wykorzystujących energię odnawialną, wersja 4).
- [16] Projekt SUVEREN II, strona projektu <https://www.suveren-nec.info/?lang=en> [dostęp: październik 2025].
- [17] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1542 z dnia 12 lipca 2023 r. w sprawie baterii i zużytych baterii, zmieniające dyrektywę 2008/98/WE i rozporządzenie

- (UE) 2019/1020 oraz uchylające dyrektywę 2006/66/WE (Dz. U. UE. L. z 2023 r. Nr 191, str. 1 z późn. zm.).
- [18] UL 9540 *Energy Storage Systems and Equipment*, 2023 Edition.
- [19] NFPA 855 *Standard for the Installation of Stationary Energy Storage Systems*, 2026 Edition.
- [20] Saleel Anthrathodiyil, PE, CFPS. Zmiany w normie NFPA 855 w wydaniu z 2026 r. <https://www.telgian.com/nfpa-855-changes-in-2026/>.
- [21] Załącznik C do normy NFPA 855.
- [22] NFPA 68 *Standard on Explosion Protection by Deflagration Venting*, 2023 Edition.
- [23] NFPA 69 *Standard on Explosion Prevention Systems*, 2024 Edition.
- [24] NFPA 72 *National Fire Alarm and Signaling Code*, 2025 Edition.
- [25] NFPA 550 *Guide to the Fire Safety Concepts Tree*, 2022 Edition.
- [26] NFPA 551 *Guide for the Evaluation of Fire Risk Assessments*, 2022 Edition.
- [27] Raporty z Międzynarodowej Konferencji Naukowej pt.: Bezpieczeństwo Nowych Technologii, <https://cnbop.pl/nauka/konferencje/konferencje-bnt>.
- [28] <https://legislacja.gov.pl/projekt/12398903>.
- [29] *First Responders Guide to Lithium-Ion Battery Energy Storage System Incidents*, The American Clean Power Association ACP.

SEN. BRIG. (RETD.) JAN KIELIN, M.SC. ENG. – he graduated from the School of Fire Service Officers in Warsaw and the Higher School of Fire Service Officers in Warsaw. In 1975 he became a licensed fire risk surveyor. He has authored many publications and translations on fire protection.

SEN. BRIG. JACEK ZBOINA, D.SC. ENG. – Deputy Director for Certification and Acceptance at CNBOP-PIB. He graduated from the Main School of Fire Service, the Warsaw School of Economics and the Polish Naval Academy in Gdynia. In 2023 he obtained habilitation in the field of social sciences in the discipline of health sciences at the Faculty of Command and Naval Operations of the Naval Academy in Gdynia. He worked as Fire Risk Surveyor under the Chief Commandant of the State Fire Service. His research and professional interests include safety, fire protection, technical fire security systems, and compliance assessment. He is the author or co-author of several dozen scientific and specialist papers on safety, fire protection, technical security systems, product testing and certification, the practical use of new technologies, and the development of innovations. He has been involved in the implementation and management of research and research & development projects.

SEN. BRIG. PAWEŁ JANIK, D.SC. ENG. – a graduate of the Main School of Fire Service, where he obtained a Master of Science degree in Fire Engineering, and of the Poznań University of Economics, where he earned his doctoral degree. In 2025, he was awarded the degree of Doctor in Science in the discipline of Safety Engineering by the Fire University. He has also completed postgraduate studies in Information Technology and Crisis Management. Prior to assuming the position of Director of CNBOP-PIB in 2018, he served at the Headquarters of the State Fire Service as Director of the Hazard Identification Bureau and as the representative of the Chief Commandant of the State Fire Service in the Committee of Competent Authorities for the Implementation of the SEVESO II Directive operating at the European Commission. He has participated as a co-investigator in national and international research projects. He is the author of the methodology for assessing the level of risk in municipalities and counties, included in the annex to the Regulation of the Minister of the Interior and Administration on the detailed rules for

ST. BRYG. W ST. SP. MGR INŻ. JAN KIELIN – absolwent Szkoły Oficerów Pożarnictwa w Warszawie oraz Wyższej Oficerskiej Szkoły Pożarniczej w Warszawie. W 1975 r. uzyskał uprawnienia rzeczoznawcy do spraw zabezpieczeń ppoż. Autor wielu publikacji oraz tłumaczeń z zakresu ochrony przeciwpożarowej.

ST. BRYG. DR HAB. INŻ. JACEK ZBOINA – Z-ca Dyrektora ds. Certyfikacji i Dopuszczzeń CNBOP-PIB. Absolwent Szkoły Głównej Służby Pożarniczej, Szkoły Głównej Handlowej w Warszawie oraz Akademii Marynarki Wojennej w Gdyni. W 2023 roku uzyskał stopień doktora habilitowanego w dziedzinie nauk społecznych w dyscyplinie nauk o bezpieczeństwie na Wydziale Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej w Gdyni. Rzeczoznawca Komendanta Głównego PSP ds. zabezpieczeń przeciwpożarowych. Jego zainteresowania badawcze oraz praca zawodowa obejmują: bezpieczeństwo, ochronę przeciwpożarową, techniczne systemy zabezpieczeń przeciwpożarowych oraz ocenę zgodności. Autor i współautor kilkunastu publikacji naukowych oraz branżowych w zakresie bezpieczeństwa, ochrony przeciwpożarowej, technicznych systemów zabezpieczeń, badań, testowania i certyfikacji wyrobów, a także wykorzystania w praktyce nowych technologii i tworzenia innowacji. W działalności badawczej i zawodowej uczestniczy w pracach w projektach badawczych i badawczo-rozwojowych – zarówno w roli wykonawcy, jak i kierownika.

ST. BRYG. DR HAB. INŻ. PAWEŁ JANIK – absolwent Szkoły Głównej Służby Pożarniczej, gdzie uzyskał tytuł magistra inżyniera pożarnictwa oraz Akademii Ekonomicznej w Poznaniu, w której obronił doktorat. Stopień doktora habilitowanego w dyscyplinie inżynieria bezpieczeństwa przyznano mu w 2025 r. w Akademii Pożarniczej. Zrealizował również studia podyplomowe z zakresu informatyki oraz zarządzania kryzysowego. Przed objęciem w 2018 r. stanowiska dyrektora CNBOP-PIB pełnił służbę w Komendzie Głównej Państwowej Straży Pożarnej jako dyrektor Biura Rozpoznawania Zagrożeń oraz przedstawiciel Komendanta Głównego PSP w działającym przy Komisji Europejskiej Komitecie Kompetentnych Władz ds. Wdrażania Dyrektywy SEVESO II. Współwykonawca krajowych i zagranicznych projektów badawczych. Twórca metodyki określania stopnia zagrożenia gmin i powiatów zawartej w załączniku do rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie szczegółowych zasad organizacji Krajowego Systemu Ratowniczo-Gaśniczego. Współautor programu studiów podyplomowych

the organization of the National Firefighting and Rescue System. He is a co-author of the postgraduate study programme in Fire and Accident Prevention (ZPA) and the author of dozens of publications on fire protection, prevention of major industrial accidents, risk assessment, and civil protection. He serves as Editor-in-Chief of the scientific journal *Safety & Fire Technology*. He is a member of the editorial board of *Przegląd Pożarniczy*, and a reviewer of research projects and articles published in scientific and technical journals.

DAMIAN BĄK, M.SC. ENG. – a graduate of the Military University of Technology, Faculty of Electronics, field of study: electronics and telecommunication. An engineering and technical specialist at Certification Department at Scientific and Research Centre for Fire Protection – National Research Institute (CNBOP-PIB).

w zakresie zapobiegania pożarom i awariom (ZPA). Autor kilkudziesięciu publikacji dotyczących ochrony przeciwpożarowej, przeciwdziałania poważnym awariom przemysłowym, oceny ryzyka oraz ochrony ludności. Redaktor naczelny czasopisma naukowego „*Safety & Fire Technology*”. Członek rady redakcyjnej w „*Przeglądzie Pożarniczym*”, recenzent projektów naukowo-badawczych oraz artykułów w periodykach naukowo-technicznych.

MGR INŻ. DAMIAN BĄK – absolwent Wojskowej Akademii Technicznej na wydziale Elektroniki na kierunku Elektronika i telekomunikacja. Specjalista inżynierijno-techniczny w Jednostce Certyfikującej Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej – Państwowego Instytutu Badawczego.

Łukasz Tyburski

Forest Research Institute / Instytut Badawczy Leśnictwa

Corresponding author / Autor korespondencyjny: l.tyburski@ibles.waw.pl

Fire Safety of Buildings in the Context of Wildfires

Bezpieczeństwo pożarowe budynków w kontekście pożarów lasów

ABSTRACT

Purpose: The purpose of this publication is to analyse legal regulations and present best practices for managing the space around buildings located near forests or other green areas.

Introduction: Progressive urbanisation near forests and agricultural areas creates a contact zone known in the literature as the wildland-urban interface (WUI). Disturbances caused by variable climatic conditions, including prolonged periods without rain, are becoming increasingly common. These conditions facilitate fire ignition, which can exhibit dangerous combustion dynamics. Such phenomena can lead to catastrophic fires, resulting in the destruction of buildings and linear infrastructure. In Poland, most buildings have concrete structures and non-flammable roof coverings, which theoretically increase their fire resistance. However, the development of buildings adjacent to forests, combined with improper vegetation management or a lack of thoughtful landscaping, creates a real risk of significant material losses. In the event of a fire in forest areas, the fire can spread into urban areas not only through the continuity of plant fuel but also via wind-blown embers. To minimise economic losses and increase residents' safety, it is essential to properly design so-called defensive zones around buildings.

Methodology: A literature review of publicly available documents and legal regulations examined best practices and guidelines for managing the space around residential buildings near forests. The document analysis focused on selected countries where the issue of fires at the interface between forests and human settlements has been studied for many years.

Conclusions: Properly shaping the space around buildings and maintaining supporting infrastructure, including the removal of dead plant matter, increases fire safety in urban areas. Implementing standards for managing the space around buildings can enhance the effectiveness of property protection in the event of fires in adjacent forests or agricultural areas. To improve fire safety, it is necessary to raise awareness among land managers regarding the proper management of vegetation and the placement of garden infrastructure elements. Failure to act in this area can result in significant property losses if fires occur in non-urbanised areas and spread to urban areas.

Keywords: safety of buildings, spatial planning, wildfires, defensive zone

Type of article: review article

Received: 26.01.2026; Reviewed: 26.03.2026; Accepted: 26.03.2026;

Author's ORCID ID: Ł. Tyburski – 0000-0001-8543-3566;

Please cite as: Safety & Fire Technology 2026, 1, 134–144, <https://doi.org/10.12845/sft.67.1.2026.6>;

This is an open access article under the CC BY-SA 4.0 license (<https://creativecommons.org/licenses/by-sa/4.0/>).

ABSTRAKT

Cel: Celem publikacji jest analiza regulacji prawnych oraz prezentacja dobrych praktyk w zakresie gospodarowania przestrzenią wokół budynków zlokalizowanych w sąsiedztwie terenów leśnych lub innych terenów zielonych.

Wprowadzenie: Postępujące procesy urbanizacyjne w sąsiedztwie terenów leśnych i rolniczych tworzą strefę styku, określaną w literaturze jako interfejs leśno-miejski (ang. *wildland-urban interface*, WUI). Coraz częściej obserwuje się zaburzenia związane ze zmiennością warunków klimatycznych, w tym wydłużające się okresy bezdeszczowe. Warunki te istotnie zwiększają podatność materiału palnego na zapłon, sprzyjając powstawaniu pożarów o niebezpieczniejszej intensywności. Mogą one przybierać charakter katastrofalny, skutkować zniszczeniem zabudowań i infrastruktury liniowej. W Polsce większość budynków stanowią obiekty o konstrukcji betonowej z niepalnymi pokryciami dachowymi, co teoretycznie zwiększa ich odporność pożarową. Jednak rozwój zabudowy w sąsiedztwie lasów, w połączeniu z niewłaściwym zarządzaniem roślinnością lub brakiem przemyślanego gospodarowania zielenią, stwarza realne zagrożenie powstania dużych strat materialnych. W przypadku pożaru na terenach leśnych ogień może przenieść się na tereny zurbanizowane nie tylko przez ciągłość paliwa roślinnego, ale także poprzez niesione wiatrem zarzewia. Aby minimalizować straty gospodarcze i zwiększyć bezpieczeństwo mieszkańców, niezbędne jest właściwe kształtowanie tzw. stref obronnych wokół budynków.

Metodologia: Przegląd literatury oparty na ogólnodostępnych dokumentach i przepisach prawnych dotyczył dobrych praktyk oraz wytycznych w zakresie zasad kreowania przestrzeni wokół budynków mieszkalnych zlokalizowanych w sąsiedztwie terenów leśnych. Analizę dokumentów przeprowadzono dla wybranych krajów, w których problem pożarów na styku lasów i osiedli ludzkich jest badany od wielu lat.

Wnioski: Właściwe kształtowanie przestrzeni wokół budynków oraz odpowiednie utrzymanie infrastruktury towarzyszącej, związane z usuwaniem martwej materii roślinnej, zwiększa bezpieczeństwo pożarowe terenów zurbanizowanych. Wdrożenie w praktyce standardów zarządzania przestrzenią wokół budynków pozwala na zwiększenie skuteczności ochrony mienia w przypadku powstania pożarów na sąsiadujących terenach leśnych lub rolniczych. W celu podniesienia bezpieczeństwa pożarowego należy zwiększać świadomość zarządców terenów w zakresie właściwego kształtowania przestrzeni roślinnej i lokalizacji elementów infrastruktury ogrodowej. Brak działań w tym zakresie w przypadku pożarów na terenach niezurbanizowanych i ich przenoszenia się na tereny zurbanizowane może prowadzić do poważnych strat materialnych.

Słowa kluczowe: bezpieczeństwo budynków, planowanie przestrzenne, pożary lasów, strefa ochronna

Typ artykułu: artykuł przeglądowy

Przyjęty: 26.01.2026; **Zrecenzowany:** 26.03.2026; **Zaakceptowany:** 26.03.2026;

Identyfikator ORCID autora: Ł. Tyburski – 0000-0002-2254-1030;

Proszę cytować: Safety & Fire Technology 2026, 1, 134–144, <https://doi.org/10.12845/sft.67.1.2026.6>;

Artykuł udostępniany na licencji CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>).

Introduction

In recent decades, the number of wildfires recorded worldwide has increased, in terms of both the frequency and the affected area [1–2]. Every year high intensity fires are recorded in different regions, which combined with the progressing urbanisation results in environmental and economic losses. Disturbances caused by variable climatic conditions are increasingly recorded, including prolonged periods without rain [3–4], which facilitate the occurrence of high dynamics fires. In face of these changes, the fire safety of buildings located near to or directly in forest and agricultural areas is increasingly important. The reason for the increased interest in this subject are catastrophic destruction of houses and settlements [5–6]. Due to improper use of building materials, lack of proper protection and errors in vegetation management, fires near buildings may cause significant property losses.

An important matter is the understanding of fire dynamics at the wildland-urban interface and ensuring an adequate level of fire safety. This approach does not eliminate the fire hazard to developed areas, but it reduces the potential losses and increases the safety of inhabitants.

In scientific literature, the problem related to the situation, in which houses are located near non-developed vegetation areas, is referred to as the wildland-urban interface (WUI) [7]. The WUI problem is analysed not only in terms of direct fire hazard, but also in the context of pollutant emissions and their negative impact on air quality and health condition of the inhabitants of such areas [8]. Another research aspect is the impact of settlement on ecosystems, e.g. by introduction of geographically alien plant species [9].

In Poland, the problem of development at the border of forest and agricultural areas is also noticeable, however there are few studies in that subject. Polish legal regulations address the fire safety of buildings, the location between structures, their design and their location in relation to forest areas. An important legal act is the Regulation of the Minister of Infrastructure of 12 April 2002 on technical conditions for buildings and their location [10]. That act stipulates that the distance between buildings and forest areas, understood as forest area (Ls), for most residential

Wprowadzenie

W ostatnich dekadach na świecie obserwuje się wzrost liczby pożarów lasów, zarówno pod względem ich częstotliwości, jak i obejmowanej powierzchni [1–2]. Każdego roku w różnych regionach świata odnotowuje się pożary o wysokiej intensywności, co w połączeniu z postępującą urbanizacją powoduje straty przyrodnicze i gospodarcze. Coraz częściej spotykane są zaburzenia związane ze zmiennością warunków klimatycznych, w tym wydłużające się okresy bezdeszczowe [3–4], sprzyjające powstawaniu intensywnie rozwijających się pożarów. W obliczu tych zmian znaczenia nabiera zagadnienie bezpieczeństwa pożarowego budynków zlokalizowanych w sąsiedztwie terenów leśnych, rolniczych lub bezpośrednio na nich znajdujących. Powodem wzrostu zainteresowania tą tematyką są zniszczenia domów, osiedli podczas pożarów o charakterze katastrofalnym [5–6]. Niewłaściwe zastosowanie materiałów budowlanych, brak odpowiedniego zabezpieczenia, błędy w zarządzaniu roślinnością powodują, że pożary w sąsiedztwie zabudowań mogą doprowadzać do istotnych strat materialnych.

Ważnym zagadnieniem jest zrozumienie dynamiki pożaru na styku lasu i terenów zurbanizowanych oraz zapewnienie właściwego poziomu bezpieczeństwa pożarowego. Takie podejście nie eliminuje zagrożenia pożarowego dla terenów zabudowanych, ale ogranicza potencjalne straty i zwiększa bezpieczeństwo mieszkańców.

W literaturze naukowej zagadnienie dotyczące sytuacji, kiedy domy znajdują się w sąsiedztwie terenów niezabudowanych pokrytych roślinnością, nazywa się *wildland-urban interface* (WUI) [7]. Zagadnienie WUI analizowane jest nie tylko pod względem bezpośredniego zagrożenia pożarowego, ale również w kontekście emisji zanieczyszczeń i ich negatywnego wpływu na jakość powietrza i stan zdrowotny mieszkańców tych stref [8]. Innym badanym aspektem jest oddziaływanie osadnictwa na ekosystemy np. poprzez wprowadzanie gatunków roślin obcych geograficznie [9].

W Polsce problem zabudowy na granicy terenów leśnych i rolniczych również jest zauważalny, jednak nie ma wielu opracowań w tym zakresie. Polskie przepisy prawne odnoszą się do bezpieczeństwa pożarowego budynków, usytuowania między obiektami, ich konstrukcji oraz usytuowania względem terenów leśnych.

buildings is 12 metres. That distance may be decreased to 7 m provided that the wall of the building from the side of the forest is built as fire wall with proper fire rating. For production buildings and warehouses, the distance depends on the fire load density inside the building. If the fire load is high, the distance may be 15 m and more. In most cases, for smaller warehouses, the applicable regulations are analogical to residential buildings. In national law, there are almost no regulations and guidelines related to the spatial planning of vegetation near buildings adjacent to forest, agricultural and other green areas.

Methods

The literature review was conducted in the Google Scholar database, using the following phrases: *wildland-urban interface*, *wildfire*, *safe building*. The publications analysed were published after 2000 and focused on managing the space around residential buildings adjacent to forest areas. The documents also included the methods of managing the outdoor infrastructure that is an integral part of the structure or located in direct vicinity of the structure. The analysis was conducted for selected countries in North America (USA), South America (Argentina, Chile), Australia and Europe (Spain, Portugal). In these countries the issue of fires at the interface between forests and human settlements has been systematically studied for many years. Educational materials on fires in these areas were excluded.

The purpose of this publication is to analyse legal regulations and present best practices for managing the space around buildings located near forests or other green areas. In connection with the purpose of the article, the following research question was raised: What conclusions and recommendations for Polish standards arise from the analysis of international practices in the field of fire safety at the *wildland-urban interface*?

Analysis of the problem

In countries with many years of experience in fighting fires at the wildland-urban interface, legal frameworks and standards were developed for managing the space around civil structures. One of such countries is the United States of America, where the Federal Emergency Management Agency (FEMA) published the *Builder's Guide to Construction in Wildfire Zones* in 2025 [11]. This publication highlights the method of construction and location of buildings in the so-called vegetation fire hazard zones.

Jednym z istotnych aktów prawnych jest Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie [10]. W akcie tym wskazano, że odległość między budynkami a gruntami leśnymi, rozumianymi jako grunt leśny (Ls), dla większości budynków mieszkalnych wynosi 12 metrów. Odległość tę można zmniejszyć do 7 m pod warunkiem, że ściana budynku od strony lasu zostanie wykonana jako ściana oddzielenia przeciwpożarowego o odpowiedniej klasie odporności ogniowej. W przypadku budynków produkcyjnych lub magazynów odległość zależy od gęstości obciążenia ogniowego wewnątrz budynku. Jeśli jest ono duże, odległość może wynosić 15 m i więcej. W większości przypadków dla mniejszych magazynów stosuje się analogicznie zasadę jak dla budynków mieszkalnych. W krajowym prawie brak jest przepisów, wytycznych odnoszących się do tego, jak powinna być gospodarowana przestrzeń roślinność znajdująca się w pobliżu budynków graniczących z terenami leśnymi, rolniczymi i innymi terenami zielonymi.

Metody

Przegląd literatury przeprowadzono w bazie Google Scholar, fraz: *wildland-urban interface*, *wildfire*, *safe building*. Analizowane publikacje wydano po 2000 roku i koncentrowały się na dobrych praktykach, aktach prawnych oraz wytycznych dotyczących zarządzania przestrzenią wokół budynków mieszkalnych sąsiadujących z terenami leśnymi. W dokumentach uwzględniono także metody zarządzania infrastrukturą zewnętrzną, stanowiącą integralną część obiektu lub znajdującą się w jego bezpośrednim otoczeniu. Analizę przeprowadzono dla wybranych krajów z Ameryki Północnej (USA), Południowej (Argentyna, Chile), Australii oraz Europy (Hiszpania, Portugalia). W tych krajach problematyka pożarów na styku lasów i osiedli ludzkich jest systematycznie badana od wielu lat. Pominięto materiały edukacyjne dotyczące pożarów na tych terenach.

Celem publikacji jest analiza regulacji prawnych oraz prezentacja dobrych praktyk w zakresie gospodarowania przestrzenią wokół budynków zlokalizowanych w sąsiedztwie terenów leśnych lub innych terenów zielonych. W związku z postawiono pytanie badawcze: Jakie wnioski i rekomendacje dla polskich standardów wynikają z analizy międzynarodowych praktyk w obszarze bezpieczeństwa pożarowego terenów położonych w strefie styku lasów i obszarów zurbanizowanych?

Analiza zagadnienia

W krajach o wieloletnim doświadczeniu w zwalczaniu pożarów na styku terenów leśnych i zurbanizowanych wypracowano ramy prawne oraz standardy zarządzania przestrzenią otaczającą obiekty budowlane. Jednym z takich krajów są Stany Zjednoczone, w których Amerykańska Federalna Agencja Zarządzania Kryzysowego (ang. *Federal Emergency Management Agency*, FEMA) w 2025 r. wydała *Poradnik dla budowniczych konstrukcji w strefach zagrożonych pożarami lasów* [11]. Publikacja ta zwraca uwagę na sposób

This study described many aspects building construction, including the problems related to vents, door and window joinery. The study focused in particular on problems related to the methods of managing the space around buildings, also including small garden infrastructure, such as arbours, grill zones, standalone garages. The study also addressed the importance of topography and location of buildings. It is particularly important for highland and mountain areas, in which locating buildings on the edge of hill and near forest areas, is especially hazardous due to the nature of fire, which could spread uphill. The authors of the study also note the responsibility of the owners of structures, which should care for proper maintenance of facilities or infrastructure, e.g. by regular removal of minor plant material from roofs, gutters, balconies and terraces. It was noted that a possible solution is to use fine metal meshes in vents, which block access of sparks from fire inside the building and its systems. This guide is a set of key recommendations, which may be implemented in many other regions of the world.

Another study related to the safety of residential structures was published by the American non-profit organisation, the Insurance Institute for Business and Home Safety (IBHS) in 2023. Its title was *Model Ordinance for Construction in WUI Area (WUI)* [12]. This document includes ready templates for legal regulations that local authorities could use to increase the resistance of buildings to fires related to vegetation. The primary purpose the guidelines is to reduce the risk of ignition of the structure caused by sparks carried by the wind and direct contact with flames. Regulations are based on IBHS scientific research that identifies the weakest points of buildings during wildfires. A key component of protection to create the so-called defensible space by strict vegetation management around the property. Model solutions recommend using non-combustible roof coverings and securing vents with meshes to protect from the ingress of sparks. The document provides a detailed description of requirements for the so-called “zero zone”, i.e. the area up to 1.5 m from the house, in which no combustible materials are allowed. The guidelines also include standards for windows, doors, terraces and façades, intended to minimise the risk of fire penetration to the inside. The postulated regulations are applicable to both newly constructed buildings and upgraded structures. The study emphasised that effective protection requires the involvement of the entire community, because fire easily spreads between closely adjacent houses.

In 2022, the Chilean National Forest Organisation (es. *Corporación Nacional Forestal*, CONAF) published the *Wildfire Prevention Manual* [13]. This document is a practical guide for local communities and it points to proper construction design and managing the space around buildings. The study, like the publications described above, points to the importance of vegetation near buildings and the characteristics of the topography. Particular attention was paid to the “zero zone” (up to 1.5 m from the foundation), which must be free from combustible materials, such as: dry grass, fuel wood, plastic garden infrastructure. The study emphasised the importance of regular maintenance of architectural details by removing plant deposits, as well as the need for securing vents in attics with fine meshes. The document also points to the need for forming local groups and organisations

budowania oraz usytuowania budynków w tzw. strefach zagrożenia pożarami roślinności. W opracowaniu opisano wiele aspektów dotyczących konstrukcji budynków, z uwzględnieniem zagadnień dotyczących otworów wentylacyjnych, stolarki drzwiowej i okiennej. Szczególną uwagę poświęcono kwestiom związanym ze sposobami zagospodarowywania przestrzeni wokół budynków, uwzględniając również małą infrastrukturę ogrodową, taką jak altany, strefy grillowe, niezależne garaże. W opracowaniu odniesiono się również do znaczenia topografii i usytuowania budynków. Jest to ważna kwestia szczególnie na terenach wyżynnych i górskich, gdzie zlokalizowanie budynków na skraju wzniesienia i w sąsiedztwie terenów leśnych jest szczególnie niebezpieczne ze względu na charakter pożaru, który może rozwijać się w górę zbocza. Autorzy opracowania zwracają również uwagę na odpowiedzialność właścicieli obiektów, którzy powinni zadbać o odpowiednią konserwację urządzeń czy utrzymanie infrastruktury, np. przez regularne usuwanie drobnych materiałów roślinnych z dachów, rynien, balkonów, tarasów. Podkreślono, że jednym z rozwiązań może być stosowanie drobnych metalowych siatek w otworach wentylacyjnych, które blokują dostawanie się do wnętrza budynku, jego instalacji iskiei pochodzących z pożaru. Przewodnik jest zbiorem kluczowych rekomendacji, które mogą zostać zaimplementowane w wielu innych regionach świata.

Kolejne opracowanie związane z bezpieczeństwem obiektów mieszkalnych wydała w 2023 r. amerykańska organizacja non-profit Instytut Ubezpieczeń Bezpieczeństwa Biznesu i Domu (ang. *Insurance Institute for Business and Home Safety*, IBHS). Jego tytuł to *Wzorcowe przepisy ograniczające ryzyko pożarów w strefach znajdujących się na styku obszarów miejskich i leśnych (WUI)* [12]. Dokument zawiera gotowe szablony regulacji prawnych, które lokalne władze mogą wykorzystać do zwiększenia odporności budynków na pożary związane z roślinnością. Głównym celem wytycznych jest ograniczenie ryzyka zapłonu konstrukcji od niesionych wiatrem iskiei oraz bezpośredniego kontaktu z płomieniami. Przepisy opierają się na badaniach naukowych IBHS, które identyfikują najsłabsze punkty budynków podczas pożarów lasów. Kluczowym elementem ochrony jest stworzenie tzw. przestrzeni obronnej (ang. *defensible space*) poprzez rygorystyczne zarządzanie roślinnością wokół posesji. Modelowe rozwiązania zalecają stosowanie niepalnych pokryć dachowych oraz zabezpieczanie otworów wentylacyjnych siatkami chroniącymi przed przedostawaniem się iskiei. Dokument szczegółowo opisuje wymagania dla tzw. „strefy zero”, czyli obszaru do 1,5 m od domu, na którym nie mogą znajdować się żadne materiały palne. Wytyczne obejmują również standardy dla okien, drzwi, tarasów oraz elewacji ściennych, co ma zminimalizować ryzyko przeniknięcia ognia do wnętrza. Proponowane przepisy dotyczą zarówno nowo wznoszonych budynków, jak i obiektów modernizowanych. W opracowaniu podkreślono, że skuteczna ochrona wymaga zaangażowania całej społeczności, ponieważ pożar łatwo przenosi się między blisko sąsiadującymi domami.

W 2022 roku w Chile Narodowa Organizacja Leśna (hiszp. *Corporación Nacional Forestal*, CONAF) wydała *Podręcznik zapobiegania pożarom lasów* [13]. Dokument ten jest praktycznym przewodnikiem dla społeczności lokalnych, zwraca uwagę na właściwe projektowanie budownictwa oraz zarządzanie przestrzenią wokół budynków. Opracowanie, podobnie jak opisane powyżej publikacje,

intended to coordinate common activities, such as the construction of fire breaks adjacent to buildings. An important problem highlighted in the publication is the development of evacuation plans, including the information on e.g. assembly points for inhabitants. An important aspect is paying attention to proper selection of plant species for gardens, prioritising the plants with higher water content and lower ignitability. It should be also noted that many structures located in smaller towns and rural areas are only made with wood materials and located directly adjacent to forests. This type of construction is at particular risk of destruction during wildfires.

In 2002, the Argentinian Ministry of Environment published the *Guide for preventing fires at the wildland-urban interface* [14]. This study is focused on the need to create passive defensible space around buildings. The strictest zone is within 2 m from the foundations of the building, where it is required to remove vegetation. Like other studies, this document recommends using construction materials with high fire rating, such as concrete, brick, stone and metal roof covering instead of wood shingles. It emphasised the importance of protection of critical points of the house, such as hoods, terraces, gutters, vents. Attention was also paid to the need for clear marking of property numbers and providing wide access roads, suitable for the parameters of fire service vehicles. The study encourages installing roof sprinkling systems and having independent water tanks equipped with combustion-powered pumps.

The Australian standard for the construction of buildings in bushfire-prone areas no. AS 3959:2018 [15], prepared by the Standards Australia Committee, is considered as one of the strictest standards for the fire protection of buildings. This standard defines technical design and construction requirements for buildings constructed in fire hazard areas. The primary purpose of the document is to highlight the need to increase the resistance of buildings located in zones exposed to sparks, thermal radiation and direct contact with fire. The provisions of the standard emphasise the protection of buildings from the so-called spark and ember attack, noting the need for sealing all slots greater than 3 mm in the structure. Vents must be secured with corrosion-resistant fine metal mesh that blocks the access of sparks to the inside of the building. The requirements for window joinery include using tempered glasses and frames made of metal or wood species with high natural fire resistance. The roof must be made with non-combustible materials (e.g. steel sheet, ceramic roofing tile) and designed to prevent the accumulation of flammable material under roof decking. The provisions of the standard are based on the system of six fire hazard levels, referred to as the Bushfire Attack Level (BAL) [16]. The lowest level is designated as BAL-LOW and the highest as BAL-FZ (*flame zone*). The BAL classification for the given plot is determined based on the local type of vegetation, topography (slope inclination) and distance of the building from combustible materials. The BAL-LOW level is low risk of destruction of the building. The highest level, BAL-FZ, is applicable to buildings exposed to direct contact with flames and requires using special protection systems and materials with the highest fire rating. For external walls in lower hazard zones (BAL 12.5, 19 and 29), it is allowed to use wood with

zwraca uwagę na znaczenie roślinności znajdującej się w sąsiedztwie budynków oraz na charakterystykę ukształtowania terenu. Szczególną uwagę zwrócono na „strefę zero” (do 1,5 m od fundamentów), która musi być pozbawiona materiałów palnych, takich jak: sucha trawa, drewno opałowe, plastikowe elementy infrastruktury ogrodowej. W opracowaniu podkreślono znaczenie regularnej konserwacji detali architektonicznych poprzez usuwanie osadów roślinnych, a także potrzebę zabezpieczenia otworów wentylacyjnych poddaszy siatkami o gęstym splocie. Dokument zwraca uwagę również na potrzebę tworzenia lokalnych grup, organizacji, których zadaniem będzie koordynowanie wspólnych działań, takich jak budowa pasów przeciwpożarowych w sąsiedztwie budynków. Ważną kwestią zaznaczoną w publikacji jest opracowywanie planów ewakuacji, które zawierają informację m.in. o miejscach zbiórki dla mieszkańców. Istotnym aspektem jest nacisk na odpowiedni dobór gatunków roślin w ogrodach, promując te o wyższej zawartości wody i mniejszej podatności na zapłon. Należy zwrócić uwagę, że liczne zabudowania zlokalizowane w mniejszych miejscowościach oraz na wsiach powstawały wyłącznie z materiałów drewnianych, a ich lokalizacja była w bezpośrednim sąsiedztwie z lasami. Taki rodzaj zabudowy jest szczególnie narażony na zniszczenia podczas pożarów lasów.

W 2002 r. argentyńskie Ministerstwo Środowiska wydało *Przewodnik zapobiegania pożarom na styku obszarów dzikich i zurbanizowanych* [14]. Opracowanie to koncentruje się na potrzebie tworzenia wokół budynków pasywnej przestrzeni obronnej. Najbardziej rygorystyczna strefa znajduje się w promieniu do 2 m od fundamentów budynku, gdzie nakazuje się usuwanie roślinności. Podobnie jak inne opracowania dokument ten rekomenduje stosowanie materiałów budowlanych o wysokiej klasie reakcji na ogień, takich jak beton, cegła, kamień oraz metalowe pokrycia dachowe zamiast gontów drewnianych. Podkreślono w nim wagę ochrony krytycznych punktów domu, takich jak okapy, tarasy, rynny, otwory wentylacyjne. Zwrócono także uwagę na potrzebę wyraźnego oznakowania numerów posesji oraz zapewnienia szerokich dróg dojazdowych, dostosowanych do parametrów pojazdów straży pożarnej. W opracowaniu zachęca się do montażu systemów zraszania dachów oraz posiadania niezależnych zbiorników na wodę wyposażonych w pompy spalinowe.

Australijska norma nr AS 3959:2018 dotycząca budowy budynków na obszarach zagrożonych pożarami buszu [15], przygotowana przez Australijski Komitet Standardów (ang. Standards Australia Committee) uznawana jest za jeden z najbardziej restrykcyjnych standardów dotyczących ochrony budynków przed pożarami. Określa ona techniczne wymagania projektowe i konstrukcyjne dla budynków wznoszonych na terenach zagrożonych pożarami. Głównym celem dokumentu jest zwrócenie uwagi na potrzebę zwiększenia odporności budynków znajdujących się w zagrożonych strefach na oddziaływanie iskier, promieniowanie cieplne oraz bezpośredni kontakt z ogniem. Zapisy normy kładą nacisk na ochronę budynków przed tzw. atakiem iskier i żagwi (ang. *ember attack*), zwracając uwagę na potrzebę uszczelniania wszelkich szczelin w konstrukcji większych niż 3 mm. Otwory wentylacyjne muszą być zabezpieczone gęstą metalową siatką z materiałów odpornych na korozję, która zablokuje wlot iskier do wnętrza budynku. Wymagania dla stolarki okiennej obejmują stosowanie szyb hartowanych oraz ram

the minimum density of 680 kg/m^3 (0.68 g/cm^3)¹. For windows and doors, it is required to use tempered glasses and frames made of metal or wood species with fire resistance to prevent heat-induced cracking. The document describes the structure of terraces and stairs and recommends using non-combustible beams or wood with increased fire rating in places exposed to the falling of embers. At the highest hazard level (BAL-FZ), it is required to use special protective barriers, such as fire protection window shutter systems or wood joinery protective screens [16]. It should be noted that strict provisions related to wood structures do not eliminate wood as construction material, despite the existence of many wildfire zones in Australia.

In Europe, some countries intensify the works on guidelines for proper management of spaces around buildings. This is because, in particular in Mediterranean countries, catastrophic fires that endanger urbanised areas increase. The Spanish *Guide for the development of municipal policies and local action plans to prevent fires at the wildland-urban interface* [17] was published by the Spanish Federation of Municipalities and Provinces (es. *Federación Española de Municipios y Provincias*, FEMP) in 2025. The guide pointed to the need for local authorities to develop policies and plans to protect from fires at the wildland-urban interface. The key component of the strategy is to promote sustainable landscape management, which consists in reducing the biomass in protection strips around settlements. The document includes guidelines for creating protection strips (Spanish: *franjas de seguridad*) to obstruct fire propagation to buildings.

In Portugal, the Integrated Rural Fires Management System (pt. *Sistema de Gestão Integrada de Fogos Rurais*, SGIFR) integrates the operation of different institutions, including the fire service, the institute of nature and forest conservation, the police, the military and the institute of meteorology. The operations of SGIFR includes a wide social campaign to educate the inhabitants how to prepare their houses and plots to increase their resistance to fires. This information is available i.a. on the website [23], which provides a simple illustration of how to manage green areas near buildings.

In some countries, general regulations include recommendations for managing the space around buildings in forest areas. Such provisions were considered i.a. in the study entitled *Building wildfire resilience into forest management planning. Practice Guide*, published by the Forestry Commission in the United Kingdom [18]. This guide pointed to the need to form appropriate circular zones near buildings. The nearer to the building, the stricter restrictions applicable in the zone. Unfortunately, such recommendations and good practices without legal enforcement are not always reflected in practice.

It is worth noting that spatial guidelines are supplemented by worldwide research on the specifics of fires in border areas between forests, agricultural areas and developments. One of the actions undertaken is preparing reliable simulations of fire spreading in such areas. Research teams postulate using high resolution topographical data [19] and integrating the physical

wykonanych z metalu lub gatunków drewna o wysokiej naturalnej odporności na ogień. Dach musi być wykonany z materiałów niepalnych (np. blacha stalowa, dachówka ceramiczna) i zaprojektowany tak, aby pod jego poszyciem nie gromadził się łatwopalny materiał. Zapisy normy opierają się na systemie sześciu poziomów zagrożenia pożarowego, nazywanych Bushfire Attack Level (BAL) [16]. Najniższy poziom został oznaczony jako BAL-LOW, najwyższy jako BAL-FZ (ang. *flame zone*). Klasyfikacja BAL dla danej działki jest ustalana na podstawie rodzaju okolicznej roślinności, ukształtowania terenu (nachylenia stoku) oraz odległości budynku od materiałów palnych. Poziom BAL-LOW oznacza niskie ryzyko zniszczenia budynku. Najwyższy poziom, BAL-FZ, dotyczy budynków narażonych na bezpośredni kontakt z płomieniami i wymaga stosowania specjalnych systemów osłonowych oraz materiałów o najwyższej odporności ogniowej. Dla ścian zewnętrznych w niższych strefach zagrożenia (BAL 12.5, 19 i 29) dopuszczalne jest stosowanie drewna o gęstości minimalnej 680 kg/m^3 (0.68 g/cm^3)¹. W przypadku okien i drzwi wymagane jest stosowanie szyb hartowanych oraz ram wykonanych z metalu lub gatunków drewna odpornych na ogień, aby zapobiec pękaniu pod wpływem ciepła. Dokument opisuje konstrukcję tarasów i schodów, zalecając stosowanie niepalnych legarów lub drewna o podwyższonej odporności ogniowej w miejscach narażonych na osiadanie żaru. Przy najwyższym poziomie zagrożenia (BAL-FZ) wymagane jest stosowanie specjalnych barier ochronnych, takich jak systemy okiennic przeciwpożarowych lub ekrany chroniące drewnianą stolarkę [16]. Należy zwrócić uwagę, że rygorystyczne zapisy dotyczące konstrukcji drewnianych nie eliminują drewna jako materiału budulcowego, pomimo obecności w Australii wielu stref zagrożonych pożarami lasów.

W Europie niektóre kraje intensyfikują prace nad przygotowaniem wytycznych dotyczących odpowiedniego zagospodarowywania przestrzeni wokół budynków. Wynika to z tego, że szczególnie w krajach basenu Morza Śródziemnego coraz częściej odnotowuje się pożary o charakterze katastrofalnym, zagrażającym terenom zurbanizowanym. Hiszpański dokument pt. *Przewodnik po opracowaniu polityk miejskich i lokalnych planów działań w celu przeciwdziałania ryzyku pożarów lasów na styku miasta i lasów* [17] został wydany przez Hiszpańską Federację Gmin i Prowincji (hiszp. *Federación Española de Municipios y Provincias*, FEMP) w 2025 roku. W przewodniku zwrócono uwagę na potrzebę opracowywania przez władze lokalne polityk i planów ochrony przed pożarami w strefie styku terenów leśnych i zurbanizowanych. Kluczowym elementem strategii jest promowanie zrównoważonego zarządzania krajobrazem, które polega na redukcji biomasy w pasach ochronnych wokół osiedli. Dokument zawiera wytyczne dotyczące tworzenia pasów bezpieczeństwa (hiszp. *franjas de seguridad*), które mają utrudniać przenoszenie się ognia na budynki.

W Portugalii funkcjonuje Zintegrowany System Zarządzania Pożarami Wiejskimi (pt. *Sistema de Gestão Integrada de Fogos Rurais*, SGIFR), który skupia działania różnych instytucji, w tym straży pożarnej, instytutu ochrony przyrody i lasów, policji, wojska, instytutu meteorologii. W ramach działania SGIFR

¹ For comparison, in Poland the density is 0.55 g/cm^3 for *larix decidua*, 0.65 g/cm^3 for *fraxinus excelsior*, 0.69 g/cm^3 for *robinia pseudoacacia*, $0.62\text{--}0.69 \text{ g/cm}^3$ for *quercus robur/quercus petraea* and 0.72 g/cm^3 for *carpinus* [22].

¹ Dla porównania w Polsce modrzew europejski posiada gęstość 0.55 g/cm^3 , jesion wyniosły 0.65 g/cm^3 , robinia akacjowa 0.69 g/cm^3 , dąb szypułkowy/bezszypułkowy $0.62\text{--}0.69 \text{ g/cm}^3$, grab 0.72 g/cm^3 [22].

approach and the physical approach to ensure balance between high computing performance and model accuracy [20]. To effectively increase the fire safety and fire protection level, it is essential to adopt an interdisciplinary approach connected with the latest scientific achievements and planning, technical and legislative practices.

prowadzona jest szeroka kampania społeczna edukująca mieszkańców, jak przygotować domy i działki, aby zwiększyć ich odporność na pożary. Informacje te można znaleźć między innymi na stronie internetowej [23], która w prosty sposób ilustruje, jak zarządzać terenami zielonymi w sąsiedztwie zabudowań.

Niektóre kraje posiadają w swoich ogólnych regulacjach zalecenia dotyczące kreowania przestrzeni wokół budynków znajdujących się na terenach leśnych. Zapisy takie zawarto m.in. w opracowaniu pt. *Budowanie odporności lasów na pożary – wytyczne dla gospodarki leśnej* wydanych przez Forestry Commission w Wielkiej Brytanii [18]. W przewodniku tym zwrócono uwagę na potrzebę tworzenia odpowiednich stref kołowych w sąsiedztwie budynków. Im bliżej budynku, tym strefa charakteryzuje się większymi restrykcjami. Niestety tego typu zalecenia i dobre praktyki, niemające umocowania prawnego, nie zawsze znajdują odzwierciedlenie w praktyce.

Warto podkreślić, że uzupełnieniem wytycznych przestrzennych są prowadzone na świecie badania nad specyfiką pożarów na obszarach granicznych między lasami, terenami rolniczymi a zabudową. Jednym z podejmowanych działań jest opracowanie wiarygodnych symulacji rozprzestrzeniania się pożaru na takich terenach. Zespoły badawcze postulują wykorzystanie wysoko-rozdzielczych danych topograficznych [19] oraz integrację podejścia empirycznego z fizycznym, co zapewni równowagę między wydajnością obliczeniową a dokładnością modelową [20]. Dla skutecznego zwiększenia poziomu bezpieczeństwa pożarowego i ochrony przeciwpożarowej niezbędne jest podejście interdyscyplinarne, nawiązujące do najnowszych osiągnięć naukowych i powiązane z praktyką planistyczną, techniczną i legislacyjną.

The problem of transitional zone in Poland

In Poland, the problem of fires at the interface of green areas and urbanised areas is not the subject of wide social discussion. However, with the progress of urbanisation, in particular near major cities, some settlements are built in direct vicinity of forest or agricultural areas with different levels of use. This applies i.a. to agricultural areas, unused for many years, overgrown by trees and bushes by natural succession. Despite these transformations in the land register, these areas are still considered as agricultural land.

When conducting fire safety activities, analogical to the mentioned regulations, it is reasonable to draw the attention of land owners to proper spatial planning and vegetation management around buildings. This requires proper education and raising awareness among social and professional groups, including architects and specialists in designing green near developments.

In Poland, the problem of residential buildings made with thin wood materials is non-existent, unlike in some countries with a warmer climate. Sometimes, however, it is observed that wood houses are built contrary to the applicable regulations, without keeping proper distances from neighbouring buildings. Another problem is development in allotment gardens, where wood infrastructure is built without considering fire safety requirement, using materials of varied technical quality. Another interesting

Zagadnienie strefy przejściowej w Polsce

W Polsce zagadnienie pożarów na styku terenów zielonych i zurbanizowanych nie jest obecnie przedmiotem szerokiej dyskusji społecznej. Jednak wraz z postępującą urbanizacją, zwłaszcza w pobliżu dużych miast, niektóre osiedla powstają w bezpośrednim sąsiedztwie terenów zalesionych lub rolniczych o różnym stopniu użytkowania. Dotyczy to między innymi terenów rolniczych od wielu lat nieużytkowanych, które w wyniku naturalnej sukcesji zostały porośnięte drzewami i krzewami. Mimo tych przemian w ewidencji gruntów powierzchnie te nadal są traktowane jako użytki rolne.

Prowadząc działania związane z bezpieczeństwem pożarowym, na wzór przytoczonych regulacji, zasadne jest zwracanie uwagi właścicieli gruntów na właściwe kształtowanie otoczenia budynków i zarządzanie roślinnością wokół nich. W tym zakresie niezbędna jest odpowiednia edukacja i podnoszenie świadomości w różnych grupach społecznych i zawodowych, w tym wśród architektów oraz osób specjalizujących się w aranżacji zieleni w otoczeniu zabudowy.

W Polsce nie występuje problem budowy domów mieszkalnych z cienkich drewnianych materiałów, jak ma to miejsce w niektórych krajach o cieplejszym klimacie. Jednak czasami obserwuje się, że domy drewniane są budowane niezgodnie z obowiązującymi przepisami, bez zachowania właściwych odległości od budynków sąsiednich. Kolejnym zagadnieniem jest zabudowa na

aspect is modernisation of houses consisting in introducing façades of wood or with wood components, in direct vicinity of bush vegetation. Buildings are also increasingly fitted with plastic façade components, which may be inflammable, hazardous to the building and release dangerous substances during the fire. Due to the trend of living close to nature without proper spatial management knowledge and fire protection, such structures may quickly catch fire in case of fire in the adjacent forest or agricultural areas. Planting bushes and trees in direct vicinity of buildings, in particular young plants, forms the so-called fuel ladder, which is particularly dangerous in case of fire.

An additional problem for spatial planning in urban areas is the use of alien species, such as different varieties of thuyas (Latin: *thuja ssp.*), which in addition to content of combustible essential oils accumulate dead organic matter in the crown. Buildings located near fallow fields, with mass monoculture of goldenrod, e.g. *solidago canadensis*, are exposed to fire hazard. In autumn and winter, the remaining dry stems ignite easily and due to mass incidence, fire may spread abruptly.

The safety of houses and urban areas requires cooperation of national authorities, local authorities and private land owners on many planes [21]. Without coordinating the activities of different groups, the objective of increasing the safety of urban areas and thus minimising economic and environmental losses will not be achieved.

Summary

The analysis of selected international guidelines and standards for managing the wildland-urban interface (WUI) shows to reduce fire losses, it is essential to adopt an approach combining spatial planning and civil engineering. The countries with experience in fighting vegetation fires have developed technical standards that focus on protecting buildings from moving sparks and embers and principles for managing vegetations near buildings. The comparison of solutions from different regions of the world confirms the universality of some principles, such as elimination of combustible materials in direct vicinity of building walls or proper spatial planning in areas adjacent to developments. In Europe, some countries started developing guidelines aimed at increasing the safety of the inhabitants of urban areas adjacent to green areas. In Poland, analogically to the documents described in the article, it is reasonable to act to raise social awareness of fire safety. Proper spatial planning around buildings is not only higher fire protection standards, but also higher safety of inhabitants and firefighters. An important aspect is the

działkach rekreacyjnych, gdzie drewniana infrastruktura powstaje bez uwzględnienia wymogów bezpieczeństwa pożarowego, z użyciem materiałów o różnej jakości technicznej. Ciekawym aspektem jest również to, że modernizacje domów polegają na wprowadzaniu elewacji drewnianych lub z elementami drewna, które bezpośrednio sąsiadują z roślinnością krzewiastą. Coraz częściej na budynkach pojawiają się także plastikowe elementy elewacyjne, które mogą być łatwopalne i stanowić zagrożenie dla budynku, a podczas pożaru emitować niebezpieczne substancje chemiczne. Trend zamieszkiwania blisko przyrody, bez odpowiedniej wiedzy dotyczącej gospodarowania przestrzenią oraz bez podejmowania działań w zakresie ochrony przeciwpożarowej, sprawia, że obiekty te w przypadku pożaru na sąsiadujących terenach leśnych lub rolniczych mogą szybko zostać objęte ogniem. Sadzenie krzewów i drzew, zwłaszcza młodych roślin, w bliskim sąsiedztwie zabudowań tworzy tzw. drabinę paliwową, która jest szczególnie niebezpieczna podczas pożaru.

Dodatkowym problemem w gospodarowaniu przestrzenią na obszarach zurbanizowanych jest stosowanie gatunków obcych, takich jak różne odmiany żywotników (łac. *thuja ssp.*), które oprócz obecności palnych olejków eterycznych, gromadzą wewnątrz korony martwą materię organiczną. Budynki zlokalizowane w sąsiedztwie ugorowanych pól, na których masowo występuje monokultura nawłoci, m.in. kanadyjskiej (łac. *solidago canadensis*), są narażone na zagrożenie pożarowe. Jesienią i zimą pozostawione suche łodygi łatwo się zapalają, a ze względu na masowe występowanie rozwój pożaru może być gwałtowny.

Bezpieczeństwo domów i terenów zurbanizowanych wymaga współdziałania na wielu płaszczyznach pomiędzy władzami krajowymi, lokalnymi oraz prywatnymi właścicielami gruntów [21]. Bez koordynacji działań między różnymi grupami nie zostanie osiągnięty cel zwiększenia bezpieczeństwa terenów zurbanizowanych, i tym samym minimalizowania strat gospodarczych i ekologicznych.

Podsumowanie

Analiza wybranych międzynarodowych wytycznych i norm dotyczących zarządzania strefą styku terenów zurbanizowanych i leśnych (WUI) wskazuje, że kluczowym elementem ograniczania strat pożarowych jest zintegrowane podejście łączące planowanie przestrzenne i inżynierię budowlaną. Państwa mające doświadczenie w walce z pożarami roślinności wypracowały standardy techniczne, które kładą nacisk na ochronę budynków przed przemieszczającymi się iskrami i żagwiami oraz opracowały zasady gospodarowania roślinnością w sąsiedztwie budynków. Porównanie rozwiązań z różnych regionów świata potwierdza uniwersalność pewnych zasad, takich jak eliminacja materiałów palnych w bezpośrednim sąsiedztwie ścian budynków czy odpowiednie planowanie przestrzenne na terenach przylegających do zabudowy. W Europie niektóre kraje rozpoczęły opracowywanie wytycznych mających na celu zwiększenie bezpieczeństwa mieszkańców terenów zurbanizowanych sąsiadujących z terenami zielonymi. W Polsce zasadne jest prowadzenie działań na rzecz podnoszenia świadomości społecznej

integration of preventative activities into urban policy so that new and upgraded developments are resistant to fire hazards.

Conclusions and recommendations

Based on the conducted analysis, conclusions and recommendations are formulated for practical implementation in Poland:

1. Develop a set of good practices and recommendations for managing vegetation in urban areas adjacent to forests, agricultural areas and other green areas. Standardise several zones near residential and utility buildings in provisions.
2. Educate different social and professional groups to raise awareness of proper vegetation management in urban areas adjacent to forest and agricultural areas. Emphasise garden infrastructure planning and restricting the use of alien plant species that have a high content of essential oils and accumulate dead organic matter in education programmes.
3. Conducting activities to increase safety in urban zone adjacent to forest and agricultural areas requires coordination between national authorities, local authorities and property owners.

List of abbreviations

BAL	Bushfire Attack Level
BAL-LOW	Bushfire Attack Level – Low
BAL-FZ	Bushfire Attack Level – Flame Zone
CONAF	Corporación Nacional Forestal, National Forest Organisation in Chile
FEMA	Federal Emergency Management Agency in the USA
IBHS	Insurance Institute for Business and Home Safety
SGIFR	Sistema de Gestão Integrada de Fogos Rurais, Integrated Rural Fire Management System
WUI	wildland–urban interface, developed areas adjacent to vegetation areas

w zakresie bezpieczeństwa pożarowego, wzorując się na opisanych w artykule dokumentach. Odpowiednio zagospodarowana przestrzeń wokół budynków to nie tylko wyższe standardy przeciwpożarowe, ale także większe bezpieczeństwo mieszkańców i strażaków. Istotnym aspektem jest integracja działań prewencyjnych z polityką urbanistyczną, aby nowa i modernizowana zabudowa powstawała w sposób odporny na zagrożenia pożarowe.

Wnioski i rekomendacje

Na podstawie przeprowadzonej analizy sformułowano wnioski i rekomendacje, jakie można wprowadzić do praktyki w Polsce:

1. Stworzenie zbioru dobrych praktyk i rekomendacji dotyczących zarządzania roślinnością na terenach zurbanizowanych sąsiadujących z lasami, terenami rolniczymi lub innymi obszarami zielonymi. W zapisach należy ustanawiać kilka stref w pobliżu budynków mieszkalnych i gospodarczych.
2. Prowadzenie edukacji dla różnych grup społecznych i zawodowych w celu podniesienia świadomości dotyczącej właściwego gospodarowania roślinnością na terenach zurbanizowanych sąsiadujących z terenami leśnymi i rolniczymi. W programach edukacyjnych należy zwrócić uwagę także na planowanie infrastruktury ogrodowej oraz ograniczanie stosowania gatunków roślin obcego pochodzenia, charakteryzujących się dużą zawartością olejów eterycznych i akumulujących martwą materię organiczną.
3. Prowadzenie działań na rzecz podnoszenia bezpieczeństwa w strefie zurbanizowanej sąsiadującej z terenami leśnymi i rolniczymi wymaga koordynacji pomiędzy władzami krajowymi, lokalnymi oraz właścicielami gruntów.

Wykaz skrótów

BAL	Bushfire Attack Level, poziom pożaru buszu
BAL-LOW	Bushfire Attack Level – Low, niski poziom pożaru buszu
BAL-FZ	Bushfire Attack Level – Flame Zone, wysoki poziom pożaru buszu
CONAF	Corporación Nacional Forestal, Narodowa Organizacja Leśna w Chile
FEMA	Federal Emergency Management Agency, Amerykańska Federalna Agencja Zarządzania Kryzysowego
IBHS	Insurance Institute for Business and Home Safety, Instytut Ubezpieczeń Bezpieczeństwa Biznesu i Domu
SGIFR	Sistema de Gestão Integrada de Fogos Rurais, Zintegrowany System Zarządzania Pożarami Wiejskimi
WUI	wildland–urban interface, tereny zabudowane sąsiadujące z obszarami pokrytymi roślinnością

AI Use Statement

The author declare that artificial intelligence tools were used in the preparation of this article only within the scope indicated below:

- language and stylistic verification of the manuscript,
- searching for and identifying potential bibliographic sources.

The author takes full responsibility for the content of the publication, including the scientific accuracy, interpretation of results, and final editing of the manuscript. Artificial intelligence tools were used solely as supporting instruments.

The journal's editorial policy prohibits the uncritical copying of AI-generated content and its inclusion in a publication without proper critical analysis, verification, and revision by the author(s).

Oświadczenie dotyczące wykorzystania AI

Autor oświadcza, że w procesie przygotowania niniejszego artykułu wykorzystano narzędzia oparte na sztucznej inteligencji wyłącznie w zakresie wskazanym poniżej:

- weryfikacja językowa i stylistyczna tekstu (InstaText),
- wyszukiwanie i identyfikacja potencjalnych źródeł bibliograficznych (Google Scholar).

Autor ponosi pełną odpowiedzialność za treść publikacji, w tym za poprawność merytoryczną, interpretację wyników oraz ostateczną redakcję tekstu. Narzędzia sztucznej inteligencji były wykorzystywane wyłącznie jako narzędzia pomocnicze.

Polityka redakcyjna czasopisma zabrania bezrefleksyjnego kopiowania treści wygenerowanych przez narzędzia AI oraz pozostawiania ich w publikacji bez krytycznej analizy, weryfikacji i redakcji przez autora(ów).

Literature / Literatura

- [1] Kelley D.I., Burton C., Di Giuseppe et al., *State of Wildfires 2024–2025*, „Earth System Science Data” 2025, 17, 5377–5488, <https://doi.org/10.5194/essd-17-5377-2025>.
- [2] Elmqvist T., Valkó O., Stoof C. et al., *Changing Wildfires: Policy Options for a Fire-literate and Fire-adapted Europe*, EASAC policy report 48, 2025, ISBN 978-3-7001-9739-3, https://easac.eu/fileadmin/user_upload/EASAC_Wildfires_final_290525.pdf [dostęp: 22.01.2026].
- [3] Hettiarachchi S., Wasko C., Sharma A., *Do Longer Dry Spells Associated With Warmer Years Compound the Stress on Global Water Resources?*, „Earth's Future” 2022, 10, 2, <https://doi.org/10.1029/2021EF002392>.
- [4] Ghazi B., Salehi H., Przybylak R., Pospieszńska A., *Projection of climate change impact on the occurrence of drought events in Poland*, „Scientific Reports” 2025, 15, 5609, <https://doi.org/10.1038/s41598-025-90488-0>.
- [5] Knapp E.E., Valachovic Y.S., Quarles S.L., Johnson N.G., *Housing arrangement and vegetation factors associated with single-family home survival in the 2018 Camp Fire, California*, „Fire Ecology” 2021, 17, 25, <https://doi.org/10.1186/s42408-021-00117-0>.
- [6] Syphard A.D., Rustigian-Romsos H., Mann M., Conlisk E., Moritz M.A., Ackerly D., *The relative influence of climate and housing development on current and projected future fire patterns and structure loss across three California landscapes*, „Global Environmental Change” 2019, 56, 41–55, <https://doi.org/10.1016/j.gloenvcha.2019.03.007>.
- [7] Radeloff V.C., Hammer R.B., Stewart S.I., Holcomb S.S., McKeefry J.F., *The wildland–urban interface in the United States*, „Ecological Applications” 2005, 15, 799–805, <https://doi.org/10.1890/04-1413>.
- [8] Tang W., Emmons L.K., Wiedinmyer C. et al., *Disproportionately large impacts of wildland-urban interface fire emissions on global air quality and human health*, „Science Advances” 2025, 11, 11, <https://doi.org/10.1126/sciadv.adr2616>.
- [9] Bar-Massada A., Radeloff V.C., Stewart S.I., *Biotic and Abiotic Effects of Human Settlements in the Wildland–Urban Interface*, „BioScience” 2014, 64, 5, 429–437, <https://doi.org/10.1093/biosci/biu039>.
- [10] Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz.U. 2002 Nr 75, poz. 690).
- [11] *Builder's Guide to Construction in Wildfire Zones*, FEMA P-737, 2025, https://www.fema.gov/sites/default/files/documents/fema_building-science_builders-guide-construction-wildfire-zones_p-737.pdf [dostęp: 23.01.2026].
- [12] *Model Ordinance for Construction in WUI Area*, Insurance Institute for Business and Home Safety, 2023, https://ibhs.org/wp-content/uploads/Wildfire_model_ordinances-in-WUI.pdf [dostęp: 23.01.2026].
- [13] Departamento de Prevención de Incendios Forestales – CONAF, *Manual Comunitario de Prevención de Incendios Forestales*, 2022, https://oficinavirtual.conaf.cl/archivos/recursos/insumos_tecnicos/Proteccion%20de%20Incendios%20Forestales/Manual%20comunitario%202022.pdf [dostęp: 21.01.2026].
- [14] *Guía para la prevención de incendios de interfaz*, 2002, República Argentina, https://www.argentina.gob.ar/sites/default/files/guia_para_prevenccion_de_incendios_de_interfase.pdf [dostęp: 22.01.2026].
- [15] AS 3959:2018 *Construction of buildings in bushfire-prone areas*, Standards Australia Committee.
- [16] *Building with Timber – Construction requirements for Bushfire Attack Levels as per AS 3959-2018*, 2018, <https://wpv.org.au/wp-content/uploads/2020/02/Building-with-Timber-%E2%80%93-Construction-requirements-for-Bushfire-Attack-Levels.pdf> [dostęp: 21.01.2026].
- [17] *Guía para la elaboración de políticas municipales y planes locales de actuación ante el riesgo de incendios forestales en la interfaz urbano-forestal*, Federación Española de

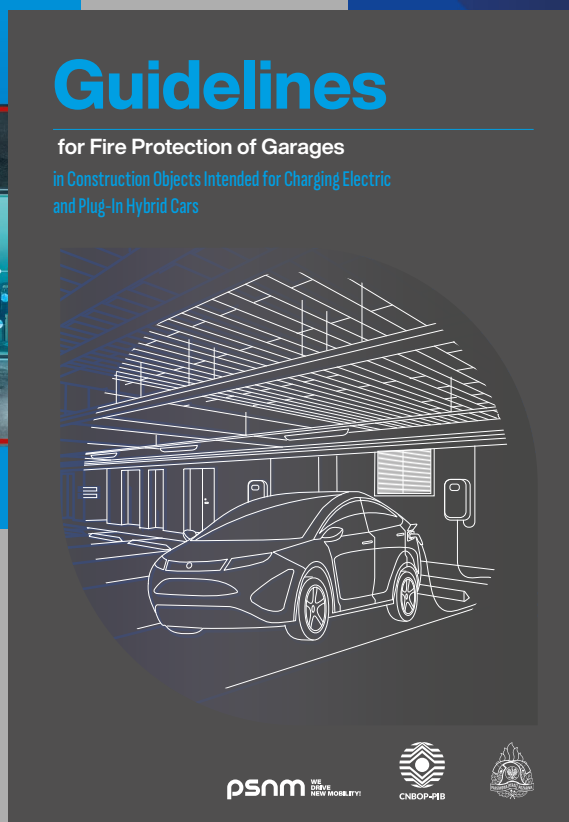
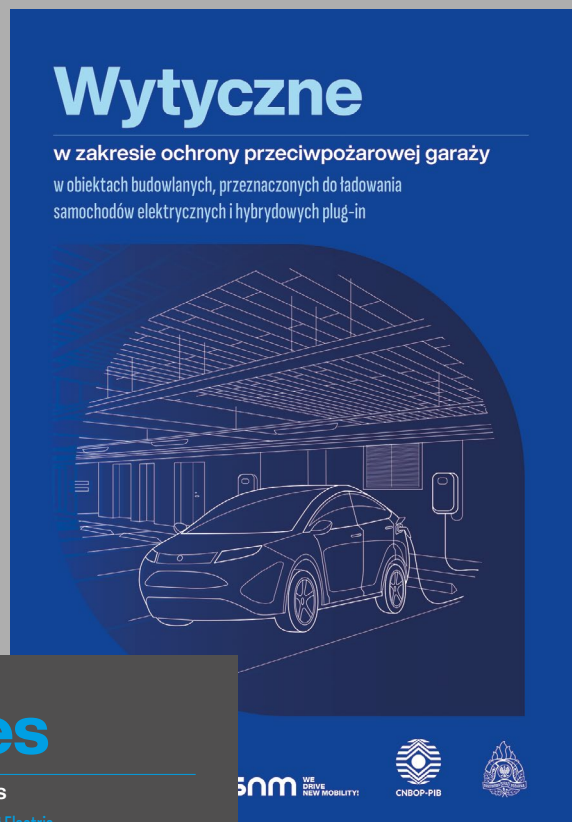
- Municipios y Provincias, 2025 [dostęp: 23.01.2026].
- [18] *Building wildfire resilience into forest management planning. Practice Guide*, Forestry Commission, 2014, <https://www.forestryresearch.gov.uk/publications/building-wildfire-resilience-into-forest-management-planning/> [dostęp: 20.01.2026].
- [19] Qin Y., Purnomo D.M.J., Theodori M. et al., *Simulations of firebrand-driven fire spread in landscape-scale Wildland-Urban-Interface (WUI) and urban conflagration models*, „Fire Safety Journal” 2026, 162, 104686, <https://doi.org/10.1016/j.firesaf.2026.104686>.
- [20] Zheng A., Ba R., Jiang W. et al., *Intelligent fire modeling in wildland-urban interface: A comprehensive review of current progress, challenges, and future perspectives*, „Journal of Safety Science and Resilience” 2026, 7, 2, 100252, <https://doi.org/10.1016/j.jnlssr.2025.100252>.
- [21] *The National Cohesive Wildland Fire Management Strategy. The Final Phase in the Development of the National Cohesive Wildland Fire Management Strategy*, 2014 [dostęp: 20.01.2026].
- [22] Godet J.D., *Atlas drewna*, Wyd. Multico, Warszawa 2008.
- [23] <https://www.sgifr.gov.pt/gestao-de-combustivel> [dostęp: 23.01.2026].

ŁUKASZ TYBURSKI, PH.D. ENG. – employee of the Forest Research Institute, Laboratory of Forest Fire Protection. His interests are related to the fire protection of different forms of natural conservation. He is the administrator of the National Forest Fire Information System.

DR INŻ. ŁUKASZ TYBURSKI – pracownik Instytutu Badawczego Leśnictwa, Laboratorium Ochrony Przeciwpowarowej Lasu. Jego zainteresowania związane są z ochroną przeciwpożarową różnych form ochrony przyrody. Jest administratorem Krajowego Systemu Informacji o Pożarach Lasów.



Wytyczne CNBOP-PIB



<https://online.cnbop.pl>

Tomasz Krasowski

Decontext Polska

Corresponding author / Autor korespondencyjny: tomasz@decontext.pl

Firefighter Operational Hygiene as a System for Reducing Secondary Exposure to Hazardous Substances Present in the Fire Environment – Review of Scientific Evidence and Normative Documents

Higiena operacyjna strażaka jako system ograniczania wtórnej ekspozycji na substancje niebezpieczne obecne w środowisku pożaru – przegląd dowodów naukowych i dokumentów normatywnych

ABSTRACT

Purpose: The purpose of the study is to provide a synthetic and critical analysis of the phenomenon of secondary exposure of firefighters to the hazardous substances present in the fire environment and to identify effective strategies to reduce that risk in systemic terms, including personal protective equipment management.

Methodology: The conducted integrated structure narrative review covered the analysis of scientific literature (field studies, laboratory experiments, biomonitoring studies), institutional reports and normative documents (PN-EN 469, PN-EN ISO 13688, ISO 23616, NFPA 1851). The analysis focused on the mechanisms of contamination of protective clothing, routes of secondary exposure and effectiveness of technical and organisational interventions.

Results: The analysis demonstrated that the secondary exposure of firefighters is multi-stage in nature and covers the subsequent phases of the operational cycle – from the incident scene, through transport and fire station functioning, to the re-use of protective clothing. Empirical studies confirm that individual interventions, such as preliminary decontamination, organisational changes or specific cleaning methods, lead to a partial reduction of the contamination level, however their effectiveness is usually limited to selected stages of the process and does not permanently reduce the total health risk.

Conclusions: Effective reduction of the secondary exposure of firefighters requires the implementation of an integrated system including technical, organisational, procedural, training and supervisory activities at all stages of the operational cycle. In this context, an important role is played by personal protective equipment management, including the application of validated decontamination processes, as part of long-term health prevention.

Keywords: operational hygiene, secondary exposure, personal protective equipment, fire service, decontamination, PPE, contamination control

Type of article: review article

Received: 09.03.2026; Reviewed: 14.04.2026; Accepted: 14.04.2026;

Author's ORCID ID: T. Krasowski – 0009-0006-7958-5065;

Please cite as: Safety & Fire Technology 2026, 1, 146–161, <https://doi.org/10.12845/sft.67.1.2026.7>;

This is an open access article under the CC BY-SA 4.0 license (<https://creativecommons.org/licenses/by-sa/4.0/>).

ABSTRAKT

Cel: Celem pracy jest syntetyczna i krytyczna analiza zjawiska wtórnej ekspozycji strażaków na substancje niebezpieczne obecne w środowisku pożaru oraz identyfikacja skutecznych strategii ograniczania tego ryzyka w ujęciu systemowym, z uwzględnieniem zarządzania środkami ochrony indywidualnej.

Metodologia: Przeprowadzono przegląd narracyjny o strukturze integracyjnej, obejmujący analizę literatury naukowej (badania terenowe, eksperymenty laboratoryjne, badania biomonitoringowe), raportów instytucjonalnych oraz dokumentów normatywnych (PN-EN 469, PN-EN ISO 13688, ISO 23616, NFPA 1851). Analiza koncentrowała się na mechanizmach skażenia odzieży ochronnej, drogach wtórnej ekspozycji oraz skuteczności interwencji technicznych i organizacyjnych.

Wyniki: Analiza wykazała, że wtórna ekspozycja strażaków ma charakter wieloetapowy i obejmuje kolejne fazy cyklu operacyjnego – od miejsca zdarzenia, poprzez transport i funkcjonowanie jednostki, aż po ponowne użytkowanie odzieży ochronnej. Badania empiryczne potwierdzają, że pojedyncze interwencje, takie jak dekontaminacja wstępna, zmiany organizacyjne czy określone metody czyszczenia, prowadzą do częściowej redukcji poziomu skażeń, jednak ich skuteczność ogranicza się zazwyczaj do wybranych etapów procesu i nie zapewnia trwałej redukcji całkowitego ryzyka zdrowotnego.

Wnioski: Skuteczne ograniczanie wtórnej ekspozycji strażaków wymaga wdrożenia zintegrowanego systemu obejmującego działania techniczne, organizacyjne, proceduralne, szkoleniowe i nadzorcze na wszystkich etapach cyklu operacyjnego. W tym kontekście istotną rolę odgrywa zarządzanie środkami ochrony indywidualnej, w tym stosowanie zwalidowanych procesów dekontaminacji, jako elementu długoterminowej profilaktyki zdrowotnej.

Słowa kluczowe: higiena operacyjna, wtórna ekspozycja, środki ochrony indywidualnej, straż pożarna, dekontaminacja, ŚOI, kontrola skażeń

Typ artykułu: artykuł przeglądowy

Przyjęty: 09.03.2026; **Zrecenzowany:** 14.04.2026; **Zaakceptowany:** 14.04.2026;

Identyfikator ORCID autora: T. Krasowski – 0009-0006-7958-5065;

Proszę cytować: Safety & Fire Technology 2026, 1, 146–161, <https://doi.org/10.12845/sft.67.1.2026.7>;

Artykuł udostępniany na licencji CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>).

Introduction

The occupational exposure of firefighters to the hazardous substances present in the fire environment is the subject of intensive epidemiological and toxicological studies. The International Agency for Research on Cancer (IARC) classified it as carcinogenic for humans (group 1) [1], while clearly pointing to the confirmed increase of the risk of specific cancers in that professional group.

The fire environment is characterised by the presence of a complex mixture of chemical substances produced by combustion of natural and synthetic materials. Literature points to the presence of e.g. polycyclic aromatic hydrocarbons (PAH), volatile and semi-volatile organic compounds, soot particles, heavy metals and per- and polyfluoroalkyl substances (PFAS) that may be toxic, mutagenic and carcinogenic [2–4].

The exposure of firefighters is not exclusively limited to the phase of direct firefighting operations. Literature increasingly notes the phenomenon of secondary exposure, understood as exposure to hazardous substances after the completion of operational activities, arising from the contact with contaminated protective clothing, equipment, surfaces and infrastructure of rescue units. These mechanisms include i.a. skin exposure, off-gassing and cross-contamination [5–7].

Biomonitoring studies confirm that secondary exposure has a real and measurable significance. The presence of PAH metabolites was found in biological samples from firefighters after firefighting operations (even when using respiratory protection) [6], [8–9]. These results show that routes other than inhalation, in particular skin contact, may have a significant impact on the total exposure dose.

The existing publications are most often focused on selected aspects of the problem, such as the effectiveness of specific decontamination methods, contamination levels of textile materials, biomonitoring results or the evaluation of individual organisational interventions. Thus, literature provides a large amount of partial data on specific components of the exposure process. At the same time, attempts are rarely made to integrate it into a consistent risk management model, covering the entire operational cycle of rescue and firefighting operations.

Consequently, the action taken in practice is often fragmented, despite the multi-stage and systemic nature of secondary exposure. Bridging that gap requires a systematic analysis of available scientific evidence and normative documents

Wprowadzenie

Ekspozycja zawodowa strażaków na substancje niebezpieczne obecne w środowisku pożaru stanowi przedmiot intensywnych badań epidemiologicznych i toksykologicznych. Międzynarodowa Agencja Badań nad Rakiem (IARC) zaklasyfikowała ją jako rakotwórczą dla ludzi (grupa 1) [1], wskazując na jednoznacznie potwierdzony wzrost ryzyka wybranych nowotworów w tej grupie zawodowej.

Środowisko pożaru charakteryzuje się obecnością złożonej mieszaniny substancji chemicznych powstających w wyniku spalania materiałów naturalnych i syntetycznych. W literaturze wskazuje się na obecność m.in. wielopierścieniowych węglowodorów aromatycznych (WWA/PAH), lotnych i półlotnych związków organicznych, cząstek sadzy, metali ciężkich oraz związków per- i polifluoroalkilowych (PFAS), które mogą wykazywać działanie toksyczne, mutagenne i kancerogenne [2–4].

Ekspozycja strażaków nie ogranicza się wyłącznie do fazy bezpośrednich działań gaśniczych. Coraz większą uwagę w literaturze zwraca się na zjawisko wtórnej ekspozycji, rozumianej jako narażenie na substancje niebezpieczne po zakończeniu działań operacyjnych, wynikające z kontaktu ze skażoną odzieżą ochronną, sprzętem, powierzchniami oraz infrastrukturą jednostek ratowniczych. Mechanizmy te obejmują m.in. ekspozycję dermalną, zjawisko *off-gassing* oraz przenoszenie krzyżowe (ang. *cross-contamination*) [5–7].

Badania biomonitoringowe potwierdzają, że wtórna ekspozycja ma wymiar rzeczywisty i mierzalny. Obecność metabolitów WWA/PAH stwierdzono w próbkach biologicznych strażaków pobranych po działaniach gaśniczych (nawet przy stosowaniu ochrony dróg oddechowych) [6], [8–9]. Wyniki te wskazują, że drogi inne niż inhalacyjne – w szczególności kontakt dermalny – mogą w istotny sposób wpływać na całkowitą dawkę narażenia.

Dotychczasowe publikacje koncentrują się najczęściej na wybranych aspektach problemu, takich jak skuteczność określonych metod dekontaminacji, poziomy skażenia materiałów tekstylnych, wyniki biomonitoringu czy ocena pojedynczych interwencji organizacyjnych. Literatura dostarcza zatem licznych danych cząstkowych dotyczących poszczególnych elementów procesu narażenia. Rzadziej podejmuje się próby ich integracji w spójny model zarządzania ryzykiem obejmujący cały cykl operacyjny działań ratowniczo-gaśniczych.

W konsekwencji praktyczne działania są fragmentaryczne, mimo że zjawisko wtórnej ekspozycji ma charakter wieloetapowy

and integration into a consistent secondary exposure reduction model, including the technical, organisational and formal conditions.

In this study, it is assumed that firefighter operational hygiene is an integrated system of technical, organisational, procedural, training and supervisory activities aimed at reducing the secondary exposure to the hazardous substances present in the fire environment. This system covers the entire operational cycle, from the incident scene, through transport and fire station functioning, to personal protective equipment management, cleaning and decontamination processes, as well as shaping hazard awareness and supervising the compliance with the adopted procedures.

Purpose of the study and research question

The purpose of this study is critical analysis of the available scientific documents and normative documents on the reduction of secondary exposure of firefighters to the hazardous substances present in the fire environment, as well as integration of dispersed research results into a cohesive systemic model of firefighter operational hygiene.

Secondary exposure, understood as exposure to hazardous substances after the completion of direct firefighting operations, arising from the contact with contaminated protective clothing, equipment, surfaces and fire station infrastructure, is multi-stage and multi-factor in nature. Scientific literature describes many interventions reducing the contamination level, such as preliminary decontamination, organisational changes, cleaning of protective clothing or modifications to fire station infrastructure. However, there is no synthetic evaluation of whether these interventions, used individually, permanently reduce the health risk.

Therefore, the following research question was formulated: Does effective and sustained reduction of the secondary exposure of firefighters require implementing an integrated system covering technical, organisational and procedural activities at all stages of the operational cycle or can it be achieved by using individual interventions at point level?

The assumed thesis was that the reduction of secondary exposure was systemic in nature and required implementing an integrated model covering the entire operational cycle, from the incident scene, through transport and fire station functioning, to personal protective equipment management and their cleaning and decontamination processes.

The fulfilment of the purpose of the study includes:

- the identification of the secondary exposure mechanisms described in literature,
- the analysis of effectiveness of individual technical and organisational interventions,
- the summary of requirements arising from normative documents,
- the integration of dispersed evidence into a cohesive systemic model of firefighter operational hygiene.

i systemowy. Wypełnienie tej luki wymaga syntetycznej analizy dostępnych dowodów naukowych oraz dokumentów normatywnych i ich integracji w spójny model ograniczania wtórnej ekspozycji, uwzględniający uwarunkowania zarówno techniczne, organizacyjne, jak i formalne.

W niniejszej pracy przyjęto, że higiena operacyjna strażaka oznacza zintegrowany system działań technicznych, organizacyjnych, proceduralnych, szkoleniowych i nadzorczych, ukierunkowanych na ograniczanie wtórnej ekspozycji na substancje niebezpieczne obecne w środowisku pożaru. System ten obejmuje cały cykl operacyjny – od miejsca zdarzenia, poprzez transport i funkcjonowanie jednostki, aż po zarządzanie środkami ochrony indywidualnej, procesy ich czyszczenia i dekontaminacji oraz kształtowanie świadomości zagrożeń i nadzór nad przestrzeganiem przyjętych procedur.

Cel pracy i pytanie badawcze

Celem niniejszej pracy jest krytyczna analiza dostępnych dowodów naukowych oraz dokumentów normatywnych dotyczących ograniczania wtórnej ekspozycji strażaków na substancje niebezpieczne obecne w środowisku pożaru, a także integracja rozproszonych wyników badań w spójny model systemowy higieny operacyjnej strażaka.

Wtórna ekspozycja, rozumiana jako narażenie na substancje niebezpieczne po zakończeniu bezpośrednich działań gaśniczych – wynikające z kontaktu ze skażoną odzieżą ochronną, sprzętem, powierzchniami oraz infrastrukturą jednostki, ma charakter wieloetapowy i wieloczynnikowy. Literatura naukowa opisuje liczne interwencje ograniczające poziom skażeń, takie jak dekontaminacja wstępna, zmiany organizacyjne, czyszczenie odzieży ochronnej czy modyfikacje infrastruktury jednostek. Brakuje jednak syntetycznej oceny, czy działania te – stosowane pojedynczo – zapewniają trwałą redukcję ryzyka zdrowotnego.

W związku z powyższym sformułowano następujące pytanie badawcze: Czy skuteczna i trwała redukcja wtórnej ekspozycji strażaków wymaga wdrożenia zintegrowanego systemu obejmującego działania techniczne, organizacyjne i proceduralne na wszystkich etapach cyklu operacyjnego, czy też możliwa jest poprzez stosowanie pojedynczych interwencji o charakterze punktowym?

Przyjęto tezę, że ograniczanie wtórnej ekspozycji ma charakter systemowy i wymaga wdrożenia zintegrowanego modelu obejmującego cały cykl operacyjny – od miejsca zdarzenia, poprzez transport i funkcjonowanie jednostki, po zarządzanie środkami ochrony indywidualnej oraz procesy ich czyszczenia i dekontaminacji.

Realizacja celu pracy obejmuje:

- identyfikację mechanizmów wtórnej ekspozycji opisanych w literaturze,
- analizę skuteczności pojedynczych interwencji technicznych i organizacyjnych,
- zestawienie wymagań wynikających z dokumentów normatywnych,
- integrację rozproszonych dowodów w spójny model systemowy higieny operacyjnej strażaka.

Methods of literary review

Literary review was conducted in a systematic and integrated manner, covering scientific publications and normative documents related to the secondary exposure of firefighters to the hazardous substances present in the fire environment.

The analysis was based on publications indexed in Web of Science, Scopus and PubMed databases, supplemented by reports of scientific institutions and sectoral organisations (i.a. NIOSH, IARC, NFPA) and normative documents (PN-EN, ISO).

The temporal range of the review covered 2010–2025, including in particular the publications of recent years, reflecting the current knowledge. In the query process, keywords in English were used, including i.a.: *firefighter exposure, secondary exposure, PPE contamination, decontamination, PAH, VOC, PFAS, laundering, off-gassing, fire station contamination*. In addition, the citation analysis method (the so-called *snowball method*) was used to identify significant thematically-related publications.

The analysis included publications meeting the following criteria:

- related to the exposure of firefighters to hazardous substances,
- related to the mechanisms of secondary exposure or contamination of protective clothing,
- including the results of empirical studies, systematic reviews or expert analyses,
- related to the methods of cleaning, decontamination or organisation of processes related to PPE management.

The following publications were excluded:

- only technological in nature, unrelated to occupational exposure,
- related to other professional groups, with results irrelevant to the fire service,
- non-compliant with qualitative criteria (e.g. no methodological data).

The analysis was qualitative and integrated in nature. The results of individual studies were compared for:

- identified mechanisms of exposure,
- level and type of detected contaminants,
- effectiveness of used interventions,
- methodological limitations.

On that basis, the available evidence was synthesised and integrated with the requirements arising from normative documents, which enabled developing a cohesive systemic model of firefighter operational hygiene.

Characteristics of secondary exposure of firefighters

Mechanisms of contamination in fire environment

The fire environment is a complex physical and chemical system, producing a broad spectrum of hazardous substances as a result of incomplete combustion of natural and synthetic materials. They include i.a. polycyclic aromatic hydrocarbons (PAH), volatile and semi-volatile organic compounds (VOC and SVOC),

Metodyka przeglądu literatury

Przegląd literatury przeprowadzono w sposób systematyczny i integracyjny, obejmujący publikacje naukowe oraz dokumenty normatywne dotyczące wtórnej ekspozycji strażaków na substancje niebezpieczne obecne w środowisku pożaru.

Analizę oparto na publikacjach indeksowanych w bazach Web of Science, Scopus oraz PubMed, uzupełnionych o raporty instytucji naukowych i organizacji branżowych (m.in. NIOSH, IARC, NFPA) oraz dokumenty normatywne (PN-EN, ISO).

Zakres czasowy przeglądu obejmował lata 2010–2025, ze szczególnym uwzględnieniem publikacji z ostatnich lat, odzwierciedlających aktualny stan wiedzy. W procesie wyszukiwania zastosowano słowa kluczowe w języku angielskim, obejmujące m.in.: *firefighter exposure, secondary exposure, PPE contamination, decontamination, PAH, VOC, PFAS, laundering, off-gassing, fire station contamination*. Dodatkowo przeprowadzono analizę cytowań (tzw. *snowball method*), umożliwiającą identyfikację istotnych publikacji powiązanych tematycznie.

Do analizy włączano publikacje spełniające następujące kryteria:

- dotyczyły ekspozycji strażaków na substancje niebezpieczne,
- odnosiły się do mechanizmów wtórnej ekspozycji lub kontaminacji odzieży ochronnej,
- zawierały wyniki badań empirycznych, przeglądów systematycznych lub analiz eksperckich,
- dotyczyły metod czyszczenia, dekontaminacji lub organizacji procesów związanych z zarządzaniem ŚOI.

Wykluczono publikacje:

- o charakterze wyłącznie technologicznym, niezwiązane z ekspozycją zawodową,
- dotyczące innych grup zawodowych bez możliwości odniesienia wyników do straży pożarnej,
- niespełniające kryteriów jakościowych (np. brak danych metodologicznych).

Analiza miała charakter jakościowy i integracyjny. Wyniki poszczególnych badań porównywano pod kątem:

- identyfikowanych mechanizmów ekspozycji,
- poziomu i rodzaju wykrywanych zanieczyszczeń,
- skuteczności stosowanych interwencji,
- ograniczeń metodologicznych.

Na tej podstawie dokonano syntezy dostępnych dowodów oraz ich integracji z wymaganiami wynikającymi z dokumentów normatywnych, co umożliwiło opracowanie spójnego modelu systemowego higieny operacyjnej strażaka.

Charakterystyka wtórnej ekspozycji strażaków

Mechanizmy skażenia w środowisku pożaru

Środowisko pożaru stanowi złożony układ fizykochemiczny, w którym wskutek niecałkowitego spalania materiałów naturalnych i syntetycznych powstaje wiele substancji niebezpiecznych. Wśród nich znajdują się m.in. wielopierścieniowe węglowodory aromatyczne (WWA/PAH), lotne i półlotne związki organiczne

soot particles, heavy metals and per- and polyfluoroalkyl substances (PFAS), characterised by high environmental sustainability and bioaccumulation capability, which distinguishes them from many other combustion products and could influence the long-term nature of exposure [3], [11].

Combustion products are deposited on the surface of protective clothing, equipment and skin of firefighters as a result of condensation, adsorption and particle deposition processes. These contaminants are not subject to automatic degradation after the completion of operations, but they may remain on the surface and in the structure of materials for a long time, turning the personal protective equipment a source of secondary exposure [5], [7].

Routes of secondary exposure

The secondary exposure of firefighters includes multiple complementary mechanisms of exposure:

1. Skin exposure – skin contact with contaminated protective clothing, equipment or surfaces. The research conducted by Fent et al. [6], [10], demonstrated that despite using respiratory protection equipment significant skin contamination occurs and skin absorption could be a significant component of the total exposure dose.
2. Off-gassing – the process of releasing volatile organic compounds (VOC) from contaminated clothing after the completion of firefighting operations. This phenomenon leads to the secondary contamination of air in vehicle cabs and fire station rooms [5], [7].
3. Cross-contamination – transfer of contaminants between clothing, equipment and work environment, including work surfaces and social areas.

Empirical studies show that listed mechanisms may occur in parallel, also leading to persistent exposure after the completion of operational activities. A schematic view of the chain of secondary exposure of the firefighter, including the subsequent stages of the transfer of contaminants in the operational cycle, presented in Figure 1.

(VOC i SVOC), cząstki sadzy, metale ciężkie oraz związki per- i polifluoroalkilowe (PFAS), charakteryzujące się wysoką trwałością środowiskową oraz zdolnością do bioakumulacji, co odróżnia je od wielu innych produktów spalania i może wpływać na długoterminowy charakter narażenia [3], [11].

Produkty spalania osadzają się na powierzchni odzieży ochronnej, sprzętu oraz skóry strażaków w wyniku procesów kondensacji, adsorpcji oraz depozycji cząstek. Zanieczyszczenia te nie ulegają samoistnej degradacji po zakończeniu działań, lecz mogą utrzymywać się na powierzchni i w strukturze materiałów przez dłuższy czas, czyniąc środki ochrony indywidualnej wtórnym źródłem ekspozycji [5], [7].

Drogi wtórnej ekspozycji

Wtórna ekspozycja strażaków obejmuje kilka uzupełniających się mechanizmów narażenia:

1. Ekspozycja dermalna – kontakt skóry ze skażoną odzieżą ochronną, sprzętem lub powierzchniami. Badania prowadzone przez Fent i wsp. [6], [10] wykazały, że pomimo stosowania aparatów ochrony dróg oddechowych dochodzi do istotnej kontaminacji skóry, a absorpcja dermalna może stanowić znaczący komponent całkowitej dawki narażenia.
2. *Off-gassing* – proces uwalniania lotnych związków organicznych (VOC) ze skażonej odzieży po zakończeniu działań gaśniczych. Zjawisko to prowadzi do wtórnego zanieczyszczenia powietrza w kabinach pojazdów oraz pomieszczeniach jednostek [5], [7].
3. Przenoszenie krzyżowe (ang. *cross-contamination*) – transfer zanieczyszczeń pomiędzy odzieżą, sprzętem oraz środowiskiem pracy, w tym powierzchniami użytkowymi i strefami socjalnymi.

Badania empiryczne wskazują, że wymienione mechanizmy mogą występować równolegle, prowadząc do utrzymywania się ekspozycji również po zakończeniu działań operacyjnych. Schematyczne ujęcie łańcucha wtórnej ekspozycji strażaka, obejmującego kolejne etapy transferu zanieczyszczeń w cyklu operacyjnym, przedstawiono na rycinie 1.

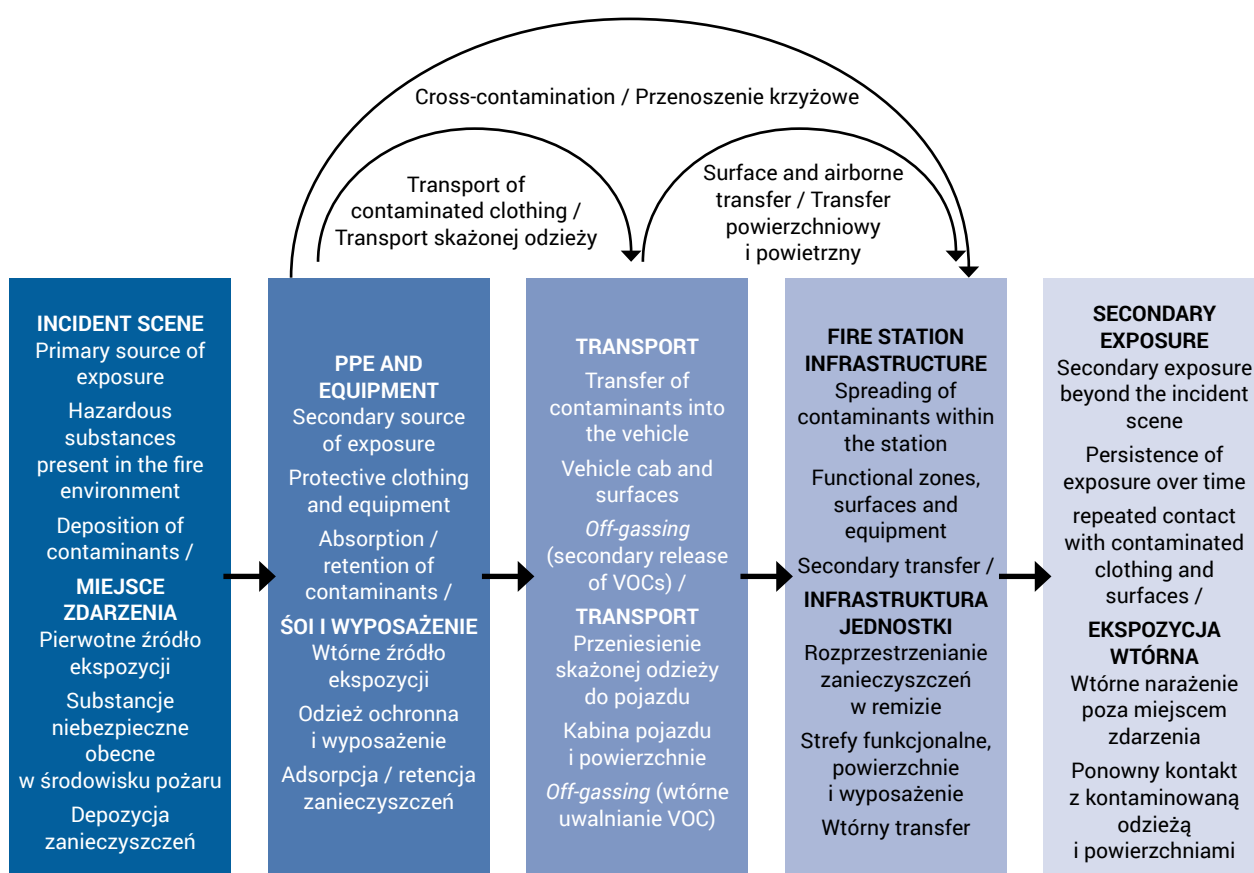


Figure 1. The chain of secondary exposure of the firefighter presenting the subsequent stages of transfer and secondary redistribution of contaminants in the operational cycle

Rycina 1. Łańcuch wtórnej ekspozycji strażaka przedstawiający kolejne etapy transferu i wtórnej redystrybucji zanieczyszczeń w cyklu operacyjnym

Source: Own elaboration.

Źródło: Opracowanie własne.

Biomonitoring and internal exposure evidence

The evidence of the significance of secondary exposure is provided by biomonitoring studies, which consist in the detection of the presence of exposure markers in biological samples from firefighters. They demonstrated that the concentration of PAH metabolites in urine of the tested personnel significantly increase after firefighting operations, even when using respiratory protection [6], [8–9]. It means that skin exposure and routes of secondary exposure may have a significant share in the total exposure of the organism.

Similarly, the presence of PFAS compounds in textile materials and biological samples indicates their capability for migration and bioaccumulation, which may be significant for health in the long-term perspective [3], [11].

Biomonitoring i dowody narażenia wewnętrznego

Dowodów na znaczenie wtórnej ekspozycji dostarczają badania biomonitoringowe, które polegają na wykrywaniu obecności markerów narażenia w próbkach biologicznych strażaków. Pokazały one, że stężenia metabolitów WWA/PAH w moczu badanych istotnie wzrastają po działaniach gaśniczych, nawet przy stosowaniu ochrony dróg oddechowych [6], [8–9]. Oznacza to, że ekspozycja dermalna oraz wtórne drogi narażenia mogą mieć istotny udział w całkowitej ekspozycji organizmu.

Podobnie, obecność związków PFAS w materiałach tekstylnych oraz próbkach biologicznych wskazuje na ich zdolność do migracji i bioakumulacji, co może mieć istotne znaczenie dla zdrowia w perspektywie długoterminowej [3], [11].

Limitations of the fragmented approach

The analysis of literature shows that most studies are focused on the assessment of the effectiveness of single interventions, such as preliminary decontamination, change of organisational practices and specific methods of cleaning of protective clothing. Although these activities lead to the measurable reduction of the

Ograniczenia podejścia fragmentarycznego

Analiza literatury wskazuje, że większość badań koncentruje się na ocenie skuteczności pojedynczych interwencji, takich jak dekontaminacja wstępna, zmiana praktyk organizacyjnych czy określone metody czyszczenia odzieży ochronnej. Choć działania te prowadzą do mierzalnej redukcji poziomu skażeń, ich

contamination level, their effectiveness is limited in nature, usually applicable to a selected stage of the process, and does not completely eliminate the contaminants or risk of secondary transfer [7], [14], [19], [21].

In the context of health risk assessment, it means that the reduction of the contamination level is not equivalent to the elimination of exposure. Thus, single interventions must be interpreted as reduction activities, not comprehensive solutions. The lack of evidence showing that isolated activities ensure a sustained reduction of the total health risk is a significant argument for the need for a systemic approach, including all stages of the operational cycle.

Hierarchy of controls as system framework for reducing the secondary exposure

Concept of hierarchy of controls

In occupational safety literature, a commonly used framework organising preventative measures is the concept of hierarchy of controls [13]. This model classifies exposure reduction measures according to their effectiveness, from the most effective (hazard elimination) to the least effective (personal protective equipment).

In classical terms, the hierarchy includes: elimination, substitution, engineering measures, administrative measures and personal protective equipment (PPE). The application of the concept to the firefighter work environment enables organising the interventions dispersed in literature and leads to the conclusion that effective control of secondary exposure requires action at multiple levels at the same time.

Elimination and substitution – reductions in operational conditions

Under rescue and firefighting operation conditions, full elimination of chemical hazards is practically impossible, because the exposure results from the nature of operations. Also substitution has application limits, although it may include systemic activities, such as limitation of the use of materials that generate toxic combustion products.

Consequently, the main burden of the reduction of exposure shifts towards engineering and administrative measures, as well as proper management of personal protective equipment.

Engineering measures

Engineering measures include technical solutions to reduce the spreading and secondary transfer of contaminants. In the practice of the fire service, it includes i.a.:

- the “clean cab” concept (spatial separation of the crew from the contaminated equipment) [16],
- ventilation and air filtering systems,
- designation of clean and dirty zones in the fire station infrastructure [17],
- separated spaces for the storage and transport of contaminated clothing [17].

These solutions do not eliminate the source of hazard, but they reduce its spreading between the subsequent stages of the operational cycle.

skuteczność ma charakter ograniczony – zazwyczaj dotyczy wybranego etapu procesu i nie eliminuje całkowicie zanieczyszczeń ani ryzyka ich wtórnego transferu [7], [14], [19], [21].

W kontekście oceny ryzyka zdrowotnego oznacza to, że redukcja poziomu skażeń nie jest równoznaczna z eliminacją narażenia. Pojedyncze interwencje należy zatem interpretować jako działania ograniczające, a nie rozwiązania kompleksowe. Brak dowodów wskazujących, że izolowane działania zapewniają trwałą redukcję całkowitego ryzyka zdrowotnego, stanowi istotny argument za koniecznością podejścia systemowego, obejmującego wszystkie etapy cyklu operacyjnego.

Hierarchia środków kontroli jako rama systemowa ograniczania wtórnej ekspozycji

Koncepcja hierarchii środków kontroli

W literaturze dotyczącej bezpieczeństwa pracy powszechnie stosowaną ramą porządkującą działania prewencyjne jest koncepcja hierarchii środków kontroli [13]. Model ten klasyfikuje środki ograniczające narażenie według ich skuteczności – od najbardziej efektywnych (eliminacja zagrożenia) po najmniej skuteczne (środki ochrony indywidualnej).

W klasycznym ujęciu hierarchia obejmuje: eliminację, substitucję, środki inżynieryjne, środki administracyjne oraz środki ochrony indywidualnej (ŚOI). Zastosowanie tej koncepcji do środowiska pracy strażaka pozwala uporządkować rozproszone w literaturze interwencje oraz prowadzi do wniosku, że skuteczna kontrola wtórnej ekspozycji wymaga działań na wielu poziomach jednocześnie.

Eliminacja i substitucja – ograniczenia w realiach operacyjnych

W warunkach działań ratowniczo-gaśniczych pełna eliminacja zagrożeń chemicznych jest w praktyce niemożliwa, ponieważ ekspozycja wynika z istoty prowadzonych działań. Substytucja również ma ograniczone zastosowanie, choć może obejmować działania systemowe, takie jak ograniczanie stosowania materiałów generujących toksyczne produkty spalania.

W konsekwencji główny ciężar redukcji ekspozycji przesuwają się w kierunku środków inżynieryjnych, administracyjnych oraz właściwego zarządzania środkami ochrony indywidualnej.

Środki inżynieryjne

Środki inżynieryjne obejmują rozwiązania techniczne ograniczające rozprzestrzenianie się zanieczyszczeń oraz ich wtórny transfer. W praktyce straży pożarnej obejmują one m.in.:

- koncepcję „clean cab” (oddzielenie przestrzeni dla załogi od skażonego sprzętu) [16],
- systemy wentylacji i filtracji powietrza,
- wyodrębnienie stref czystych i brudnych w infrastrukturze jednostki [17],
- wydzielone przestrzenie do przechowywania i transportu skażonej odzieży [17].

Rozwiązania te nie eliminują źródła zagrożenia, lecz ograniczają jego rozprzestrzenianie się pomiędzy kolejnymi etapami cyklu operacyjnego.

Administrative and organisational measures

Administrative measures include operational procedures, work organisation and training activities focused on reducing the secondary exposure. In practice, they include i.a.: preliminary decontamination at the incident scene, isolation of contaminated clothing, prohibition to transport PPE in the vehicle cab, application of the division into clean and dirty zones and the requirement of personal hygiene after operations.

Empirical studies show that these activities may lead to a measurable reduction of the level of selected exposure indicators, however their effectiveness is conditional in nature and depends on the consequences of their application and the organisational implementation level [6], [8], [14–15].

It should be emphasised that administrative measures do not remove contaminants from the structure of materials and do not eliminate the source of exposure, but only reduce their transfer. Consequently, they should be considered as system component, not as a standalone solution.

Personal protective equipment and decontamination procedures

Personal protective equipment (PPE) is the final line of protection in the control hierarchy. Their effectiveness depends not only on protection parameters, but also on the usage, maintenance and effectiveness of cleaning and decontamination processes.

Studies show that standard water washing leads to the reduction of selected contaminant levels however its effectiveness is limited in relation to some persistent substances [18–22]. In this context, it is crucial to differentiate operational soiling and contamination, as introduced, e.g., in ISO 23616 [25]. In case of contamination of protective clothing, it may be necessary to apply advanced decontamination processes, of which the effectiveness should be confirmed in a validated manner [18], [25].

It should be emphasised that even effective cleaning processes do not completely eliminate the risk of secondary exposure if they are not integrated with other system components.

Conclusions arising from the use of the hierarchy of controls

The analysis of the secondary exposure of firefighters using the concept of hierarchy of controls shows that individual activities, even locally effective, do not lead to sustained reduction of the total health risk. The effectiveness of the activities only increases if they are implemented in parallel at different levels of the system, including technical and organisational solutions, as well as personal protective equipment management. It means that the reduction of secondary exposure should be considered as a system process that requires the integration of activities at all stages of the operational cycle.

At present, secondary exposure reduction activities are primarily focused on lower hierarchy levels (administrative measures and PPE), with inadequate use of engineering and system

Środki administracyjne i organizacyjne

Środki administracyjne obejmują procedury operacyjne, organizację pracy oraz działania szkoleniowe ukierunkowane na ograniczanie wtórnej ekspozycji. W praktyce obejmują one m.in.: dekontaminację wstępną na miejscu zdarzenia, izolację skażonej odzieży, zakaz przewożenia ŚOI w kabinie pojazdu, stosowanie podziału na strefy czyste i brudne oraz obowiązek higieny osobistej po działaniach.

Badania empiryczne wskazują, że działania te mogą prowadzić do mierzalnej redukcji poziomu wybranych wskaźników narażenia, jednak ich skuteczność ma charakter warunkowy i zależy od konsekwencji ich stosowania oraz poziomu organizacyjnego wdrożenia [6], [8], [14–15].

Należy podkreślić, że środki administracyjne nie usuwają zanieczyszczeń ze struktury materiałów ani nie eliminują źródła ekspozycji, a jedynie ograniczają ich transfer. W konsekwencji powinny być traktowane jako element systemu, a nie jako rozwiązanie samodzielne.

Środki ochrony indywidualnej i procesy dekontaminacji

Środki ochrony indywidualnej (ŚOI; PPE) stanowią ostatnią linię ochrony w hierarchii kontroli. Ich skuteczność zależy nie tylko od parametrów ochronnych, lecz również od sposobu użytkowania, konserwacji oraz skuteczności procesów czyszczenia i dekontaminacji.

Badania wskazują, że standardowe pranie wodne prowadzi do redukcji poziomu wybranych zanieczyszczeń, jednak jego skuteczność jest ograniczona w odniesieniu do niektórych substancji o charakterze trwałym [18–22]. W tym kontekście kluczowe znaczenie ma rozróżnienie pomiędzy zabrudzeniem eksploatacyjnym (ang. *soiling*) a skażeniem (ang. *contamination*), wprowadzone m.in. w normie ISO 23616 [25]. W przypadku skażenia odzieży ochronnej konieczne może być zastosowanie procesów zaawansowanej dekontaminacji, których skuteczność powinna być potwierdzona w sposób zwalidowany [18], [25].

Należy podkreślić, że nawet skuteczne procesy czyszczenia nie eliminują całkowicie ryzyka wtórnej ekspozycji, jeżeli nie są zintegrowane z pozostałymi elementami systemu.

Wnioski wynikające z zastosowania hierarchii środków kontroli

Analiza wtórnej ekspozycji strażaków z wykorzystaniem koncepcji hierarchii środków kontroli wskazuje, że pojedyncze działania – nawet skuteczne lokalnie – nie prowadzą do trwałego zmniejszenia całkowitego ryzyka zdrowotnego. Skuteczność działań wzrasta dopiero w przypadku ich równoległego wdrożenia na różnych poziomach systemu, obejmujących rozwiązania techniczne, organizacyjne oraz zarządzanie środkami ochrony indywidualnej. Oznacza to, że redukcję wtórnej ekspozycji należy traktować jako proces systemowy, wymagający integracji działań na wszystkich etapach cyklu operacyjnego.

Obecnie działania ograniczające wtórną ekspozycję koncentrują się głównie na niższych poziomach hierarchii (środki administracyjne i ŚOI), przy niedostatecznym wykorzystaniu środków

measures. Single interventions, despite documented effectiveness in reducing the selected routes of exposure, only affect parts of the secondary exposure chain and do not ensure full control over it in the system perspective. The schematic view of this phenomenon is presented in Figure 2.

inżynieryjnych i systemowych. Pojedyncze interwencje, mimo udokumentowanej skuteczności w ograniczaniu wybranych dróg narażenia, oddziałują jedynie na fragmenty łańcucha wtórnej ekspozycji i nie zapewniają jego pełnej kontroli w ujęciu systemowym. Schematyczne ujęcie tego zjawiska przedstawiono na rycinie 2.

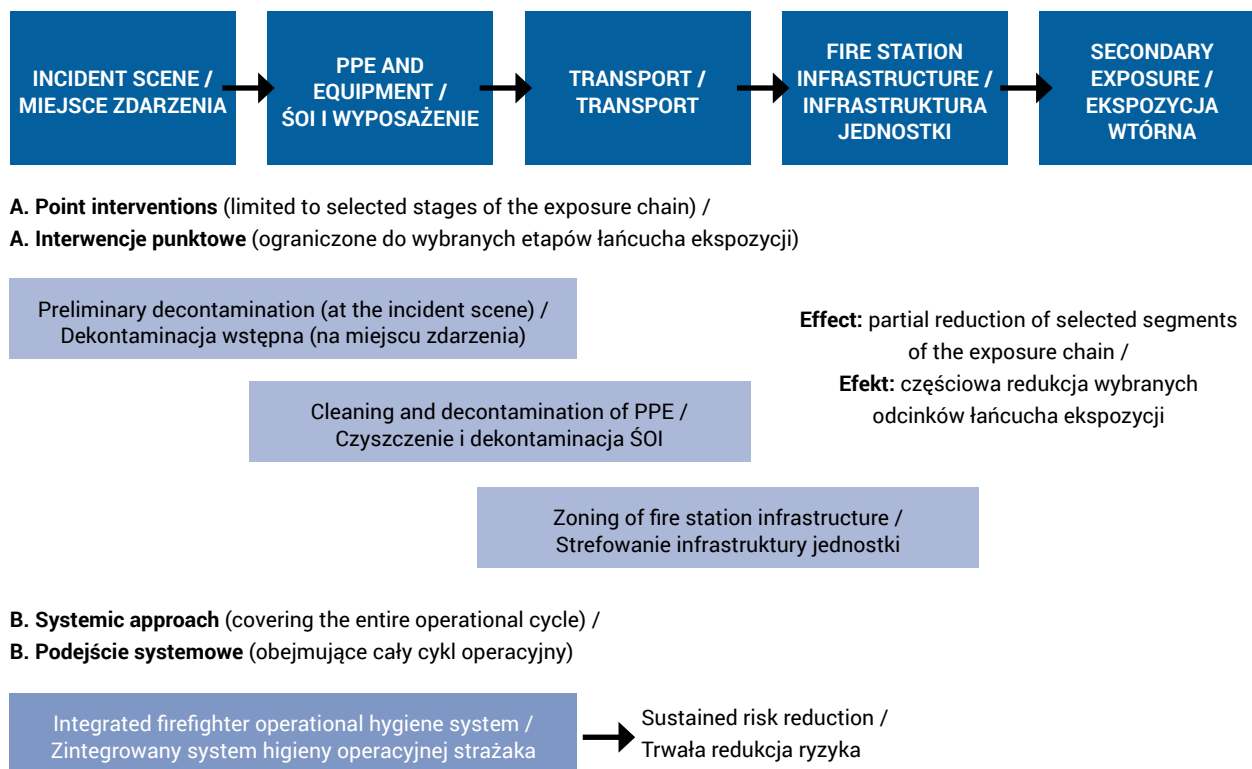


Figure 2. Limitations of single interventions in the reduction of secondary exposure of firefighters and significance of the systemic approach including the entire operational cycle

Rycina 2. Ograniczenia pojedynczych interwencji w redukcji wtórnej ekspozycji strażaków oraz znaczenie podejścia systemowego obejmującego cały cykl operacyjny

Source: Own elaboration.

Źródło: Opracowanie własne.

Normative framework as part of the secondary exposure reduction system

PN-EN 469:2021 – Requirements for special clothing

PN-EN 469:2021 Protective clothing for firefighters – performance requirements for clothing used during rescue and firefighting activities specifies the requirements for the protection properties of clothing under the conditions of heat and flame impact, as well as the principles of use and maintenance [23].

Although the standard does not directly address the matters of secondary chemical exposure, according to it clothing should be maintained to retain the protection properties for the entire period of use, also including the cleaning and maintenance processes. At the same time, the recommendations of the information appendix to this document specify caution practices focused on the reduction of exposure resulting from the use of contaminated clothing, including the need to use a complete set

Ramy normatywne jako element systemu ograniczania wtórnej ekspozycji

PN-EN 469:2021 – Wymagania dla odzieży specjalnej

Norma PN-EN 469:2021 Odzież ochronna dla strażaków – wymagania użytkowe dotyczące odzieży stosowanej podczas działań ratowniczo-gaśniczych określa wymagania dla właściwości zabezpieczających odzieży w warunkach oddziaływania ciepła i płomienia, a także odnosi się do zasad jej użytkowania i konserwacji [23].

Choć norma nie dotyczy bezpośrednio zagadnień wtórnej ekspozycji chemicznej, według jej zapisów odzież powinna być utrzymywana w stanie zapewniającym zachowanie właściwości ochronnych przez cały okres użytkowania, co obejmuje również procesy czyszczenia i konserwacji. Jednocześnie zalecenia ujęte w załączniku informacyjnym tego dokumentu wskazują praktyki ostrożnościowe ukierunkowane na ograniczanie narażenia

of personal protective equipment, to avoid introducing contaminated clothing into the vehicle cab or for sealed packaging after incident and further cleaning after the return to the fire station.

In these terms the standard, despite the formal focus on material and performance requirements, is part of a broader approach to the systemic reduction of secondary exposure. At the same time, it emphasises the importance of the correct use, handling and maintenance of protective clothing as a significant component of firefighter health risk management.

PN-EN ISO 13688:2013 – General requirements for protective clothing

PN-EN ISO 13688:2013 Protective clothing – General requirements introduces the rule of non-harmful materials and elimination of the negative impact on user health in expected conditions of use [24].

In the context of secondary exposure, it means that protective clothing, also after multiple use and cleaning, should not be a source of secondary exposure.

This principle extends the classical understanding of the safety of protective clothing, indicating that its assessment should include not only protection properties at the time of manufacture, but also the impact of use and deterioration processes and the potential accumulation of contaminants during operation.

ISO 23616:2024 – Personal protective equipment management

ISO 23616:2024 Cleaning, inspection and repair of firefighter PPE is a comprehensive elaboration on personal protective equipment management for the fire service [25].

This document introduces a process approach, which includes:

- regular inspections,
- classification of soiling and contamination,
- cleaning and decontamination,
- process documentation,
- clothing life cycle management.

The document highlights the need for using procedures based on risk assessment and with confirmed effectiveness of cleaning processes. It is also very important to distinguish between routine cleaning and advanced decontamination and proper qualification of clothing for appropriate process type.

In the context of secondary exposure, it is worth emphasising that the subject standard shifts the point of gravity from the cleaning technology itself to process management. It assumes that the effectiveness of the reduction of exposure does not arise from the use of a single technical solution, but its proper inclusion in a consistent operational management system.

NFPA 1851:2020 – Programme management of protective clothing

NFPA 1851:2020 Standard on Selection, Care, and Maintenance of Protective Ensembles for Structural Fire Fighting and Proximity Fire Fighting defines a comprehensive protective clothing management programme [26].

wynikającego z użytkowania skażonej odzieży, w tym konieczność stosowania kompletnego zestawu środków ochrony indywidualnej, unikania wprowadzania skażonej odzieży do kabiny pojazdu, wdrażania procedur jej oczyszczania lub szczelnego pakowania po zdarzeniu oraz dalszego czyszczenia po powrocie do jednostki.

W tym ujęciu norma, mimo że formalnie koncentruje się na wymaganiach materiałowych i użytkowych, stanowi element szerszego podejścia do systemowego ograniczania wtórnej ekspozycji. Podkreśla jednocześnie znaczenie prawidłowego użytkowania, obiegu oraz utrzymania odzieży ochronnej jako istotnego komponentu zarządzania ryzykiem zdrowotnym strażaków.

PN-EN ISO 13688:2013 – Ogólne wymagania dla odzieży ochronnej

Norma PN-EN ISO 13688:2013 Odzież ochronna – Wymagania ogólne wprowadza zasadę nieszkodliwości materiałów oraz eliminację negatywnego wpływu odzieży na zdrowie użytkownika w przewidywalnych warunkach użytkowania [24].

W kontekście wtórnej ekspozycji oznacza to, że odzież ochronna – również po wielokrotnym użytkowaniu i czyszczeniu – nie powinna stanowić wtórnego źródła narażenia.

Zasada ta rozszerza klasyczne rozumienie bezpieczeństwa odzieży ochronnej, wskazując, że jej ocena powinna uwzględniać nie tylko właściwości ochronne w momencie produkcji, lecz także wpływ procesów użytkowania, degradacji oraz potencjalnej kumulacji zanieczyszczeń w trakcie eksploatacji.

ISO 23616:2024 – Zarządzanie środkami ochrony indywidualnej

Norma ISO 23616:2024 stanowi kompleksowe opracowanie dotyczące zarządzania środkami ochrony indywidualnej w straży pożarnej [25].

Dokument ten wprowadza podejście procesowe obejmujące:

- regularne inspekcje,
- klasyfikację zabrudzeń i skażeń,
- czyszczenie i dekontaminację,
- dokumentowanie procesów,
- zarządzanie cyklem życia odzieży.

Dokument podkreśla konieczność stosowania procedur opartych na ocenie ryzyka oraz potwierdzonej skuteczności procesów czyszczenia. Bardzo ważne znaczenie ma również rozróżnienie pomiędzy czyszczeniem rutynowym a zaawansowaną dekontaminacją oraz właściwa kwalifikacja odzieży do odpowiedniego rodzaju procesu.

W kontekście wtórnej ekspozycji warto podkreślić, że omawiana norma przesuwą punkt ciężkości z samej technologii czyszczenia na zarządzanie procesem. Zakłada bowiem, że skuteczność ograniczania narażenia nie wynika z zastosowania pojedynczego rozwiązania technicznego, lecz z jego właściwego włączenia w spójny system operacyjny.

NFPA 1851:2020 – Programowe zarządzanie odzieżą ochronną

Norma NFPA 1851:2020 definiuje kompleksowy program zarządzania odzieżą ochronną [26].

Wprowadza ona m.in.:

- rozróżnienie pomiędzy czyszczeniem rutynowym i zaawansowanym,

It introduces i.a.:

- the distinction between routine and advanced cleaning,
- the requirement of inspection after every use,
- the requirement of periodical advanced cleaning,
- the requirement of keeping records,
- the designation of organisational responsibilities.

This model is systemic in nature and assumes that the effectiveness of activities depends on the continuity, repeatability and quality control of the applied processes [26].

In the context of secondary exposure, NFPA 1851 emphasises the importance of reducing the contact with contaminated clothing and eliminating the transfer of contaminants between subsequent stages of operational activities and fire station environment.

Synthesis of normative frameworks

The analysis of normative documents indicates that although individual standards are focused on different aspects (protection parameters, non-harmful materials, PPE management), they are connected by a common component: they consider the use, handling, cleaning and supervision over protective clothing as integral part of the safety system.

The summary of PN-EN 469, PN-EN ISO 13688, ISO 23616 and NFPA 1851 indicates that their requirements, despite being formulated in different regulatory systems, are consistent in terms of the interpretation direction and support the concept of systemic secondary exposure risk management.

In these terms, normative frameworks do not constitute a collection of separate requirements, but form a complementary basis for the development of an integrated firefighter operational hygiene system, in which crucial importance is assigned to the continuity of activities, their mutual connections and effective supervision over the fulfilment of the assumed procedures.

Integration of evidence and systemic operational hygiene model

Synthesis of results and systemic perspective

The analysis of available data indicates that the effectiveness of secondary exposure reduction activities depends on the simultaneous use of many complementary measures. In literature, many interventions are described, both technical and organisational, aimed to reduce selected routes of exposure, however their effectiveness is most often partial and applicable to specific stages of the process.

The use of the hierarchy of controls as interoperational framework enable organising the accessible exposure reduction strategies. It indicates that activities, such as using respiratory protection, preliminary decontamination, shower after incident or cleaning of protective clothing, are important components of risk reduction, but they primarily affect specific exposure mechanisms.

Consequently, individual interventions, despite documented effectiveness, do not ensure sustained reduction of the total health risk. Only a parallel and coordinated implementation,

- obowiązek inspekcji po każdym użyciu,
- wymóg okresowego czyszczenia zaawansowanego,
- konieczność prowadzenia dokumentacji,
- wyznaczenie odpowiedzialności organizacyjnej.

Model ten ma charakter systemowy i zakłada, że skuteczność działań zależy od ich ciągłości, powtarzalności oraz kontroli jakości realizowanych procesów [26].

W kontekście wtórnej ekspozycji norma NFPA 1851 podkreśla znaczenie ograniczania kontaktu ze skażoną odzieżą oraz eliminowania transferu zanieczyszczeń pomiędzy kolejnymi etapami działań operacyjnych i środowiskiem jednostki.

Synteza ram normatywnych

Analiza dokumentów normatywnych wskazuje, że choć poszczególne normy koncentrują się na różnych aspektach (parametry ochronne, nieszkodliwość materiałów, zarządzanie ŚOI), łączy je wspólny element: traktowanie użytkowania, obiegu, czyszczenia i nadzoru nad odzieżą ochronną jako integralnej części systemu bezpieczeństwa.

Zestawienie norm PN-EN 469, PN-EN ISO 13688, ISO 23616 oraz NFPA 1851 wskazuje, że ich wymagania – choć powstały w różnych systemach regulacyjnych – są spójne w zakresie kierunku interpretacyjnego i wspierają koncepcję systemowego zarządzania ryzykiem wtórnej ekspozycji.

W tym ujęciu ramy normatywne nie stanowią zbioru odrębnych wymagań, lecz tworzą komplementarną podstawę dla budowy zintegrowanego systemu higieny operacyjnej strażaka, w którym kluczowe znaczenie ma ciągłość działań, ich wzajemne powiązanie oraz skuteczny nadzór nad realizacją przyjętych procedur.

Integracja dowodów i model systemowy higieny operacyjnej

Synteza wyników i ujęcie systemowe

Analiza dostępnych danych wskazuje, że skuteczność działań ograniczających wtórną ekspozycję zależy od jednoczesnego zastosowania wielu uzupełniających się środków. W literaturze opisano liczne interwencje – zarówno techniczne, jak i organizacyjne – które prowadzą do redukcji wybranych dróg narażenia, jednak ich efektywność ma najczęściej charakter częściowy i odnosi się do określonych etapów procesu.

Zastosowanie hierarchii środków kontroli jako ramy interpretacyjnej pozwala uporządkować dostępne strategie ograniczania ekspozycji. Wskazuje ono, że działania takie jak stosowanie ochrony dróg oddechowych, dekontaminacja wstępna, prysznic po zdarzeniu czy czyszczenie odzieży ochronnej stanowią istotne elementy ograniczania ryzyka, lecz oddziałują głównie na wybrane mechanizmy narażenia.

W konsekwencji pojedyncze interwencje – mimo udokumentowanej skuteczności – nie zapewniają trwałej redukcji całkowitego ryzyka zdrowotnego. Dopiero ich równoległe i skoordynowane

including all stages of the operational cycle, enables a significant reduction of secondary exposure.

The above relationships, presented schematically in Figure 2, illustrating the partial nature of point activities and the need to integrate them into a cohesive systemic model.

Systemic operational hygiene model

In response to the gap identified in literature, consisting in the lack of a systemic model to integrate technical, organisational and management activities in the entire operational cycle, a systemic firefighter operational hygiene model is proposed, including the following:

- incident scene,
- transport,
- fire station infrastructure,
- PPE management,
- cleaning and decontamination processes,
- training and supervision.

A schematic image of the model, with relationships between its components and their continuity in the operational cycle, is presented in Figure 3. This model integrates the components described in literature and in normative documents, assuming that the effectiveness of the reduction of exposure is directly dependent on the continuity of activities at all stages.

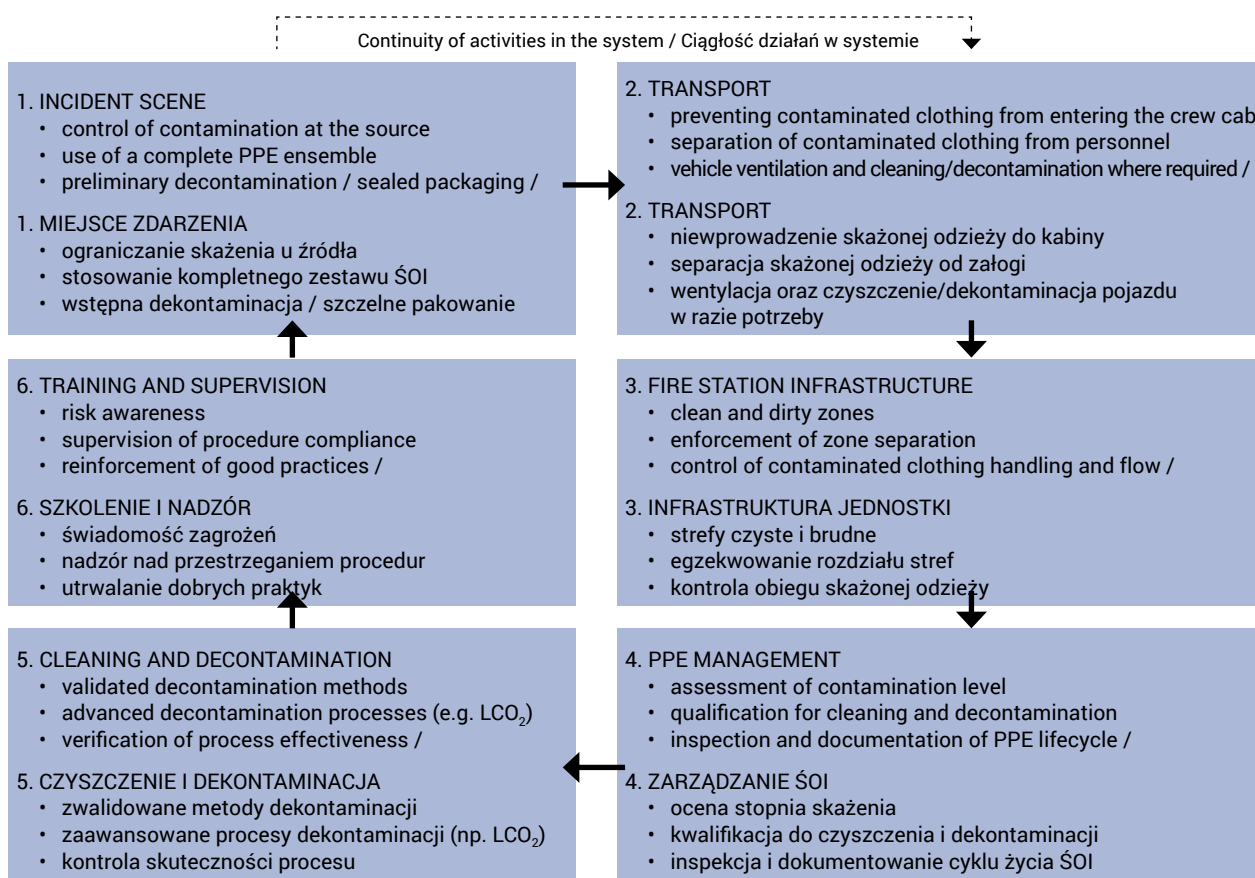


Figure 3. Systemic firefighter operational hygiene model including the entire operational cycle ("end-to-end")

Rycina 3. Model systemowy higieny operacyjnej strażaka obejmujący cały cykl operacyjny ("end-to-end")

Source: Own elaboration.

Źródło: Opracowanie własne.

wdrożenie, obejmujące wszystkie etapy cyklu operacyjnego, pozwala na istotne ograniczenie wtórnej ekspozycji.

Powyższe zależności przedstawiono schematycznie na rycinie 2, obrazującej fragmentaryczny charakter działań punktowych oraz konieczność ich integracji w spójny model systemowy.

Model systemowy higieny operacyjnej

W odpowiedzi na zidentyfikowaną w literaturze lukę, polegającą na braku syntetycznego modelu integrującego działania techniczne, organizacyjne i zarządcze w całym cyklu operacyjnym, zaproponowano model systemowy higieny operacyjnej strażaka obejmujący:

- miejsce zdarzenia,
- transport,
- infrastrukturę jednostki,
- zarządzanie ŚOI,
- procesy czyszczenia i dekontaminacji,
- szkolenie i nadzór.

Schematyczne ujęcie modelu, wraz z relacjami pomiędzy jego elementami oraz ich ciągłością w cyklu operacyjnym, przedstawiono na rycinie 3. Model ten integruje elementy opisane w literaturze oraz w dokumentach normatywnych i zakłada, że skuteczność ograniczania ekspozycji bezpośrednio zależy od ciągłości działań na wszystkich etapach.

Requirements for system effectiveness and practical implications

The effectiveness of activities aimed at reducing the secondary exposure of firefighters depends on their integration into a cohesive system including all stages of the operational cycle. The analysis of literature and normative documents indicates that point activities, despite documented effectiveness in relation to selected mechanisms of exposure, do not ensure a sustained reduction of the total health risk.

A requirement for system effectiveness is parallel and coordinated implementation of technical, organisational and procedural solutions, including in particular: clearly defined operational procedures and infrastructure enabling the separation of clean and dirty zones, assignment of organisational responsibility, process documentation and control system and application of cleaning and decontamination methods with confirmed effectiveness.

The lack of any of these components may lead to systemic gaps, resulting in re-introduction of contaminants into the work environment and lower effectiveness of other activities.

In practice, the implementation of the systemic model requires not only the availability of proper technical solutions, but also change of the organisational approach and building hazard awareness among firefighters. It includes the development of operation and training procedures and effective application supervision and control mechanisms.

Limitations of the review

This study is an integrated structure narrative review in nature, which entails specific methodological limitations. The analysis was not conducted in the formal systematic review mode (e.g. in accordance with PRISMA guidelines) and the selection of literature is purpose- and problem-based in nature, aimed at identifying repeatable mechanisms of secondary exposure and system components.

Firstly, the analysis is based on publications with various methods, including field tests, laboratory experiments, biomonitoring studies and review elaborations, which hinders the direct comparisons of results and quantitative synthesis of data.

Secondly, the available literature lacks uniform indicators that enable a comprehensive assessment of health risk reduction arising from the implementation of the integrated operational hygiene system. Most studies are focused on the reduction of the concentration of selected contaminants or biomarkers at specific points of the process, without a long-term assessment of health impact.

Thirdly, some normative documents and operational guidelines are regional in nature and reflect the specific organisational systems of individual countries, which may limit their feasibility for direct implementation in other legal and institutional conditions.

It should be also considered that publication bias may occur, consisting in a higher frequency of publication of the results confirming the effectiveness of specific interventions than neutral or

Warunki skuteczności systemu i implikacje dla praktyki

Skuteczność działań ukierunkowanych na ograniczanie wtórnej ekspozycji strażaków zależy od ich integracji w spójny system obejmujący wszystkie etapy cyklu operacyjnego. Analiza literatury oraz dokumentów normatywnych wskazuje, że działania punktowe – mimo udokumentowanej skuteczności w odniesieniu do wybranych mechanizmów narażenia – nie zapewniają trwałej redukcji całkowitego ryzyka zdrowotnego.

Warunkiem skuteczności systemu jest równoległe i skoordynowane wdrożenie rozwiązań technicznych, organizacyjnych i proceduralnych, obejmujących w szczególności: jednoznacznie zdefiniowane procedury operacyjne, infrastrukturę umożliwiającą separację stref czystych i brudnych, przypisanie odpowiedzialności organizacyjnej, system dokumentowania i kontroli procesów oraz stosowanie metod czyszczenia i dekontaminacji o potwierdzonej skuteczności.

Brak któregokolwiek z tych elementów może prowadzić do powstawania luk systemowych, skutkujących ponownym wprowadzaniem zanieczyszczeń do środowiska pracy oraz ograniczeniem efektywności pozostałych działań.

W praktyce wdrożenie modelu systemowego wymaga nie tylko dostępności odpowiednich rozwiązań technicznych, lecz także zmiany podejścia organizacyjnego oraz budowania świadomości zagrożeń wśród strażaków. Obejmuje to rozwój procedur operacyjnych, szkolenia oraz skuteczne mechanizmy nadzoru i kontroli ich stosowania.

Ograniczenia przeglądu

Niniejsza praca ma charakter przeglądu narracyjnego o strukturze integracyjnej, co wiąże się z określonymi ograniczeniami metodologicznymi. Analiza nie była prowadzona w trybie formalnego przeglądu systematycznego (np. zgodnie z wytycznymi PRISMA), a dobór literatury ma charakter celowy i problemowy, ukierunkowany na identyfikację powtarzalnych mechanizmów wtórnej ekspozycji oraz elementów systemowych.

Po pierwsze, analiza opiera się na publikacjach o zróżnicowanej metodologii – obejmujących badania terenowe, eksperymenty laboratoryjne, badania biomonitoringowe oraz opracowania przeglądowe – co utrudnia bezpośrednie porównywanie wyników i ilościową syntezę danych.

Po drugie, w dostępnej literaturze brak jest jednolitych wskaźników pozwalających na kompleksową ocenę redukcji ryzyka zdrowotnego wynikającej z wdrożenia zintegrowanego systemu higieny operacyjnej. Większość badań koncentruje się na redukcji stężeń wybranych zanieczyszczeń lub biomarkerów w określonym punkcie procesu, bez długoterminowej oceny skutków zdrowotnych.

Po trzecie, część dokumentów normatywnych i wytycznych operacyjnych ma charakter regionalny i odzwierciedla specyfikę systemów organizacyjnych poszczególnych krajów, co może ograniczać możliwość ich bezpośredniej implementacji w innych realiach prawnych i instytucjonalnych.

Należy również uwzględnić możliwość występowania biasu publikacyjnego, polegającego na częstszej publikacji wyników potwierdzających skuteczność określonych interwencji niż wyników

negative results. Despite the indicated limitations, the review enables identification of repeatable mechanisms of secondary exposure and common components of risk reduction strategies, which constitutes a basis for formulating the system model.

Conclusions

The presented model is conceptual in nature and constitutes a synthetic attempt at integrating the available scientific evidence and normative frameworks in system terms. It requires further empirical verification under operational conditions, in particular to evaluate the effectiveness of individual components and their mutual interactions. At the same time, it may constitute a point of reference for designing organisational procedures, training programmes and directions for further research on the reducing the secondary exposure of firefighters.

The most important conclusions of this article may be formulated as follows:

1. Secondary exposure of firefighters to hazardous substances present in the fire environment is multi-stage in nature and includes both direct contact with contaminants and their secondary transfer by protective clothing, equipment and fire station infrastructure.
2. The available empirical data confirm the effectiveness of selected interventions reducing the exposure, such as preliminary decontamination, organisational changes and specific methods of cleaning of protective clothing, however their impact is partial in nature and applicable to selected stages of the exposure process.
3. The reduction of the material contamination level is not equivalent to the elimination of exposure, which results from the multi-route nature of exposure, including i.a. dermal and inhalation routes and secondary transfer of contaminants.
4. The analysis of literature and normative documents (PN-EN 469, PN-EN ISO 13688, ISO 23616, NFPA 1851) indicates that effective reduction of the health risk requires an integrated approach, including parallel application of technical, organisational and procedural measures.
5. The proposed “end-to-end” systemic firefighter operational hygiene model integrates the exposure reduction components dispersed in literature and provides an organisational framework for the implementation of activities at all stages of the operational cycle.
6. The effectiveness of the organisational activities to reduce secondary exposure depends on their consistency and quality control, but not on the application of individual technical or organisational solutions.
7. Advanced technologies of material decontamination, including solutions using liquid carbon dioxide (LCO₂), may be an important component of the exposure reduction system, however their effectiveness depends on the integration with other components of operational hygiene and on application within validated and supervised frameworks.

neutralnych lub negatywnych. Mimo wskazanych ograniczeń przegląd umożliwia identyfikację powtarzalnych mechanizmów wtórnej ekspozycji oraz wspólnych elementów strategii ograniczania ryzyka, co stanowi podstawę do sformułowania modelu systemowego.

Wnioski

Prezentowany model ma charakter koncepcyjny i stanowi syntetyczną próbę integracji dostępnych dowodów naukowych oraz ram normatywnych w ujęciu systemowym. Wymaga on dalszej weryfikacji empirycznej w warunkach operacyjnych, w szczególności w zakresie oceny skuteczności poszczególnych jego elementów oraz ich wzajemnych interakcji. Jednocześnie może stanowić punkt odniesienia dla projektowania procedur organizacyjnych, programów szkoleniowych oraz kierunków dalszych badań nad ograniczaniem wtórnej ekspozycji strażaków.

Najważniejsze wnioski z niniejszego artykułu można sformułować następująco:

1. Wtórna ekspozycja strażaków na substancje niebezpieczne obecne w środowisku pożaru ma charakter wieloetapowy i obejmuje zarówno bezpośredni kontakt z zanieczyszczeniami, jak i ich wtórne przenoszenie poprzez odzież ochronną, sprzęt oraz infrastrukturę jednostek.
2. Dostępne dane empiryczne potwierdzają skuteczność wybranych interwencji ograniczających ekspozycję, takich jak dekontaminacja wstępna, zmiany organizacyjne czy określone metody czyszczenia odzieży ochronnej, jednak ich oddziaływanie ma charakter częściowy i odnosi się do wybranych etapów procesu narażenia.
3. Redukcja poziomu skażeń materiałowych nie jest równoznaczna z eliminacją narażenia, co wynika z wielodrogowego charakteru ekspozycji, obejmującego m.in. drogi dermalne, inhalacyjne oraz wtórny transfer zanieczyszczeń.
4. Analiza literatury oraz dokumentów normatywnych (PN-EN 469, PN-EN ISO 13688, ISO 23616, NFPA 1851) wskazuje, że skuteczna redukcja ryzyka zdrowotnego wymaga podejścia zintegrowanego, obejmującego równoległe zastosowanie środków technicznych, organizacyjnych i proceduralnych.
5. Zaproponowany model systemowy higieny operacyjnej strażaka w ujęciu „end-to-end” integruje rozproszone w literaturze elementy ograniczania ekspozycji i stanowi ramę organizacyjną dla wdrażania działań na wszystkich etapach cyklu operacyjnego.
6. Skuteczność działań ograniczających wtórna ekspozycję zależy od ich ciągłości, spójności oraz kontroli jakości, a nie od zastosowania pojedynczych rozwiązań technicznych lub organizacyjnych.
7. Zaawansowane technologie dekontaminacji materiałowej, w tym rozwiązania wykorzystujące ciekły dwutlenek węgla (LCO₂), mogą stanowić istotny element systemu ograniczania ekspozycji. Ich skuteczność zależy jednak od ich właściwego powiązania z pozostałymi elementami higieny operacyjnej oraz od prowadzenia procesów dekontaminacji w sposób zwalidowany i nadzorowany.

8. The implementation of the systemic operational hygiene model constitutes a justified direction for reducing the health risk for firefighters, however its effectiveness requires further studies in the validation of individual components and their impact on the actual exposure levels.

AI Use Statement

The author declares that artificial intelligence tools were used in the preparation of this article only within the scope indicated below:

- searching for and identifying potential bibliographic sources (ChatGPT).

The author takes full responsibility for the content of the publication, including the scientific accuracy, interpretation of results, and final editing of the manuscript. Artificial intelligence tools were used solely as supporting instruments. The journal's editorial policy prohibits the uncritical copying of AI-generated content and its inclusion in a publication without proper critical analysis, verification, and revision by the author.

Literature / Literatura

- [1] IARC, *Occupational Exposure as a Firefighter*, IARC Monographs on the Identification of Carcinogenic Hazards to Humans, Vol. 132, International Agency for Research on Cancer, Lyon 2023.
- [2] Stec A.A., Dickens K.E., Salden M., et al., *Occupational Exposure to Polycyclic Aromatic Hydrocarbons and Elevated Cancer Incidence in Firefighters*, „Scientific Reports” 2018, 8(1), 2476, <https://doi.org/10.1038/s41598-018-20616-6>.
- [3] Mazumder N.U.S., Hossain M.T., Jahura F.T., Girase A., Hall A.S., Lu J., Ormond R.B., *Firefighters' exposure to per- and polyfluoroalkyl substances (PFAS) as an occupational hazard: a review*, „Front Mater” 2023, 10, 1143411, <https://doi.org/10.3389/fmats.2023.1143411>.
- [4] Wikoff D.S., Rager J.E., Chappell G.A., Fitch S., Haws L., Borghoff S.J., *A framework for systematic evaluation and quantitative integration of mechanistic data in assessments of potential human carcinogens*, „Toxicol Sci” 2019, 167(2), 322–335. <https://doi.org/10.1093/toxsci/kfy279>.
- [5] Fent K.W., Evans D.E., Booher D., et al., *Volatile organic compounds off-gassing from firefighters' personal protective equipment ensembles after use*, „J Occup Environ Hyg” 2015, 12(6), 404–414, <https://doi.org/10.1080/15459624.2015.1025135>.
- [6] Fent K.W., Eisenberg J., Snawder J. et al., *Systemic exposure to PAHs and benzene in firefighters suppressing controlled structure fires*, „Ann Occup Hyg” 2014, 58(7), 830–845, <https://doi.org/10.1093/annhyg/meu036>.
- [7] Fent K.W., Alexander B., Roberts J. et al., *Contamination of firefighter personal protective equipment and skin and the effectiveness of decontamination procedures*, „Journal of Occupational and Environmental Hygiene” 2017, 14(10), 801–814, <https://doi.org/10.1080/15459624.2017.1334904>.
- [8] Hwang J., Xu C., Grunsted P. et al., *Urinary Metabolites of Polycyclic Aromatic Hydrocarbons in Firefighters: A Systematic Review and Meta-Analysis*, „International Journal of Environmental Research and Public Health” 2022, 19(14), 8475, <https://doi.org/10.3390/ijerph19148475>.
- [9] Fent K.W., Toennis C., Sammons D. et al., *Firefighters' absorption of PAHs and VOCs during controlled residential fires by job assignment and fire attack tactic*, „Journal of Exposure Science & Environmental Epidemiology” 2020, 30(2), 338–349, <https://doi.org/10.1038/s41370-019-0145-2>.
- [10] Fent K.W., Eisenberg J., Evans D. et al., *Evaluation of Dermal Exposure to Polycyclic Aromatic Hydrocarbons in Fire Fighters*, Health Hazard Evaluation Report No. 2010-0156-3196, National Institute for Occupational Safety and Health, Cincinnati 2013, <https://www.cdc.gov/niosh/hhe/reports/pdfs/2010-0156-3196.pdf>.
- [11] Rosenfeld P.E. et al., *Perfluoroalkyl substances exposure in firefighters: sources and implications*, „Environ Res” 2023, 220, 115164, <https://doi.org/10.1016/j.envres.2022.115164>.
- [12] Bolstad-Johnson D.M., Burgess J.L., Crutchfield C.D. et al., *Characterization of firefighter exposures during fire overhaul*, „AIHA J” 2000, 61(5), 636–641, <https://doi.org/10.1080/15298660008984572>.
- [13] Horn G.P., Fent K.W., Kerber S., Smith D.L., *Hierarchy of contamination control in the fire service: Review of exposure control options to reduce cancer risk*, „Journal of Occupational and Environmental Hygiene” 2022, 19(9), 538–557, <https://doi.org/10.1080/15459624.2022.2100406>.

Oświadczenie dotyczące wykorzystania AI

Autor oświadcza, że w procesie przygotowania niniejszego artykułu wykorzystano narzędzia oparte na sztucznej inteligencji wyłącznie w zakresie wskazanym poniżej:

- wyszukiwanie źródeł bibliograficznych (ChatGPT).

Autor ponosi pełną odpowiedzialność za treść publikacji, w tym za poprawność merytoryczną, interpretację wyników oraz ostateczną redakcję tekstu. Narzędzia sztucznej inteligencji były wykorzystywane wyłącznie jako narzędzia pomocnicze. Polityka redakcyjna czasopisma zabrania bezrefleksyjnego kopiowania treści wygenerowanych przez narzędzia AI oraz pozostawiania ich w publikacji bez krytycznej analizy, weryfikacji i redakcji przez autora.

- [14] Burgess J.L., Hoppe-Jones C., Griffin S.C. et al., *Evaluation of Interventions to Reduce Firefighter Exposures*, „Journal of Occupational and Environmental Medicine” 2020, 62(4), 279–288, <https://doi.org/10.1097/JOM.0000000000001815>.
- [15] Rogula-Kozłowska W., Bralewska K., Rogula-Kopiec P. et al., *Respirable particles and polycyclic aromatic hydrocarbons at two Polish fire stations*, „Building and Environment” 2020, 184, 107255, <https://doi.org/10.1016/j.buildenv.2020.107255>.
- [16] International Association of Fire Fighters, *The Clean Cab Concept*, IAFF, Washington, DC, 2017.
- [17] International Association of Fire Fighters, *Fire Station Design: Best Practices to Reduce Exposures*, IAFF, Washington, DC, 2018.
- [18] Krasowski T., *Cleaning and Decontamination of Firefighters’ Protective Clothing in Liquid Carbon Dioxide (LCO₂) – Literature Review and Conclusions for National Practice*, „Safety & Fire Technology” 2025, 66(2), 98–111, <https://doi.org/10.12845/sft.66.2.2025.6>.
- [19] Mayer A.C., Fent K.W., Bertke S. et al., *Firefighter hood contamination: Efficiency of laundering to remove PAHs and FRs*, „Journal of Occupational and Environmental Hygiene” 2019, 16(2), 129–140, <https://doi.org/10.1080/15459624.2018.1540877>.
- [20] Horn G.P., Kerber S., Andrews J. et al., *Impact of Repeated Exposure and Cleaning on Protective Properties of Structural Firefighting Turnout Gear*, „Fire Technology” 2021, 57(2), 791–813, <https://doi.org/10.1007/s10694-020-01021-w>.
- [21] Salmi R., Laitinen J., Evaluation of the decontamination methods for turnout gear, „Journal of Occupational and Environmental Hygiene” 2025, published online: 3 October 2025, 1–17, <https://doi.org/10.1080/15459624.2025.2555299>.
- [22] Girase A., Thompson D., Ormond R.B., Comparative Analysis of the Liquid CO₂ Washing with Conventional Wash on Firefighters’ Personal Protective Equipment (PPE), „Textiles” 2022, 2(4), 624–632, <https://doi.org/10.3390/textiles2040036>.
- [23] PN-EN 469:2021 Odzież ochronna dla strażaków – wymagania użytkowe dotyczące odzieży stosowanej podczas działań ratowniczo-gaśniczych.
- [24] PN-EN ISO 13688:2013 Odzież ochronna – wymagania ogólne.
- [25] ISO 23616:2024, *Cleaning, inspection and repair of firefighters’ personal protective equipment (PPE)*, International Organization for Standardization.
- [26] NFPA 1851:2020 Standard on selection, care, and maintenance of protective ensembles for structural fire fighting and proximity fire fighting.
- [27] Fire Protection Research Foundation, *Improved PPE Cleaning Best Practices/Exposure Assessment: Expanding Firefighting PPE Cleaning Validation Procedures by Improving Best Practices and Exposure Assessment Methods*, NFPA, Quincy, MA, 2022.

BRIG. (RETD.) TOMASZ KRASOWSKI, M.SC. ENG. – a graduate of the Main School of Fire Service, Director of Technology and Development at Decontex Polska, and retired State Fire Service officer. He served for over 30 years, holding positions including commander of JRG 2 in Siedlce, commander of the “Siedlce” Specialized Chemical Rescue Group, and deputy commander of the Municipal Fire Service in Siedlce. He was a member of the teams of the Chief Commander of the State Fire Service responsible for developing strategies, regulations, and executive acts related to fire safety and emergency rescue. Author of numerous industry publications and speaker at numerous rescue seminars and workshops. Creator of the blog “Strażak XXI wieku” (Firefighter of the 21st Century) and initiator of nationwide training projects in the area of tactics and safety in rescue operations.

BRYG. W ST. SP. MGR INŻ. TOMASZ KRASOWSKI – absolwent Szkoły Głównej Służby Pożarniczej, Dyrektor ds. Technologii i Rozwoju w Decontex Polska oraz funkcjonariusz PSP w stanie spoczynku. Służbę pełnił przez ponad 30 lat, zajmując m.in. stanowiska dowódcy JRG 2 w Siedlcach, Dowódcy Specjalistycznej Grupy Ratownictwa Chemicznego „Siedlce” oraz Zastępcy Komendanta Miejskiego PSP w Siedlcach. Był członkiem zespołów Komendanta Głównego PSP odpowiedzialnych za opracowanie strategii, regulaminów oraz aktów wykonawczych związanych z bezpieczeństwem pożarowym i ratownictwem interwencyjnym. Autor wielu publikacji branżowych oraz prelegent licznych seminariów i warsztatów ratowniczych. Twórca bloga „Strażak XXI wieku” oraz inicjator ogólnopolskich projektów szkoleniowych z zakresu taktyki i bezpieczeństwa działań ratowniczych.

Norbert Tuśnio

Fire Univeristy / Akademia Pożarnicza

Corresponding author / Autor korespondencyjny: ntusnio@apoz.edu.pl

Modular Mobile Crisis Management Support Systems – Implementation Prospects Based on the Analysis of the Beirut Explosion (2020)

Modułowe mobilne systemy wspomagania zarządzania kryzysowego – perspektywy wdrożenia na podstawie analizy wybuchu w Bejrucie (2020)

ABSTRACT

Purpose: The purpose of this article is a comprehensive analysis of implementation options of modular mobile crisis management support systems (MMCMSS) in the context of contemporary CBRNE hazards, including in particular incidents involving ammonium nitrate. The article is conceptual and analytical in nature and its purpose is to fill the research gap on the integration of mobile technologies with crisis response systems.

Introduction: Technological disasters, such as the Beirut port explosion (2020), revealed critical gaps in crisis response systems – shortage of mobile command structures, lack of interoperability of rescue services, inadequate chemical identification in the first stage of the incident and lack of social trust in state institutions. To address these challenges, the article presents the author's concept of MMCMSS, which integrates mobile CBRN laboratories, command centres with satellite communication and unmanned reconnaissance platforms (UAV, UGV, USV). This system, based on modular architecture and compliant with NATO and EU standards, is designed to shorten the response time, increase the safety of rescuers and improve the quality of operational decision-making.

Methodology: The study employed a literature review, analysis of normative documents, and a case study of the 2020 Beirut explosion. The research was based on international reports (CSB, BARPI, ISPRA), field tests, and interviews with non-governmental organisations. Also, comparative analysis of national solutions (mobile CBRNE laboratories of the State Fire Service implemented in 2023) and SWOT analysis were used. The study is qualitative, based on the review of available sources.

Conclusions: The MMCMSS are a valid direction of development of safety systems, however the implementation requires overcoming significant barriers: legal (fragmented regulations, lack of standards for BSL-3 mobile laboratories), organisational (excess responsibilities, personnel deficits) and technological (communication-dependence, energy restrictions). It is necessary to undertake standardisation, legislation and investment actions at the national and EU level. The experience of Beirut shows that even relatively developed systems may be unprepared for disasters if they do not have flexible and resilient response structures. The key success factor is building social trust and integrating the operations of all entities of the safety system.

Keywords: safety engineering, crisis management, mobile systems, CBRNE, ammonium nitrate

Type of article: case study

Received: 19.04.2026; Reviewed: 07.05.2026; Accepted: 07.05.2026;

Author's ORCID ID: N. Tuśnio – 0000-0003-0878-8499;

Please cite as: Safety & Fire Technology 2026, 1, 162–194, <https://doi.org/10.12845/sft.67.1.2026.8>;

This is an open access article under the CC BY-SA 4.0 license (<https://creativecommons.org/licenses/by-sa/4.0/>).

ABSTRAKT

Cel: Celem artykułu jest kompleksowa analiza możliwości wdrożenia modułowych mobilnych systemów wspomagania zarządzania kryzysowego (MMCZK) w kontekście współczesnych zagrożeń CBRNE, ze szczególnym uwzględnieniem zdarzeń z udziałem azotanów amoniu. Artykuł ma charakter koncepcyjno-analityczny i ma za zadanie wypełnić lukę badawczą dot. integracji mobilnych technologii z systemami reagowania kryzysowego.

Wprowadzenie: Katastrofy technologiczne, takie jak wybuch w porcie w Bejrucie (2020), uświadomiły krytyczne luki w systemach reagowania kryzysowego – deficyt mobilnych struktur dowodzenia, brak interoperacyjności służb ratowniczych, niewystarczające rozpoznanie chemiczne w pierwszej fazie zdarzenia oraz brak zaufania społecznego do instytucji państwowych. W odpowiedzi na te wyzwania w artykule przedstawiono autorską koncepcję MMCZK, integrującą mobilne laboratoria CBRN, centra dowodzenia z łącznością satelitarną oraz bezzałogowe platformy rozpoznawcze (UAV, UGV, USV). System ten, oparty na modułowej architekturze i zgodny ze standardami NATO oraz UE, ma na celu skrócenie czasu reakcji, zwiększenie bezpieczeństwa ratowników oraz poprawę jakości podejmowanych decyzji operacyjnych.

Metodologia: W badaniach zastosowano metody analizy literatury przedmiotu, dokumentów normatywnych oraz studium przypadku wybuchu w Bejrucie (2020), oparte na raportach międzynarodowych (CSB, BARPI, ISPRA), badaniach terenowych oraz wywiadach z przedstawicielami organizacji pozarządowych. Wykorzystano również analizę porównawczą rozwiązań krajowych (mobilne laboratoria CBRNE Państwowej Straży Pożarnej wdrożone w 2023 r.) oraz analizę SWOT. Badanie ma charakter jakościowy, oparty na systematycznym przeglądzie dostępnych źródeł.

Wnioski: MMCZK stanowią zasadny kierunek rozwoju systemów bezpieczeństwa, jednak ich wdrożenie wymaga pokonania istotnych barier prawnych (rozdrobienie regulacji, brak norm dla mobilnych laboratoriów BSL-3), organizacyjnych (nadmiar kompetencji, deficyty kadrowe) i technologicznych (zależność od łączności, ograniczenia energetyczne). Konieczne jest podjęcie działań normalizacyjnych, legislacyjnych oraz inwestycyjnych na poziomie krajowym i unijnym. Doświadczenia z Bejrutu wskazują, że nawet stosunkowo rozwinięte systemy mogą być nieprzygotowane na katastrofy, jeśli nie dysponują elastycznymi i odpornymi strukturami reagowania. Kluczowym czynnikiem sukcesu jest budowa zaufania społecznego oraz integracja działań wszystkich podmiotów systemu bezpieczeństwa.

Słowa kluczowe: inżynieria bezpieczeństwa, zarządzanie kryzysowe, systemy mobilne, CBRNE, azotan amonu

Typ artykułu: studium przypadku

Przyjęty: 19.04.2026; Zrecenzowany: 07.05.2026; Zaakceptowany: 07.05.2026;

Identyfikator ORCID autora: N. Tuśnio – 0000-0003-0878-8499;

Proszę cytować: Safety & Fire Technology 2026, 1, 162–194, <https://doi.org/10.12845/sft.67.1.2026.8>;

Artykuł udostępniany na licencji CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>).

Introduction

Chemical, biological, radiological, nuclear and explosive hazards (CBRNE) are some of the most important challenges for contemporary public safety systems [1]. In the literature of the subject, a consistent increase in interest in these problems is noticeable, as expressed by the growing number of scientific publications and research projects funded by the European Union and NATO. Contemporary crisis management is faced by increasingly complex and unpredictable hazards, of which the nature often exceeds the framework of traditional response procedures and structures. The changing structure of hazards, increasingly including technological, industrial and environmental phenomena, compels the adjustment of state structures and crisis response mechanisms to the new civilisation reality.

The increasing social expectations to assure safety lead to the need to create flexible and dynamic response systems, capable of minimising the impact of both sudden and gradually escalating incidents. Today safety, understood as public good, requires not only stable legal frameworks, but also modern technical instruments to enable quick hazard identification and response. In this context, the capability to conduct operations in chemically contaminated or explosion hazard environments, where traditional intervention methods entail an unacceptably high risk for rescuers, becomes particularly important.

Some of the most dangerous yet real hazards include incidents with chemical substances, including the highly explosive ammonium nitrate (NH_4NO_3). The incidents, such as explosions in Oppau (1921, 561 dead), Texas City (1947, approx. 580 dead), Toulouse (2001, 31 dead, 2500 injured), West (2013, 15 dead, including 12 firefighters) or Beirut (2020, 218 dead, 7500 injured, 300,000 displaced) [8], illustrate the scale of potential human, infrastructural and environmental losses that could be caused by improper storage, transport or management of that substance [2–3]. All of these incidents confirm the crucial importance of: early identification, prevention and interoperability of response structures.

Wprowadzenie

Zagrożenia chemiczne, biologiczne, radiologiczne, nuklearne i wybuchowe (CBRNE) należą do najpoważniejszych wyzwań, przed jakimi stoją współczesne systemy bezpieczeństwa powszechnego [1]. W literaturze przedmiotu można zauważyć systematyczny wzrost zainteresowania tą problematyką, czego wyrazem jest rosnąca liczba publikacji naukowych oraz projektów badawczych finansowanych przez Unię Europejską i NATO. Współczesne zarządzanie kryzysowe stoi w obliczu coraz bardziej złożonych i nieprzewidywalnych zagrożeń, których profil nierzadko wykracza poza ramy tradycyjnych procedur i struktur reagowania. Zmieniające się spektrum zagrożeń, obejmujące coraz częściej zjawiska o charakterze technologicznym, przemysłowym i środowiskowym, wymusza dostosowanie struktur państwowych oraz mechanizmów reagowania kryzysowego do nowych realiów cywilizacyjnych.

Rosnące oczekiwania społeczne dotyczące zapewnienia bezpieczeństwa wiążą się z koniecznością tworzenia elastycznych, dynamicznych systemów reagowania, zdolnych do minimalizacji skutków zarówno zdarzeń nagłych, jak i narastających procesowo. Bezpieczeństwo – pojmowane jako dobro publiczne – wymaga dziś nie tylko stabilnych ram prawnych, ale również nowoczesnych instrumentów technicznych umożliwiających szybkie rozpoznanie i reagowanie na sytuacje zagrożenia. W tym kontekście szczególnego znaczenia nabiera zdolność do prowadzenia działań w środowisku skażonym chemicznie lub zagrożonym wybuchem, gdzie tradycyjne metody interwencji są obciążone niedopuszczalnie wysokim ryzykiem dla ratowników.

Do najbardziej niebezpiecznych, a zarazem realnych zagrożeń należą incydenty z udziałem substancji chemicznych, w tym wysoce wybuchowego azotanu amonu (NH_4NO_3). Wydarzenia, takie jak wybuch w Oppau (1921, 561 ofiar), Teksas City (1947, ok. 580 ofiar), Tuluzie (2001, 31 ofiar, 2500 rannych), West (2013, 15 ofiar, w tym 12 strażaków) czy Bejrucie (2020, 218 ofiar, 7500 rannych, 300 000 przesiedlonych) [8], uwiadamiają skalę

Ammonium nitrate, despite being commonly used as nitrogen-based fertiliser in agriculture and as component of explosives in industry, shows high vulnerability to thermal conditions and potentially explosive under improper storage conditions. Its physical and chemical properties, capacity for hygroscopicity, self-sustaining exothermic decomposition (SSD) above 210°C and for deflagration to detonation transition (DDT) in the presence of reducing substances, it is one of the most hazardous oxidising materials [2]. The history of incidents, starting from the disaster in Oppau (1921) to explosions in Texas (1947), Toulouse (2001) and Beirut (2020), shows that such phenomena are global and applicable to both highly developed and developing countries.

Contemporary crisis management systems, including the Polish national rescue and firefighting system (KSRG), despite well-developed legal and institutional structures, show deficits in the mobility of technical resources, interoperability of services and quick access to reliable operational data in the first phase of the incident. The analysis of international experiences shows that systemic gaps still remain in civil protection from incidents involving highly explosive chemicals [3].

The following systemic gaps are identified:

1. Shortage of mobile and interoperational response structures – existing systems are to a large extent based on the stationary infrastructure of crisis management centres and traditional rescue vehicles. In case of large scale disasters, that infrastructure is often destroyed or becomes unavailable. There is a shortage of lightweight, quickly movable and autonomous units ready for quick deployment in the zero zone within several minutes.
2. Inadequate integration of unmanned and sensor-based technologies – although unmanned aerial vehicles (UAV) and unmanned ground vehicles (UGV) are increasingly used in rescue operations, their use in specific scenarios of hazards related to ammonium nitrate (identification of thermal hot spots, measurement of NO_x and NH_3 concentrations, mapping of impact zones) still requires systematic organisation and integration into standard operating procedures (SOP). In addition, there are no integrated platforms to combine data from UAVs, IoT sensors, mobile CBRN laboratories and GIS systems in a single decision-making utility for easy deployment in the field.
3. Gaps in chemical identification and personnel protection – the experience of incidents in Saint-Romain-en-Jarez (2003) and West (2013) show that rescue services often lack knowledge on the type and amount of hazardous substances before entering the hazard zone. There is a shortage of mobile analytical laboratories capable to operate in field conditions, as well as deflagration to detonation transition (DDT) risk early warning systems. This results in unnecessary losses among rescuers (as in West, where 12 firefighters died) and delays in the evacuation of civilian population.
4. Regulation and competence fragmentation – in Poland, like in other countries, the responsibility for ammonium nitrate supervision is dispersed between several

potencjalnych strat ludzkich, infrastrukturalnych i środowiskowych, jakie może spowodować nieprawidłowe magazynowanie, transport czy zarządzanie tą substancją [2–3]. Każde z tych zdarzeń potwierdza, że kluczowe znaczenie mają: wczesne rozpoznanie, prewencja oraz interoperacyjność struktur reagowania.

Azotan amonu, mimo powszechnego zastosowania w rolnictwie jako nawóz azotowy i w przemyśle jako komponent materiałów wybuchowych, charakteryzuje się wysoką wrażliwością termiczną oraz potencjałem wybuchowym w warunkach niewłaściwego przechowywania. Jego właściwości fizykochemiczne – higroskopijność, zdolność do samopodtrzymującego się rozkładu egzotermicznego (SSD) powyżej 210°C oraz możliwość przejścia deflagracji w detonację (DDT) w obecności substancji redukujących – czynią go jednym z najbardziej niebezpiecznych materiałów utleniających [2]. Historia zdarzeń, począwszy od katastrofy w Oppau w 1921 r., przez wybuchy w Teksasie (1947), Tuluzie (2001), aż po Bejrut (2020), pokazuje, że zjawiska te mają wymiar globalny i dotyczą zarówno państw wysoko rozwiniętych, jak i rozwijających się.

Współczesne systemy zarządzania kryzysowego, w tym polski krajowy system ratowniczo-gaśniczy (KSRG), mimo dobrze rozwiniętych struktur prawnych i instytucjonalnych, wykazują deficyty dotyczące mobilności zasobów technicznych, interoperacyjności między służbami oraz szybkiego dostępu do wiarygodnych danych operacyjnych w pierwszej fazie zdarzenia. Analiza doświadczeń międzynarodowych wskazuje, że wciąż istnieją luki systemowe w zakresie ochrony ludności przed skutkami zdarzeń z udziałem substancji chemicznych o wysokim potencjale wybuchowym [3].

Zidentyfikowano następujące kluczowe luki systemowe:

1. Deficyt mobilnych i interoperacyjnych struktur reagowania – istniejące systemy opierają się w dużej mierze na stacjonarnej infrastrukturze centrów zarządzania kryzysowego oraz tradycyjnych pojazdów ratowniczych. W przypadku katastrofy na dużą skalę infrastruktura ta często ulega zniszczeniu lub staje się niedostępna. Brakuje lekkich, wysokomobilnych, autonomicznych jednostek, które mogłyby zostać wdrożone w strefę zero w ciągu kilkunastu minut.
2. Niewystarczająca integracja technologii bezzałogowych i sensorowych – mimo że drony (UAV) i roboty naziemne (UGV) są coraz powszechniej stosowane w ratownictwie, ich wykorzystanie w specyficznych scenariuszach zagrożeń związanych z azotanem amonu (identyfikacja gorących punktów termicznych, pomiar stężeń NO_x i NH_3 , mapowanie strefy rażenia) nie zostało dotychczas usystematyzowane i włączone w standardowe procedury operacyjne (SOP). Brakuje również zintegrowanych platform łączących dane z dronów, sensorów IoT, mobilnych laboratoriów CBRN i systemów GIS w jednym, łatwym do wdrożenia w terenie narzędziu decyzyjnym.
3. Luki w rozpoznaniu chemicznym i ochronie personelu – doświadczenia ze zdarzeń w Saint-Romain-en-Jarez (2003) i West (2013) pokazują, że służby ratownicze często nie dysponują wiedzą o rodzaju i ilości składowanych substancji niebezpiecznych przed wejściem w strefę zagrożenia.

ministries and inspections (Ministry of Agriculture and Rural Development, Voivodship Inspectorate of Environmental Protection, State Fire Service [10], State Plant Health and Seed Inspection Service, maritime offices and, in transport, also Road Transport Inspection and Ministry of National Defence). There is no single and binding planning document defining unified storage, monitoring and response standards.

5. The inadequate use of the potential of national dual use technologies, Poland has advanced solutions for mobile robotics (Łukasiewicz Research Network – PIAP: Patrol, Gryf, Ibis, HUNTeR robots) and unmanned surface vessels (Łukasiewicz Research Network – Warsaw Institute of Technology: Manta water drone). However, their use in crisis management for civilian purposes remains to be fully developed and tested in scenarios involving ammonium nitrate.

The identified gaps confirm the need to develop a new crisis management model based on mobility, modularity and interoperability, capable of adaptation in dynamically evolving hazard conditions, including incidents involving ammonium nitrate that require immediate situation analysis, coordination between institutions and precise technical support in the field.

Brakuje mobilnych laboratoriów analitycznych zdolnych do pracy w warunkach polowych, a także systemów wczesnego ostrzegania o ryzyku przejścia deflagracji w detonację (DDT). Konsekwencją są niepotrzebne straty wśród ratowników (jak w West, gdzie zginęło 12 strażaków) oraz opóźnienia w ewakuacji ludności cywilnej.

4. Fragmentacja regulacyjna i kompetencyjna – w Polsce, podobnie jak w innych państwach, odpowiedzialność za nadzór nad azotanem amonu jest rozproszona między kilka resortów i inspekcji (MRiRW, WIOŚ, PSP [10], PIORiN, urzędy morskie, a w przypadku transportu – także ITD i MON). Brakuje jednego, wiążącego dokumentu planistycznego, który określałby jednolite standardy magazynowania, monitorowania i reagowania.
5. Niedostateczne wykorzystanie potencjału krajowych technologii podwójnego zastosowania – Polska posiada zaawansowane rozwiązania w zakresie robotyki mobilnej (Sieć Badawcza Łukasiewicz – PIAP: roboty Patrol, Gryf, Ibis, HUNTeR) oraz bezzałogowych systemów nawodnych (Sieć Badawcza Łukasiewicz – Warszawski Instytut Technologiczny: dron wodny Manta). Jednak ich zastosowanie w zarządzaniu kryzysowym na potrzeby cywilne nie zostało dotychczas w pełni rozwinięte i przetestowane w scenariuszach z udziałem azotanu amonu.

Zidentyfikowane luki potwierdzają konieczność opracowania nowego modelu zarządzania kryzysowego opartego na mobilności, modułowości i interoperacyjności, zdolnego do adaptacji w warunkach dynamicznie zmieniających się zagrożeń – w tym zdarzeń z udziałem azotanu amonu, które wymagają natychmiastowej analizy sytuacyjnej, koordynacji międzyinstytucjonalnej i precyzyjnego wsparcia technicznego w terenie.

Purpose and scope of analysis

The purpose of analysis is the multi-aspect analysis of implementation options of modular mobile crisis management support systems (MMCMSS) in Poland and in European Union structures, considering the technical, organisational, normative aspects and the identification of barriers and implementation recommendations. The article is conceptual and analytical in nature and it constitutes an input to the discussion on the directions of modernisation of the crisis management system in Poland.

The scope of the article includes:

- analysis of the theoretical basis for crisis management in the context of CBRNE hazards;
- presentation of the authors concept of MMCMSS, including the functional principles, modular structure and use scenarios;
- detailed technical analysis of the mobile CBRNE laboratory of the State Fire Service as key component of the system;
- case study of the Beirut explosion (2020) as reference for the evaluation of the usability of MMCMSS;
- evaluation of system effectiveness and implementability, including barriers and recommendations.

Cel i zakres analizy

Celem analizy jest wieloaspektowa ocena możliwości wdrożenia modułowych mobilnych systemów wspomagania zarządzania kryzysowego (MMCZK) w Polsce i w strukturach Unii Europejskiej, z uwzględnieniem aspektów technicznych, organizacyjnych, normatywnych oraz identyfikacji barier i rekomendacji wdrożeniowych. Artykuł ma charakter koncepcyjno-analityczny i stanowi głos w dyskusji nad kierunkami modernizacji systemu zarządzania kryzysowego w Polsce.

Zakres artykułu obejmuje:

- analizę teoretycznych podstaw zarządzania kryzysowego w kontekście zagrożeń CBRNE;
- przedstawienie autorskiej koncepcji MMCZK, w tym założeń funkcjonalnych, struktury modułowej i scenariuszy użycia;
- szczegółową analizę techniczną mobilnego laboratorium CBRNE PSP jako kluczowego komponentu systemu;
- studium przypadku wybuchu w Bejrucie (2020) jako punktu odniesienia dla oceny przydatności MMCZK;
- ocenę efektywności i możliwości wdrożenia systemu z uwzględnieniem barier i rekomendacji.

Research methodology

The study was based on the qualitative analysis of legal documents, technical standards, design documentation and literature of the subject. The following research methods were used:

1. Analysis of literature and normative documents – including the review of legal acts (Crisis Management Act of 2017 [11], Civil Protection and Civil Defence Act of 2024 [12], implementing regulations), technical standards (PN-EN, ISO, VDI 2083 [18]) and guidelines NATO (STANAG 4632 [19], AEP-66 re. SIBCRA [20]). The analysis also covered scientific publications on crisis management, safety engineering and mobile technologies.
2. Comparative analysis of technical solutions – on mobile CBRNE laboratories of the State Fire Service (implemented in 2023 at the Municipal Headquarters of the State Fire Service in Warszawa and Poznań) and international solutions (MIRACLE and ObsSAS projects, TOXI-Triage system). The comparison covered technical, operational and cost aspects.
3. Case study – the Beirut port explosion (4 August 2020) as reference for the evaluation of the usability of MMCSS in actual disasters. The analysis was based on international reports (CSB, BARPI, ISPRA), UN documents and field tests.
4. SWOT analysis – used to evaluate the strengths and weaknesses of the proposed solution and identification of opportunities and threats related to its implementation. The SWOT analysis was conducted based on technical, organisational, economic and social criteria.

The data sources included:

- national and EU legal acts (acts, regulations, directives);
- technical standards (PN-EN, ISO, VDI, DIN);
- technical documentation of mobile CBRNE laboratories of the State Fire Service [1], [7];
- post-accident reports and disaster analyses (CSB, BARPI, ISPRA) [2], [4–5];
- field tests and expert interviews (e.g. research by Sakr [6], interviews with representatives of non-government organisations);
- research projects and national initiatives (Kieleckie Centrum Nowoczesnego Zarządzania Kryzysowego, letter of intent of the Kielce University of Technology and Łukasiewicz Research Network).

The presented analysis consists in certain restrictions to consider in the interpretation of results:

1. No quantitative studies in actual explosion conditions – for obvious ethical and safety reasons, it was not possible to conduct experiments with actual detonation of large volumes of AA in site conditions. The conclusions on the effectiveness of the proposed solutions in an actual incident are derived from analogies (experiences of West and Beirut disasters), computer simulations and site experiments replicating the selected response phases.
2. Limited test sample – in terms of expert interviews, although intentionally selected and including key

Metodologia badań

Badanie oparto na analizie jakościowej dokumentów prawnych, norm technicznych, dokumentacji projektowej oraz literatury przedmiotu. Zastosowano następujące metody badawcze:

1. Analiza literatury i dokumentów normatywnych – obejmująca przegląd aktów prawnych (ustawa o zarządzaniu kryzysowym z 2007 r. [11], ustawa o ochronie ludności i obronie cywilnej z 2024 r. [12], rozporządzenia wykonawcze), norm technicznych (PN-EN, ISO, VDI 2083 [18]) oraz wytycznych NATO (STANAG 4632 [19], AEP-66 dot. SIBCRA [20]). Analizą objęto również publikacje naukowe z zakresu zarządzania kryzysowego, inżynierii bezpieczeństwa oraz technologii mobilnych.
2. Analiza porównawcza rozwiązań technicznych – dotycząca mobilnych laboratoriów CBRNE Państwowej Straży Pożarnej (wdrożonych w 2023 r. do KM PSP w Warszawie i Poznaniu) oraz rozwiązań międzynarodowych (projekty MIRACLE, ObsSAS, system TOXI-Triage). Porównanie obejmowało aspekty techniczne, operacyjne i kosztowe.
3. Studium przypadku – wybuch w porcie w Bejrucie (4 sierpnia 2020 r.) jako punkt odniesienia dla oceny przydatności MMCZK w rzeczywistych zdarzeniach katastroficznych. Analizę oparto na raportach międzynarodowych (CSB, BARPI, ISPRA), dokumentach ONZ oraz badaniach terenowych.
4. Analiza SWOT – zastosowana do oceny mocnych i słabych stron proponowanego rozwiązania oraz identyfikacji szans i zagrożeń związanych z jego wdrożeniem. Analiza SWOT została przeprowadzona w oparciu o kryteria techniczne, organizacyjne, ekonomiczne i społeczne.

Źródła danych obejmowały:

- akty prawne krajowe i unijne (ustawy, rozporządzenia, dyrektywy);
- normy techniczne (PN-EN, ISO, VDI, DIN);
- dokumentację techniczną mobilnych laboratoriów CBRNE PSP [1], [7];
- raporty powypadkowe i analizy katastrof (CSB, BARPI, ISPRA) [2], [4–5];
- badania terenowe i wywiady eksperckie (m.in. badania Sakr [6], wywiady z przedstawicielami organizacji pozarządowych);
- projekty badawcze i inicjatywy krajowe (Kieleckie Centrum Nowoczesnego Zarządzania Kryzysowego, list intencyjny Politechniki Świętokrzyskiej i Sieci Badawczej Łukasiewicz).

Prezentowana analiza podlega pewnym ograniczeniom, które należy uwzględnić przy interpretacji wyników:

1. Brak badań ilościowych w warunkach rzeczywistego wybuchu – z oczywistych względów etycznych i bezpieczeństwa nie było możliwe przeprowadzenie eksperymentów z rzeczywistą detonacją dużych ilości AA w warunkach poligonowych. Wnioski dotyczące skuteczności proponowanych rozwiązań w rzeczywistym zdarzeniu wywodzone są z analogii (doświadczenia z katastrof w West i Bejrucie), symulacji komputerowych oraz

representatives of the State Fire Service, administration and natural environment, it is limited. No survey studies were conducted on a larger group of operations officers.

3. Limited conditions of site tests – site tests were conducted under specific weather and terrain conditions. The systems were not tested under extreme conditions (strong winds, negative temperatures, dense fog, heavy precipitation).
4. Limited access to sensitive information – the access to ammonium nitrate storage locations, their technical condition and inspection procedures was limited to protect classified information and business secrets.

Despite these limitations, the presented analysis is a valuable input to the discussion on the directions of modernisation of the crisis management system in Poland.

eksperymentów poligonowych odtwarzających wybrane fazy reagowania.

2. Ograniczona próba badawcza w zakresie wywiadów eksperckich – choć dobrana celowo i obejmująca kluczowych przedstawicieli PSP, administracji i środowiska naukowego – jest ograniczona. Nie przeprowadzono badań ankietowych na większej grupie funkcjonariuszy operacyjnych.
3. Ograniczone warunki testów poligonowych – badania poligonowe przeprowadzono w określonych warunkach atmosferycznych i terenowych. Nie testowano systemów w warunkach ekstremalnych (silny wiatr, ujemne temperatury, gęsta mgła, intensywne opady).
4. Ograniczony dostęp do danych wrażliwych – dostęp do danych dotyczących lokalizacji magazynów azotanu amonu, ich stanu technicznego oraz procedur kontrolnych był ograniczony ze względu na ochronę informacji niejawnych i tajemnicy przedsiębiorstwa.

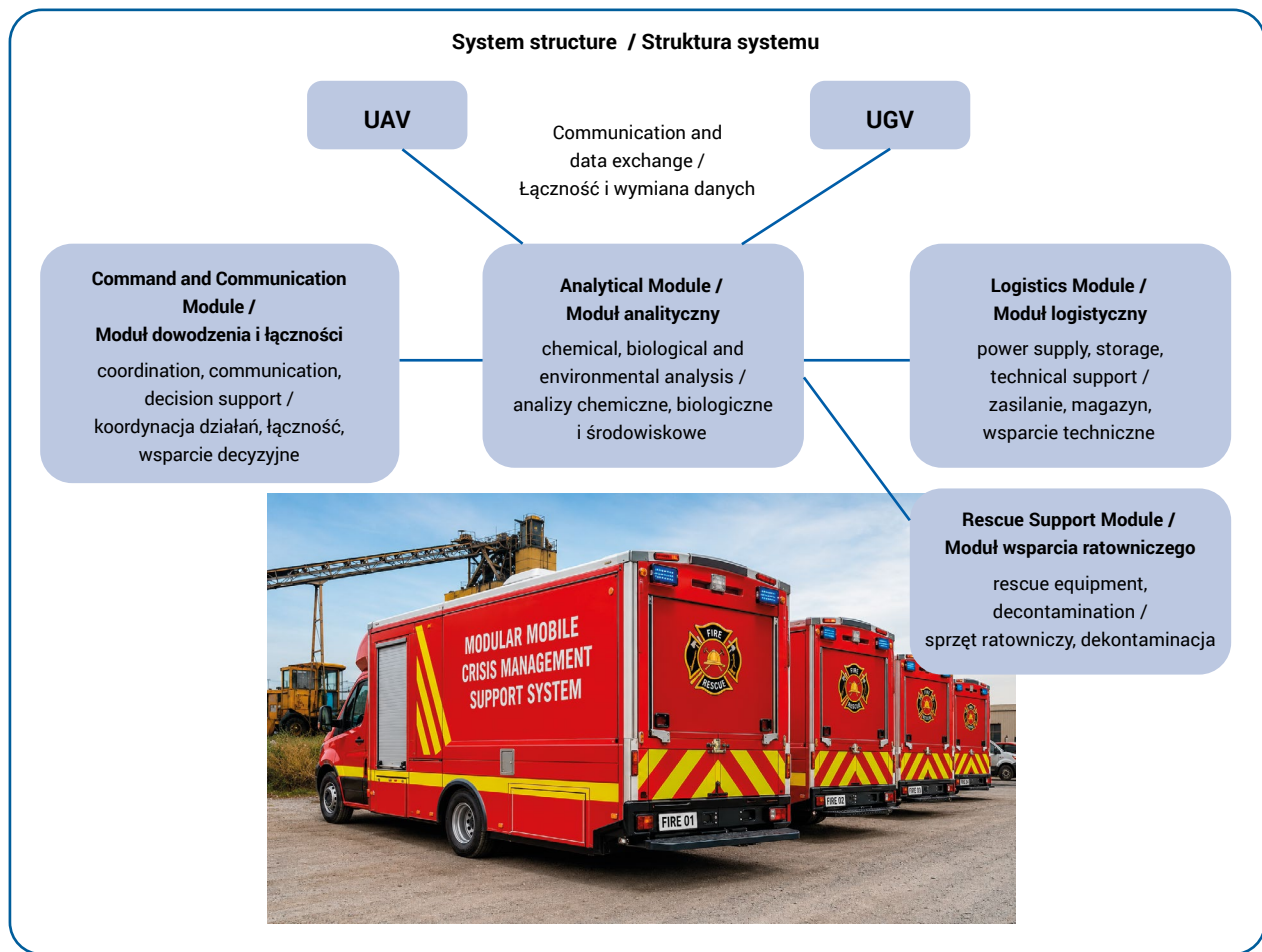
Pomimo tych ograniczeń, przedstawiona analiza stanowi wartościowy wkład w dyskusję nad kierunkami modernizacji systemu zarządzania kryzysowego w Polsce.

Concept of modular mobile crisis management support systems

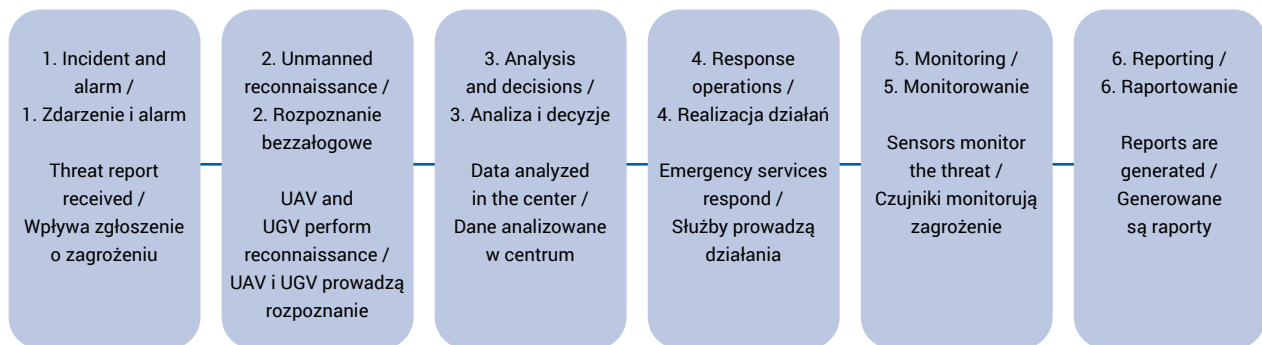
The design of the modular mobile crisis management support system, of which the structure, advantages and example course of operations is presented in Figure 1, is based on the principle of ensuring a high level of operational autonomy, interoperability and technological configuration flexibility. The foundation of the concept is the capability for independent operation in emergency conditions, while maintaining the continuity of IT, communication and analytical functions, independent of the stationary structure [3].

Koncepcja modułowych mobilnych systemów wspomagania zarządzania kryzysowego

Projekt modułowego mobilnego systemu wspomagania działań kryzysowych, którego strukturę, korzyści i przykładowy przebieg działań przedstawiono na rycinie 1, opiera się na założeniu zapewnienia wysokiego poziomu autonomii operacyjnej, interoperacyjności oraz elastyczności konfiguracji technologicznej. Fundamentem koncepcji jest zdolność do niezależnego działania w warunkach awaryjnych, z zachowaniem ciągłości funkcji informatycznych, komunikacyjnych i analitycznych, niezależnie od infrastruktury stacjonarnej [3].



Example course of operations / Przykładowy przebieg działań



Implementation benefits / Korzyści wdrożenia

- Faster response and decision-making / Szybsza reakcja i podejmowanie decyzji
- System flexibility and scalability / Elastyczność i skalowalność systemu
- Better coordination of services / Lepsza koordynacja służb
- Higher operational effectiveness / Wyższa skuteczność działań
- Increased safety / Większe bezpieczeństwo

Figure 1. Concept of modular mobile crisis management support systems – structure, advantages and example course of operations

Rycina 1. Koncepcja modułowych mobilnych systemów wspomaganie zarządzania kryzysowego – struktura, korzyści i przykładowy przebieg działań

Source: Own elaboration.

Źródło: Opracowanie własne.

Functionally, the system must be focused on supporting multi-faceted incidents, with heavy emphasis on CBRNE incidents, including incidents involving explosive substances, such as ammonium nitrate. The template for the designed platform are the solutions implemented in mobile laboratories of the State Fire Service with sealed workspace, segmentation of functional zones (operational, analytical, biological, technical), power self-sufficiency (generators, VFI-rated UPS) and integration with CBRN Reachback systems and GIS/ICT networks [1], [7]. These solutions enable the detection and analysis of hazardous substances at the incident scene, without the need to transport the samples. This shortens the response time and increases the safety of operators.

From the technical perspective, it is assumed to use container-based and modular system structure, which is easy to scale and reconfigure depending on the incident scenario. The system must be equipped with data servers, local ITC networks (LAN/WLAN), satellite communication and full support with analytical data for real time operation. Edge computing solutions are also essential to enable local data processing, supported by artificial intelligence systems for early hazard detection and development prediction.

The functional assumptions of MMCSS include:

- modularity and specialisation – division into independent functional modules (analytics, command, logistics, communication, decontamination), which may operate independently or as one unified system. The analytics module uses State Fire Service solutions (GC-MS, FTIR, Ramana/XRF spectrometers) for quick identification of hazardous substances in air, water and soil, including toxic gases (NO_x , NH_3) and explosive residues. The command module integrates AI and Big Data systems for predicting the contamination distribution and crisis resource management;
- operator and environmental safety – use of pressure zones (pressure cascade -30 Pa), disinfection airlocks (BSL-3), PID/IMS gas concentration sensors and alarm systems for explosion hazard zones. The ventilation system with HEPA H14 filters clean air at 99.995% level for particles $0.3 \mu\text{m}$ particles;
- interoperability – compliance with NATO standards (STANAG 4632, AEP-66) and KSRG principles to enable cooperation with the State Fire Service, the military and EU ERCC. The CBRN Reachback platform enables consulting experts (e.g. CLKP, IAEA) in sample analysis, which is particularly important for rare or unknown substances;
- innovations in the context of explosion hazard, AI algorithms for simulating exposure zones and optimum emergency escape routes (inspired by the iSCAPE project), remediation module with the databases of Voivodship Inspectorate of Environmental Protection. The prediction system uses contamination propagation models in real time, while integrating weather, topography and city planning data.

Technical assumptions project a platform to place on semi-trailer with pneumatic suspension (modelled after State Fire

Funkcjonalnie system musi być zorientowany na obsługę incydentów wielowątkowych, z dużym naciskiem na zdarzenia CBRNE, w tym z udziałem substancji wybuchowych takich jak azotan amonu. Wzorem dla projektowanej platformy są rozwiązania wdrożone w mobilnych laboratoriach PSP, w których zapewniono hermetyczność przestrzeni roboczej, segmentację stref funkcyjnych (operacyjna, analityczna, biologiczna, techniczna), samowystarczalność zasilania (agregaty, UPS-y klasy VFI) oraz integrację z systemami CBRN Reachback i sieciami GIS/ICT [1], [7]. Rozwiązania te umożliwiają detekcję i analizę substancji niebezpiecznych w miejscu zdarzenia, bez konieczności transportu próbek. Pozwala to skrócić czas reakcji i zwiększyć bezpieczeństwo operatorów.

Z technicznego punktu widzenia zakłada się wykorzystanie kontenerowej, modułowej struktury systemu, która może być łatwo skalowana i rekonfigurowana w zależności od scenariusza zdarzenia. System musi być wyposażony w serwery danych, lokalne sieci teleinformatyczne (LAN/WLAN), łączność satelitarną oraz pełne wsparcie dla pracy w czasie rzeczywistym z danymi analitycznymi. Kluczowe znaczenie mają tu również rozwiązania klasy *edge computing*, umożliwiające lokalne przetwarzanie danych, wsparte systemami sztucznej inteligencji do wczesnego wykrywania zagrożeń i predykcji ich rozwoju.

Założenia funkcjonalne MMCZK obejmują:

- modułowość i specjalizację – podział na niezależne moduły funkcjonalne (analityczny, dowodzenia, logistyczny, komunikacyjny, dekontaminacyjny), które mogą działać samodzielnie lub jako jeden spójny system. Moduł analityczny wykorzystuje rozwiązania PSP (GC-MS, FTIR, spektrometry Ramana/XRF) do szybkiej identyfikacji substancji niebezpiecznych w powietrzu, wodzie i glebie, w tym gazów toksycznych (NO_x , NH_3) oraz pozostałości wybuchowych. Moduł dowodzenia integruje systemy AI i Big Data do predykcji rozprzestrzeniania skażeń oraz zarządzania zasobami kryzysowymi;
- bezpieczeństwo operatorów i środowiska – zastosowanie stref ciśnieniowych (kaskada ciśnień -30 Pa), słuz dezynfekcyjnych (BSL-3), czujników stężeń gazów PID/IMS oraz systemów alarmowych dla stref zagrożonych wybuchem. System wentylacyjny z filtrami HEPA H14 zapewnia oczyszczanie powietrza na poziomie 99,995% dla cząstek o wielkości $0,3 \mu\text{m}$;
- interoperacyjność – zgodność z normami NATO (STANAG 4632, AEP-66) oraz zasadami KSRG, umożliwiającą współpracę z PSP, wojskiem i ERCC UE. Platforma CBRN Reachback umożliwia konsultacje z ekspertami (np. CLKP, IAEA) w analizie próbek, co jest szczególnie istotne w przypadku rzadkich lub nieznanymi substancji;
- innowacje w kontekście zagrożenia wybuchowego – algorytmy AI do symulacji stref rażenia i optymalnych tras ewakuacji (inspirowane projektem iSCAPE), moduł remediacji zintegrowany z bazami danych WIOŚ. System predykcji wykorzystuje modele rozprzestrzeniania się skażeń w czasie rzeczywistym, integrując dane meteorologiczne, topograficzne i urbanistyczne.

Założenia techniczne przewidują platformę na naczepie z zawieszeniem pneumatycznym (wzorowaną na laboratoriach PSP),

Service laboratories), deployment time ≤ 45 minutes, operational autonomy ≥ 72 hours and integration with Smart City systems [7].

The structure of the designed MMCMSS is based on multi-functional segmentation, which enables simultaneous reconnaissance, analytics, command and communication operations. The system consists of physical container modules or special bodies on goods vehicle chassis, enabling the independent functioning of each segment or integration in the task system [3].

czas rozstawienia ≤ 45 minut, niezależność operacyjną ≥ 72 godzin oraz integrację z systemami Smart City [7].

Struktura projektowanego MMCZK opiera się na wielofunkcyjnej segmentacji funkcjonalnej, umożliwiającej jednoczesne prowadzenie działań rozpoznawczych, analitycznych, dowódczych i komunikacyjnych. System składa się z fizycznych modułów kontenerowych lub zabudów specjalistycznych na podwoziach pojazdów ciężarowych, z możliwością niezależnego funkcjonowania każdego segmentu lub ich integracji w układzie zadaniowym [3].

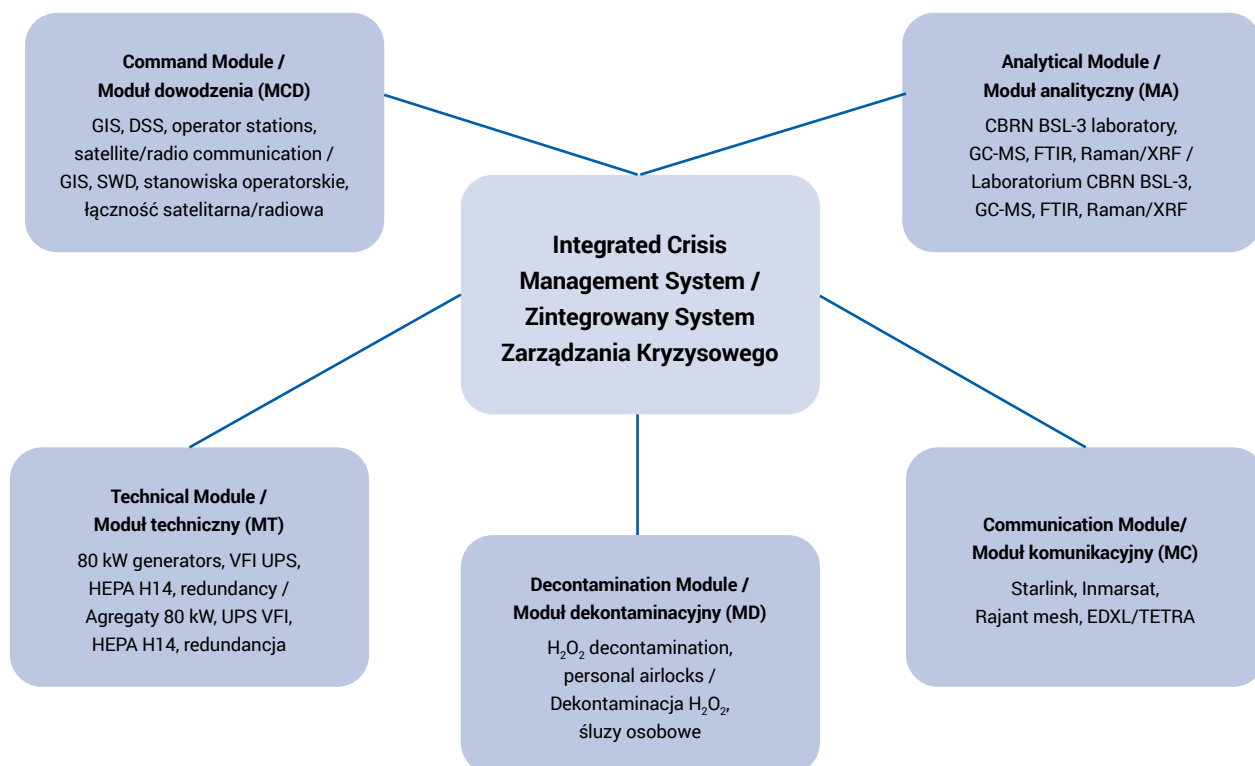


Figure 2. Components of modular mobile crisis management support systems

Rycina 2. Elementy składowe modułowych mobilnych systemów wspomagania zarządzania kryzysowego

Source: Own elaboration.

Źródło: Opracowanie własne.

The basic modules of the system shown in Figure 2 include:

1. Command module (MCD) – field control station, equipped with ICT infrastructure, GIS tools, operator stations and satellite, radio and network communication. This module functions as the “brain” of operation, which integrates the data from mobile laboratory, drones, ground cameras, GPS, rescue teams and environmental sensors in a single GIS platform. It is equipped with decision-making support systems (SWD) and links to exchange data with crisis management centres at the voivodship and national level.
2. Analytics module (MA) – CBRN-rated mobile laboratory (compliant with BSL-3 standards), which enables physical, chemical and biological analysis of samples in field conditions. The equipment includes GC-MS, FTIR, Ramana/XRF spectrometers, ion chronograph and

Pokazane na rycinie 2 podstawowe moduły systemu obejmują:

1. Moduł dowodzenia (MCD) – stanowisko kierowania w terenie, wyposażone w infrastrukturę ICT, narzędzia GIS, stanowiska operatorskie oraz łączność satelitarną, radiową i sieciową. Moduł ten pełni funkcję „mózgu” operacji, integrując dane z laboratorium mobilnego, dronów, kamer naziemnych, GPS zespołów ratowniczych i czujników środowiskowych na jednej platformie GIS. Wyposażony jest w systemy wspomagania decyzji (SWD) oraz łączy do wymiany danych z centrami zarządzania kryzysowego szczebla wojewódzkiego i krajowego.
2. Moduł analityczny (MA) – mobilne laboratorium klasy CBRN (zgodne z normami BSL-3), umożliwiające analizę fizykochemiczną i biologiczną próbek w warunkach polowych. Wyposażenie obejmuje GC-MS, FTIR, spektrometry

radiation detectors. This module enables identification of hazardous substances (including AA thermal decomposition products AA: NO_x and NH₃) directly on site, without the time-consuming transport of samples to stationary test units. The time to obtain reliable results of analysis can be shortened from several hours to 45–90 minutes from vehicle deployment [7].

3. Technical module (MT) – power generators (80 kW), VFI-rated UPSs, air conditioning and air filtering systems (HEPA H14 filters). It ensures the power self-sufficiency and independence of external infrastructure. The power supply system is redundant. A failure of one source does not interrupt the power supply to critical equipment.
4. Communication module (MC) – responsible for maintaining internal and external communication continuity, even if the civilian infrastructure is lost. It includes satellite communication (Starlink, Inmarsat), mesh network (Rajant BreadCrumb®) and data exchange systems (EDXL, CAP, TETRA). It provides sufficient throughput for video transmission from drones in real-time and analytics data exchange with expert centres.
5. Decontamination module (MD) – supports the decontamination of equipment and samples and protection of the personnel operating in chemical contamination zones. Equipped with gas decontamination systems (hydrogen peroxide) and personnel airlocks with water shower. It enables the decontamination of personnel and equipment without the need to leave the hazard zone.

The logical structure of the system is service-based, with each module performing operational functions (OF) in conformity with EU standardisation and MIRACLE project principles. This enables interoperability, not only between modules, but also with external entities of the crisis management system, such as the State Fire Service, Police, State Sanitary Inspection or local- and voivodship-level crisis management centres [1].

With its modularity, the system can be implemented in a scalable model, from a single vehicle to support local operations to a comprehensive set of operational components functioning as a mobile command base in case of mass or cross-border incidents. Two operating modes are designed: the “Fast Response” mode (activation of the analytics module and the command module within 30 minutes) and the “Full Scale” mode (deployment of all modules within 90 minutes) [3].

The effectiveness of the MMCMS depends on the degree of integration with the already functioning institutional and technical infrastructure of the public safety system. The designed concept provides for full operational compliance with national and local crisis management structures, including the command stations of the State Fire Service, State Fire Service units specialised in chemical reconnaissance and chemical rescue (SGRChem-Eko), as well as civilian crisis management centres of public administration [3].

From the technical perspective, integration involves above all interoperational communication (radio, satellite, IP), data formats (e.g. GIS, EDXL, CAP), command software compatibility and operability in complex IT environments. The mobile data centre,

Ramana/XRF, chromatograf jonowy oraz detektory radiacyjne. Moduł ten umożliwia identyfikację substancji niebezpiecznych (w tym produktów rozkładu termicznego AA – NO_x i NH₃) bezpośrednio w miejscu zdarzenia, z pominięciem czasochłonnego transportu próbek do stacjonarnych jednostek badawczych. Czas uzyskania wiarygodnych wyników analizy może zostać skrócony z kilkunastu godzin do 45–90 minut od momentu rozstawienia pojazdu [7].

3. Moduł techniczny (MT) – agregaty prądowłórcze (80 kW), UPS-y klasy VFI, klimatyzacja i systemy filtracji powietrza (filtry HEPA H14). Zapewnia samowystarczalność energetyczną i niezależność od infrastruktury zewnętrznej. System zasilania jest zredundowany – awaria jednego źródła nie powoduje przerw w dostawie energii do urządzeń krytycznych.
4. Moduł komunikacyjny (MC) – odpowiedzialny za utrzymanie ciągłości łączności wewnętrznej i zewnętrznej, także w warunkach utraty infrastruktury cywilnej. Obejmuje łączność satelitarną (Starlink, Inmarsat), sieci mesh (Rajant BreadCrumb®) oraz systemy wymiany danych (EDXL, CAP, TETRA). Zapewnia przepustowość wystarczającą do transmisji obrazu z dronów w czasie rzeczywistym oraz wymiany danych analitycznych z centrami eksperckimi.
5. Moduł dekontaminacyjny (MD) – wspierający dekontaminację wyposażenia i próbek oraz ochronę personelu działającego w strefach skażeń chemicznych. Wyposażony w systemy dekontaminacji gazowej (nadtlenek wodoru) oraz słuzy osobowe z prysznicem wodnym. Umożliwia dekontaminację personelu i sprzętu bez konieczności opuszczania strefy zagrożenia.

Struktura logiczna systemu oparta jest na modelu usługowym, w którym każdy moduł realizuje funkcje operacyjne (ang. *operational functions*, OF) zgodne z zasadami standaryzacji UE i projektu MIRACLE. Dzięki temu możliwa jest interoperacyjność nie tylko między modułami, ale także z zewnętrznymi podmiotami systemu zarządzania kryzysowego, takimi jak Państwowa Straż Pożarna, Policja, Państwowa Inspekcja Sanitarna czy centra zarządzania kryzysowego szczebla lokalnego i wojewódzkiego [1].

Modułowość systemu umożliwia jego wdrożenie w modelu skalowalnym – od pojedynczego pojazdu wspierającego lokalne działania, po kompleksowy zestaw elementów operacyjnych funkcjonujący jako mobilna baza dowodzenia w przypadku zdarzeń o charakterze masowym lub transgranicznym. Przewidziano dwa tryby operacyjne: tryb „Fast Response” (uruchomienie modułu analitycznego i dowodzenia w 30 minut) oraz tryb „Full Scale” (rozwiniecie wszystkich modułów w 90 minut) [3].

Skuteczność MMCZK zależy od stopnia integracji z już funkcjonującą infrastrukturą instytucjonalną i techniczną systemu bezpieczeństwa publicznego. Projektowana koncepcja zakłada pełną zgodność operacyjną z krajowymi i lokalnymi strukturami zarządzania kryzysowego, w tym ze stanowiskami kierowania Państwowej Straży Pożarnej, jednostkami PSP specjalizującymi się w rozpoznaniu chemicznym i ratownictwie ekologicznym (SGRChem-Eko), a także z cywilnymi centrami zarządzania kryzysowego administracji publicznej [3].

described in the concept by the Kielce University of Technology, is designed as compatible with voivodship crisis management centres, the Alert RCB platform and the national ITC system (SWD PSP) [9].

The design provides for three-level integration:

1. Integration with crisis infrastructure – direct radio communication with SGRChem-Eko, data exchange with the mobile laboratory of the State Fire Service in the CBRN Reachback format, sharing NH_4NO_3 analysis results in real time, integration with IoT Smart City sensors (NH_3/NO_x concentration monitors), automatic notifications to the VAS warning system.
2. Procedural compatibility – the adaptation of the SIBCRA NATO (AEP-66) model for sampling after NH_4NO_3 explosions (sequence: XRF explosive residue analysis → IC waters toxicity analysis → secondary detonation risk assessment), harmonisation with the National Crisis Management Plan with regards to evacuation and contamination neutralisation (Voivodship Inspectorate of Environmental Protection procedures for nitrates).
3. Technical interoperability – hybrid cloud (IBM/Cloudware) with prediction algorithms based on the iSCAPE model, automatic contamination data transfer via the CECIS platform to EU ERCC, access to the ammonium nitrate warehouse register of the Ministry of National Defence and Ministry of Internal Affairs and Administration, integration with the military CBRN hazard detection system.

An additional integration aspect is system readiness to cooperate with international partners under the EU Civil Protection Mechanism. Mobile laboratories of the State Fire Service, as component of SGRChem-Eko, are already part of European operations structures and modular command centres can be developed according to the same model. This enables Polish units to participate in cross-border training, support operations and development of common response procedures for incidents with hazardous materials [1].

The application of the MMCMSS is justified above all in the context of complex crisis incidents, with a high level of chemical, biological or explosive danger, as traditional stationary proves insufficient or unavailable. Four detailed use scenarios have been developed [3].

Scenario 1 – Explosion hazard in NH_4NO_3 warehouse

Fire in ammonium nitrate warehouse in river port or industrial facility. Detonation and toxic gas (NO_x , NH_3) emission risk. The analytics module of the State Fire Service (GC-MS, FTIR) identifies the gas concentration and critical temperature ($>300^\circ\text{C}$) within 45 minutes. The AI command module simulates explosion risk zones by integrating data from IoT sensors and weather forecasts. Automatic alerts to the contamination and notification detection system order evacuation of the population; the

Z punktu widzenia technicznego integracja dotyczy przede wszystkim interoperacyjności łączności (radiowej, satelitarnej, IP), formatów danych (np. GIS, EDXL, CAP), kompatybilności oprogramowania dowodzenia oraz możliwości pracy w środowiskach złożonych informatycznie. Mobilne centrum danych, opisane w koncepcji Politechniki Świętokrzyskiej, projektowane jest z uwzględnieniem kompatybilności z wojewódzkimi centrami zarządzania kryzysowego, platformą Alert RCB oraz krajowym systemem teleinformatycznym (SWD PSP) [9].

Projekt zakłada trójpoziomową integrację:

1. Integracja z infrastrukturą kryzysową – bezpośrednia łączność radiowa z SGRChem-Eko, wymiana danych z mobilnym laboratorium PSP w formacie CBRN Reachback, udostępnianie wyników analiz NH_4NO_3 w czasie rzeczywistym, integracja z czujnikami IoT Smart City (monitoring stężeń NH_3/NO_x), automatyczne powiadomienia do systemu ostrzegania DSO.
2. Zgodność proceduralna – adaptacja modelu SIBCRA NATO (AEP-66) dla poboru próbek po wybuchach NH_4NO_3 (sekwencja: identyfikacja pozostałości wybuchowych XRF → analiza toksyczności wód IC → ocena ryzyka wtórnej detonacji), harmonizacja z Krajowym Planem Zarządzania Kryzysowego w zakresie ewakuacji i neutralizacji skażeń (protokoły WIOŚ dla azotanów).
3. Interoperacyjność techniczna – chmura hybrydowa (IBM/Cloudware) z algorytmami predykcji opartymi na modelu iSCAPE, automatyczne przesyłanie danych o skażeniach via platforma CECIS do ERCC UE, dostęp do rejestru MON i MSWiA magazynów saletry amonowej, integracja z systemem wykrywania zagrożeń CBRN wojska.

Dodatkowym aspektem integracyjnym jest gotowość systemu do współpracy z partnerami międzynarodowymi w ramach Mechanizmu Ochrony Ludności UE. Mobilne laboratoria PSP, będące komponentem SGRChem-Eko, stanowią już część struktur operacyjnych europejskich, a modułowe centra dowodzenia mogą być rozwijane zgodnie z tym samym modelem interoperacyjnym. Umożliwia to udział polskich jednostek w transgranicznych ćwiczeniach, operacjach wsparcia oraz rozwój wspólnych procedur reagowania na incydenty z udziałem materiałów niebezpiecznych [1].

Zastosowanie MMCZK znajduje uzasadnienie przede wszystkim w kontekście złożonych zdarzeń kryzysowych, w których występuje wysoki poziom zagrożenia chemicznego, biologicznego lub wybuchowego, a tradycyjna infrastruktura stacjonarna okazuje się niewystarczająca lub niedostępna. Opracowano cztery szczegółowe scenariusze użycia [3].

Scenariusz 1 – Zagrożenie wybuchem w magazynie NH_4NO_3

Pożar w magazynie saletry amonowej w porcie rzeczny lub zakładzie przemysłowym. Ryzyko detonacji i emisji toksycznych gazów (NO_x , NH_3). Moduł analityczny PSP (GC-MS, FTIR) w ciągu 45 minut identyfikuje stężenie gazów i temperaturę krytyczną ($>300^\circ\text{C}$). Moduł dowodzenia AI symuluje strefy ryzyka wybuchu, integrując dane z czujników IoT i prognoz pogody. Automatyczne alerty do systemu wykrywania skażeń i powiadamiania nakazują ewakuację ludności; straż pożarna wdraża prewencyjne

fire service applies preventative cooling to the warehouse. With early detection of the thermal decomposition of NH_4NO_3 , detonation can be prevented.

Scenario 2 – Ammonium nitrate explosion in industrial zone

NH_4NO_3 detonation in chemical facility. Effects: soil contamination with nitrates, air contamination with NO_x . The logistics module neutralises soil contamination with nitrate binding agents (in accordance with Voivodship Inspectorate of Environmental Protection procedures). The drones of the State Fire Service with 3D mapping (LIDAR) generate a contamination map in GIS. The Reachback platform sends water analysis results (IC spectrometer) to CLKP for the purposes of water intake risk assessment. It results in the reconstruction of the course of explosion and quick remediation of the soil and groundwater.

Scenario 3 – Cross-border training in the EU mechanism

Simulation of NH_4NO_3 spreading on the PL-CZ border, with EU ERCC involvement. The command module integrates data from Czech air sensors via the CECIS platform. The NATO SIBCRA procedure: soil sampling by the State Fire Service and XRF analysis in real time. AI interface test: the contamination spreading prediction algorithm (iSCAPE model) verifies consistence with partner data. It results in the confirmation of interoperability with EU systems and effectiveness of Reachback procedures.

Scenario 4 – Long-term monitoring of NH_4NO_3 transport

Supervision over ammonium nitrate transport in urban agglomeration (sabotage risk). The analytics module as mobile control point: PID/IMS sensors along the travel route measure the NH_3 concentration, the GIS system tracks tankers in real time. Integration with MON base: automatic checking of permissible transport routes for hazardous materials. It results in the detection and blocking of an illegal tanker parking attempt near the water intake.

Technical system analysis on the example of the mobile CBRNE laboratory of the State Fire Service

The mobile CBRNE analysis laboratory of the State Fire Service, being a key component of the MMCMSS, was designed as self-sufficient unit, intended for operation in field conditions, in accordance with the requirements for BSL-3 structures (biological safety level used in laboratories testing for microbes, which may cause severe or lethal diseases in people). The vehicle design and engineering solutions in use enable conducting chemical, biological and radiation analyses, while keeping the users and environment in full safety [7].

The laboratory body was produced based on a special design 3-axle semi-trailers with pneumatic suspension to enable safe transport of equipment sensitive to shocks and vibrations. The semi-trailer was equipped with hydraulic stabilisation supports to enable operation in stationary mode, without the need to attach a tractor unit. The time to deploy and achieve operational readiness is not more than 45 minutes [7].

chłodzenie magazynu. Wczesne wykrycie procesu termicznego rozkładu NH_4NO_3 pozwala zapobiec detonacji.

Scenariusz 2 – Wybuch saletry amonowej w strefie przemysłowej

Detonacja NH_4NO_3 w zakładzie chemicznym. Skutki: skażenie gleby azotanami, skażenie powietrza NO_x . Moduł logistyczny neutralizuje skażenia gleby środkami wiążącymi azotany (według procedur WIOŚ). Drony PSP z mapowaniem 3D (LIDAR) tworzą mapę skażeń w GIS. Platforma Reachback przesyła wyniki analiz wody (spektrometr IC) do CLKP w celu oceny ryzyka dla ujęć wody. Rezultatem jest odtworzenie przebiegu wybuchu oraz szybka remediacja gleby i wód gruntowych.

Scenariusz 3 – Ćwiczenia transgraniczne w mechanizmie UE

Symulacja rozsypania się NH_4NO_3 na granicy PL-CZ z udziałem ERCC UE. Moduł dowodzenia integruje dane z czeskich czujników powietrza via platformę CECIS. Procedura SIBCRA NATO: pobór próbek gleby przez PSP i analiza XRF w czasie rzeczywistym. Test interfejsu AI: algorytm predykcji rozprzestrzeniania skażeń (model iSCAPE) weryfikuje zgodność z danymi partnerów. Rezultatem jest potwierdzenie interoperacyjności z systemami UE i skuteczności procedur Reachback.

Scenariusz 4 – Długotrwały monitoring transportu NH_4NO_3

Nadzór nad transportem saletry amonowej przez aglomerację miejską (ryzyko sabotażu). Moduł analityczny jako mobilny punkt kontroli: czujniki PID/IMS na trasie przejazdu mierzą stężenie NH_3 , system GIS śledzi lokalizację cystern w czasie rzeczywistym. Integracja z bazą MON: automatyczne sprawdzanie dopuszczalnych tras przewozu materiałów niebezpiecznych. Rezultatem jest wykrycie i zablokowanie próby nielegalnego postoju cysterny w pobliżu ujęcia wody.

Analiza techniczna systemu na przykładzie mobilnego laboratorium CBRNE PSP

Mobilne laboratorium analityczne CBRNE PSP, stanowiące kluczowy komponent MMCK, zostało zaprojektowane jako samowystarczalna jednostka, przeznaczona do pracy w warunkach terenowych zgodnie z wymaganiami dla obiektów klasy BSL-3 (poziom bezpieczeństwa biologicznego stosowany w laboratoriach badających drobnoustroje, które mogą powodować poważne lub śmiertelne choroby u ludzi). Konstrukcja pojazdu oraz zastosowane rozwiązania inżynierskie pozwalają na prowadzenie analiz chemicznych, biologicznych i radiacyjnych z zachowaniem pełnego bezpieczeństwa użytkowników oraz otoczenia [7].

Zabudowę laboratoryjną wykonano na bazie specjalnie zaprojektowanej trzyosiowej naczepy z zawieszeniem pneumatycznym, umożliwiającej bezpieczny transport urządzeń wrażliwych na wstrząsy i wibracje. Naczepę wyposażono w hydrauliczne podpory stabilizujące, umożliwiające pracę w trybie stacjonarym, bez konieczności podpięcia ciągnika siodłowego. Czas

The functional layout of the laboratory consists of four main compartments [7]:

1. Operational compartment (A) – the sliding segment of the semi-trailer designed to manage onboard systems, operating as the supervision centre and climate buffer. After deploying the vehicle, the sliding structure extends the workspace. This compartment is equipped with operator stations, data visualisation systems and external communication.
2. Biological compartment (B) – the laboratory meeting the BSL-3 class air-tightness requirements, equipped with class III sealed glove box, fume hood, autoclave, decontamination system, HVAC system and airlocks: input and personnel. The compartment maintains negative pressure –30 Pa in relation to the environment, which prevents the outflow of potentially contaminated air.
3. Chemical compartment (C) – central part of the laboratory, designed for physical and chemical analyses, equipped with chromatographs, spectrometers, explosion-proof fume hood and laboratory sink with drainage to waste tanks. This is the largest workspace, which enables comprehensive qualitative and quantitative analysis of hazardous substances.
4. Technical zones – contains support systems (filters, ventilation, power supply systems). Located on vehicle sides, ensures easy access to devices that require maintenance.

The mobile CBRNE laboratory of the State Fire Service is equipped with advanced analytical equipment that enable identification of a wide spectrum of chemical, biological and radiation hazards. Equipment was selected according to the capability of quick and precise identification of hazardous substances with varied environmental matrices [1], [7].

The chemical module includes:

- GC-MS gas chromatograph with FPD and FTIR detectors – used to detect and identify combat agents, pesticides, aromatic and chlorinated compounds. It enables the analysis of gas, liquid and solid samples with detection at ppm/ppb level;
- the FTIR/ATR spectrometer with gas and liquid analysis attachment – enables quick identification of chemical substances in environmental samples. The ATR (attenuated total reflectance) technology enables the analysis without sample preparation;
- the spectrophotometer UV-VIS (HACH DR6000) – used to determine contaminants in water and soil (ChZT, BZT, heavy metals, pesticides). It enables running more than 200 different tests with wavelength selection;
- ion chromatograph (IC) – enables simultaneous and automatic analysis of the most important anions (chlorides, sulphates, nitrates, phosphates) and cations (sodium, potassium, calcium, magnesium) in water samples. It shortens the time of environmental quality assessment compared to traditional methods of single UV-VIS analysis;
- microscope and manual Ramana spectrometers – used to analyse solids and explosives. Ramana spectroscopy

rozstawienia i osiągnięcia gotowości operacyjnej wynosi nie więcej niż 45 minut [7].

Układ funkcjonalny laboratorium składa się z czterech głównych przedziałów [7]:

1. Przedział operacyjny (A) – rozsuwany segment naczepy przeznaczony do zarządzania systemami pokładowymi, pełniący funkcję centrum nadzoru i bufora klimatycznego. Po rozstawieniu pojazdu konstrukcja wysuwana zwiększa przestrzeń roboczą. Przedział ten wyposażony jest w stanowiska operatorskie, systemy wizualizacji danych oraz łączność zewnętrzną.
2. Przedział biologiczny (B) – laboratorium spełniające warunki hermetyczności klasy BSL-3, wyposażone w komorę rękawicową klasy III, dygestorium, autoklaw, system dekontaminacji, system HVAC oraz służę: podawczą i osobową. Przedział utrzymuje podciśnienie –30 Pa względem otoczenia, co zapobiega wydostawaniu się potencjalnie skażonego powietrza.
3. Przedział chemiczny (C) – centralna część laboratorium przeznaczona do analiz fizykochemicznych, wyposażona w chromatografy, spektrometry, dygestorium przeciwwybuchowe oraz zlew laboratoryjny z systemem odpływu do zbiorników odpadów. Jest to największa przestrzeń robocza, umożliwiającą kompleksową analizę jakościową i ilościową substancji niebezpiecznych.
4. Strefy techniczne – zawierające instalacje wspierające (filtry, wentylacja, systemy zasilania). Zlokalizowane po bokach pojazdu, zapewniają łatwy dostęp do urządzeń wymagających konserwacji.

Mobilne laboratorium CBRNE PSP jest wyposażone w zaawansowany sprzęt analityczny umożliwiający identyfikację szerokiego spektrum zagrożeń chemicznych, biologicznych i radiacyjnych. Przy doborze aparatury kierowano się zdolnością do szybkiej i precyzyjnej identyfikacji substancji niebezpiecznych w zróżnicowanych matrycach środowiskowych [1], [7].

Moduł chemiczny obejmuje:

- chromatograf gazowy GC-MS z detektorami FPD i FTIR – służący do detekcji i identyfikacji środków bojowych, pestycydów, związków aromatycznych i chlorowcopochodnych. Umożliwia analizę próbek gazowych, ciekłych i stałych z detekcją na poziomie ppm/ppb;
- spektrometr FTIR/ATR z przystawką do analizy gazów i cieczy – umożliwiający szybką identyfikację substancji chemicznych w próbkach środowiskowych. Technika ATR (ang. *attenuated total reflectance*) pozwala na analizę bez przygotowania próbki;
- spektrofotometr UV-VIS (HACH DR6000) – stosowany do oznaczania zanieczyszczeń w wodzie i glebie (ChZT, BZT, metale ciężkie, pestycydy). Umożliwia przeprowadzenie ponad 200 różnych testów z automatycznym doбором długości fali;
- chromatograf jonowy (IC) – umożliwiający równoczesną, automatyczną analizę najważniejszych anionów (chlorki, siarczany, azotany, fosforany) oraz kationów (sód, potas, wapń, magnez) w próbkach wodnych. Znacznie skraca czas oceny jakości środowiska w porównaniu do tradycyjnych metod pojedynczych analiz UV-VIS;

enables identifying substances by directly illuminating the sample with a laser beam, with no need to prepare it.

- PID and IMS/AP4C sets – for quick identification of hazardous substances in air. Photoionisation detectors (PID) measure the concentration of volatile organic compounds and ion mobility spectrometers (IMS) identify combat agents and toxic industrial agents;
- XRF spectrometers – for element composition analysis. It enables identifying heavy metals and other elements in solid samples without destroying them.

The biological module is designed based on BSL-3 class biological safety requirements, applicable when working with high risk airborne microbes. The equipment includes [7]:

- PCR detection unit – an advanced system that isolates genetic material (DNA or RNA) and analyses it for pathogens, which enables simultaneous identification of at least 10 different biological agents considered as biological weapon. The unit is suitable for safe operation inside the glow box in negative pressure conditions;
- one time colorimetric tests – for quick pre-assessment of samples, primarily designed to analyse powders and loose substances, which enable detecting proteins, bacterial spores and pH reaction determination;
- bioluminescence meter – for detecting, in accordance with ATP methods, on surfaces and in liquid substances, which enable quick assessment of the biological contamination degree;
- mechanical homogeniser – for preparing biological samples in hermetically sealed, single use samples, which reduces the risk of releasing infective material during the processing;
- sample preparation systems – including laboratory centrifuges, shakers for mixing small volumes and set of automatic pipettes with filters suitable for autoclave sterilisation.

Radiation and nuclear hazards are detected using [7]:

- polimaster radiation spectrometer – detection of alpha, beta, gamma and neutron radiation, with capability for data transmission to the laboratory management system;
- portable gamma radiation spectrometer based on semiconductor HPGe detector – for identifying more than 400 different radioactive isotopes. Designed for identification and quantitative analysis of radionuclides emitting gamma radiation and detailed spectral characteristics of environmental samples (soil, water, air, industrial materials).

Spectrometric measurements are conducted in accordance with standard operating procedures of the International Atomic Energy Agency (IAEA) and NATO, with acquisition time from 1–5 minutes (quick scanning) to 15–60 minutes (accurate quantitative analysis). These devices are fully compatible with SIBCRA procedures and data exchange systems under CBRN Reachback [7].

The laboratory features advanced filtering and airflow control units as basis of safe handling of biologically and radiologically hazardous materials. The ventilation system integrated with filtering ventilation assembly generates a precisely controlled

- mikroskop i ręczne spektrometry Ramana – służące do analizy substancji stałych i materiałów wybuchowych. Spektroskopia Ramana pozwala na identyfikację substancji przez bezpośrednie oświetlenie próbki wiązką lasera, bez konieczności jej przygotowania;
- zestawy PID i IMS/AP4C – do szybkiego rozpoznania substancji niebezpiecznych w powietrzu. Detektory fotojonizacyjne (PID) mierzą stężenie lotnych związków organicznych, a spektrometry ruchliwości jonów (IMS) identyfikują czynniki bojowe i toksyczne przemysłowe;
- spektrometry XRF – do analizy składu pierwiastkowego. Umożliwiają identyfikację metali ciężkich i innych pierwiastków w próbkach stałych bez ich niszczenia.

Moduł biologiczny został zaprojektowany w oparciu o wymagania bezpieczeństwa biologicznego klasy BSL-3, obowiązujące przy pracy z mikroorganizmami o wysokim stopniu ryzyka, przenoszonymi drogą powietrzną. Wyposażenie obejmuje [7]:

- urządzenie do wykrywania techniką PCR – zaawansowany system izolujący materiał genetyczny (DNA lub RNA) i analizujący go pod kątem patogenów, pozwalający na jednoczesną identyfikację co najmniej dziesięciu różnych czynników biologicznych uznawanych za broń biologiczną. Urządzenie jest przystosowane do bezpiecznej pracy wewnątrz komory rękawicowej w warunkach podciśnienia;
- jednorazowe testy kolorymetryczne – do szybkiej, wstępnej oceny próbek, przeznaczone głównie do analizy proszków i substancji sypkich, umożliwiające wykrywanie białek, spor bakteryjnych oraz określenie odczynu pH;
- bioluminometr – do wykrywania zgodnie z metodyką ATP na powierzchniach i w próbkach ciekłych, umożliwiającą szybką ocenę stopnia zanieczyszczenia biologicznego;
- homogenizator mechaniczny – do przygotowania próbek biologicznych w hermetycznie zamykanych, jednorazowych próbkach, co ogranicza ryzyko uwolnienia materiału zakaźnego podczas obróbki;
- systemy przygotowania próbek – obejmujące wirówki laboratoryjne, wytrząsarki do mieszania małych objętości oraz zestaw automatycznych pipet z filtrami przystosowanych do sterylizacji w autoklawie.

Do identyfikacji zagrożeń radiacyjnych i nuklearnych służą [7]:

- spektrometr promieniowania Polimaster – detekcja promieniowania alfa, beta, gamma i neutronów, z możliwością przesyłu danych do systemu zarządzania laboratorium;
- przenośny spektrometr promieniowania gamma oparty na detektorze półprzewodnikowym HPGe – identyfikujący ponad 400 różnych izotopów promieniotwórczych. Przeznaczony do identyfikacji i ilościowej analizy radionuklidów emitujących promieniowanie gamma oraz szczegółowej charakterystyki widmowej próbek środowiskowych (gleba, woda, powietrze, materiały przemysłowe).

Pomiary spektrometryczne są prowadzone zgodnie ze standardowymi procedurami operacyjnymi Międzynarodowej Agencji Energii Atomowej (IAEA) i NATO, z czasami akwizycji od 1–5 minut (szybkie skanowanie) do 15–60 minut (dokładne analizy ilościowe). Urządzenia te są w pełni kompatybilne z procedurami

pressure cascade to direct the airflow in accordance with zone principles and to eliminate cross-contamination risks [7].

All the air supplied to the laboratory space moves through a multi-step cleaning system, including pre-filters and high efficiency HEPA carbon filters, H14 class, which meet the requirements of PN-EN 1822 [17]. HEPA H14 filters are characterised by the particle arrest effectiveness of 99.995% for 0.3 μm particles. Filter enclosures, designed in accordance with the guidelines of PN-EN ISO 14644-3 [16], feature the leakage control and installation air-tightness function to provide the highest possible safety level before contamination leakage to the outside. System design enables decontamination of filter enclosures using hydrogen peroxide to maintain a sterile work environment [7].

Airflow parameters in the laboratory are precisely selected to ensure optimum operating conditions. The air handling unit operates the flow of 1500 m^3/h , using only external air, which excludes the recirculation of potentially contaminated air. The fan in use ensures effective air exchange at 1500 m^3/h , while maintaining proper environmental parameters in specific operating ranges. The system is designed to maintain the minimum airflow at 120 m^3/h even if any exhaust is inactive [7].

A key component of the safety system is to maintain precise a precise pressure cascade, in which the personnel airlock operates at the reference pressure of 0 Pa, however the biological compartment (B) operates at the negative pressure of -30 Pa. The ventilation and air conditioning system is controlled in fully automatic mode to ensure continuous control over the pressure cascade. During operation in the BSL-3 mode, including biological hazards, the ventilation supporting the glow box in compartment B can be disconnected to stabilise proper pressure cascade [7].

The biological compartment is equipped with advanced gas decontamination system using hydrogen peroxide to enable full sterilisation of the compartment, glow box and filtering system components. The decontamination of personnel is provided by specially designed personnel airlock equipped with water shower and protective clothing, as well as the interlock system, which prevents simultaneous opening of doors to the contaminated zone and the clean zone. The interlock system enables opening of two doors at the same time, which prevents uncontrolled airflow between zones [7].

The climate conditions in the laboratory are strictly controlled. The air supplied to individual compartments is precisely conditioned: compartments B and C are maintained in the relative humidity range of 30–50% and temperature of 22–27°C, while the technical area operates at similar humidity, although it allows a broader temperature range: 22–29°C. The air conditioning system maintains the inlet air temperature equal to the current car interior temperature (± 2 °C).

However, it should be reserved that, as noted by Bugaj and Janik [7], the mobile laboratory cannot be formally classified as fully-fledged BSL-3 laboratory, because in accordance with normative definitions this type of laboratories must be a permanent and stationary building structure. The laboratory semi-trailer of the State Fire Service as mobile structure that does not meet that requirement. It does not have an ISO 14644-3 validation certificate either. Notwithstanding, the designed functional layout and

SIBCRA oraz systemami wymiany danych w ramach CBRN Reachback [7].

Laboratorium dysponuje zaawansowanymi układami filtracji i kontroli przepływu powietrza, stanowiącymi podstawę bezpieczeństwa pracy z materiałami niebezpiecznymi biologicznie i radiologicznie. System wentylacyjny zintegrowany z zespołem filtrowentylacyjnym generuje precyzyjnie kontrolowaną kaskadę ciśnień, kierując przepływ powietrza zgodnie z zasadami strefowości i eliminując możliwość kontaminacji krzyżowej [7].

Całość powietrza dostarczanego do przestrzeni laboratoryjnej przechodzi przez wielostopniowy układ oczyszczania, obejmujący filtry wstępne oraz wysoko wydajne filtry węglowe HEPA klasy H14, które spełniają wymagania normy PN-EN 1822 [17]. Filtry HEPA H14 charakteryzują się skutecznością zatrzymywania cząstek na poziomie 99,995% dla cząstek o wielkości 0,3 μm . Obudowy filtrów, zaprojektowane zgodnie z wytycznymi normy PN-EN ISO 14644-3 [16], posiadają funkcję kontroli upływu i szczelności montażu, zapewniając najwyższy poziom zabezpieczenia przed wydostaniem się zanieczyszczeń na zewnątrz. Konstrukcja systemu umożliwia dekontaminację obudowy filtrów przy wykorzystaniu nadtlenu wodoru, gwarantując utrzymanie sterylności środowiska pracy [7].

Parametry przepływu powietrza w laboratorium zostały precyzyjnie dobrane dla zapewnienia optymalnych warunków pracy. Centrala wentylacyjna obsługuje przepływ 1500 m^3/h , wykorzystując wyłącznie powietrze zewnętrzne, co wyklucza recyrkulację potencjalnie skażonego powietrza. Zastosowany wentylator zapewnia efektywną wymianę powietrza na poziomie 1500 m^3/h , utrzymując odpowiednie parametry środowiskowe w poszczególnych przedziałach roboczych. System został zaprojektowany tak, aby nawet przy braku pracy któregoś z wyciągów zachowany był minimalny przepływ powietrza na poziomie 120 m^3/h [7].

Kluczowym elementem systemu bezpieczeństwa jest utrzymanie precyzyjnej kaskady ciśnień, gdzie służa osobowa funkcjonuje przy ciśnieniu odniesienia 0 Pa, natomiast przedział biologiczny (B) pracuje przy podciśnieniu -30 Pa. Sterowanie systemem wentylacji i klimatyzacji odbywa się w pełni automatycznie, zapewniając ciągłą kontrolę nad kaskadą ciśnień. W przypadku pracy w trybie BSL-3, obejmującej zagrożenia biologiczne, istnieje możliwość odłączenia wentylacji obsługującej dygestorium w przedziale B, w celu stabilizacji właściwej kaskady ciśnień [7].

Przedział biologiczny wyposażono w zaawansowany system dekontaminacji gazowej wykorzystujący nadtlenek wodoru, umożliwiający pełną sterylizację przedziału, komory rękawicowej oraz elementów systemu filtracyjnego. Dekontaminację personelu zapewnia specjalnie zaprojektowana służa osobowa wyposażona w prysznic wodny i odzież ochronną, a także system interlock, zapobiegający jednoczesnemu otwarciu drzwi do stref skażenia i strefy czystej. System interlock uniemożliwia otwarcie dwojga drzwi jednocześnie, co zapobiega niekontrolowanemu przepływowi powietrza między strefami [7].

Warunki klimatyczne w laboratorium podlegają ścisłej kontroli. Powietrze dostarczane do poszczególnych przedziałów jest precyzyjnie kondycjonowane: przedziały B i C utrzymywane są w zakresie 30–50% wilgotności względnej przy temperaturze 22–27 °C, zaś obszar techniczny funkcjonuje przy podobnej

technologies in use enable effective analysis of high risk samples in field conditions, in accordance with the best practices of biological safety.

Mobile CBRNE laboratories of the State Fire Service are designed in accordance with NATO guidelines and standards and national doctrine documents of Polish Armed Forces. The manufacturer of the laboratory declares the compliance of the design with the requirements in the following documents [7]:

- STANAG 4632 – Deployable NBC Analytical Laboratory – the standard defining the requirements for mobile laboratories capable of analysing contaminated materials in operation conditions;
- AEP-66 – NATO Handbook for Sampling and Identification of Biological, Chemical and Radiological Agents (SIBCRA) – the guide with standard CBRN sample collection, protection and identification procedures;
- DD/3.8(B) – Defence from mass destruction weapon in connected operations – national doctrine for common operations of the military and civilian services in the CBRN hazard environment;
- DD 4.10(A) – Medical security of the Armed Forces of the Republic of Poland – doctrine describing the medical and laboratory support in operations using biological and chemical agents.

In accordance with manufacturer's declaration, the application of these standards is essential for ensuring the readiness for CBRNE reconnaissance and analysis missions according to SIBCRA procedures and remote analytical support under the so-called "CBRN Reachback" model. The CBRN Reachback model is an integrated remote analytical support system that enables the units operating in CBRNE hazard environment to remotely transmit data, analysis results and samples to expert centres and reference laboratories outside the operation zone. This system ensures ongoing remote consultation, information exchange and operation recommendations with specialists and its purpose is to increase the effectiveness, safety and interoperability [7].

As part of international cooperation, the Union Civil Protection Mechanism (UCPM), managed by the European Commission, aimed to support response activities and mutual help of EU member states in case of natural and technological disasters, is significant as well. As part of UCPM, the Emergency Response Coordination Centre (ERCC) operates, responsible for 24-hour monitoring of crisis situations and resource coordination (transport, rescue teams, equipment). The states involved in the mechanism have access to the Common Emergency Communication and Information System (CECIS), as well as the European Help Reserve (rescEU) [1].

wilgotności, lecz dopuszcza szerszy zakres temperatur: 22–29°C. System klimatyzacji utrzymuje temperaturę powietrza na wlocie równą aktualnej temperaturze wnętrza pojazdu ($\pm 2^\circ\text{C}$).

Należy jednak zastrzec, że – jak wskazują Bugaj i Janik [7] – mobilne laboratorium nie może być formalnie sklasyfikowane jako pełnoprawne laboratorium BSL-3, ponieważ zgodnie z normatywnymi definicjami laboratorium tego typu muszą być trwałą, nieruchomą konstrukcją budowlaną. Nacze laboratorium PSP jako konstrukcja przemieszczenia mobilnego nie spełnia tego wymogu. Brak jest również certyfikacji walidacyjnej zgodnie z ISO 14644-3. Mimo to zaprojektowany układ funkcjonalny i zastosowane technologie umożliwiają skuteczne wykonywanie analiz próbek wysokiego ryzyka w warunkach terenowych, zgodnie z najlepszymi praktykami bezpieczeństwa biologicznego.

Mobilne laboratoria CBRNE PSP zostały zaprojektowane z uwzględnieniem wytycznych i standardów NATO oraz krajowych dokumentów doktrynalnych Sił Zbrojnych RP. Producent laboratorium deklaruje zgodność projektu z wymaganiami zawartymi w następujących dokumentach [7]:

- STANAG 4632 – Deployable NBC Analytical Laboratory – standard określający wymagania dla mobilnych laboratoriów zdolnych do analizy materiałów skażonych w warunkach operacyjnych;
- AEP-66 – NATO Handbook for Sampling and Identification of Biological, Chemical and Radiological Agents (SIBCRA) – informator zawierający standardowe procedury poboru, zabezpieczenia i identyfikacji próbek CBRN;
- DD/3.8(B) – Obrona przed bronią masowego rażenia w operacjach połączonych – krajowa doktryna dotycząca wspólnych działań wojska i służb cywilnych w środowisku zagrożeń CBRN;
- DD 4.10(A) – Zabezpieczenie medyczne Sił Zbrojnych Rzeczypospolitej Polskiej – doktryna opisująca wsparcie medyczne i laboratoryjne w operacjach z udziałem czynników biologicznych i chemicznych.

Zgodnie z deklaracją producenta zastosowanie tych norm ma istotne znaczenie dla zapewnienia gotowości do realizacji misji rozpoznania i analizy CBRNE według procedur SIBCRA oraz zdalnego wsparcia analitycznego w modelu tzw. „CBRN Reachback”. Model CBRN Reachback to zintegrowany system zdalnego wsparcia analitycznego, umożliwiający jednostkom działającym w środowisku zagrożeń CBRNE zdalne przekazywanie danych, wyników analiz oraz próbek do ośrodków eksperckich i laboratoriów referencyjnych znajdujących się poza strefą operacyjną. System ten zapewnia bieżącą konsultację zdalną, wymianę informacji i rekomendacji operacyjnych z udziałem specjalistów, a jego celem jest zwiększenie skuteczności, bezpieczeństwa i interoperacyjności [7].

W ramach współpracy międzynarodowej istotne znaczenie ma również Unijny Mechanizm Ochrony Ludności (ang. *Union Civil Protection Mechanism*, UCPM), zarządzany przez Komisję Europejską, którego celem jest wspieranie działań reagowania i wzajemna pomoc państw członkowskich UE w przypadku katastrof naturalnych i technologicznych. W ramach UCPM funkcjonuje Centrum Koordynacji Reagowania Kryzysowego (ang. *Emergency Response Coordination Centre*, ERCC), odpowiedzialne za

Case study: Beirut port explosion (2020)

On 4 August 2020, approx. 15:00 GMT, one of the greatest explosions unrelated to military operations in contemporary history occurred. Warehouse number 12 (Hangar 12) stored approx. 2750 tons of ammonium nitrate, deposited in 2014, after the stoppage of ship *Rhosus*, carrying the cargo from Georgia and Mozambique. For six years, the substance was stored in an unregulated manner, without proper technical supervision, fire protection or inspection of the physical and chemical condition of the stored material [6].

On the day of the incident, welding works at the warehouse gate, identified as the most probable cause of ignition of bags with fireworks and other inflammable materials nearby (e.g. wood cable reels, containers with kerosene and hydrochloric acid). The fire caused the first minor explosion, which triggered a secondary fire and intensive smoke emissions. Approx. 30 seconds later, the second much stronger explosion occurred, which caused the formation of the characteristic fireball and shockwave similar to a mushroom cloud [6].

The explosion was perceivable within the radius of several tens of kilometres, resulting in shocks comparable with earthquake with the magnitude of 3.3 on the Richter scale. The shockwave lead to the destruction or damage of more than 50 hospital buildings, tens of schools, hotels, stores and residential buildings. The windows were broken as far as 15 miles from the epicentres and the sound explosion was heard on Cyprus, more than 240 km away [6].

The disaster resulted in at least 218 dead, more than 7500 injured and estimated 300,000 residents of Beirut left homeless. Districts located in direct vicinity of the port, such as Karantina, Gemmayzeh, Jisr and Geitawi, were particularly affected. The lack of evacuation plans, fire detection systems and crisis management procedures caused chaos and delays in rescue operations [6].

From the perspective of the direct initiation mechanism, it was found that the incident was initiated by welding works at the warehouse entrance, in which in addition to AA in bags inflammable materials were stored. The presence of these components created an environment that highly favoured the development of deflagration and detonation reactions. In accordance with the described mechanism, deflagration transitioned to detonation (DDT), leading to the release of energy equivalent to the explosion of approx. 1100 tons of trotyl (TNT) [6].

At the system and organisation level, the main cause was institutional failure: lack of proper regulations on classification and supervision over the storage of hazardous chemical

całodobowe monitorowanie sytuacji kryzysowych i koordynację zasobów (transport, ekipy ratownicze, wyposażenie). Państwa uczestniczące w mechanizmie mają dostęp do wspólnej platformy wymiany informacji (ang. *Common Emergency Communication and Information System*, CECIS), a także do Europejskiej Rezerwy Pomocy (rescEU) [1].

Studium przypadku: wybuch w porcie w Bejrucie (2020)

W dniu 4 sierpnia 2020 r., około godziny 15:00 GMT, w porcie w Bejrucie doszło do jednego z najpotężniejszych wybuchów niezwiązanych z działaniami wojennymi w historii współczesnej. W magazynie numer 12 (Hangar 12) znajdowało się około 2750 ton azotanu amonu, który został zdeponowany w 2014 r. po zatrzymaniu statku *Rhosus*, przewożącego ładunek z Gruzji do Mozambiku. Przez sześć lat substancja była przechowywana w sposób nieregulowany, bez odpowiedniego nadzoru technicznego, zabezpieczeń przeciwpożarowych ani kontroli jej stanu fizykochemicznego [6].

W dniu zdarzenia prowadzone były prace spawalnicze przy bramie magazynu, które – według ustaleń – najprawdopodobniej doprowadziły do zapłonu znajdujących się w pobliżu worków z fajerwerkami i innych materiałów łatwopalnych (m.in. drewnianych bębnow kablowych, pojemników z naftą i kwasem solnym). W wyniku pożaru doszło do pierwszego, mniejszego wybuchu, który wywołał pożar wtórny i intensywne emisje dymu. Około 30 sekund później nastąpił drugi, znacznie silniejszy wybuch, w wyniku którego powstała kula ognia i fala uderzeniowa przypominająca grzyb atomowy [6].

Wybuch był odczuwalny w promieniu kilkudziesięciu kilometrów, powodując wstrząsy porównywalne z trzęsieniem ziemi o magnitudzie 3,3 w skali Richtera. Fala uderzeniowa doprowadziła do zniszczenia lub uszkodzenia ponad 50 budynków szpitalnych, dziesiątek szkół, hoteli, sklepów oraz domów mieszkalnych. Siła wybuchu wybiła okna nawet w odległości 15 mil od epicentrum, a jego odgłos był słyszalny na Cyprze, oddalonym o ponad 240 km [6].

W wyniku katastrofy śmierć poniosło co najmniej 218 osób, ponad 7500 zostało rannych, a szacunkowo 300 tys. mieszkańców Bejrutu zostało pozbawionych dachu nad głową. Szczególnie dotknięte zostały dzielnice położone w bezpośrednim sąsiedztwie portu, takie jak Karantina, Gemmayzeh, Jisr i Geitawi. Brak planów ewakuacyjnych, systemów wykrywania pożaru oraz procedur zarządzania kryzysowego spowodował chaos i opóźnienia w działaniach ratowniczych [6].

Z punktu widzenia bezpośredniego mechanizmu inicjacyjnego ustalono, że zdarzenie zostało wywołane pożarem spowodowanym pracami spawalniczymi prowadzonymi przy wejściu do magazynu, w którym – poza workowanym AA – znajdowały się również materiały łatwopalne. Obecność tych komponentów stworzyła środowisko wysoce sprzyjające rozwojowi reakcji deflagacyjnych i detonacyjnych. Zgodnie z opisanym mechanizmem pierwotna deflagracja przekształciła się w detonację (ang. *deflagration to detonation transition*, DDT), prowadząc do uwolnienia energii odpowiadającej wybuchowi około 1100 ton trotylu (TNT) [6].

substances, lack of inspections, safety audits and proper crisis response procedures. In 2020, in Lebanon there were no integrated regulations on the storage of ammonium nitrate, in accordance with international standards (e.g. NFPA). In addition, port management structures did not have a warning system, emergency plan or trained chemical incident response teams [6].

In case of the Beirut disaster, the crisis response was characterised above all by spontaneous local non-government organisations and civic community, which had to bridge the gap left by unprepared and decentralised state structures. State institutions, including mainly the Lebanese Army, assumed functions of ensuring safety, donation management and help distribution, however the lack of a current crisis management plan and inadequate logistic resources made the state response chaotic and limited [6].

Based on the research by Sakr [6], which included 25 interviews with representatives of non-government organisations and initiatives involved in the response to the explosion, the following key problems were identified:

1. No coordination with the state – out of 25 respondents, 9 refused to cooperate with the state. The main causes:
 - lack of leadership and organisation – state intervention by the Lebanese Army was delayed (the Forward Emergency Room was formed several days after the explosion) and the division of zones between organisations was not logical from the perspective of the entities already operating in the field. The respondents noted that when the state started organising help “relief work was almost done”;
 - lack of trust in the state – the respondents noted corruption as the main cause of the lack of trust. International donors did not trust the state either and provided the assets directly to non-government organisations. One of the respondents stated: “The responsibility of the state is that the explosion shouldn’t happen first; they are the cause of what we are living, so how to coordinate with them” [6];
 - lack of experience of the Lebanese Army in humanitarian work – the army, used to rigid and hierarchical operation, was incapable of effective coordination of the work of humanitarian organisations. The respondents noted that “the Lebanese Army is not involved in humanitarian work” and “they have nothing to do with humanitarian work” [6].
2. The preparation level – all respondents agreed that the level of preparation of the state for disasters was very low. There are no current crisis management plans, while existing procedures are archaic and unadjusted to the scale of incident. One of the respondents stated: “In disaster management, very few are the institutions that are prepared for disasters in Lebanon. The main shortcoming is that on the level of the State, we do not have an updated disaster management plan”. Non-government organisations were poorly prepared as well – only 5 of 25 were involved earlier in disaster response [6].
3. Cooperation between organisations – 23 of 25 respondents cooperated with other organisations. The forms of

Na poziomie systemowym i organizacyjnym główną przyczyną była niewydolność instytucjonalna: brak odpowiednich regulacji dotyczących klasyfikacji i nadzoru nad przechowywaniem niebezpiecznych substancji chemicznych, brak inspekcji, audytów bezpieczeństwa oraz odpowiednich procedur reagowania kryzysowego. W Libanie przed 2020 r. nie obowiązywały zintegrowane przepisy dotyczące przechowywania azotanu amonu zgodne z międzynarodowymi standardami (np. NFPA). Dodatkowo, portowe struktury zarządzania nie posiadały systemu ostrzegania, planu awaryjnego ani przeszkolonych zespołów reagowania na incydenty chemiczne [6].

W przypadku katastrofy w Bejrucie reakcja kryzysowa polegała przede wszystkim na spontanicznej mobilizacji lokalnych organizacji pozarządowych oraz społeczności obywatelskiej, która musiała wypełnić lukę pozostawioną przez nieprzygotowane i zdecentralizowane struktury państwowe. Państwowe instytucje, w tym głównie Libańska Armia, przejęły funkcje związane z zapewnieniem bezpieczeństwa, zarządzaniem darowiznami i dystrybucją pomocy, jednak brak aktualnych planów zarządzania kryzysowego oraz niedostateczne zasoby logistyczne spowodowały, że odpowiedź państwa była chaotyczna i ograniczona [6].

Zgodnie z badaniami Sakr [6], które objęły 25 wywiadów z przedstawicielami organizacji pozarządowych i inicjatyw zaangażowanych w reakcję na wybuch, zidentyfikowano następujące kluczowe problemy:

1. Brak koordynacji z państwem – spośród 25 respondentów, 9 odmówiło współpracy z państwem. Główne przyczyny to:
 - brak przywództwa i organizacji – interwencja państwa realizowana przez Libańską Armię nastąpiła z opóźnieniem (Forward Emergency Room utworzono kilka dni po wybuchu), a podział stref między organizacje nie był logiczny z perspektywy podmiotów już działających na miejscu. Respondenci wskazywali, że w chwili rozpoczęcia organizacji pomocy „działania pomocowe były praktycznie zakończone”;
 - brak zaufania do państwa – respondenci wskazywali na korupcję jako główną przyczynę braku zaufania. Międzynarodowi darczyńcy również nie ufali państwu, przekazując środki bezpośrednio organizacjom pozarządowym. Jeden z respondentów stwierdził: „Odpowiedzialność państwa polega na tym, że do eksplozji w ogóle nie powinno było dojść; to ono odpowiada za sytuację, w której obecnie się znajdujemy, więc trudno mówić o koordynacji działań z jego udziałem [6];
 - brak doświadczenia Libańskiej Armii w pracy humanitarnej – armia, przyzwyczajona do działania w sposób sztywny i zhierarchizowany, nie potrafiła skutecznie koordynować pracy organizacji humanitarnych. Respondenci wskazywali, że „Armia Libańska nie uczestniczy w działaniach humanitarnych” i „ich działalność nie jest związana z pomocą humanitarną” [6].

cooperation included: sharing resources, referrals and communication aimed to avoid duplicate operations. At the same time, respondents mentioned chaos and duplication of operations in the first days of explosion, which also resulted from the improvised nature of the response. One of the respondents described it as follows: "It was chaotic because you would see the same house receiving help from different organizations while its neighbours did not receive anything" [6].

Sakr [6] notes that although the state was not completely absent (represented by the Lebanese Army and the Beirut commune), its role was minimal and disorganised. The main factors restricting the role of the state are: lack of resources and funds, lack of trust (both social and international) and lack of experience in humanitarian work. Non-government organisations did not form a "parallel state", but they bridged the gap left by the state by creating their own cooperation networks.

The Beirut disaster showed that effective crisis management in case of hazards related to ammonium nitrate required a systemic approach, including both prevention and supervision, as well as response and reconstruction. The experiences of Beirut showed the following key conclusions [6]:

- lack of a central coordination unit – one of the main problems proved to be the complete lack of a national coordination structure to coordinate rescue, reconstruction and aid distribution operations. Consequently, operations were fragmented, often independently by different organisations, which resulted in duplication of operations and incoherent messaging;
- loss of trust in state institutions – social perception of the widespread corruption and impunity of the administration caused both the inhabitants of Beirut and foreign donors to show deep scepticism towards state structures. Many foreign organisations decided to provide help directly to local NGOs, while bypassing government channels;
- inadequate coordination lead to ineffective aid distribution – the reports showed cases of excessive distribution of food, while other needs (e.g. help in renovations, healthcare) were neglected. There was no integrated platform for data exchange between aid organisations, the government, the army and local communities;
- lack of reconstruction strategy and fund tracking – the influx of major foreign and national funds was not covered by a single reporting and control system. It is necessary to introduce a digital aid tracking system, publicly available and transparent both for beneficiaries and donors;
- the need to build a permanent crisis response system – the incident showed that *ad hoc* operations, conducted without a risk management plan, are unable to properly protect the society in disaster situations. The conclusions from Beirut clearly indicate the need to form a national crisis management unit, capable of coordinating aid and reconstruction operations with the public sector, private sector, civil society and international partners.

2. Poziom przygotowania – wszyscy respondenci zgodzili się, że poziom przygotowania państwa na katastrofy jest bardzo niski. Brakuje aktualnych planów zarządzania kryzysowego, a istniejące procedury są archaiczne i niedostosowane do skali zdarzenia. Jeden z respondentów stwierdził: „W zakresie zarządzania kryzysowego jedynie nieliczne instytucje w Libanie są przygotowane na wystąpienie katastrof. Głównym problemem jest to, że na poziomie państwa nie istnieje aktualny plan zarządzania kryzysowego”. Również organizacje pozarządowe były słabo przygotowane – tylko 5 z 25 było zaangażowanych wcześniej w reakcję na katastrofy [6].
3. Współpraca między organizacjami – 23 z 25 respondentów współpracowało z innymi organizacjami. Formy współpracy obejmowały: dzielenie się zasobami (ang. *sharing resources*), przekazywanie przypadków (ang. *referrals*) oraz komunikację w celu unikania duplikacji działań. Jednocześnie respondenci wskazywali na chaos i duplikację działań w pierwszych dniach po wybuchu, co wynikało z improwizowanej natury reakcji. Jeden z respondentów opisał to następująco: „Sytuacja była chaotyczna, ponieważ można było zaobserwować, że ten sam dom otrzymywał pomoc od różnych organizacji, podczas gdy sąsiednie gospodarstwa nie otrzymywały żadnego wsparcia.” [6].

Sakr [6] wskazuje, że mimo iż państwo nie było całkowicie nieobecne (reprezentowane przez Libańską Armię i gminę Bejrutu), jego rola była minimalna i zdeorganizowana. Główne czynniki ograniczające rolę państwa to: brak zasobów i funduszy, brak zaufania (zarówno społecznego, jak i międzynarodowego) oraz brak doświadczenia w pracy humanitarnej. Organizacje pozarządowe nie stanowiły „państwa równoległego”, ale wypełniały lukę pozostawioną przez państwo, tworząc własne sieci współpracy.

Katastrofa w Bejrucie unaoczniała, że skuteczne zarządzanie kryzysowe w przypadku zagrożeń związanych z azotanem amonu wymaga podejścia systemowego, obejmującego zarówno prewencję i nadzór, jak i reagowanie oraz odbudowę. Doświadczenia z Bejrutu wskazują na następujące kluczowe wnioski [6]:

- brak centralnej jednostki koordynacyjnej – jednym z głównych problemów okazał się całkowity brak krajowej struktury koordynującej działania ratownicze, odbudowę i dystrybucję pomocy. W wyniku tego działania podejmowane były fragmentarycznie, często niezależnie przez różne organizacje, co skutkowało duplikacją działań i niespójnością przekazu;
- zanik zaufania do instytucji państwowych – społeczna percepcja szeroko rozpowszechnionej korupcji i bezkarności administracyjnej sprawiła, że zarówno mieszkańcy Bejrutu, jak i zagraniczni darczyńcy wykazywali głęboki sceptycyzm wobec państwowych struktur. Wiele organizacji zagranicznych zdecydowało się przekazywać pomoc bezpośrednio lokalnym NGO, z pominięciem kanałów rządowych;
- niedostateczna koordynacja doprowadziła do nieefektywnej dystrybucji pomocy – raporty wykazały przypadki nadmierowej dystrybucji żywności, podczas gdy inne potrzeby (np. pomoc w remontach, opieka medyczna) były zaniedbywane. Zabrakło zintegrowanej platformy

From the perspective of the MMCSS, the implementation of the mobile support system could:

- ensure quick formation of the command point with satellite communication, integrating data from drones, environmental sensors and GIS systems;
- enable cooperation between services, local authorities, the military and non-government organisations;
- ensure access to real medical potential data (hospital bed, respirator and medical personnel availability);
- support decision-making regarding the evacuation, cooling of warehouses or decontamination.

The experience of Beirut proves that even countries with relatively developed institutions could be unprepared for crisis if they have flexible and resilient response systems. The Modular Mobile Crisis Management Centre, as project addressing the needs of the 21st century, offers a real utility to minimise the disaster impact by quick launch of an integrated and technologically advanced command node [9].

wymiany danych między organizacjami pomocowymi, rządem, armią i społecznościami lokalnym;

- brak strategii odbudowy i śledzenia środków finansowych – napływ ogromnych funduszy zagranicznych i krajowych nie został objęty jednolitym systemem raportowania i kontroli. Konieczne jest wprowadzenie cyfrowego systemu śledzenia pomocy (ang. *aid tracker*), dostępnego publicznie i transparentnego zarówno dla beneficjentów, jak i darczyńców;
- konieczność budowy trwałego systemu reagowania kryzysowego – wydarzenie pokazało, że działania ad hoc, prowadzone w warunkach braku planu zarządzania ryzykiem, nie są w stanie odpowiednio zabezpieczyć społeczeństwa w sytuacjach katastrofy. Wnioski z Bejrutu wskazują jednoznacznie na potrzebę utworzenia krajowej jednostki ds. zarządzania kryzysowego, zdolnej do koordynacji działań pomocowych i odbudowy z udziałem sektora publicznego, prywatnego, społeczeństwa obywatelskiego i partnerów międzynarodowych.

Z perspektywy MMCZK wdrożenie mobilnego systemu wspomagania mogłoby:

- zapewnić szybkie utworzenie punktu dowodzenia z łącznością satelitarną, integrującego dane z dronów, czujników środowiskowych i systemów GIS;
- umożliwić koordynację między służbami, władzami lokalnymi, wojskiem i organizacjami pozarządowymi;
- zapewnić dostęp do rzeczywistych danych o potencjale medycznym (dostępność łóżek szpitalnych, respiratorów, personelu medycznego);
- wspierać podejmowanie decyzji o ewakuacji, chłodzeniu magazynów czy dekontaminacji.

Doświadczenie Bejrutu dowodzi, że nawet państwa o stosunkowo rozwiniętych instytucjach mogą być nieprzygotowane na kryzysy, jeśli nie dysponują elastycznymi i odpornymi systemami reagowania. Modułowe i Mobilne Centrum Zarządzania Kryzysowego, jako projekt wpisujący się w potrzeby XXI wieku, oferuje realne narzędzie do minimalizacji skutków katastrof poprzez szybkie uruchomienie zintegrowanego, technologicznie zaawansowanego węzła dowodzenia [9].

Normative and legal aspects

The operation of mobile CBRNE laboratories of the State Fire Service is embedded in a complex system of legal regulations, including both national regulations and international standards. The legal basis is the State Fire Service Act (Journal of Laws of 1991, no. 88, item 400), which specifies the organisation and its scope of operations, including the fulfilment of chemical and environmental rescue tasks [1]. The executive regulations for that Act, above all the regulation on the special organisation of KSRG [14], define CBRNE hazards as “hazards caused by chemical, biological, radioactive, nuclear and explosive hazards, which due to its properties were used or could be used intentionally to cause hazards to human life and health, animals and natural environment” [1].

The key document is The Principles of organisation of chemical and environmental rescue in the national rescue and

Aspekty normatywne i prawne

Działalność mobilnych laboratoriów CBRNE PSP jest osadzona w złożonym systemie regulacji prawnych, obejmującym zarówno przepisy krajowe, jak i normy międzynarodowe. Podstawę prawną stanowi ustawa o Państwowej Straży Pożarnej (Dz.U. 1991 Nr 88, poz. 400), która określa organizację i zakres jej działania, w tym realizację zadań z zakresu ratownictwa chemicznego i ekologicznego [1]. Przepisy wykonawcze do tej ustawy, przede wszystkim rozporządzenie dotyczące szczegółowej organizacji KSRG [14], definiują zagrożenia CBRNE jako „zagrożenia powodowane przez czynniki chemiczne, biologiczne, radioaktywne, nuklearne oraz wybuchowe, które ze względu na swoje właściwości zostały użyte lub mogły zostać użyte w sposób celowy do wywołania zagrożenia dla życia i zdrowia ludzi, zwierząt oraz środowiska naturalnego” [1].

firefighting system [15], which introduces the division into five levels of operational readiness [1]:

- 1) level A – chemical protection,
- 2) level B – chemical reconnaissance,
- 3) level C – special reconnaissance,
- 4) level D – decontamination,
- 5) level L – laboratory analysis.

The implemented mobile CBRNE laboratories of the State Fire Service correspond to the highest readiness level (L). The laboratory analysis includes operations that require using advanced methods and analytical measures, exceeding the chemical reconnaissance and special reconnaissance capability levels. The SGRChem-Eko readiness level L, with qualified personnel, ensures substantive support in incident data interpretation and analysis results obtained by KSRG entities [1].

The scope of tasks of the laboratory includes: direct involvement in operations on the incident scene, completion of the analysis of samples provided by units connected to KSRG and remote interpretation of the submitted chemical analysis results.

In accordance with *The Principles of organisation of chemical and environmental rescue ...*, when dispatching directly to direct rescue operations of SGRChem-Eko at the readiness level L, SGRChem-Eko at readiness level B is also dispatched every time. The purpose is to ensure a comprehensive approach to hazard identification. The chemical reconnaissance group (B) supports the analytical operations of the laboratory (L) [1].

Another important document is the Civil Protection and Civil Defence Act of 5 December 2024 (Journal of Laws of 2024, item 1907), which introduced a new organisational and functional structure of civil protection, integrating the before dispersed competences of the entities responsible for crisis response, emergency management and civil defence. The Act requires civil protection bodies (commune heads, starostes, voivods, minister of the internal affairs) to create and maintain mobile resources (Article 10 Section 1 Point 7, Article . 11 Section 1 Point 9, Article 33), to integrate ITC systems (Article 31) and to conduct regular training sessions (Article 52–53) [12].

Pursuant to the Article 33 Section 3 of that Act, civil protection resources should be capable of autonomous operation for at least 72 hours, directly corresponding with the assumptions of the MMCSS (power, communication and analytical independence). The MMCSS also aligns with the requirement to integrate ICT systems (Article 31), with open ICT infrastructure and compatibility with EDXL, CAP and TETRA protocols.

The amendment to the Act of 7 November 2025 (Journal of Laws of 2025, item 1705) introduces additional integration mechanisms for medical potential data (Beneficiary Potential Registration System – EPS) with the Central Register of Civil Protection and Civil Defence Resources. It opens the opportunity to provide the MMCSS with access to real data on hospital bed, respirator and medical personnel availability, essential for mass chemical explosion impact management [13].

The design and construction of the mobile CBRNE laboratory of the State Fire Service were based on the need to meet stringent requirements arising from applicable legal and normative acts. The design included the following categories of standards [7]:

Kluczowym dokumentem są Zasady organizacji ratownictwa chemicznego i ekologicznego w krajowym systemie ratowniczo-gaśniczym [15], które wprowadzają podział na pięć poziomów gotowości operacyjnej [1]:

- 1) poziom A – zabezpieczenie chemiczne,
- 2) poziom B – rozpoznawanie chemiczne,
- 3) poziom C – rozpoznawanie specjalne,
- 4) poziom D – dekontaminacja,
- 5) poziom L – analiza laboratoryjna.

Wdrożone mobilne laboratoria CBRNE PSP odpowiadają najwyższemu poziomowi gotowości (L). Analiza laboratoryjna obejmuje działania wymagające użycia zaawansowanych metod i środków analitycznych, przewyższających możliwości poziomów rozpoznania chemicznego i rozpoznania specjalnego. SGRChem-Eko poziomu gotowości L dzięki wykwalifikowanemu personelowi zapewnia wsparcie merytoryczne w interpretacji danych o zdarzeniu i wyników analizy uzyskanych przez podmioty KSRG [1].

Zakres zadań laboratorium obejmuje: bezpośredni udział w działaniach na miejscu zdarzenia, wykonanie analizy próbek dostarczonych przez jednostki włączone do KSRG oraz zdalną interpretację przesłanych wyników analizy chemicznej.

Zgodnie z *Zasadami organizacji ratownictwa chemicznego i ekologicznego...*, podczas dysponowania do bezpośrednich działań ratowniczych SGRChem-Eko poziomu gotowości L każdorazowo jest dysponowana również SGRChem-Eko poziomu gotowości B. Ma to na celu zapewnienie kompleksowego podejścia do identyfikacji zagrożeń – grupa rozpoznania chemicznego (B) wspiera działania analityczne laboratorium (L) [1].

Istotne znaczenie ma również ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024, poz. 1907), która wprowadza nową strukturę organizacyjną i funkcjonalną ochrony ludności, integrującą dotychczas rozproszone kompetencje podmiotów odpowiedzialnych za reagowanie kryzysowe, zarządzanie sytuacjami nadzwyczajnymi oraz obronę cywilną. Ustawa ta nakłada na organy ochrony ludności (wójtów, starostów, wojewodów, ministra właściwego do spraw wewnętrznych) obowiązek tworzenia i utrzymywania zasobów mobilnych (art. 10 ust. 1 pkt 7, art. 11 ust. 1 pkt 9, art. 33), integracji systemów teleinformatycznych (art. 31) oraz prowadzenia ćwiczeń cyklicznych (art. 52–53) [12].

Zgodnie z art. 33 ust. 3 tej ustawy zasoby ochrony ludności powinny być zdolne do autonomicznego działania przez co najmniej 72 godziny – co bezpośrednio koresponduje z założeniami MMCZK (autonomia energetyczna, łącznościowa i analityczna). MMCZK wpisuje się również w obowiązek integracji systemów teleinformatycznych (art. 31) – dzięki otwartej architekturze ICT i zgodności z protokołami EDXL, CAP i TETRA.

Nowelizacja ustawy z dnia 7 listopada 2025 r. (Dz.U. 2025, poz. 1705) wprowadza dodatkowe mechanizmy integracji danych o potencjale medycznym (System Ewidencji Potencjału Świadczeniodawcy – EPS) z Centralną Ewidencją Zasobów Ochrony Ludności i Obrony Cywilnej. Otwiera to możliwość wyposażenia MMCZK w dostęp do rzeczywistych danych o dostępności łóżek szpitalnych, respiratorów i personelu medycznego – kluczowych w zarządzaniu skutkami masowego wybuchu chemicznego [13].

Projektowanie i budowa mobilnego laboratorium CBRNE PSP opierały się na konieczności spełnienia rygorystycznych wymagań

- standards for laboratory infrastructure and equipment:
 - PN-EN 13150:2004 – Workbenches for laboratories – Dimensions, safety and durability requirements and test methods,
 - PN-EN 14175-1 to 14175-6 – Fume cupboards – vocabulary, technical requirements, test methods, recommendations for installation and operation,
 - PN-EN 14727:2006 – Laboratory furniture – Storage units for laboratories – Requirements and test methods;
- standards for water, clean rooms and decontamination:
 - PN-EN ISO 3696:1999 – Water for Analytical Laboratory Use,
 - PN-EN ISO 14644-1, -3, -4 – Cleanrooms and associated controlled environments – classification of cleanliness, test methods, design and start-up,
 - VDI 2083 part 19 – Cleanroom technology – classification and testing of air-tightness of enclosures;
- biotechnological and biological safety standards:
 - PN-EN 12128:2000 – Microbiological laboratories air-tightness levels,
 - PN-EN 12469:2002 – Performance criteria for microbiological safety cabinets,
 - PN-EN 1822-1:2009 – Classification and testing of HEPA and ULPA filters,
 - Canadian Biosafety Standard (CBS), 2nd Ed. 2007 – Canadian biological safety standard (BSL-3);
- power supply and automation:
 - PN-EN 62040 – Uninterruptible power systems (UPS).

In the context of the increasing role of interoperability and need to conduct activities in an international environment, mobile CBRNE analysis laboratory of the State Fire Service, also considering NATO guidelines and standards. In particular, reference was made to the requirements included in STANAG 4632 (Deployable NBC Analytical Laboratory) and AEP-66 (NATO Handbook for Sampling and Identification of Biological, Chemical and Radiological Agents – SIBCRA) [7].

In international cooperation, the Union Civil Protection Mechanism (UCPM), managed by the European Commission, is significant as well. As part of UCPM, the Emergency Response Coordination Centre (ERCC) operates, responsible for 24-hour monitoring of crisis situations and resource coordination. The states involved in the mechanism have access to the Common Emergency Communication and Information System (CECIS), as well as the European Help Reserve (rescEU) [1].

Although multiple regulations exist, significant normative gaps were identified, which could impede the implementation of the MMCMSS [3], [7]:

- lack of standards for the air-tightness of mobile biological modules in field conditions – VDI 2083 part 19 defines the requirements for stationary enclosures and isolators, but it does not provide for design specifics of mobile (vehicles, containers), exposed to shocks, vibrations and variable weather conditions;

wynikających z obowiązujących aktów prawnych i normatywnych. Przy projektowaniu uwzględniono następujące kategorie norm [7]:

- normy dotyczące infrastruktury laboratoryjnej i wyposażenia:
 - PN-EN 13150:2004 – Stoły robocze dla laboratoriów – Wymiary, wymagania bezpieczeństwa i metody badań,
 - PN-EN 14175-1 do 14175-6 – Wyciągi laboratoryjne – słownictwo, wymagania techniczne, metody badań, zalecenia dotyczące instalacji i eksploatacji,
 - PN-EN 14727:2006 – Meble laboratoryjne – Meble laboratoryjne do przechowywania – Wymagania i metody badań;
- normy dla wody, pomieszczeń czystych i dekontaminacji:
 - PN-EN ISO 3696:1999 – Jakość wody w laboratoriach analitycznych,
 - PN-EN ISO 14644-1, -3, -4 – Pomieszczenia czyste i środowiska kontrolowane – klasyfikacja czystości, metody badań, projektowanie i uruchamianie,
 - VDI 2083 część 19 – Technologia pomieszczeń czystych – klasyfikacja i testowanie szczelności obudów;
- normy biotechnologiczne i bezpieczeństwa biologicznego:
 - PN-EN 12128:2000 – Stopnie hermetyczności laboratoriów mikrobiologicznych,
 - PN-EN 12469:2002 – Kryteria działania komór bezpiecznej pracy mikrobiologicznej,
 - PN-EN 1822-1:2009 – Klasyfikacja i badania filtrów HEPA i ULPA,
 - Canadian Biosafety Standard (CBS), 2nd Ed. 2007 – Kanadyjski standard bezpieczeństwa biologicznego (BSL-3);
- systemy zasilania i automatyki:
 - PN-EN 62040 – Systemy bezprzerwowego zasilania (UPS).

W kontekście rosnącej roli interoperacyjności oraz potrzeby prowadzenia działań w środowisku międzynarodowym, mobilne laboratorium analityczne CBRNE PSP zaprojektowano również z uwzględnieniem wytycznych i standardów NATO. W szczególności odniesiono się do wymagań zawartych w STANAG 4632 (Deployable NBC Analytical Laboratory) oraz AEP-66 (NATO Handbook for Sampling and Identification of Biological, Chemical and Radiological Agents – SIBCRA) [7].

W ramach współpracy międzynarodowej istotne znaczenie ma również Unijny Mechanizm Ochrony Ludności (ang. *Union Civil Protection Mechanism*, UCPM), zarządzany przez Komisję Europejską. W ramach UCPM funkcjonuje Centrum Koordynacji Reagowania Kryzysowego (ang. *Emergency Response Coordination Centre*, ERCC), odpowiedzialne za całodobowe monitorowanie sytuacji kryzysowych i koordynację zasobów. Państwa uczestniczące w mechanizmie mają dostęp do wspólnej platformy wymiany informacji (ang. *Common Emergency Communication and Information System*, CECIS), a także do Europejskiej Rezerwy Pomocy (rescEU) [1].

Pomimo istnienia wielu regulacji, zidentyfikowano istotne luki normatywne, które mogą utrudniać wdrożenie MMCZK [3], [7]:

- brak norm dla hermetyczności mobilnych modułów biologicznych w warunkach polowych – VDI 2083 część

- lack of validation certificate of mobile BSL-3 laboratories – in accordance with normative definitions, BSL-3 laboratories must be a permanent and stationary building structure. The mobile laboratory of the State Fire Service as mobile structure that does not meet that requirement. It does not have an ISO 14644-3 validation certificate either [7];
- the dispersion of regulations on ammonium nitrate – in Poland ammonium nitrate is under supervision of several ministries (Ministry of Agriculture and Rural Development, Ministry of Internal Affairs and Administration, Ministry of National Defence and Ministry of Environment) and inspections (Voivodship Inspectorate of Environmental Protection, State Plant Health and Seed Inspection Service, Road Transport Inspection and maritime offices), which impedes quick information exchange and coordination of prevention and response activities;
- lack of a single and publicly available cartography tool – Poland, despite having a register of high risk (ZDR) and increased risk (ZZR) plants, managed by the Voivodship Inspectorate of Environmental Protection) and registers of the State Fire Service, does not have a single and publicly available cartography tool for ammonium nitrate, including temporary storage and ports as well;
- lack of unified port and transshipment terminal inspection procedures – the Italian experience after the Beirut disaster shows that the crucial problem was the storage of ammonium nitrate in ports, which may be governed by the International Maritime Dangerous Goods Code (IMDG) and International Ship and Port Facility Security Code (ISPS), are not always covered by the full regime of the Seveso directive, in particular in terms of spatial planning and long-term storage control.

- 19 określa wymagania dla stacjonarnych obudów i izolatorów, ale nie przewiduje specyfiki konstrukcji mobilnych (pojazdów, kontenerów), które podlegają wstrząsom, drganiom i zmiennym warunkom atmosferycznym;
- brak certyfikacji walidacyjnej mobilnych laboratoriów BSL-3 – zgodnie z normatywnymi definicjami, laboratoria BSL-3 muszą być trwałą, nieruchomą konstrukcją budowlaną. Mobilne laboratorium PSP jako konstrukcja przemieszczania mobilnego nie spełnia tego wymogu. Brak jest również certyfikacji walidacyjnej zgodnie z ISO 14644-3 [7];
 - rozdrobnienie regulacji dotyczących azotan amonu – w Polsce za azotan amonu odpowiada kilka resortów (MRiRW, MSWiA, MON, MŚ) oraz inspekcji (WIOŚ, PIORiN, ITD, urzędy morskie), co utrudnia szybką wymianę informacji i koordynację działań prewencyjnych i reaktywnych;
 - brak jednolitego, ogólnodostępnego narzędzia kartograficznego – Polska, mimo posiadania ewidencji zakładów o dużym ryzyku (ZDR) i zwiększonym ryzyku (ZZR) prowadzonej przez WIOŚ oraz rejestrów PSP, nie dysponuje spójnym, ogólnodostępnym narzędziem kartograficznym dla azotan amonu, które uwzględniałoby także składy tymczasowe i porty;
 - brak ujednoliconych procedur kontroli portów i terminali przeładunkowych – doświadczenia włoskie po katastrofie w Bejrucie pokazują, że kluczowym problemem okazało się składowanie azotan amonu w portach, które choć podlegają przepisom Międzynarodowego Kodeksu Ładunków Niebezpiecznych (IMDG) i Międzynarodowego Kodeksu Ochrony Statków i Obiektów Portowych (ISPS), nie zawsze są objęte pełnym rygorom dyrektywy Seveso, szczególnie w zakresie planowania przestrzennego i kontroli długoterminowego magazynowania.

Effectiveness and implementation feasibility assessment

To assess the effectiveness of mobile crisis management support systems, it is required to assume a set of multi-dimensional criteria, which reflect not only their technical capabilities, but also operational, organisational and interoperational capabilities. In case of solutions based on modular mobile units, such as command centres, CBRN analytical laboratories or mobile data processing systems – it is important for the assessment to include actual use conditions, including dynamic chemical and industrial hazard scenarios [3].

1. Operational criteria:

- response time (time to achieve full operational readiness from mobilisation; response time ≤ 45 min for the basic mode, ≤ 90 min for the full mode);
- analytical effectiveness (% of correct identifications of hazardous substances; analytical effectiveness $\geq 98\%$ for GC-MS/FTIR);
- operational autonomy (time of continuous operation without external support; operational autonomy ≥ 72 h – power supply, filtering, communication).

Ocena efektywności i możliwości wdrożenia

Ocena efektywności systemów mobilnych wspierających zarządzanie kryzysowe wymaga przyjęcia zestawu wielowymiarowych kryteriów, które odzwierciedlają nie tylko ich zdolności techniczne, ale również operacyjne, organizacyjne i interoperacyjne. W przypadku rozwiązań opartych na modułowych jednostkach mobilnych – takich jak centra dowodzenia, laboratoria analityczne CBRN czy systemy mobilnego przetwarzania danych – istotne jest, aby ocena ta uwzględniała warunki rzeczywistego użycia, w tym dynamiczne scenariusze zagrożeń chemicznych i przemysłowych [3].

1. Kryteria operacyjne:

- czas reakcji (czas osiągnięcia pełnej gotowości operacyjnej od momentu mobilizacji; czas reakcji ≤ 45 min dla trybu podstawowego, ≤ 90 min dla trybu pełnego);
- skuteczność analityczna (% poprawnych identyfikacji substancji niebezpiecznych; skuteczność analityczna $\geq 98\%$ dla GC-MS/FTIR);
- autonomia operacyjna (czas ciągłej pracy bez wsparcia zewnętrznego; autonomia operacyjna ≥ 72 h – zasilanie, filtracja, łączność).

2. Technical criteria:
 - system reliability (MTBF – Mean Time Between Failures) under extreme conditions (-20°C to +45°C);
 - cybersecurity (resistant to DDoS attacks, compliance with the NIS2 directive);
 - normative compliance (compliance with the requirements of VDI 2083 p. 19, PN-EN ISO 14644-3).
3. System-level criteria:
 - interoperability (number of integrated internal systems – KSRG, ERCC, MON);
 - interoperability (time to add a new module, “plug & play” architecture);
 - lifecycle cost (LCC)
4. Social and organisational criteria:
 - user acceptance (satisfaction survey among the officers of the State Fire Service/SGRChem-Eko);
 - training effectiveness (time for operators to master procedures);
 - influence on safety (reduction of evacuation zones with precise prediction).

The SWOT analysis conducted and included in Table 1 enables a complete assessment of the implementation potential of the MMCMS by identification of strengths and weaknesses and identification of opportunities and threats arising from the organisational, technological and regulatory context [3].

2. Kryteria techniczne:
 - niezawodność systemów (MTBF – Mean Time Between Failures) w warunkach ekstremalnych (-20°C do +45°C);
 - cyberbezpieczeństwo (odporność na ataki DDoS, zgodność z dyrektywą NIS2);
 - zgodność normatywna (spełnienie wymagań VDI 2083 p. 19, PN-EN ISO 14644-3).
3. Kryteria systemowe:
 - interoperacyjność (liczba zintegrowanych systemów zewnętrznych – KSRG, ERCC, MON);
 - skalowalność (czas dodania nowego modułu, architektura „plug & play”);
 - koszty cyklu życia LCC.
4. Kryteria społeczno-organizacyjne:
 - akceptacja użytkowników (badania satysfakcji wśród funkcjonariuszy PSP/SGRChem-Eko);
 - efektywność szkoleń (czas opanowania procedur przez operatorów);
 - wpływ na bezpieczeństwo (redukcja stref ewakuacyjnych dzięki precyzyjnej predykcji).

Przeprowadzona i zamieszczona w tabeli 1 analiza SWOT pozwala na całościową ocenę potencjału wdrożeniowego MMCZK poprzez identyfikację jego mocnych i słabych stron oraz rozpoznanie szans i zagrożeń wynikających z kontekstu organizacyjnego, technologicznego i regulacyjnego [3].

Table 1. SWOT analysis of the implementation potential of the MMCMS
Tabela 1. Analiza SWOT dotycząca potencjału wdrożeniowego MMCZK

Strengths / Mocne strony:	Weaknesses / Słabe strony:
• High mobility and operational flexibility, enabling quick deployment in any area and system configuration in accordance with the requirements of the given crisis incident • In accordance with technical standards (PN-EN, ISO, BSL-3), enabling interoperability with existing structures of the State Fire Service and Crisis Management Centre • Technological integration with GIS, ICT systems and CBRN platforms, which supports decision-making in real time • Modularity, enabling system scaling as needed – from a single analytical module to a comprehensive command centre • Contamination prediction algorithms (the iSCAPE model), integrated with urban IoT sensors, reducing the response time by 40% compared to traditional systems • Lower operation costs compared to foreign systems / • Wysoka mobilność i elastyczność operacyjna, umożliwiające szybkie rozmieszczenie w dowolnym terenie i konfigurację systemu zgodnie z wymaganiami danego zdarzenia kryzysowego • Zgodność z normami technicznymi (PN-EN, ISO, BSL-3), umożliwiającą interoperacyjność z istniejącymi strukturami PSP i CZK • Integracja technologiczna z systemami GIS, ICT i platformami CBRN, co wspiera podejmowanie decyzji w czasie rzeczywistym • Modularność, pozwalająca skalować system w zależności od potrzeb – od pojedynczego modułu analitycznego po kompleksowe centrum dowodzenia • Algorytmy predykcji skażeń (model iSCAPE) zintegrowane z miejskimi czujnikami IoT, redukujące czas reakcji o 40% vs. systemy tradycyjne • Niższe koszty operacyjne w porównaniu z systemami zagranicznymi	• High initial costs connected with the purchase, certification and maintenance of advanced mobile infrastructure • Need for special training of the personnel, in particular in analytical equipment operation (GC-MS/FTIR operator training: 120 h), cybersecurity and decontamination procedures • Risk of inadequate redundancy of power supply, data transmission and availability of spare parts in case of system failure in field conditions • Lack of full validation of BSL-3 for mobile biological modules (VDI 2083), which restricts the operability with high risk pathogens • Depending on communication – satellite/5G failure paralyses the AI module (≥90% of functions require data transmission) • Deficit of qualified AI specialists among firefighters (operational readiness <60% in 24/7 mode) / • Wysokie koszty początkowe związane z zakupem, certyfikacją i utrzymaniem zaawansowanej infrastruktury mobilnej • Potrzeba specjalistycznego przeszkolenia personelu, zwłaszcza w zakresie obsługi sprzętu analitycznego (szkolenie operatora GC-MS/FTIR: 120 h), cyberbezpieczeństwa i procedur dekontaminacyjnych • Ryzyko niewystarczającej redundancji w zakresie zasilania, transmisji danych i dostępności części zamiennych w przypadku awarii systemu w warunkach terenowych • Brak pełnej walidacji BSL-3 dla mobilnych modułów biologicznych (VDI 2083), co ogranicza możliwość pracy z patogenami wysokiego ryzyka • Zależność od łączności – awaria satelity/5G paraliżuje moduł AI (≥90% funkcji wymaga transmisji danych) • Deficyt wykwalifikowanych specjalistów AI wśród strażaków (gotowość operacyjna <60% w trybie 24/7)

Opportunities / Szanse	Threats / Zagrożenia
• Opportunity to obtain EU funding (Horizon Europe, rescEU, Cohesion Fund), in particular in the field of critical infrastructure and CBRN response • Extension of applications beyond critical operations – e.g. for training purposes, environmental testing, mass event protection or hazardous materials transport support • Construction of interoperability of national competences in international cooperation (e.g. from EU CBRN CoE), which strengthens the operational position of Poland in the EU Civil Protection Mechanism • Inclusion in the rescEU mechanism as standard for chemical incidents • “Living Lab” development – implementation of the test platform with the Kielce University of Technology • Integration with the EPS system (from 2027) – access to real medical potential data / • Możliwość pozyskania finansowania z funduszy unijnych (Horyzont Europa, rescEU, Fundusz Spójności), szczególnie w obszarze odporności infrastruktury krytycznej i reagowania CBRN • Rozszerzenie zastosowań poza działania kryzysowe – np. do celów szkoleniowych, badań środowiskowych, zabezpieczania imprez masowych czy wsparcia przy transporcie materiałów niebezpiecznych • Budowa interoperacyjnych kompetencji krajowych w ramach współpracy międzynarodowej (np. z EU CBRN CoE), co zwiększa pozycję operacyjną Polski w ramach Mechanizmu Ochrony Ludności UE • Włączenie do mechanizmu rescEU jako standardu dla zdarzeń chemicznych • rozwój „Living Lab” – wdrożenie platformy testowej z udziałem Politechniki Świętokrzyskiej • Integracja z systemem EPS (od 2027 r.) – dostęp do rzeczywistych danych o potencjale medycznym	• Complexity of regulatory and institutional barriers, which can impede the process of certification, approval for use or inclusion in the National Crisis Response Plan • Possible low level of social or administration acceptance, arising from the lack of system usability awareness or bias towards investment costs • Potential disruption of the technological component supply chain, which may influence the rate of system manufacture, service and modification in the long term • Risk of nitrate warehouse data interception (cloud attack) – need to implement “cyber-airlock” as per NIS2 • Function doubling by mobile laboratories of the Ministry of National Defence – need for clear division of competences: civilian (NH_4NO_3) vs. military (military CBRN) / • Złożoność barier regulacyjnych i instytucjonalnych, które mogą spowalniać proces certyfikacji, dopuszczenia do użytkowania lub włączenia do Krajowego Planu Reagowania Kryzysowego • Możliwość niskiego poziomu akceptacji społecznej lub administracyjnej, wynikającego z braku świadomości użyteczności systemu lub uprzedzeń wobec kosztów inwestycyjnych • Potencjalne zakłócenia łańcucha dostaw komponentów technologicznych, które mogą wpływać na tempo produkcji, serwisowania i modernizacji systemów w dłuższej perspektywie • Ryzyko przejścia danych o magazynach saletry (atak na chmurę) – konieczność wdrożenia „cyber-śluzu” zgodnej z NIS2 • Dublowanie funkcji przez mobilne laboratoria MON – konieczność wyraźnego podziału kompetencji: cywilne (NH_4NO_3) vs. wojskowe (CBRN militarne)

Source: Own elaboration.

Źródło: Opracowanie własne.

The MMCMSS implementation process may encounter multi-level challenges, which can be divided into three main categories [3]:

1. Legal barriers:

- regulation fragmentation – ammonium nitrite is supervised by the Ministry of Internal Affairs and Administration (storage), the Ministry of Defence (transport), the Voivodship Inspectorate of Environmental Protection (environmental impact), which leads to delays in response (>4 h). Lack of one single planning document (“ NH_4NO_3 Code”) results in incoherent procedures and fragmented responsibility;
- lack of standards for the air-tightness of mobile biological modules in field conditions – VDI 2083 part 19 defines the requirements for stationary enclosures, but it does not provide for design specifics of mobile. Lack of validation certificate of mobile BSL-3 laboratories as per ISO 14644-3;
- conflict of the NIS2 directive with local urban data access regulations (Smart City) – risk of sanctions for disclosing NH_4NO_3 warehouse data. Need to prepare “cyber-airlock” with quantum encryption.

2. Organisational barriers:

- excess responsibilities – the State Fire Service (KSRG), Road Transport Inspection, Voivodship Inspectorate of Environmental Protection

Proces wdrożenia MMCKZK może napotkać na wielopoziomowe wyzwania, które można podzielić na trzy główne kategorie [3]:

1. Bariery prawne:

- rozdrobnienie regulacji – azotan amonu podlega MSWiA (magazynowanie), MON (transport), WIOŚ (skutki środowiskowe), co prowadzi do opóźnień w reakcji (>4 h). Brak jednego, wiążącego dokumentu planistycznego („Kodeksu NH_4NO_3 ”) skutkuje niespójnością procedur i rozproszeniem odpowiedzialności;
- brak norm dla hermetyczności mobilnych modułów biologicznych w warunkach polowych – VDI 2083 p. 19 określa wymagania dla stacjonarnych obudów, ale nie przewiduje specyfiki konstrukcji mobilnych. Brak certyfikacji walidacyjnej mobilnych laboratoriów BSL-3 zgodnie z ISO 14644-3;
- konflikt dyrektywy NIS2 z lokalnymi przepisami o dostępie do danych miejskich (Smart City) – ryzyko sankcji za udostępnianie danych o magazynach NH_4NO_3 . Konieczność opracowania „cyber-śluzu” z szyfrowaniem kwantowym.

2. Bariery organizacyjne:

- nadmiar kompetencji – PSP (KSRG), ITD, WIOŚ – nakładające się obowiązki prowadzą do chaosu w strefie zero. Konieczność ustanowienia jednego dowództwa operacyjnego dla zdarzeń z NH_4NO_3 ;

- overlapping responsibilities lead to chaos in the zero zone. The need to establish a single operational command for NH_4NO_3 incidents;
- personnel deficits – GC-MS/FTIR operator training: 120 h (the State Fire Service); lack of AI specialists among firefighters. Operational readiness <60% in the 24/7 mode. Need to develop the certification programme in cooperation with the Kielce University of Technology;
- poor system integration – the IBM Cloud platform (KCNZK) does not connect with the military system of the Ministry of Defence, lack of access to the nitrate warehouse register. The need to develop the API interface as per STANAG 4632.

3. Technological barriers:

- dependency on communication – AI module (KCNZK) requires 100 Mbps; in industrial areas (ports, factories) 5G coverage <20%, which causes the loss of NH_4NO_3 contamination prediction function. Need to implement the LTE-satellite mesh network (e.g. Starlink);
- power limitations – power supply to modules of the State Fire Service: 80 kW; no compatibility with generators of the Rail Protection Guard, which prevents cooperation in cross-border incidents. Need for unification of PN-EN 62040 standards;
- lack of validation of mobile BSL-3 laboratories – the laboratory of the State Fire Service does not meet full BSL-3 requirements (lack of tightness tests as per ISO 14644-3), risk of contamination when working with pathogens. Need to develop a portable testing chamber for tightness tests in the field.

Based on the conducted functional analysis, assessment of effectiveness and identification of implementation barriers, a series of recommendations can be formulated to increase the chance for practical development and long-term development of MMCMS [3], [7].

1. Practical recommendations:

- legal consolidation – passing of the " NH_4NO_3 Code" to unify the provisions on warehousing, transport and neutralisation (Ministry of Internal Affairs and Administration/Ministry of National Defence/Voivodship Inspectorate of Environmental Protection). The aim is to shorten the response time to <2 h. An inter-ministerial team (Ministry of Internal Affairs and Administration/Ministry of National Defence/Ministry of Environment) for preparation of the act draft;
- appointment of the Responsibility Centre for Ammonium Nitrate at the Headquarters of the State Fire Service, coordinating all services. The centre should be responsible for collecting data on warehouses, preparing procedures and coordinating training;

- deficyty kadrowe – szkolenie operatora GC-MS/FTIR: 120 h (PSP); brak specjalistów AI wśród strażaków. Gotowość operacyjna <60% w trybie 24/7. Konieczność opracowania programu certyfikacji we współpracy z Politechniką Świętokrzyską;
- słaba integracja systemów – platforma IBM Cloud (KCNZK) nie łączy się z wojskowym systemem MON, brak dostępu do rejestru magazynów saletry. Konieczność opracowania interfejsu API zgodnego z STANAG 4632.

3. Bariery technologiczne:

- zależność od łączności – moduł AI (KCNZK) wymaga 100 Mbps; w terenach przemysłowych (porty, fabryki) zasięg 5G <20%, co powoduje utratę funkcji predykcji skażeń NH_4NO_3 . Konieczność wdrożenia sieci mesh LTE-satelita (np. Starlink);
- ograniczenia energetyczne – zasilanie modułów PSP: 80 kW; brak kompatybilności z agregatami Straży Ochrony Kolei, co uniemożliwia współdziałanie w zdarzeniach transgranicznych. Konieczność unifikacji standardów PN-EN 62040;
- brak walidacji mobilnych laboratoriów BSL-3 – laboratorium PSP nie spełnia pełnych wymogów BSL-3 (brak testów szczelności wg ISO 14644-3), ryzyko skażenia przy pracy z patogenami. Konieczność opracowania przenośnej komory testowej do pomiarów szczelności w terenie.

Na podstawie przeprowadzonej analizy funkcjonalnej, oceny efektywności oraz identyfikacji barier wdrożeniowych, można sformułować szereg rekomendacji mających na celu zwiększenie szans praktycznego wdrożenia oraz długofalowego rozwoju MMCZK [3], [7].

1. Rekomendacje praktyczne:

- konsolidacja prawna – uchwalenie „Kodeksu NH_4NO_3 ” ujednolicającego przepisy dotyczące magazynowania, transportu i neutralizacji (MSWiA/MON/WIOŚ). Celem jest skrócenie czasu reakcji do <2 h. Należy powołać międzyresortowy zespół (MSWiA/MON/MŚ) do opracowania projektu ustawy;
- powołanie Centrum Kompetencji ds. Saletry Amonowej przy Komendzie Głównej PSP, koordynującego wszystkie służby. Centrum powinno być odpowiedzialne za gromadzenie danych o magazynach, opracowywanie procedur oraz koordynację ćwiczeń;
- program certyfikacji operatorów z użyciem symulatorów AR/VR (scenariusze wybuchu NH_4NO_3) – we współpracy z Politechniką Świętokrzyską. Celem jest przygotowanie 120 operatorów rocznie. Program powinien obejmować zarówno obsługę sprzętu analitycznego, jak i procedury dowodzenia i koordynacji;
- wdrożenie programu pilotażowego MMCZK w wybranym województwie (np. w ramach koncepcji Kieleckiego Centrum Nowoczesnego Zarządzania Kryzysowego). Program powinien zakładać integrację z infrastrukturą stałą, regularne ćwiczenia (w tym

- the operator certification programme using AR/VR simulators (NH_4NO_3 explosion scenarios) – in cooperation with the Kielce University of Technology. The purpose is to prepare 120 operators per year. The programme should include both analytical equipment operation and command and coordination procedures;
 - the implementation of the MMCMSS pilot programme in the selected voivodship (e.g. under supervision of Kieleckie Centrum Nowoczesnego Zarządzania Kryzysowego). The programme should assume integration with stationary infrastructure, regular training (including CBRN hazard and ammonium nitrate explosion scenarios), operational assessment and acquisition of evaluation data;
 - securing long-term funding sources – through mechanisms of the European Union (Horizon Europe, rescEU, Cohesion Fund) and inclusion of CBRN subjects and mobile crisis technologies for national research and development strategies (e.g. FEnIKS Operational Programme, National Smart Specialisations).
2. Development recommendations:
- hybrid communication – introduction of the LTE-satellite mesh network (Starlink) in command modules, which ensure 100% coverage of Poland. The system should automatically switch between networks depending on their availability and throughput;
 - certification of mobile BSL-3+ modules according to the modified standard VDI 2083 p. 19, in cooperation with CNBOP-PIB i IBM. The purpose is full validation of tightness (ISO 14644-3) until 2026. Procedures should be prepared for testing the tightness in field conditions, including the specifics of mobile structures;
 - development of predictive analytics AI algorithms – prediction of secondary NH_4NO_3 detonations based on historical data (temperature, humidity, storage time, contamination) as part of the NATO SPS grant. The purpose is to reduce false alarms by 40%;
 - integration of mobile systems into international mechanisms – in particular for capacity catalogues of the EU Civil Protection Mechanism, CBRN CoE catalogue and regional cooperation platforms (e.g. Visegrad Group, Three Seas Initiative). This will ensure not only cross-border cooperation opportunities, but also increase the credibility and readiness of Poland to respond to emergencies at the European level.
3. Key Performance Indicators (KPI) after full implementation:
- NH_4NO_3 incident response time: ≤ 45 min (at present: 120 min);
 - contamination identification precision: $\geq 99\%$ (GC-MS + AI);
 - prevented losses cost: $\geq 3:1$ (investment vs. damage);
- scenariusze zagrożeń CBRN i wybuchu azotanów), ocenę operacyjną i pozyskanie danych ewaluacyjnych;
- zabezpieczenie źródeł finansowania długoterminowego – poprzez mechanizmy Unii Europejskiej (Horyzont Europa, rescEU, Fundusz Spójności) oraz włączenie tematów CBRN i mobilnych technologii kryzysowych do krajowych strategii badań i rozwoju (np. Program Operacyjny FEnIKS, Krajowe Inteligentne Specjalizacje).
2. Rekomendacje rozwojowe:
- hybrydowa łączność – wdrożenie sieci mesh LTE-satelita (Starlink) w modułach dowodzenia, zapewniające pokrycie zasięgiem 100% terenu Polski. System powinien automatycznie przełączać się między sieciami w zależności od ich dostępności i przepustowości;
 - certyfikacja mobilnych modułów BSL-3+ według zmodyfikowanej normy VDI 2083 p. 19, we współpracy z CNBOP-PIB i IBM. Celem jest pełna walidacja szczelności (ISO 14644-3) do 2026 r. Należy opracować procedury testowania szczelności w warunkach polowych, uwzględniające specyfikę konstrukcji mobilnych;
 - rozwój algorytmów AI predictive analytics – predykcja wtórnych detonacji NH_4NO_3 na podstawie danych historycznych (temperatura, wilgotność, czas składowania, zanieczyszczenia) w ramach grantu NATO SPS. Celem jest redukcja fałszywych alarmów o 40%;
 - włączenie systemów mobilnych do mechanizmów międzynarodowych – w szczególności do katalogów zdolności Mechanizmu Ochrony Ludności UE, katalogu CBRN CoE oraz platform współpracy regionalnej (np. Grupa Wyszehradzka, Trójmorze). Zapewni to nie tylko możliwość współpracy transgranicznej, ale również zwiększy wiarygodność i gotowość Polski do reagowania na sytuacje nadzwyczajne na poziomie europejskim.
3. Wskaźniki skuteczności KPI (ang. *Key Performance Indicators*) po pełnym wdrożeniu:
- czas reakcji na zdarzenia z NH_4NO_3 : ≤ 45 min (obecnie: 120 min);
 - dokładność identyfikacji skażeń: $\geq 99\%$ (GC-MS + AI);
 - koszt unikniętych strat: $\geq 3:1$ (inwestycja vs. potencjalne zniszczenia);
 - redukcja powierzchni stref krytycznych o 40%; oraz wzrost pozycji Polski w mechanizmie rescEU jako lidera ds. zdarzeń chemicznych.
4. Kluczowy czynnik sukcesu – wdrożenie „Living Lab” przy Politechnice Świętokrzyskiej jako poligonu testowego do kalibracji sensorów IoT w ekstremalnych warunkach (temperatura $>300^\circ\text{C}$), integracji z systemami wojskowymi MON w scenariuszach sabotażu oraz cyklicznych ćwiczeń z PSP SGRChem-Eko. Living Lab powinien umożliwiać testowanie systemu w warunkach zbliżonych do

- reduction of critical zone surface by 40%; and improvement of the position of Poland in the rescEU mechanism as leader for chemical incidents.
4. Key success factor – implementation of the “Living Lab” at the Kielce University of Technology as test site for IoT sensor calibration in extreme conditions (temperature >300°C), integration with military systems of the Ministry of National Defence in sabotage scenarios and regular training with the State Fire Service SGRChem-Eko. The Living Lab should enable testing the system in conditions similar to real, with the involvement of all interested entities (the State Fire Service, the military, the Voivodship Inspectorate of Environmental Protection, local-government administration) [9].

Discussion

The presented concept of the MMCMSS uses verified technical solutions, such as mobile CBRNE laboratories of the State Fire Service [1], [7] and PIAP robot family (Patrol, Gryf, Ibis, Fenix, HUNTeR, Shiba II) developed by the Łukasiewicz Research Network. However, in contrast with the existing and limited scope solutions of the MMCMSS integrates reconnaissance, command, analysis and decontamination functions in one cohesive operating system.

On the international scale, it is worth noting the MIRACLE project (“Mobile Laboratory Capacity for the Rapid Assessment of CBRN Threats Located within and outside the EU”) funded by the European Union, of which the purpose was to develop the CBRN hazard assessment capability directly in the place of occurrence [1]. In addition, the ObSAS project (“Observis Mobile CBRNE Labs”) develops the concept of mobile laboratories and command centres in the context of general CBRN hazards. However, there is no systematic research on their application to specific ammonium nitrate explosion scenarios.

The comparison to reference EU systems (e.g. TOXI-Triage) shows advantages of the MMCMSS in terms of NH_4NO_3 analysis time and better adaptation to urban infrastructure due to integration with the Smart City platform. Operational costs of the MMCMSS are also lower than of the TOXI-Triage system [3].

In the context of development of national capabilities in the field of modern and integrated crisis management, the initiative to create Kieleckie Centrum Nowoczesnego Zarządzania Kryzysowego (KCNZK, Kielce Centre of Modern Crisis Management) is particularly noteworthy. This project, pursued in cooperation with the Kielce University of Technology and the city of Kielce, projects the creation of a modular and mobile operating centre, capable of operating both in stationary conditions and in situations that require quick movement of resources and personnel into the hazard zone [9].

The purpose of the undertaking is to develop innovative research and operational infrastructure to enable responding to a wide spectrum of hazards, including natural disasters, chemical incidents, cyberattacks and military incidents. The project is based on strict cooperation of the scientific sector, local

rzeczywistych, z udziałem wszystkich zainteresowanych podmiotów (PSP, wojsko, WIOŚ, administracja samorządowa) [9].

Dyskusja

Przedstawiona koncepcja MMCZK wykorzystuje sprawdzone rozwiązania techniczne, takie jak mobilne laboratoria CBRNE PSP [1], [7] oraz rodzinę robotów PIAP (Patrol, Gryf, Ibis, Fenix, HUNTeR, Shiba II) rozwijaną w ramach Sieci Badawczej Łukasiewicz. Jednak w odróżnieniu od dotychczasowych, wycinkowych rozwiązań MMCZK integruje funkcje rozpoznania, dowodzenia, analizy i dekontaminacji w jeden spójny system operacyjny.

W skali międzynarodowej warto zwrócić uwagę na projekt MIRACLE („Mobile Laboratory Capacity for the Rapid Assessment of CBRN Threats Located within and outside the EU”) finansowany przez Unię Europejską, którego celem było rozwijanie zdolności oceny zagrożeń CBRN bezpośrednio w miejscu ich wystąpienia [1]. Również projekt ObSAS („Observis Mobile CBRNE Labs”) rozwija koncepcje mobilnych laboratoriów i centrów dowodzenia w kontekście ogólnych zagrożeń CBRN. Jednak brak jest systematycznych badań nad ich zastosowaniem w specyficznych scenariuszach wybuchów azotanu amonu.

Porównanie z referencyjnymi systemami UE (np. TOXI-Triage) wskazuje na przewagę MMCZK w zakresie czasu analizy NH_4NO_3 oraz lepszej adaptacji do infrastruktury miejskiej dzięki integracji z platformą Smart City. Koszty operacyjne MMCZK są również niższe niż w przypadku systemu TOXI-Triage [3].

W kontekście rozwoju krajowych zdolności w obszarze nowoczesnego i zintegrowanego zarządzania kryzysowego szczególną uwagę należy zwrócić na inicjatywę utworzenia Kieleckiego Centrum Nowoczesnego Zarządzania Kryzysowego (KCNZK). Projekt ten, realizowany we współpracy Politechniki Świętokrzyskiej oraz miasta Kielce, zakłada stworzenie modułowego i mobilnego centrum operacyjnego, zdolnego do działania zarówno w warunkach stacjonarnych, jak i w sytuacjach wymagających szybkiego przemieszczenia zasobów i personelu w rejon zagrożenia [9].

Celem przedsięwzięcia jest rozwój innowacyjnej infrastruktury badawczo-operacyjnej umożliwiającej reagowanie na szerokie spektrum zagrożeń, w tym katastrofy naturalne, zdarzenia chemiczne, cyberataki oraz incydenty militarne. Projekt opiera się na ścisłej współpracy sektora naukowego, samorządowego

government and defence industry, which aligns with European and national directions of building systemic resilience [9].

The concept of the centre includes the use of advanced technologies, such as artificial intelligence systems, environmental sensors, independent power sources, integrated crisis communication links and decision support systems. The planned units will be modular in nature, enabling reconfiguration depending on the type and scale of incident, which in practice means high application flexibility and operational mobility [9].

From the MMCMS perspective, the KCNZK project is a valuable case study illustrating the possibility of practical use of mobile and modular technological solutions in crisis management, including in scenarios involving hazardous materials, such as ammonium nitrate.

The presented concept of the MMCMS, despite its potential, has some limitations, which should be included in the interpretation of results (see section Methodology):

- lack of quantitative studies under actual explosion conditions,
- limited test sample,
- limited site test conditions,
- limited access to sensitive information,
- lack of full validation of the system – the assumed concept of the MMCMS is a proprietary technical and organisational proposition, which still remains to be fully validated in certification mode in accordance with PN-EN, ISO standards or NATO guidelines. The presented technical parameters are design values, not results of independent certification tests.

The directions for further studies include:

1. Modelling operational effectiveness of mobile systems under various hazard conditions – both in simulation (agent, FEM and CFD simulation modelling) and empirical terms (data analysis from exercise and actual incidents).
2. Application of artificial intelligence and edge computing in decision support processes, environmental data analysis and situation reconnaissance. Development of algorithms for automatic identification of chemical hazards (e.g. identification of volatile compounds after ammonium nitrate explosion) and prediction of contaminant propagation.
3. Research on interoperability and standardisation of procedures – in particular in the context of integration of mobile support systems with national and European Union crisis response structures. Further research is necessary on the harmonisation of SOP procedures, definitions of operational function (OF) and multi-agent management models (ICS, ERCC).
4. Research on social acceptance, legal safety and institutional responsibility – analysis of perception of mobile systems among decision-makers, rescuers and local communities – in particular in the context of chemical hazards.
5. Verification of the concept in cross-border and multi-national conditions – through involvement in international training (e.g. EU MODEX, CBRN CoE) and system testing in diverse cultural and infrastructural environments.

i przemysłu obronnego, co wpisuje się w europejskie i krajowe kierunki budowy odporności systemowej [9].

Koncepcja centrum uwzględnia zastosowanie zaawansowanych technologii, takich jak systemy sztucznej inteligencji, sensoryka środowiskowa, niezależne źródła zasilania, zintegrowane łącza łączności kryzysowej oraz systemy wspomagania decyzji. Planowane jednostki będą miały charakter modułowy, umożliwiając ich rekonfigurację w zależności od rodzaju i skali zdarzenia, co w praktyce oznacza wysoką elastyczność zastosowania i operacyjną mobilność [9].

Z perspektywy MMCZK projekt KCNZK stanowi wartościowe studium przypadku ilustrujące możliwości praktycznego zastosowania mobilnych i modułowych rozwiązań technologicznych w zarządzaniu kryzysowym, w tym również w scenariuszach z udziałem materiałów niebezpiecznych, takich jak azotan amonu.

Prezentowana koncepcja MMCZK, mimo swojego potencjału, podlega pewnym ograniczeniom, które należy uwzględnić przy interpretacji wyników (zob. punkt Metodologia):

- brak badań ilościowych w warunkach rzeczywistego wybuchu,
- ograniczona próba badawcza,
- ograniczone warunki testów poligonowych,
- ograniczony dostęp do danych wrażliwych,
- brak pełnej walidacji systemu – przyjęta koncepcja MMCZK jest autorską propozycją techniczno-organizacyjną, która nie została jeszcze poddana pełnej walidacji w trybie certyfikacji zgodnej z normami PN-EN, ISO lub wytycznymi NATO. Przedstawione parametry techniczne są wartościami projektowymi, a nie wynikami niezależnych testów certyfikacyjnych.

Do kierunków dalszych badań należą:

1. Modelowanie efektywności operacyjnej systemów mobilnych w zróżnicowanych warunkach zagrożeń – zarówno w ujęciu symulacyjnym (modelowanie agentowe, symulacje FEM i CFD), jak i empirycznym (analiza danych z ćwiczeń i rzeczywistych zdarzeń).
2. Zastosowanie sztucznej inteligencji i *edge computing* w procesach wspomagania decyzji, analizy danych środowiskowych i rozpoznania sytuacyjnego. Opracowanie algorytmów umożliwiających automatyczne rozpoznanie zagrożenia chemicznego (np. identyfikacja lotnych związków po wybuchu azotanu amonu) oraz predykcję rozprzestrzeniania się skażeń.
3. Badania nad interoperacyjnością i standaryzacją procedur – zwłaszcza w kontekście integracji mobilnych systemów wsparcia z krajowymi i unijnymi strukturami reagowania kryzysowego. Niezbędne są dalsze badania nad harmonizacją procedur SOP, definicją funkcji operacyjnych (OF) oraz modelami zarządzania wieloagentowego (ICS, ERCC).
4. Badania w zakresie akceptacji społecznej, bezpieczeństwa prawnego i odpowiedzialności instytucjonalnej – analiza postrzegania mobilnych systemów przez decydentów, ratowników i społeczności lokalne – zwłaszcza w kontekście zagrożeń chemicznych.
5. Weryfikacja koncepcji w warunkach transgranicznych i wielonarodowych – poprzez udział w ćwiczeniach

międzynarodowych (np. EU MODEX, CBRN CoE) oraz testowanie systemów w środowiskach zróżnicowanych kulturowo i infrastrukturalnie.

Summary

In view of the increasing frequency and scale of technological and chemical hazards, including in particular uncontrolled ammonium nitrate explosions, crisis management is required to convert into a more dynamic, flexible and technologically supported system. Modular mobile crisis management support systems are a real tool of implementation of state security politics, supporting the achievement of the objectives of the Civil Protection and Civil Defence Act in terms of civil protection, ensuring continuous operation of public institutions and reinforcing social resistance to hazards, including to disaster explosions of ammonium nitrate.

Conclusions

The conducted analysis leads to the following conclusions:

1. The MMCMS is a key direction of development of safety systems. The identified system gaps, deficit of early chemical reconnaissance, lack of interoperable command structures, insufficient integration of unmanned technologies, regulatory fragmentation, justify the need to implement an integrated mobile crisis management support system. The experiences of disasters in Saint-Romain-en-Jarez, West i Beirut show that the lack of proper protections and inadequate knowledge of rescue services may lead to catastrophic effects [2], [4], [6].
2. Modularity as strategic system characteristic. The division of the MMCMS into independent, yet interoperable modules (command, analysis, technical, communication and decontamination) enables clear adjustment to the type and scale of hazard – from local chemical leakage to industrial disaster with regional range. The “plug & play” setup and two operating modes (“Fast Response” – 30 min, “Full Scale” – 90 min) optimise the use of resources [3].
3. Operational autonomy as essential requirement. The principle of independence on stationary infrastructure (deployment time ≤ 45 min, autonomy ≥ 72 h., generator 80 kW, VFI UPS, HEPA H14 filtering, satellite communication) is essential for operation in the ammonium nitrate explosion zone, in which infrastructure is destroyed. The MMCMS meets the requirement of Article 33 Section 3 of the Civil Protection and Civil Defence Act (resources for at least 3 days) [3], [11].
4. Need for standardisation and system integration. The implementation of the MMCMS requires developing the national functional specification for mobile support systems, including the requirements for modularity, interoperability, BSL-3 standards, communication and power

Podsumowanie

W obliczu rosnącej częstotliwości oraz skali zagrożeń technologicznych i chemicznych, w tym szczególnie niekontrolowanych wybuchów azotanu amonu, zarządzanie kryzysowe staje przed koniecznością przekształcenia się w system bardziej dynamiczny, elastyczny i wsparty technologicznie. Modułowe mobilne systemy wspomaganie zarządzania kryzysowego stanowią realne narzędzie wdrażania polityki bezpieczeństwa państwa, wspierające realizację celów ustawy o ochronie ludności i obronie cywilnej w zakresie ochrony ludności, zapewnienia ciągłości działania instytucji publicznych oraz wzmacniania odporności społecznej na zagrożenia – w tym na katastrofalne wybuchy azotanu amonu.

Wnioski

Przeprowadzona analiza prowadzi do następujących wniosków:

1. MMCZK stanowi kluczowy kierunek rozwoju systemów bezpieczeństwa. Zidentyfikowane luki systemowe – deficyt wczesnego rozpoznania chemicznego, brak interoperacyjnych struktur dowodzenia, niewystarczająca integracja technologii bezzałogowych, fragmentacja regulacyjna – uzasadniają konieczność wdrożenia zintegrowanego, mobilnego systemu wspomaganie zarządzania kryzysowego. Doświadczenia z katastrof w Saint-Romain-en-Jarez, West i Bejrucie pokazują, że brak odpowiednich zabezpieczeń oraz niedostateczna wiedza służb ratowniczych mogą prowadzić do katastrofalnych skutków [2], [4], [6].
2. Modułowość jako strategiczna cecha systemu. Podział MMCZK na niezależne, lecz interoperacyjne moduły (dowodzenia, analityczny, techniczny, komunikacyjny, dekontaminacyjny) umożliwia elastyczne dostosowanie do charakteru i skali zdarzenia – od lokalnego wycieku chemicznego po katastrofę przemysłową o zasięgu regionalnym. Konfiguracja „plug & play” oraz dwa tryby operacyjne („Fast Response” – 30 min, „Full Scale” – 90 min) zapewniają optymalne wykorzystanie zasobów [3].
3. Autonomia operacyjna jako warunek konieczny. Założenie niezależności od infrastruktury stacjonarnej (czas rozstawienia ≤ 45 min, autonomia ≥ 72 godz., agregat 80 kW, UPS VFI, filtracja HEPA H14, łączność satelitarna) jest kluczowe dla działania w strefie wybuchu azotanu amonu, gdzie infrastruktura ulega zniszczeniu. MMCZK spełnia wymagania art. 33 ust. 3 ustawy o ochronie ludności i obronie cywilnej (zasoby na co najmniej 3 dni) [3], [11].
4. Konieczność standaryzacji i integracji systemów. Wdrożenie MMCZK wymaga opracowania narodowej specyfikacji funkcjonalnej dla mobilnych systemów wsparcia, obejmującej wymagania dotyczące modułowości, interoperacyjności, norm BSL-3, łączności i zasilania.

supply. It is also essential to unify SOP procedures and ensure interoperability with the systems of the State Fire Service, Crisis Management Centre, RCB and EU (ERCC, CECIS, rescEU) and NATO (STANAG 4632, AEP-66) mechanisms [1], [7].

5. Need for legislative changes. It is essential to pass the "NH₄NO₃ Code" to unify the regulations on storage, transport and neutralisation, as well as to develop standards for air-tightness of mobile biological modules in field conditions (VDI 2083 p. 19). It is also essential to develop unified port and transshipment terminal inspection procedures, including the maximum storage time and the requirement to keep warehouse temperature and humidity records.
6. High development potential, yet with significant barriers. The SWOT analysis confirms the high potential of the MMCSS, however it also shows significant barriers – high initial costs, personnel deficit (shortage of AI specialists among firefighters, long operator training time), regulatory fragmentation, which must be included at the stage of implementation.
7. The Beirut disaster as argument for the MMCSS implementation. The experience of Beirut shows that even countries with relatively developed institutions could be unprepared for crisis if they have flexible and resilient response systems. The implementation of the MMCSS could ensure quick formation of the command station with satellite communication, integration of data from drones and environmental sensors and coordination between services, local authorities, the military and non-government organisations [6].

Niezbędne jest również ujednolicenie procedur SOP oraz zapewnienie interoperacyjności z systemami PSP, CZK, RCB, a także z mechanizmami UE (ERCC, CECIS, rescEU) i NATO (STANAG 4632, AEP-66) [1], [7].

5. Potrzeba zmian legislacyjnych. Niezbędne jest uchwalenie „Kodeksu NH₄NO₃” ujednolicającego przepisy dotyczące magazynowania, transportu i neutralizacji, a także opracowanie norm dla hermetyczności mobilnych modułów biologicznych w warunkach polowych (VDI 2083 p. 19). Konieczne jest również opracowanie jednolitych procedur kontroli portów i terminali przeładunkowych, z uwzględnieniem maksymalnego czasu składowania oraz obowiązku prowadzenia rejestru temperatury i wilgotności w magazynach.
6. Wysoki potencjał wdrożeniowy, ale z istotnymi barierami. Analiza SWOT potwierdza wysoki potencjał MMCZK, jednak wskazuje również na istotne bariery – wysokie koszty początkowe, deficyty kadrowe (brak specjalistów AI wśród strażaków, długi czas szkolenia operatorów), fragmentację regulacyjną – które muszą zostać uwzględnione na etapie wdrażania.
7. Katastrofa w Bejrucie jako argument za wdrożeniem MMCZK. Doświadczenia z Bejrutu pokazują, że nawet państwa o stosunkowo rozwiniętych instytucjach mogą być nieprzygotowane na kryzysy, jeśli nie dysponują elastycznymi i odpornymi systemami reagowania. Wdrożenie MMCZK mogłoby zapewnić szybkie utworzenie punktu dowodzenia z łącznością satelitarną, integrację danych z dronów i czujników środowiskowych oraz koordynację między służbami, władzami lokalnymi, wojskiem i organizacjami pozarządowymi [6].

List of abbreviations

AA	ammonium nitrate
AI	artificial intelligence
ATR	attenuated total reflectance
BSL-3	biosafety level 3
CBRNE	chemical, biological, radiological, nuclear and explosive hazards
CECIS	EU Common Emergency Communication and Information System
CFD	computational fluid dynamics
DDT	deflagration to detonation transition
ERCC	Emergency Response Coordination Centre
FTIR	Fourier transform infrared spectroscopy
GC-MS	gas chromatography – mass spectrometry
GIS	geographic information system
HEPA	high efficiency particulate air filter
HPGe	high purity germanium detector
HVAC	heating, ventilation, and air conditioning
IAEA	International Atomic Energy Agency
IC	ion chromatography

Wykaz skrótów

AA	azotan amonu
AI	sztuczna inteligencja
ATR	technika tłumionego całkowitego odbicia
BSL-3	trzeci poziom bezpieczeństwa biologicznego
CBRNE	zagrożenia chemiczne, biologiczne, radiologiczne, nuklearne i wybuchowe
CECIS	wspólny system komunikacji i informacji kryzysowej UE
CFD	obliczeniowa mechanika płynów
DDT	przejście deflagracji w detonację
ERCC	Centrum Koordynacji Reagowania Kryzysowego UE
FTIR	spektroskopia w podczerwieni z transformacją Fouriera
GC-MS	chromatografia gazowa sprzężona ze spektrometrią mas
GIS	system informacji geograficznej
HEPA	wysoko skuteczny filtr cząstek stałych
HPGe	detektor półprzewodnikowy wysokiej czystości

ICT	information and communications technology	HVAC	ogrzewanie, wentylacja i klimatyzacja
IMS	ion mobility spectrometry	IAEA	Międzynarodowa Agencja Energii Atomowej
IoT	Internet of Things	IC	chromatografia jonowa
KSRG	National Rescue and Firefighting System	ICT	technologie informacyjno-komunikacyjne
MMCMSS	modular mobile crisis management support systems	IMS	spektrometria ruchliwości jonów
PID	photoionization detector	IoT	internet rzeczy
PSP	State Fire Service	KSRG	krajowy system ratowniczo-gaśniczy
rescEU	European Help Reserve	MMCZK	modułowe mobilne systemy wspomagania zarządzania kryzysowego
SGRChem-Eko	specialised chemical and environmental rescue group	PID	detektor fotojonizacyjny
SIBCRA	Sampling and Identification of Biological, Chemical and Radiological Agents (NATO)	PSP	Państwowa Straż Pożarna
SOP	standard operating procedures	rescEU	Europejska Rezerwa Pomocy
STANAG	Standardization Agreement	SGRChem-Eko	specjalistyczna grupa ratownictwa chemiczno-ekologicznego
UCPM	Union Civil Protection Mechanism	SIBCRA	procedury pobierania i identyfikacji próbek CBRN (NATO)
UAV	unmanned aerial vehicle	SOP	standardowe procedury operacyjne
UGV	unmanned ground vehicle	STANAG	umowa standaryzacyjna NATO
USV	unmanned surface vessel	UCPM	Unijny Mechanizm Ochrony Ludności
UPS	uninterruptible power supply	UAV	bezzałogowy statek powietrzny
UV-VIS	ultraviolet and visible light spectrophotometry	UGV	bezzałogowy pojazd naziemny
XRF	X-ray fluorescence	USV	bezzałogowy pojazd nawodny
		UPS	zasilacz bezprzewodowy
		UV-VIS	spektrofotometria w ultrafiolecie i świetle widzialnym
		XRF	spektrometria fluorescencji rentgenowskiej

AI Use Statement

The author declare that artificial intelligence tools were used in the preparation of this article only within the scope indicated below:

- improving graphic readability (ChatGPT).

The author takes full responsibility for the content of the publication, including the scientific accuracy, interpretation of results, and final editing of the manuscript. Artificial intelligence tools were used solely as supporting instruments.

The journal's editorial policy prohibits the uncritical copying of AI-generated content and its inclusion in a publication without proper critical analysis, verification, and revision by the author.

Oświadczenie dotyczące wykorzystania AI

Autor oświadcza, że w procesie przygotowania niniejszego artykułu wykorzystano narzędzia oparte na sztucznej inteligencji wyłącznie w zakresie wskazanym poniżej:

- poprawa czytelności grafik (ChatGPT).

Autor ponosi pełną odpowiedzialność za treść publikacji, w tym za poprawność merytoryczną, interpretację wyników oraz ostateczną redakcję tekstu. Narzędzia sztucznej inteligencji były wykorzystywane wyłącznie jako narzędzia pomocnicze. Polityka redakcyjna czasopisma zabrania bezrefleksyjnego kopiowania treści wygenerowanych przez narzędzia AI oraz pozostawiania ich w publikacji bez krytycznej analizy, weryfikacji i redakcji przez autora.

Literature / Literatura

- [1] Bugaj G., *Funkcjonalność mobilnego laboratorium CBRNE Państwowej Straży Pożarnej w świetle przepisów prawnych oraz założeń operacyjnych Krajowego Systemu Ratowniczo-Gaśniczego*, „Przegląd Bezpieczeństwa Wewnętrznego” 2026, 34(18), 57–77.
- [2] U.S. Chemical Safety and Hazard Investigation Board. Investigation Report: West Fertilizer Company Fire and Explosion (CSB Report No. 2013-02-I-TX). Washington, DC: CSB, 2016.
- [3] Tuśnio N., *Modułowe mobilne systemy wspomagania zarządzania kryzysowego w kontekście identyfikacji, oceny i minimalizacji ryzyka zdarzeń z udziałem azotanu amonu*, Kaliskie Towarzystwo Przyjaciół Nauk, Kalisz 2026.
- [4] French Ministry of Sustainable Development – DGPR / SRT / SDRA / BARPI. Fire inside a barn and explosion of fertilizer, October 2, 2003, Saint Romain-en-Jarez [Loire], France (ARIA Report No. 25669), Paris: BARPI 2010.
- [5] ISPRA. Mappatura dei pericoli di incidente rilevante in Italia. Edizione 2013 (Raport nr 181/2013). Rome: ISPRA, 2013.
- [6] Sakr T.E., *Disaster Management and Community Response in Lebanon: The Case of Beirut Port Explosion*, American University of Beirut, 2022.

- [7] Bugaj G., Janik P., *CBRNE Mobile Analytical Laboratory of the State Fire Service – Analysis of Technical and Normative Solutions Applied*, Safety & Fire Technology 2025, 65(1), 78–97, <https://doi.org/10.12845/sft.65.1.2025.7>.
- [8] Feltynowski M., *Trudna akcja ratownicza po eksplozji w Bejrucie*, „Przemysł Chemiczny” 2020, 9, 1269–1272, <https://doi.org/10.15199/62.2020.9.2>.
- [9] *Inicjatywa budowy modelowego mobilnego centrum danych dla zarządzania kryzysowego w Kielcach*, Portal internetowy Politechniki Świętokrzyskiej, <https://tu.kielce.pl/kielcie-centrum-nowoczesnego-zarzadzania-kryzysowego/> [dostęp: 20.03.2025]
- [10] Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz.U. 1991, Nr 88, poz. 400).
- [11] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007, Nr 89, poz. 590).
- [12] Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024, poz. 1907).
- [13] Ustawa z dnia 7 listopada 2025 r. o zmianie ustawy o systemie informacji w ochronie zdrowia oraz ustawy o ochronie ludności i obronie cywilnej (Dz.U. 2025, poz. 1705).
- [14] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 17 września 2021 r. w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego (Dz.U. 2021, poz. 1737).
- [15] Zasady organizacji ratownictwa chemicznego i ekologicznego w krajowym systemie ratowniczo-gaśniczym, KG PSP, Warszawa 2025.
- [16] PN-EN ISO 14644-3:2020 – Pomieszczenia czyste i związane z nimi środowiska kontrolowane – Część 3: Metody badań.
- [17] PN-EN 1822-1:2009 – Wysokoskuteczne filtry powietrza (EPA, HEPA i ULPA) – Część 1: Klasyfikacja, badanie parametrów, znakowanie.
- [18] VDI 2083 Blatt 19:2009-12 – Reinraumtechnik – Klassifizierung und Messung der Leckage von Gehäusen und Isolatoren.
- [19] STANAG 4632 (Edition 1) – Deployable NBC Analytical Laboratory. Brussels: NATO Standardization Agency, 2005.
- [20] AEP-66 – NATO Handbook for Sampling and Identification of Biological, Chemical and Radiological Agents (SIBCRA). Brussels: NATO Standardization Agency, 2015.

SR. BRIG. NORBERT TUŚNIO, PH.D. ENG. – assistant professor in the Division of Rescue Operations Management, Firefighting Operations and Communication (Department of Rescue Operations, Faculty of Rescue Operations, Safety Engineering and Civil Protection, Fire University). Specialised in safety engineering, in particular crisis management, fire safety and using modern technologies in rescue operations. Author and co-author of numerous scientific publications, including monographs and articles indexed in international bases on e.g. fire modelling, explosion hazards and use of unmanned systems in rescue operations. Participated in and directed research and development projects funded from national and European Union funds. Active in the scientific community as reviewer and organiser of conferences, conducting didactic and training activities. Completed domestic and international research internships, focused on the practical use of research in safety systems.

ST. BRYG. DR INŻ. NORBERT TUŚNIO – adiunkt w Zakładzie Kierowania Działaniami Ratowniczymi, Działań Gaśniczych i Łączności (Katedra Działań Ratowniczych, Wydział Inżynierii Bezpieczeństwa i Ochrony Ludności Akademii Pożarniczej). Specjalizuje się w inżynierii bezpieczeństwa, w szczególności w zarządzaniu kryzysowym, bezpieczeństwie pożarowym oraz wykorzystaniu nowoczesnych technologii w ratownictwie. Jest autorem i współautorem licznych publikacji naukowych, w tym monografii oraz artykułów indeksowanych w bazach międzynarodowych, dotyczących m.in. modelowania pożarów, zagrożeń wybuchowych oraz zastosowania bezzałogowych systemów w działaniach ratowniczych. Uczestniczył i kierował projektami badawczo-rozwojowymi finansowanymi ze środków krajowych i europejskich. Aktywnie działa w środowisku naukowym jako recenzent i organizator konferencji, prowadzi działalność dydaktyczną oraz szkoleniową. Odbił staże naukowe w kraju i za granicą, koncentrując się na praktycznym zastosowaniu badań w systemach bezpieczeństwa.

SZKOLENIA SPECJALISTYCZNE CNBOP-PIB

stacjonarne / hybrydowe / on-line



**szkolenia dla rzeczoznawców
ds. zabezpieczeń ppoż.**



**szkolenia dla projektantów,
instalatorów, konserwatorów
i specjalistów**



**szkolenia dotyczące wyrobów
stosowanych w ochronie ppoż.**

GWARANTUJEMY

- ✓ wysoki poziom merytoryczny
- ✓ różnicowany stopień zaawansowania
– dostosowany do wiedzy i umiejętności kursantów
- ✓ optymalny dobór zagadnień
- ✓ wykwalifikowaną kadrę wykładowców

OFERUJEMY

- ✓ aktualną wiedzę i praktyczne umiejętności
w wybranym obszarze
- ✓ uznawany na rynku certyfikat lub zaświadczenie
- ✓ ćwiczenia projektowe

WYKAZ SZKOLEŃ

01 | Szkolenie dla konserwatorów systemów sygnalizacji pożarowej

02 | Szkolenia dla rzeczoznawców do spraw zabezpieczeń przeciwpożarowych

03 | Szkolenie dla projektantów systemów wentylacji pożarowej w obiektach budowlanych

04 | Szkolenie dla projektantów, instalatorów i konserwatorów dźwiękowych systemów ostrzegawczych

05 | Przegląd i konserwacja systemów wentylacji pożarowej w obiektach budowlanych

06 | Szkolenie dla konserwatorów podręcznego sprzętu gaśniczego

07 | Szkolenie dla projektantów, instalatorów i konserwatorów systemów sygnalizacji pożarowej

08 | Dyrektywa ATEX. Ocena ryzyka związanego z możliwością wystąpienia atmosfery wybuchowych – podejście praktyczne

09 | Instrukcja bezpieczeństwa pożarowego. Praktyczne wskazówki opracowania dokumentu z przykładami

10 | Stałe urządzenia gaśnicze tryskaczowe w ochronie przeciwpożarowej

11 | Przeciwpożarowy wyłącznik prądu „PWP”

12 | Planowanie i organizacja ewakuacji ludzi z budynków

13 | Szkolenie dla konserwatorów hydrantów zewnętrznych i wewnętrznych

14 | Szkolenie Inspektorów Ochrony Przeciwpożarowej

15 | Stałe urządzenia gaśnicze gazowe w ochronie przeciwpożarowej

16 | Oświetlenie awaryjne – projektowanie, instalacja i konserwacja

17 | Szkolenie z zakresu ochrony ppoż. dotyczące drzwi i innych zamknięć przeciwpożarowych. Dobór, montaż, przegląd i konserwacja

18 | Szkolenie aktualizujące dla Inspektorów Ochrony Przeciwpożarowej

19 | Oddymianie grawitacyjne

Jerzy Kosiński

*Naval Academy in Gdynia / Akademia Marynarki Wojennej**Corresponding author / Autor korespondencyjny: j.kosinski@amw.gdynia.pl*

Subversive Operations in Cyberspace

Działania dywersyjne w cyberprzestrzeni

ABSTRACT

Purpose: The purpose of the article is to analyse subversive operations in cyberspace. The author attempts to present cyberspace as operational environment, but also to define and organise the notions of subversion, sabotage and disinformation in the digital context.

Introduction: The subject of the study is the phenomenon of subversion in cyberspace as one of key components of contemporary hybrid conflicts. Based on the analysis of the literature of the subject and case analyses (e.g. attacks on the Ukrainian energy system), the author describes the notional framework of subversion, sabotage and disinformation, conducts an analysis in technical (malware operation), legal (the Tallinn Manual) and social (impact of disinformation on the society) terms. The article also discusses operational mechanisms of the MITRE ATT&CK framework and cybernetic models used to describe subversion in cyberspace. The article presents cyberspace as the fifth domain of warfare, equivalent to the land, maritime, air, and space domains. This status was formally recognized in, among others, documents issued by the United States Department of Defense as early as 2011. Cyberspace has become an area, in which non-kinetic operations – system disruption, sabotage, disinformation – may cause real consequences, comparable to traditional military operations. The author underlines that information is a strategic resource and manipulation has become a weapon. The classical understanding of subversion must be expanded to the digital environment. Subversion in cyberspace enables simultaneous attacks on technical infrastructure, information systems, and public sentiment.

Methodology: The article used definition-notion analysis, legal analysis (in terms of sovereignty, cyberattack impact comparable to attacks with force, state responsibility for controlled or tolerated groups), system and operational analysis and the MITRE ATT&CK framework) and case studies (attacks on the Ukrainian energy system 2015–2022, ransomware WannaCry 2017 and attack on the BadeSaba app 2026).

Conclusions: Due to its relatively low cost, scalability, and the difficulty of attributing attacks, digital subversion has largely supplanted traditional forms of sabotage and disinformation. It is a control system process that accompanies hybrid operations. A cyberattack may cause impact equivalent to the use of force, while misinformation can be as destructive as technical sabotage.

Keywords: cyberspace, disinformation, subversion, sabotage, fire protection infrastructure

Type of article: review article

Received: 18.03.2026; **Reviewed:** 26.05.2026; **Accepted:** 27.05.2026;

Author's ORCID ID: J. Kosiński – 0000-0003-3823-4526;

Please cite as: Safety & Fire Technology 2026, 1, 196–209, <https://doi.org/10.12845/sft.67.1.2026.9>;

This is an open access article under the CC BY-SA 4.0 license (<https://creativecommons.org/licenses/by-sa/4.0/>).

ABSTRAKT

Cel: Celem artykułu jest analiza działań dywersyjnych w cyberprzestrzeni. Autor podejmuje próbę ukazania cyberprzestrzeni jako środowiska operacyjnego, a także zdefiniowania i uporządkowania pojęć dywersji, sabotażu i dezinformacji w kontekście cyfrowym.

Wprowadzenie: Przedmiotem pracy jest zjawisko dywersji w cyberprzestrzeni, stanowiące jeden z kluczowych elementów współczesnych konfliktów hybrydowych. Bazując na analizie literatury przedmiotu oraz studiach przypadków (m.in. ataków na ukraiński system energetyczny), autor opisuje ramy pojęciowe dywersji, sabotażu i dezinformacji, przeprowadza analizę techniczną (działanie złośliwego oprogramowania ang. *malware*), prawną (Poradnik Talliński) oraz społeczną (wpływ dezinformacji na społeczeństwo). W artykule omówiono również mechanizmy operacyjne ramy MITRE ATT&CK, a także modele cybernetyczne wykorzystywane do opisu dywersji w cyberprzestrzeni. Artykuł ukazuje cyberprzestrzeń jako piątą domenę działań zbrojnych, równorzędną wobec lądu, morza, powietrza i kosmosu, co zostało formalnie potwierdzone, m.in. w dokumentach Departamentu Obrony USA już w 2011 roku. Cyberprzestrzeń stała się obszarem, w którym operacje niekinetyczne – zakłócanie systemów, sabotaż, dezinformacja – mogą wywołać realne skutki, porównywalne z tradycyjnymi działaniami militarnymi. Autor podkreśla, że informacja jest zasobem strategicznym, a manipulacja informacją stała się narzędziem walki. Klasyczne rozumienie dywersji musi zostać rozszerzone o środowisko cyfrowe. Dywersja w cyberprzestrzeni umożliwia połączenie uderzenia jednocześnie w infrastrukturę techniczną, systemy informacyjne i emocje społeczne.

Metodologia: W artykule wykorzystano analizę definicyjno-pojęciową, analizę prawną (w zakresie suwerenności, skutków cyberataków porównywalnych do tych z użyciem siły, odpowiedzialności państwa za działania grup kontrolowanych lub tolerowanych), analizę systemową i operacyjną (modele cybernetyczne i framework MITRE ATT&CK) oraz studium przypadku (ataków na ukraińską energetykę 2015–2022, ransomware WannaCry 2017 oraz ataku na aplikację BadaSaba 2026).

Wnioski: Ze względu na niski koszt, skalę działania i trudność przypisania ataku dywersja cyfrowa zdominowała tradycyjne formy sabotażu i dezinformacji. Jest procesem systemowego sterowania, towarzyszącym operacjom hybrydowym. Cyberatak może wywołać skutki równoważne użyciu siły, a dezinformacja jest równie destrukcyjna, jak sabotaż techniczny.

Słowa kluczowe: cyberprzestrzeń, dezinformacja, dywersja, sabotaż, infrastruktura ochrony przeciwpożarowej

Typ artykułu: artykuł przeglądowy

Przyjęty: 18.03.2026; **Zrecenzowany:** 26.05.2026; **Zaakceptowany:** 27.05.2026;

Identyfikator ORCID autora: J. Kosiński – 0000-0003-3823-4526;

Proszę cytować: Safety & Fire Technology 2026, 1, 196–209, <https://doi.org/10.12845/sft.67.1.2026.9>;

Artykuł udostępniany na licencji CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>).

Introduction

The truism that in the age of dynamic technological progress information has become a strategic resource is most often related to national economy. However, it should be remembered that information has always been essential in defining military potential. The traditional perception of the battlefield has been expanded to cyberspace, which has become the perfect environment for non-kinetic operations aiming to defeat the opponent [1, p. 40–48]. In the beginning of the second decade of the 21st century, cyberspace was listed as one more combat domain in official documents. *US Department of Defence Strategy for Operating in Cyberspace* of 2011 equated operations in the cyberspace with military operations in the land, sea, air and cosmos [2, p. 5]. Disrupting enemy systems, causing damage and disinformation using cyberspace or against it have become operations of the standard repertoire of every army. Operations disrupting state systems, in particular damaging critical infrastructure (e.g. healthcare, energy system, justice system), causing impact physically or in the digital environment and infringing on the sovereignty of the state subjected to the attack [3, p. 17] – they are no longer a vision of the future. In the field of fire protection, the knowledge and risk reduction of cyberattacks, sabotage and disinformation affecting fire protection infrastructure should increase the effectiveness of fire detection, alarm and fighting systems and support the operational readiness of fire services.

Wstęp

Truizm mówiący o tym, że w dobie gwałtownego postępu technologicznego informacja stała się zasobem strategicznym, odnoszony jest najczęściej do gospodarki państwa. Trzeba jednak pamiętać, że informacja od zawsze miała kluczowe znaczenie dla potencjału militarnego. Tradycyjne postrzeganie pola walki uległo rozszerzeniu o cyberprzestrzeń, która stała się idealnym środowiskiem do prowadzenia działań o charakterze niekinetycznym, zmierzających do pokonania przeciwnika [1, s. 40–48]. Na początku drugiej dekady XXI wieku cyberprzestrzeń została wymieniona w oficjalnych dokumentach jako kolejna domena walki. *Strategia Operacji w Cyberprzestrzeni Departamentu Obrony USA* z 2011 roku zrównała działania w cyberprzestrzeni z działaniami zbrojnymi prowadzonymi na lądzie, morzu, w powietrzu i kosmosie [2, s. 5]. Zakłócanie funkcjonowania systemów przeciwnika, powodowanie szkód i dezinformacja z wykorzystaniem cyberprzestrzeni lub przeciwko niej stały się działaniami ze standardowego zestawu każdej armii. Operacje zakłócające działanie systemów państwowych – w szczególności uszkadzające infrastrukturę krytyczną (np. służby zdrowia, energetyki, sądownictwa), powodujące skutki fizyczne lub w środowisku cyfrowym i naruszające suwerenność państwa będącego obiektem ataku [3, s. 17] – nie są już tylko wizją przyszłości. W obszarze ochrony przeciwpożarowej znajomość oraz ograniczanie ryzyka cyberataków, sabotażu i dezinformacji oddziałujących na infrastrukturę ochrony przeciwpożarowej powinny zwiększać skuteczność systemów wykrywania, alarmowania i gaszenia pożarów oraz wspierać gotowość operacyjną służb pożarniczych.

Definition and understanding of the cyberspace

The understanding of the nature of contemporary subversion requires a precise definition of the environment, in which it is operated. Cyberspace can be considered in two key perspectives:

- 1) the technological perspective, which includes data, information and infrastructure required to process it, including hardware, software, operating systems and network protocols;

Definicja i rozumienie cyberprzestrzeni

Zrozumienie natury współczesnej dywersji wymaga precyzyjnego zdefiniowania środowiska, w którym jest realizowana. Cyberprzestrzeń można rozpatrywać w dwóch kluczowych perspektywach:

- 1) perspektywie technologicznej, która obejmuje dane, informacje oraz infrastrukturę niezbędną do ich przetwarzania, w tym sprzęt, oprogramowanie, systemy operacyjne i protokoły sieciowe;

- 2) the full perspective, which includes not only technology, but also the human as the creator, manager and consumer of data and information.

One of the most referenced definitions of cyberspace, viewed from the technological perspective, is the one included in the *Dictionary of Military and Associated Terms* of the US Department of Defence. According to it, cyberspace is: "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" [4, p. 45].

Also K. Liderman emphasises the technology and writes that "the environment (consisting of land, water, air, cosmos and the electromagnetic field) and objects placed in that environment, which have the potential to shape the electromagnetic field and to detect changes and store information on these changes" [5, p. 22].

The notion of cyberspace was introduced to the Polish legal system by the amendment to the Act of 30 August 2011 on the Martial Law and authority of the Commander-in-Chief and applicable rules of subordination to the constitutional bodies of the Republic of Poland. In literature, a series of objections to the correctness of that definition may be found [6, p. 8], [7, p. 20].

The full view of the cyberspace has also been noticed in the cybersecurity doctrine of the Republic of Poland of 2015, in which "user relations" were added to the technological definition [8, p. 7]. The human is as responsible for system dynamics as the data and technology. IT systems could not operate without the human (even AI will not replace the human completely). A widely known statement on cybersecurity is that the users are its weakest link. Therefore the users are often targeted by direct attacks. Their thoughts and interactions with IT systems are part of cyberspace, because they evidence activity conducted in the digital environment. Human-to-human and human-to-ITC system interactions are the most frequent vector of subversive attacks, sabotage and disinformation.

- 2) perspektywie pełnej, która uwzględnia nie tylko technologię, ale również człowieka jako twórcę, zarządcę i konsumenta danych i informacji.

Jedną z najczęściej przywoływanych definicji cyberprzestrzeni, postrzeganej z perspektywy technologicznej, jest ta, która znajduje się w *Słowniku Pojęć Militarnych i Pokrewnych* Departamentu Obrony USA. Według niej cyberprzestrzeń to: „globalna domena środowiska informacyjnego składająca się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także wbudowane procesory i sterowniki” [4, s. 45].

Również K. Liderman kładzie nacisk na technologię, pisząc, że cyberprzestrzeń to „środowisko (na które składa się ląd, woda, powietrze, kosmos oraz pole elektromagnetyczne) i umieszczone w tym środowisku obiekty posiadające zdolność kształtowania pola elektromagnetycznego i wykrywania jego zmian oraz magazynowania informacji o tych zmianach” [5, s. 22].

Do polskiego porządku prawnego pojęcie cyberprzestrzeni zostało wprowadzone nowelizacją ustawy z dnia 30 sierpnia 2011 roku o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom RP. W literaturze możemy znaleźć szereg zastrzeżeń co do poprawności tej definicji [6, s. 8], [7, s. 20].

Pełna perspektywa cyberprzestrzeni została już zauważona w doktrynie cyberbezpieczeństwa Rzeczypospolitej Polskiej z 2015 roku, gdzie do definicji technologicznej dodano „relacje z użytkownikami” [8, s. 7]. Człowiek jest tak samo odpowiedzialny za dynamikę systemu, jak dane i technologia. Systemy informatyczne nie mogłyby funkcjonować bez człowieka (nawet AI nie zastąpi go całkowicie). Powszechnie znanym stwierdzeniem dotyczącym cyberbezpieczeństwa jest, że użytkownicy są jego najsłabszym ogniwem. Dlatego użytkownicy są często celem bezpośrednich ataków. Ich myśli oraz interakcje z systemami informatycznymi stanowią część cyberprzestrzeni, ponieważ są przejawem aktywności realizowanej w środowisku cyfrowym. To właśnie interakcje międzyludzkie i ludzi z systemami teleinformatycznymi stanowią najczęstszy wektor ataków dywersyjnych, sabotażu i dezinformacji.

Subversion, sabotage and disinformation

In safety sciences, it is essential to distinguish the notions of: subversion, sabotage and disinformation, which are often used interchangeably in the common language.

Subversion is defined as destructive operations conducted in the territory of the state or land occupied by the state conducted in the political, social, economic and military field by the opposite side to lower the defence level, related in particular to the sovereignty, independence and survival of the given state and the quality of life of its society [9]. Contemporary subversion is often non-conventional and covert in nature, aiming at disturbing the state life without a formal declaration of war. Subversion is a notion that covers primarily sabotage (physical) and disinformation (psychological and informational) operations. The remaining subversive operations include provocations, propaganda

Dywersja, sabotaż, dezinformacja

W naukach o bezpieczeństwie kluczowe jest rozróżnienie pojęć: dywersja, sabotaż i dezinformacja, które w języku potocznym często bywają stosowane zamiennie.

Dywersja definiowana jest jako działania destrukcyjne prowadzone na terytorium państwa lub terenie przez niego zajmowanym, realizowane w sferze politycznej, społecznej, gospodarczej i militarnej przez stronę przeciwną w celu osłabienia poziomu obronności, a dotyczące w szczególności suwerenności, niezależności i przetrwania danego państwa oraz jakości życia jego społeczeństwa [9]. Współczesna dywersja często ma charakter niekonwencjonalny i ukryty, zmierzając do zakłócenia życia państwowego bez formalnego wypowiedzenia wojny. Dywersja jest pojęciem obejmującym głównie działania sabotażowe (fizyczne) i dezinformacyjne (psychologiczno-informacyjne). Pozostałe działania dywersyjne, to

operations, psychological operations, terrorism [10, p. 463–469], [11, p. 209–230], broadly understood disruptions of the operation of the state, military or economy.

Sabotage is deliberate non-fulfilment or improper fulfilment of one's duties with an intention to cause disorganisation, losses and damage [12, p. 502]. It is intentional disorganisation by physical destruction of machines, tools or defective fulfilment of duties (disruption of the operation of infrastructure, equipment, resources or processes). Sabotage is focused on causing real losses, i.e. damage, failure, delay. In the digital context (computer sabotage) it consists in destroying, deleting or modifying data of special importance for the defence or the functioning of the bodies of the state.

Disinformation is a process of deliberate misleading by transmitting fake content to achieve political, social, economic or military benefits (e.g. by causing bad decisions, chaos, panic or conflicts). It is a form of psychological subversion that lowers or completely destroying the morale of the society and the trust in state institutions [1, p. 96–104]. P. Dela notes that disinformation is planned and conducted systematically and professionally, always via the mass media, targeting the society, a social group or the public opinion. Its objective is to replace, in the consciousness and, above all, the subconsciousness of the target audience, views considered unfavourable by the disinformation actor with those considered favourable to it. In general, disinformation creates a fake image of reality in the audience [13], [14, p. 52]. Furthermore, it creates information chaos, i.e. an excessive influx of information of little useful value [15, p. 51].

Contemporary subversion operations, both in the physical world and in the digital world, are characterised by the following features:

- flexibility – adaptation of the operating methods to the conditions of fulfilment of tasks, applicable above all to the land infrastructure and the political and military situation.
- mobility – quick movement, abrupt attack and quick retreat from the region (site) of the completed subversive attack,
- autonomy – decentralised command enabling real-time modifications of the plan,
- simplicity – use of small groups and simple equipment and means to achieve spectacular impact,
- variable tactics – avoiding previously used operation schemes and adjusting them to objective or site [16].

m.in. prowokacje, działania propagandowe, akcje psychologiczne, terroryzm [10, s. 463–469], [11, s. 209–230], szeroko rozumiane zakłócenia pracy państwa, armii czy gospodarki.

Sabotaż to umyślne niewypełnianie albo wypełnianie wadliwie swoich obowiązków w zamiarze wywołania dezorganizacji, strat i szkód [12, s. 502]. To zamierzona dezorganizacja, poprzez fizyczne niszczenie maszyn, narzędzi lub niewłaściwe wykonywanie obowiązków (zakłócanie działania infrastruktury, sprzętu, zasobów lub procesów). Sabotaż nastawiony jest na powodowanie realnych strat – uszkodzeń, awarii, opóźnień. W kontekście cyfrowym (sabotaż komputerowy) polega on na niszczeniu, usuwaniu lub zmianie danych o szczególnym znaczeniu dla obronności lub funkcjonowania organów państwa.

Dezinformacja jest procesem celowego wprowadzania w błąd poprzez przekazywanie fałszywych treści w celu osiągnięcia korzyści politycznych, społecznych, gospodarczych lub militarnych (np. przez wywołanie błędnych decyzji, chaosu, paniki lub konfliktów). Stanowi ona formę psychologicznej dywersji, obniżając lub całkowicie niszcząc morale społeczeństwa i zaufanie do instytucji państwowych [1, s. 96–104]. P. Dela zwraca uwagę, że dezinformacja jest planowana i prowadzona w sposób systematyczny, profesjonalny, zawsze za pośrednictwem mass mediów i jest adresowana do społeczeństwa, grupy społecznej, opinii publicznej. Jej celem jest zastąpienie w świadomości, a przede wszystkim podświadomości odbiorcy będącego przedmiotem tych działań, poglądów uznawanych za niekorzystne dla dezinformatora takimi, które uważa on za korzystne dla siebie. Ogólnie rzecz ujmując, dezinformacja tworzy w umysłach odbiorców fałszywy obraz rzeczywistości [13], [14, s. 52]. Dodać do tego należy wytworzenie chaosu informacyjnego – otrzymywania zbyt wielu informacji o małej wartości użytecznej [15, s. 51].

Współczesne działania dywersyjne, zarówno w świecie fizycznym, jak i cyfrowym, charakteryzują się następującymi cechami:

- elastyczność – dostosowanie metod działania do warunków towarzyszących realizacji powierzonych zadań, dotyczących przede wszystkim infrastruktury terenu oraz sytuacji polityczno-militarnej,
- ruchliwość – szybkie przemieszczanie się, gwałtowność ataku i szybkość wycofania z rejonu (obiektu) dokonanego aktu dywersyjnego,
- samodzielność – zdecentralizowane dowodzenie umożliwiające modyfikację planów w czasie rzeczywistym,
- prostota – wykorzystanie niewielkich grup i nieskomplikowanego sprzętu i środków do osiągnięcia spektakularnych skutków,
- zmienność taktyki – unikanie wcześniej stosowanych schematów działania i dostosowywanie ich do celu lub obiektu [16].

Operational model of attacks in cyberspace

As suggested earlier, cyberspace has become an environment that favours subversive operations. In 2015, MITRE Corporation published the resource, of which the purpose is to

Model operacyjny ataków w cyberprzestrzeni

Jak wcześniej zasugerowano, cyberprzestrzeń stała się środowiskiem sprzyjającym prowadzeniu dywersji. W 2015 r. firma MITRE Corporation udostępniła publicznie zasób, którego celem

systematise the operations of cybercriminals and APT groups (advanced persistent threat).

The analysis of subversive operations in cyberspace based on the MITRE ATT&CK Framework [17] divides the attack into 14 tactics, of which many correspond to subversion features, e.g.:

- reconnaissance – consists acquiring information on the target,
- establishing initial access – by means of e.g. spearphishing or gaps in remote services.
- execution and persistence of presence – activation of scripts and establishing access after system restart,
- lateral movement – spreading within the network of the victim,
- impact – the final phase, in which the theft, destruction of resources or disruption of system functions occurs.

The MITRE ATT&CK Framework is a very useful tool to describe and analyse digital forms of subversion, such as: infrastructural sabotage, disinformation, influence operations, interception of applications, websites and communication systems, hybrid operations supporting kinetic operations. The framework enables the identification and organisation of individual stages of operations in cyberspace.

For example, in the process of disinformation conducted in cyberspace, the following stages may be distinguished: definition of the target of disinformation and plan of its fulfilment, preparation of fake information with comments, identification and capture of intermediate objects to extend the impact range, publication of fake information with comments, initiation of the information campaign in social media, connected with duplication of the content placed in intermediate objects, reinforcement of the message by sending e-mails from captured e-mail accounts of persons intended to increase the credibility of the message [18, p. 21–22].

jest systematyzacja sposobów działania cyberprzestępców i grup APT (ang. *advanced persistent threat*).

Analiza działań dywersyjnych w cyberprzestrzeni opierająca się na Frameworku MITRE ATT&CK [17] dzieli atak na 14 taktyk, z których wiele odpowiada cechom dywersji, np.:

- rozpoznanie (ang. *reconnaissance*) – polega na zbieraniu informacji o celu,
- uzyskanie dostępu początkowego (ang. *initial access*) – realizowane poprzez wykorzystanie np. spearphishingu lub luk w usługach zdalnych,
- wykonanie i utrwalenie obecności (ang. *execution, persistence*) – uruchomienie skryptów i zapewnienie sobie dostępu po restarcie systemu,
- ruch boczny (ang. *lateral movement*) – rozprzestrzenianie się wewnątrz sieci ofiary,
- wpływ (ang. *impact*) – finalna faza, w której następuje kradzież, niszczenie zasobów lub zakłócenie funkcji systemowych.

Framework MITRE ATT&CK jest narzędziem bardzo przydatnym do opisu i analizy cyfrowych form dywersji, takich jak: sabotaż infrastruktury, dezinformacja, operacje wpływu, przejęcia aplikacji, stron, systemów komunikacji, działań hybrydowych wspierających operacje kinetyczne. Framework umożliwia identyfikację oraz uporządkowanie poszczególnych etapów działań prowadzonych w cyberprzestrzeni.

Przykładowo, w procesie dezinformacji realizowanej w cyberprzestrzeni można wyróżnić następujące etapy: określenie celu dezinformacji i planu jej przeprowadzenia, przygotowanie fałszywej informacji wraz z komentarzami, zidentyfikowanie i przejęcie obiektu użytego do dezinformacji, zidentyfikowanie i przejęcie obiektów pośrednich dla zwiększenia zasięgu oddziaływania, publikacja fałszywej informacji wraz z komentarzami, rozpoczęcie kampanii informacyjnej w portalach społecznościowych związanej z powielaniem treści umieszczonych w obiektach pośrednich, wzmocnienie przekazu poprzez rozsyłanie maili z przejętych kont pocztowych osób, które mają uwiarygodnić przekaz [18, s. 21–22].



Figure 1. Stages of disinformation in cyberspace

Rycina 1. Etapy dezinformacji realizowanej w cyberprzestrzeni

Source/Źródło: P. Dela, R. Janczewski, J. Syta, *Dezinformacja i propaganda w sektorze bankowym* [18].

Case studies

Attacks on the Ukrainian energy system (2015–2022)

The attacks on the Ukrainian energy system in 2015–2022 are a classic example of cybersubversion aimed at critical infrastructure. In December 2015, the power was shut down for several hours for 230,000 users in Ukraine, using the BlackEnergy 3 malware. It was an upgraded version of BlackEnergy of 2007, designed for DDoS attacks, which began to be used by APT groups as an advanced tool used in operations against states [19]. The attack was started 8 months before the blackout, when an employee of one of energy grid operators opened an Excel attachment with a BlackEnergy version that scanned IT and OT networks to collect data on network topology, hardware and software. It moved laterally, creating backdoors and installing additional tools (e.g. KillDisk). In the moment of the actual attack, the attackers operated the industrial interface manually (the operators saw the cursor moving on its own, when the attackers assumed control over the SCADA system), which is extremely rare for cyberattacks. KillDisk was erasing disk contents, thus destroying systems and impeding the recovery. The telephone support centre of the energy grid operators were overloaded (DoS attack) to obstruct reporting failures and delay the response.

Studia przypadków

Ataki na ukraiński system energetyczny (2015–2022)

Ataki na ukraiński system energetyczny w latach 2015–2022 stanowią klasyczny przykład cyberdywersji wymierzonej w infrastrukturę krytyczną. W grudniu 2015 roku nastąpiło kilkugodzinne wyłączenie prądu dla 230 000 odbiorców w Ukrainie przy użyciu oprogramowania malware BlackEnergy 3. Było ono udoskonaloną wersją BlackEnergy z 2007 r., przeznaczonego do ataków DDoS, który z czasem zaczął być wykorzystywany przez grupy APT jako zaawansowane narzędzie stosowane w operacjach przeciwko państwom [19]. Atak rozpoczął się osiem miesięcy przed blackoutem, gdy pracownik jednego z operatorów otworzył załącznik Excel zawierający wariant BlackEnergy, który skanował sieci IT i OT, zbierając dane o topologii sieci, urządzeniach, oprogramowaniu. Wykonywał ruch boczny, tworzył backdoory i instalował dodatkowe narzędzia (m.in. KillDisk). W momencie właściwego ataku, atakujący manualnie operowali interfejsem przemysłowym (operatorzy widzieli samoczynnie przesuwający się kursor, gdy napastnicy przejmowali kontrolę nad systemem SCADA), co jest wyjątkowo rzadkie w cyberatakach. KillDisk wymazywał zawartość dysków, niszcząc systemy i utrudniając przywrócenie ich działania. Telefoniczne centra obsługi operatorów energii zostały przeciążone (atak DoS), aby utrudnić zgłaszanie awarii i opóźnić reakcję.

One year later, in December 2016, the energy grid of Kyiv was attacked (the blackout covered approx. 1/5 of Kyiv for approx. 1 hour) using the Industroyer modular software [20]. It was the first malware dedicated for attacks on energy grids. It featured modules supporting industrial protocols. As opposed to BlackEnergy, Industroyer required no human interaction during the sabotage [21].

In April 2022, Ukrainian energy grids were to be destabilised using the Industroyer2 malware [22]. The attempt was prevented by the collaboration of CERT-UA and ESET. Industroyer2 is not based on hardware vulnerabilities, it does not attack any specific manufacturer, but it uses the standard industrial protocol of IEC-60870-5-104, commonly used in European energy grids. Using it, it may assume control over the grid, including the commands to open/close switches. The attackers had been in the network of energy grid operators at least since February 2022. In March, they prepared the environment, compiled the file with coded parameters and setup adjusted to a specific network of the victim (which proves full knowledge of its network) and tools for destroying systems (Windows, Linux, Solaris) of the victim, impeding the response and eliminating the tracks [23].

These operations were connected with information operations intended to cause panic and accuse the authorities of incapacity. The attacks on the Ukrainian energy system in 2015–2022 may be described using the cybernetic model. They were operations to control social and technical systems, including interference with infrastructure (energy), interference with information (announcements, chaos), interference with social perception (fear, uncertainty), response of the authorities and society, and adaptation to the conditions of the attackers.

Rok później, w grudniu 2016 r. przeprowadzono atak na sieć energetyczną w Kijowie (blackout objął ok. jedną piątą Kijowa przez ok. godzinę) z wykorzystaniem modułowego oprogramowania Industroyer [20]. Był to pierwszy malware przeznaczony do ataków na sieci energetyczne. Posiadał moduły obsługujące protokoły przemysłowe. W odróżnieniu od BlackEnergy, Industroyer nie potrzebował interakcji człowieka przy wykonaniu sabotażu [21].

W kwietniu 2022 r. miało dojść do destabilizacji sieci energetycznych Ukrainy za pomocą malware Industroyer2 [22]. Próba została udaremniona dzięki współpracy CERT-UA i ESET. Industroyer2 nie bazuje na podatnościach sprzętowych, nie atakuje konkretnego producenta, lecz wykorzystuje standardowy protokół przemysłowy IEC-60870-5-104, powszechnie stosowany w europejskich sieciach energetycznych. Z jego użyciem może przejąć kontrolę nad siecią, w tym wydawać polecenia otwierania/zamykania wyłączników. Atakujący byli w sieci operatorów energetycznych co najmniej od lutego 2022 roku. W marcu przygotowali środowisko, skompilowali plik z zakodowanymi parametrami i konfiguracją dopasowaną do konkretnej sieci ofiary (co świadczy o pełnej wiedzy na temat jej sieci). Dysponowali narzędziami do niszczenia systemów (Windows, Linux, Solaris) ofiary, utrudnienia reakcji, zacierania śladów [23].

Działania te były połączone z operacjami informacyjnymi mającymi na celu wywołanie paniki i oskarżenie władz o nieudolność. Ataki na ukraiński system energetyczny z lat 2015–2022 można opisać w modelu cybernetycznym. Były one bowiem operacjami sterowania systemami społecznym i technicznym, obejmującymi ingerencję w infrastrukturę (energia), ingerencję w informację (komunikaty, chaos), ingerencję w percepcję społeczną (strach, niepewność), reakcje władz i społeczeństwa oraz adaptację do warunków atakujących.

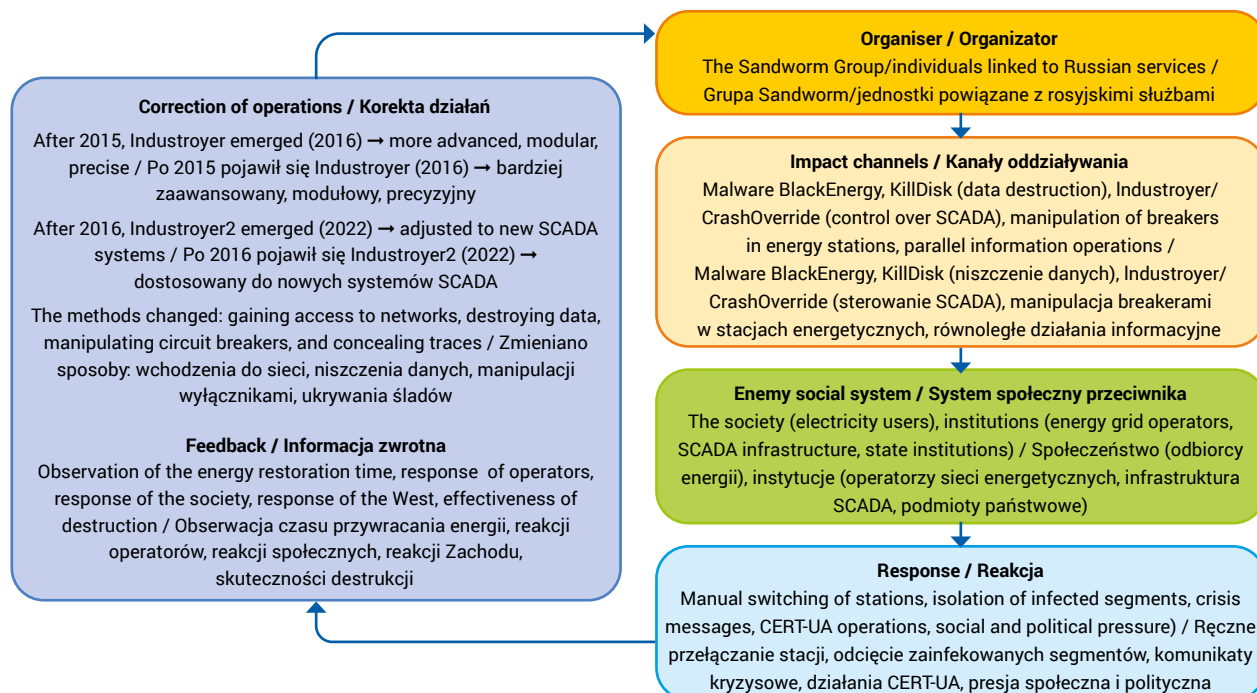


Figure 2. The cybernetic model of the attacks on the Ukrainian energy system in 2015–2022

Rycina 2. Model cybernetyczny ataków na ukraiński system energetyczny z lat 2015–2022

Source: Own elaboration.

Źródło: Opracowanie własne.

In all of these cases, the purpose of the attackers was sabotage (blackout), combined with disinformation (narrative of panic, incapacity of authorities), meant to disrupt the functioning of the state (subversion). The operations were attributed to the Sandworm Group [24] linked to GRU (Russian *Glavnoye Razvedyvatel'noye Upravleniye* – Main Intelligence Directorate, the Russian military intelligence service, responsible, i.a., for special operations and cyberoperations beyond national borders).

The WannaCry ransomware campaign (2017)

In mid-May 2017, this attack infected almost 300,000 devices, operating globally in more than 150 countries. It attacked hospitals (NHS), logistics companies, corporations and public institutions. It used the EternalBlue gap¹ in SMBv1 (an exploit developed at the National Security Agency) and its purpose was not only financial gains (the ransom paid was not collected from the three bitcoin addresses connected with the attack until November 2021), but above all to cause chaos on an international scale.

WannaCry [25] gained access to systems by the EternalBlue exploit, which enabled remote use of the code without authentication. Next, it started the dropper, which extracted ransomware components and the worm module, created and started the mssecsvc2.0 service designed for executing and further spreading of the malware (as system service). It modified ACL to grant full rights to all users and hide its files and directories. It deleted snapshots and recovery points. It scanned disks for files to encrypt (Office, PDF, multimedia, keys, certificates) and the local network segment in search of hosts with open SMB. After finding such a host, it automatically moved to it, copied its own files and attempted to start a copy of malware. Finally, it encrypted data using AES and RSA) and left a ransom demand of approx. USD 300–600 in Bitcoin. For communication with victims, the TOR was used with a proprietary encryption mechanism. The global WannaCry epidemic was stopped by Marcus Hutchins [26, p. 179–182], who registered the domain used by the *kill switch* mechanism, thus activating its operation. After stopping the first attack wave, mutations started emerging without the *kill switch*, with other *kill switch* domains, with errors corrected, with other environmental testing methods, with different encryption keys. The entire operation followed the phases of subversive attacks: approach to the object, entrance to the site area, damage or destruction, and retreat from the place of the subversive act.

¹ EternalBlue was also used by the Sandworm Group in the NotPetya attack initiated on 27 June 2017.

We wszystkich tych przypadkach celem atakujących było przeprowadzenie sabotażu (wyłączenie prądu), powiązane z dezinformacją (narracja o panice, nieudolności władz), co miało doprowadzić do zakłócenia funkcjonowania państwa (dywersja). Działania zostały przypisane grupie Sandworm [24] związanej z GRU (ros. *Glavnoye Razvedyvatel'noye Upravleniye* – Głównemu Zarządowi Wywiadowczemu, rosyjskiej wojskowej służbie wywiadowczej, odpowiadającej m.in. za operacje specjalne i cyberoperacje poza granicami kraju).

Kampania ransomware WannaCry (2017)

Atak ten zainfekował w połowie maja 2017 r. prawie 300 tys. urządzeń, działając globalnie w ponad 150 krajach. Uderzył w szpitale (NHS), firmy logistyczne, korporacje i instytucje publiczne. Wykorzystano w nim lukę EternalBlue¹ w SMBv1 (eksploita opracowywana w National Security Agency), a celem była nie tylko korzyść finansowa (z powiązanych z atakiem trzech adresów bitcoin do listopada 2021 r. nie pobrano wpłaconych okupów), ale przede wszystkim wywołanie chaosu na skalę międzynarodową.

WannaCry [25] zdobywał dostęp do systemów poprzez exploit EternalBlue, umożliwiając zdalne wykonanie kodu bez uwierzytelnienia. Następnie uruchamiał program droppera, który wypakowywał komponenty ransomware oraz moduł robaka, tworzył i uruchamiał usługę mssecsvc2.0 przystosowaną do wykonywania i dalszego rozprzestrzeniania malware (jako usługa systemowa). Modyfikował ACL, aby nadać pełne prawa wszystkim użytkownikom oraz ukrywać swoje pliki i katalogi. Usuwał snapshoty i punkty przywracania. Skanował dyski w poszukiwaniu plików do zaszyfrowania (Office, PDF, multimedia, klucze, certyfikaty) oraz segment sieci lokalnej w poszukiwaniu hostów z otwartym SMB. Po znalezieniu takiego hosta automatycznie na niego przechodził, kopiował własne pliki i próbował uruchomić kopię malware. W końcu szyfrował dane (używał algorytmów AES i RSA) i pozostawiał żądanie okupu 300–600 USD w Bitcoinach. Do komunikacji z ofiarami wykorzystywał TOR z własnym mechanizmem kryptograficznym. Globalną epidemię WannaCry zatrzymał Marcus Hutchins [26, s. 179–182], który zarejestrował domenę wykorzystywaną przez mechanizm *kill switch*, aktywując tym samym jego działanie. Po zatrzymaniu pierwszej fali ataku zaczęły pojawiać się mutacje bez *kill switcha*, z innymi domenami *kill switch*, z poprawionymi błędami, z innymi metodami testu środowiska, z innymi kluczami szyfrującymi. Cała operacja była zbieżna z fazami ataków dywersyjnych – podejściem do obiektu działania, wejściem na teren obiektu, dokonaniem uszkodzeń lub niszczeń oraz odejściem z miejsca aktu dywersji.

¹ EternalBlue zostało wykorzystane także przez grupę Sandworm w ataku NotPetya rozpoczętym 27 czerwca 2017 roku.

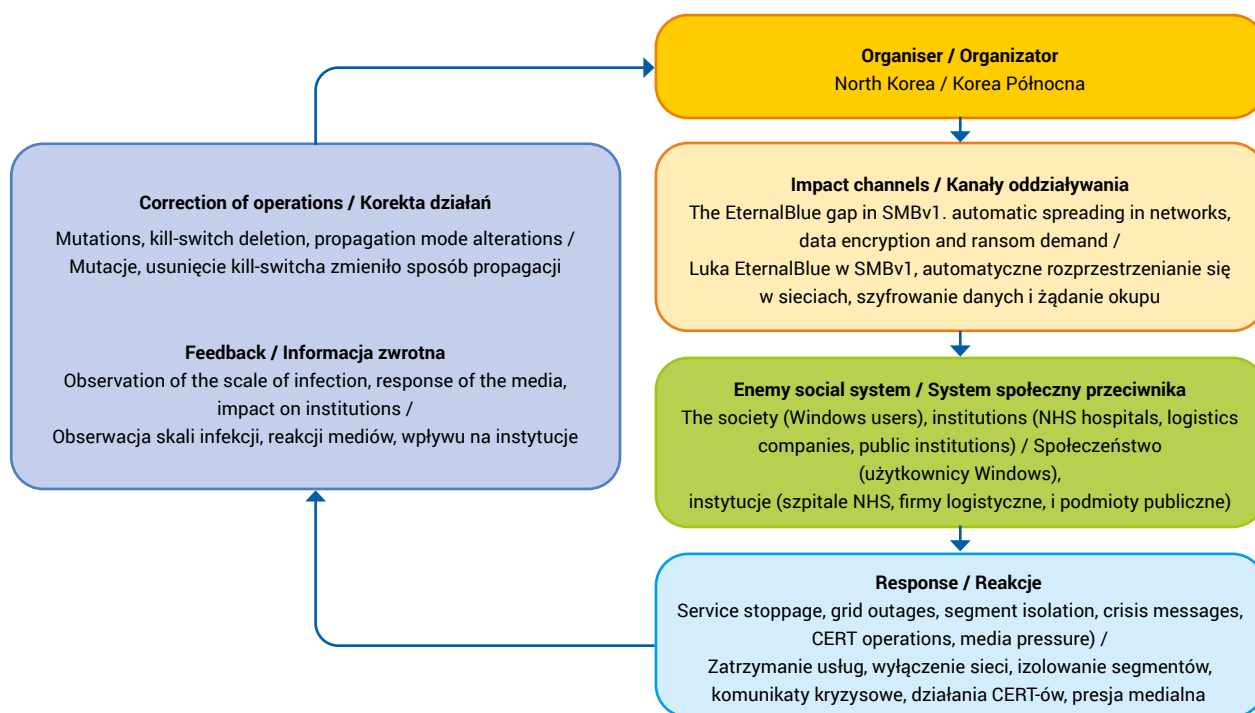


Figure 3. Cybernetic model of the WannaCry attack
Rycina 3. Model cybernetyczny ataku WannaCry

Source: Own elaboration.

Źródło: Opracowanie własne.

The purpose of this subversive attack was to destabilise the social life, test the opportunities to assume control of a large number of computers. The responsibility for the WannaCry attack is attributed to the North Korean Lazarus Group [27], subordinate to the Reconnaissance General Bureau of the General Staff in charge of secret operations.

Capture of the BadeSaba app (2026)

BadeSaba is one of the most popular Iranian religious apps – calendar and prayer schedule. It is used by more than 5 million religious persons, including state and military personnel. In parallel with the airstrikes of 28 February 2026 by the United States of America and Israel, the app ceased to send standard prayer reminders and started publishing mass psychological messages instead, e.g. “The aid is on the way”, “Put your weapons down”, “The judgement time has come”, “Join the liberation army to liberate Iran”.

Celem działania tego ataku dywersyjnego była destabilizacja systemu społecznego, przetestowanie możliwości przejęcia kontroli nad dużą liczbą komputerów. Odpowiedzialność za atak WannaCry przypisuje się północnokoreańskiej grupie Lazarus [27] podlegającej Biuru Wywiadu Generalnego Departamentu Sztabu Generalnego, zarządzającego tajnymi operacjami.

Przejęcie aplikacji BadeSaba (2026)

BadeSaba to jedna z najpopularniejszych irańskich aplikacji religijnych – kalendarz i harmonogram modlitw. Wykorzystywana jest przez ponad 5 mln osób religijnych, w tym pracowników państwowych, wojskowych. Równoległe z nalotami prowadzonymi 28 lutego 2026 r. przez USA i Izrael aplikacja przestała wysyłać standardowe przypomnienia o modlitwach i zamiast tego zaczęła publikować masowe komunikaty psychologiczne, m.in. „Pomoc jest w drodze”, „Odłóżcie broń”, „Nadszedł czas sądu”, „Dołączcie do armii wyzwoleniczej, aby uwolnić Iran”.

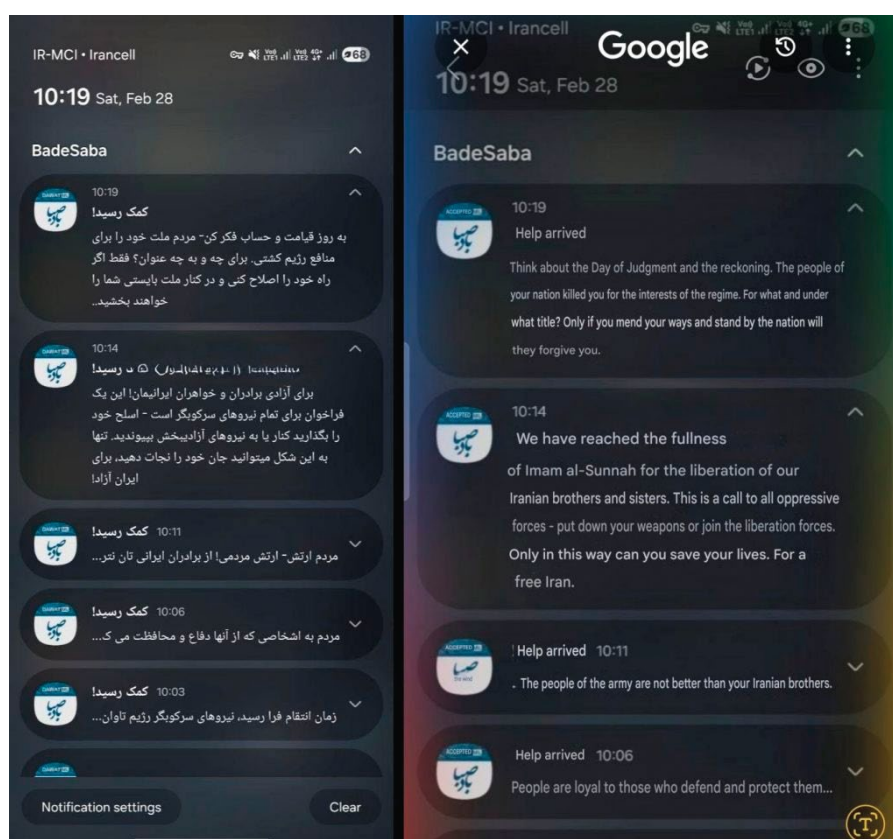


Figure 4. Messages in the BadeSaba app and their Google translations
Rycina 4. Komunikaty w aplikacji BadeSaba i ich tłumaczenie Google

Source: <https://hackread.com/popular-iranian-app-badesaba-hacked-alerts/> [access: 20.04.2026].

Źródło: <https://hackread.com/popular-iranian-app-badesaba-hacked-alerts/> [dostęp: 20.04.2026].

The messages directly called the security forces and soldiers to put down their weapons, promised amnesty and threatened with “reckoning of the repressive Iranian forces”. The analysis of this disinformation shows that the attackers had to:

- know the backend structure of the BadeSaba system, the notification system (API keys, FCM/APNs), server dependencies and linked domains,
- identify the admin accounts, which they compromised later on,
- prepare management servers (C2), tools, accounts used at the later stage,
- prepare exploits and messaging panel access methods,
- capture keys (API/login) to the notification system or app backend,
- prepare messages for automatic delivery at specific time in advance,
- become embedded in the app backend, probably weeks before the activation,
- obtain administration rights to enable sending notifications to millions of recipients,
- restrict the user capability to verify information (during the attack, the throughput dropped to 4% of the nominal value).

Wiadomości wprost wzywały siły bezpieczeństwa i żołnierzy do złożenia broni, obiecywały amnestię, a także straszyły „rozliczeniem represyjnych sił irańskich”. Analiza tej dezinformacji wskazuje, że atakujący musieli:

- znać strukturę zaplecza (backendu) systemu BadeSaba, system powiadomień (API keys, FCM/APNs), zależności serwerowe oraz powiązane domeny,
- rozpoznać konta administratorów, które później przejęli,
- przygotować serwery zarządzające (C2), narzędzia, konta użyte w późniejszej fazie,
- opracować exploity lub mechanizmy umożliwiające uzyskanie dostępu do panelu wysyłającego komunikaty,
- przejąć klucze (API/logowania) do systemu powiadomień lub backendu aplikacji,
- przygotować wcześniej komunikaty do automatycznej wysyłki o określonej porze,
- osadzić się w backendzie aplikacji, prawdopodobnie na tygodnie przed aktywacją,
- uzyskać prawa administracyjne pozwalające na wysyłanie powiadomień do milionów odbiorców,
- ograniczyć zdolność użytkowników do weryfikacji informacji (przy ataku nastąpił spadek przepustowości do 4% normalnej).

The attack was a subversive psychological operation in cyberspace, because:

- Iranian state websites (IRNA, ISNA) were modified or disabled;
- mass notifications were sent, urging the soldiers to capitulate, promising amnesty, threatening with judgement for “regime” forces;
- Iran experienced the intended drop of communication to several percent;
- the combination of messages with explosions was to cause panic, chaos and potential collapse of the morale of the security forces.

It should be mentioned that Iran used disinformation, often AI-powered, e.g. on the attack on the USS Abraham Lincoln in the Arabian Sea [29].

Conclusion

Cyberspace has become the preferred environment for subversive operations due to the low operating cost and perpetrator identification difficulty. Bots, fake accounts, intermediate servers, and spoofing of trusted sources are often used. Like in classic subversion, operating “from concealment” and impeding identification of the attacker are essential.

Subversion is no longer focused on the broadly interpreted military only, but threatens social and economic stability of the state directly. Disinformation, manipulation of narratives, seeding panic or distrust by creating fake pages, documents, leaks, memes is meant to influence the emotions and decisions of the audience. In the context of case studies presented, a cyberattack is only a technical incident, while cybernetic operations in subversion is a control process addressing the information, social or technical system. Cybernetic operations include influence operations, manipulation of narratives, control of social behaviours, control of information exchange. The purpose does not have to be direct destruction of infrastructure, it suffices to disrupt the functioning of systems, not only ITC systems.

In the field of fire safety, the operation of fire detection and signalling systems may lead to delayed fire detection or false alarms, remote damage to firefighting automation and control systems or disorganisation of information and operation systems.

Effective counteraction of subversion in cyberspace requires operations in many areas. It is necessary to start from education and building hazard awareness (critical thinking and fake news recognition skills). Continuous monitoring of cyberhazards and quick incident response are required (e.g. by national or sectoral CERT teams). Quick data exchange on hazards within international and national structures is essential. The training of the State Fire Service personnel on recognising disinformation and running crisis communication, as well as resistance monitoring and tests (penetration tests, hybrid training including digital and physical attacks), are components that enable resisting subversive attacks.

Enemy entities do not care that international law is fully applicable also in cyberspace. The purpose should be to introduce

Atak był dywersyjną operacją psychologiczną w cyberprzestrzeni, gdyż:

- irańskie portale państwowe (IRNA, ISNA) zostały zmienione lub wyłączone;
- wysłano masowe powiadomienia, wzywające żołnierzy do kapitulacji, obiecujące amnestię, grożące osądzeniem „reżimowych” sił;
- Iran doświadczył celowo wywołanego spadku łączności do kilku procent;
- połączenie wysłanych wiadomości z eksplozjami miało wywołać panikę, chaos i potencjalny upadek morale sił bezpieczeństwa.

Warto wspomnieć, że również wspierający Iran posługiwali się dezinformacją, często wspomaganą przez AI, np. o ataku na pancernik USS Abraham Lincoln na Morzu Arabskim [29].

Zakończenie

Cyberprzestrzeń stała się preferowanym środowiskiem prowadzenia działań dywersyjnych ze względu na niski koszt operacji i trudność w identyfikacji sprawcy. Często wykorzystywane są boty, fałszywe konta, serwery pośredniczące, podszywanie się pod legalne źródła. Podobnie jak w klasycznej dywersji kluczowe jest działanie „z ukrycia” i utrudnianie identyfikacji atakującego.

Dywersja nie jest już ukierunkowana tylko na szeroko interpretowaną domenę wojskową, lecz bezpośrednio zagraża stabilności społecznej i gospodarczej państwa. Dezinformacja, manipulowanie narracjami, sianie paniki lub nieufności poprzez tworzenie fałszywych stron, dokumentów, przecieków, memów ma wpływać na emocje i decyzje odbiorców. W kontekście przedstawionych studiów przypadku cyberatak to tylko techniczny incydent, natomiast działania cybernetyczne w dywersji to proces sterowania systemem informacyjnym, społecznym lub technicznym. Działania cybernetyczne to m.in. operacje wpływu, manipulacja narracjami, sterowanie zachowaniami społecznymi, kontrola przepływu informacji. Celem nie musi być bezpośrednie zniszczenie infrastruktury – wystarczy zaburzenie funkcjonowania systemów, nie tylko teleinformatycznych.

W obszarze bezpieczeństwa pożarowego zakłócenie działania systemów wykrywania i sygnalizacji pożaru może prowadzić do opóźnionego wykrycia pożaru lub fałszywych alarmów, zdalnego uszkodzenia automatyki gaśniczej i systemów sterujących lub dezorganizacji systemów informacyjnych i operacyjnych.

Skuteczna walka z dywersją w cyberprzestrzeni wymaga działań w wielu obszarach. Rozpocząć należy od edukacji i budowania świadomości zagrożeń (umiejętności krytycznego myślenia i rozpoznawania fake newsów). Prowadzony musi być stały monitoring cyberzagrożeń i zapewnione szybkie reagowanie na incydenty (np. przez krajowe lub sektorowe zespoły CERT). Niezbędna jest szybka wymiana danych o zagrożeniach w ramach struktur międzynarodowych i krajowych. Szkolenia personelu PSP w zakresie rozpoznawania dezinformacji i realizacji komunikacji kryzysowej oraz monitorowanie i testy odporności (testy penetracyjne, ćwiczenia hybrydowe obejmujące ataki cyfrowe i fizyczne) są elementami zapewniającymi możliwości odparcia ataków dywersyjnych.

the compliance mechanisms included in the Tallinn Manual [3], according to which the cyberattack may be considered as use of force, if its impact is comparable to a traditional kinetic attack (e.g. infrastructural damage, physical damage, disruption of primary state security systems). States, in turn, cannot use cyber-operations to force political changes, disrupt elections, influence state politics or force other countries to act in their own internal affairs. The state shall be responsible for this type of operations, conducted by state bodies, entities acting on its behalf, groups under its direction or control, as well as operations that the state failed to prevent despite its capabilities.

List of abbreviations

ACL	(access control list) – set of rules or configurations specifying which network packages may pass the network device and which are rejected. Using ACL lists, network admins may enforce security rules, restrict unauthorised access and mitigate potential security hazards, while defining the permissible traffic.
API	(application programming interface) – software interface of the application.
APN	(access point name) – name of the access point.
APT	(advanced persistent threat) – criminal groups that operate for a long time and use advanced tools, often supported by a state or acting in its interest.
Dropper	type of malware designed to install other malware. It acts as a agent carrying an other harmful executable file.
FCM	(Firebase Cloud Messaging Apple Push Notification) – multi-platform solution for sending messages.
SCADA	(Supervisory Control and Data Acquisition) – IT system supervising the course of the technological or production process.
SMB	(server message block) – network communication protocol used to share files, printers and other resources in local network.
Snapshots	data enabling restoring the computer to an earlier saved condition.

AI Use Statement

The author declares that no artificial intelligence tools were used in the preparation of this article to generate text, analyses, graphics, or other elements of the publication.

The authors take full responsibility for the content of the publication, including the scientific accuracy, interpretation of results, and the final editing of the manuscript.

According to the journal's editorial policy, the uncritical copying of AI-generated content and its inclusion in a publication without proper critical analysis, verification, and revision by the author is prohibited.

Wrogie podmioty nie zważają na to, że prawo międzynarodowe obowiązuje w pełni również w cyberprzestrzeni. Należy dążyć do wprowadzenia mechanizmów respektowania zasad zapisanych w Poradniku Tallińskim [3] według których cyberatak może zostać uznany za użycie siły, jeśli jego skutki są porównywalne do tradycyjnego ataku kinetycznego (np. uszkodzenie infrastruktury, szkody fizyczne, zakłócenie podstawowych systemów państwa). Z kolei państwa nie mogą cyberoperacjami wymuszać zmiany polityki, zakłócać wyborów, wpływać na politykę innych krajów czy zmuszać je do działań w swoich sprawach wewnętrznych. Państwo ponosi odpowiedzialność za działania tego rodzaju prowadzone przez jego organy, podmioty działające z jego upoważnienia oraz grupy przez nie kierowane lub kontrolowane, a także za działania, którym nie zapobiegło mimo posiadanych możliwości.

Wykaz skrótów

ACL	zestaw reguł lub konfiguracji określających, które pakiety sieciowe mogą przepływać przez urządzenie sieciowe, a które są odrzucane. Korzystając z list ACL, administratorzy sieci mogą egzekwować zasady bezpieczeństwa, ograniczać nieautoryzowany dostęp i łagodzić potencjalne zagrożenia bezpieczeństwa, definiując, jaki ruch jest dozwolony.
API	interfejs programowania aplikacji.
APN	nazwa punktu dostępowego.
APT	grupy przestępcze, działające długotrwale i korzystające z zaawansowanych narzędzi, często wspierane przez państwo lub działające w jego interesie.
Dropper	rodzaj złośliwego oprogramowania odpowiedzialnego za instalację innego złośliwego oprogramowania. Działa jako nośnik zawierający w sobie inny szkodliwy plik wykonywalny.
FCM	wieloplatformowe rozwiązanie do przesyłania wiadomości.
SCADA	system informatyczny nadzorujący przebieg procesu technologicznego lub produkcyjnego.
SMB	sieciowy protokół komunikacyjny służący do udostępniania plików, drukarek oraz innych zasobów w sieci lokalnej.
Snapshots	dane umożliwiające przywrócenie komputera do zapamiętanego wcześniej stanu.

Oświadczenie dotyczące wykorzystania AI

Autor oświadcza, że w procesie przygotowania niniejszego artykułu nie korzystano z narzędzi opartych na sztucznej inteligencji do generowania treści, analiz, grafik ani innych elementów publikacji.

Autor ponosi pełną odpowiedzialność za treść publikacji, w tym za poprawność merytoryczną, interpretację wyników oraz redakcję tekstu.

Zgodnie z polityką redakcyjną czasopisma zabronione jest bezrefleksyjne kopiowanie treści wygenerowanych przez narzędzia AI oraz pozostawianie ich w publikacji bez krytycznej analizy, weryfikacji i redakcji przez autora.

Literature / Literatura

- [1] Dela P., *Założenia działań w cyberprzestrzeni*, PWN, Warszawa 2022.
- [2] Department of Defense Strategy for Operating in Cyberspace, 2011, <https://csrc.nist.gov/cssrc/media/projects/ispab/documents/dod-strategy-for-operating-in-cyberspace.pdf> [dostęp: 20.04.2026].
- [3] Tallinn Manual 2.0, Zasada suwerenności (Sovereignty), https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_-_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press_2017_.pdf [dostęp: 20.04.2026].
- [4] DoD Dictionary of Military and Associated Terms, The Joint Staff, Washington DC 2025.
- [5] Liderman K., *Wprowadzenie do cyberbezpieczeństwa. Podstawowe pojęcia*, Wyd. ECSC 2025.
- [6] Nowak A., *Cyberprzestrzeń jako nowa jakość zagrożeń*, „Zeszyty Naukowe AON” 2013, 3(92), 5–46.
- [7] Liderman K., Książkowski A., *Cyberbezpieczeństwo łańcuchów dostaw*, „Cybersecurity&Cybercime” 2025, 2(8), 9–27.
- [8] Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej, Warszawa 2015.
- [9] Wiśniewski B., *Uwarunkowania badań dywersji w naukach o bezpieczeństwie*, I Warsztaty „Podstawowe problemy przeciwstawiania się dywersji”, Akademia WSB, Dąbrowa Górnicza 2025.
- [10] Zubrzycki W., *Tak zwany terroryzm*, Wyd. WSPol, Szczytно 2017.
- [11] Ścibiorek Z., Wiśniewski B., Kuc R., Dawidczyk A. (red.), *Bezpieczeństwo wewnętrzne. Podręcznik akademicki*, Wyd. Adam Marszałek, Toruń 2017.
- [12] Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych z almanachem*, PWN, Warszawa 2007.
- [13] Dela P., *Wybrane problemy współczesnej dezinformacji*, XVII Ogólnopolska Konferencja Naukowa „Bezpieczna przyszłość cyfrowa – instytucje, strategie, technologie, ludzie”, Akademia Nauk Stosowanych WSGE im. A. De Gasperi w Józefowie, Józefów 2025.
- [14] Aleksandrowicz T., *Zagrożenia dla bezpieczeństwa państwa w ujęciu systemowym. Budowanie zdolności defensywnych i osensywnych w infosferze*, Difin, Warszawa 2021.
- [15] Pokruszyński W., *Współczesne bezpieczeństwo narodowe*, Wyd. WSGE, Józefów 2009.
- [16] Wiśniewski B., *Natura współczesnej dywersji*, I Warsztaty „Podstawowe problemy przeciwstawiania się dywersji”, Akademii WSB, Dąbrowa Górnicza 2025.
- [17] <https://attack.mitre.org/> [dostęp: 20.04.2026].
- [18] Dela P., Janczewski R., Syta J., *Dezinformacja i propaganda w sektorze bankowym*, <https://pabwib.pl/produkt/dezinformacja-i-propaganda-w-sektorze-bankowym/> 2022, [dostęp: 20.04.2026].
- [19] <https://attack.mitre.org/software/S0089/> [dostęp: 20.04.2026].
- [20] <https://attack.mitre.org/software/S0604/> [dostęp: 20.04.2026].
- [21] <https://attack.mitre.org/campaigns/C0025/> [dostęp: 20.04.2026].
- [22] <https://attack.mitre.org/software/S1072/> [dostęp: 20.04.2026].
- [23] <https://attack.mitre.org/campaigns/C0034/> [dostęp: 20.04.2026].
- [24] <https://attack.mitre.org/groups/G0034/> [dostęp: 20.04.2026].
- [25] <https://attack.mitre.org/software/S0366/> [dostęp: 20.04.2026].
- [26] Greenberg A., Sandworm. *Nowa era cyberwojny i polowanie na najbardziej niebezpiecznych hakerów Kremla*, Warszawa 2021.
- [27] <https://attack.mitre.org/groups/G0032/> [dostęp: 20.04.2026].
- [28] <https://hackread.com/popular-iranian-app-badesaba-hacked-alerts/> [dostęp: 20.04.2026].
- [29] Walia G., *US sinks Iranian warship and claims Tehran missiles did not even touch USS Abraham Lincoln*. *US Central Command statement and USS Abraham Lincoln current status explained*, <https://economictimes.indiatimes.com/news/international/us/us-sinks-iranian-warship-and-claims-tehran-missiles-did-not-even-touch-uss-abraham-lincoln-us-central-command-statement-and-uss-abraham-lincoln-current-status-explained-jamaran-class-corvette-at-a-chah-bahar-pier-irans-islamic-revolutionary-guard-corps/articleshow/128920451.cms> [dostęp: 20.04.2026].

JERZY KOSIŃSKI, D.SC. – associate professor of the Naval Academy in Gdynia. Since 2020, director of the Maritime Security Centre of the Naval Academy in Gdynia. Since 2018, served in the police, dealing with cybercrime, digital evidence, online open-source intelligence and online copyright infringements. Served as vice-president for studies at the Police Academy in Szczytно. Organiser of cyclic international conferences “Techniczne aspekty przestępczości teleinformatycznej” (Technical Aspects of ITC crime), continued as “Przestępczość teleinformatyczna XXI” (ITC crime XXI). Author of many publications (e.g. monograph “Paradygmaty cyberprzestępczości” (Paradigms of

DR HAB. JERZY KOSIŃSKI – profesor nadzwyczajny Akademii Marynarki Wojennej w Gdyni. Od 2020 r. dyrektor Morskiego Centrum Bezpieczeństwa AMW. Do 2018 r. pełnił służbę w policji, w której zajmował się cyberprzestępczością, dowodami cyfrowymi, białym wywiadem internetowym i naruszeniami własności intelektualnej w Internecie. Pełnił funkcję prorektora ds. studiów Wyższej Szkoły Policji w Szczytynie. Organizator cyklicznych konferencji międzynarodowych „Techniczne aspekty przestępczości teleinformatycznej”, kontynuowanych pod nazwą „Przestępczość teleinformatyczna XXI”. Autor wielu publikacji (m.in. monografii „Paradygmaty cyberprzestępczości”) i wystą-

cybercrime) and conference lectures in his scientific speciality. Court expert on computer crime and payment cards listed by the District Court in Olsztyn. Conducted training on cybercrime for police services of other countries (e.g. Armenia, China, Moldova).

pień na konferencjach z zakresu swojej specjalności naukowej. Biegły sądowy z zakresu przestępczości komputerowej i kart płatniczych z listy Sądu Okręgowego w Olsztynie. Prowadził także szkolenia z zakresu cyberprzestępczości dla służb policyjnych innych krajów (m.in. Armenia, Chiny, Mołdawia).

Sławomir Paszek

Department of Emergency Medicine of the Medical University of Warsaw / Zakład Medycyny Ratunkowej Warszawskiego Uniwersytetu Medycznego

Zofia Czaplińska-Paszek

Department of Anesthesiology and Intensive Care of the Provincial Hospital in Skierniewice / Oddział Anestezjologii i Intensywnej Terapii Wojewódzkiego Szpitala Zespołowego w Skierniewicach

Corresponding author / Autor korespondencyjny: slawomir.paszek@wum.edu.pl

Using the Kendrick Extrication Device in the National Rescue and Firefighting System

Stosowanie kamizelki Kendricka w krajowym systemie ratowniczo-gaśniczym

ABSTRACT

Purpose: The aim of this study was to assess the frequency of Kendrick extrication device (KED) use among rescuers and to analyse the current scientific evidence regarding its effectiveness and safety. The study was motivated by differences observed in recent years in the qualified first aid training programmes for State Fire Service (PSP) and Volunteer Fire Service (OSP) firefighters with regard to the use of this device.

Project and methods: The study was conducted between July 2022 and March 2026 among 210 firefighters, using a diagnostic survey with an original questionnaire distributed via Google Forms. The survey was addressed to firefighters serving in both professional and volunteer fire protection units. The questionnaire was disseminated through social media platforms and professional groups bringing together individuals involved in fire protection services. Responses concerning the frequency of Kendrick Extrication Device use, equipment availability, and subjective assessment of its usefulness in rescue operations were analysed. In addition, a review of the current scientific literature on the effectiveness, safety, and potential complications of the Kendrick extrication device in prehospital medicine was conducted using publications available in PubMed, Scopus, and Google Scholar.

Results: More than half of the surveyed rescuers reported not having used the Kendrick Extrication Device in practice while providing qualified first aid. A substantial proportion of respondents also indicated that this device was not available in the equipment of their rescue units. The most frequently reported reason for the device's limited use was the time required to apply it properly during patient extrication. Analysis of the available literature suggests that the use of spinal immobilisation devices in selected situations may be associated with a risk of complications and prolonged patient extrication time.

Conclusion: The study findings indicate limited use of the Kendrick extrication device in rescue practice and low availability of this equipment in State Fire Service units. Respondents identified the time-consuming nature of device application during patient extrication as the main reason for abandoning its use. Current scientific evidence suggests that rapid patient extrication without this type of equipment may be a safe alternative in selected clinical situations. The results obtained may support the rationale for limiting the use of the Kendrick Extrication Device and highlight the need for further research into more intuitive and effective methods for patient extrication and stabilization.

Keywords: Kendrick extrication device, traffic accident, casualty evacuation, spinal injury, prehospital medicine

Type of article: original scientific article

Received: 19.03.2026; **Reviewed:** 27.05.2026; **Accepted:** 27.05.2026;

Authors' ORCID IDs: S. Paszek – 0009-0009-5059-3426; Z. Czaplińska-Paszek – 0000-0003-2429-8262;

Percentage contribution: S. Paszek – 90%; Z. Czaplińska-Paszek – 10%;

Please cite as: Safety & Fire Technology 2026, 1, 210–222, <https://doi.org/10.12845/sft.67.1.2026.10>;

This is an open access article under the CC BY-SA 4.0 license (<https://creativecommons.org/licenses/by-sa/4.0/>).

ABSTRAKT

Cel: Celem niniejszej pracy była ocena częstości stosowania kamizelki Kendricka przez ratowników oraz analiza aktualnych dowodów naukowych dotyczących skuteczności i bezpieczeństwa jej użycia. Wybór tematu był podyktowany obserwowanymi w ostatnich latach różnicami w programie kursu kwalifikowanej pierwszej pomocy dla strażaków PSP i OSP odnoszącymi się do tego urządzenia.

Projekt i metody: Badanie zostało przeprowadzone w okresie od lipca 2022 roku do marca 2026 roku w grupie 210 strażaków. Zrealizowano je metodą sondażu diagnostycznego z wykorzystaniem autorskiego kwestionariusza ankiety udostępnionego za pośrednictwem formularzy Google. Ankieta była skierowana do strażaków pełniących zawodową oraz ochotniczą służbę w jednostkach ochrony przeciwpożarowej. Kwestionariusz rozpowszechniano w mediach społecznościowych oraz grupach branżowych skupiających osoby zajmujące się ochroną przeciwpożarową. Analizie poddano odpowiedzi dotyczące częstości stosowania kamizelki Kendricka, jej dostępności oraz subiektywnej oceny przydatności w działaniach ratowniczych. Dodatkowo

przeprowadzono przegląd aktualnego piśmiennictwa naukowego dotyczącego skuteczności, bezpieczeństwa oraz potencjalnych powikłań związanych ze stosowaniem kamizelki Kendrica w medycynie przedszpitalnej. Uwzględniono w nim publikacje dostępne w bazach PubMed, Scopus i Google Scholar.

Wyniki: Ponad połowa ankietowanych ratowników zadeklarowała, że w praktyce nie wykorzystuje kamizelki Kendrica podczas udzielania kwalifikowanej pierwszej pomocy. Znaczna część respondentów wskazała również na brak tego urządzenia w wyposażeniu jednostek ratowniczych. Najczęściej wskazywaną przyczyną ograniczonego stosowania omawianego sprzętu była jego czasochłonność w prawidłowej aplikacji podczas ewakuacji poszkodowanego. Analiza dostępnego piśmiennictwa sugeruje, że stosowanie urządzeń do unieruchamiania kręgosłupa w wybranych sytuacjach może wiązać się z ryzykiem powikłań oraz wydłużeniem czasu ewakuacji pacjenta.

Wnioski: Wyniki badania wskazują na ograniczone wykorzystanie kamizelki Kendrica w praktyce ratowniczej oraz niski poziom dostępności tego sprzętu w jednostkach PSP. Respondenci jako główną przyczynę rezygnacji z jej stosowania wskazywali czasochłonność obsługi urządzenia podczas ewakuacji poszkodowanego. Aktualne doniesienia naukowe sugerują, że szybka ewakuacja pacjenta bez stosowania tego typu sprzętu może stanowić bezpieczną alternatywę w wybranych sytuacjach klinicznych. Uzyskane wyniki sugerują zasadność ograniczania wykorzystania kamizelki Kendrica oraz potrzebę dalszych badań nad bardziej intuicyjnymi i efektywnymi metodami ewakuacji i stabilizacji pacjentów.

Słowa kluczowe: kamizelka Kendrica, wypadek komunikacyjny, ewakuacja poszkodowanych, uraz kręgosłupa, medycyna przedszpitalna

Typ artykułu: oryginalny artykuł naukowy

Przyjęty: 19.03.2026; **Zrecenzowany:** 27.05.2026; **Zaakceptowany:** 27.05.2026;

Identyfikatory ORCID autorów: S. Paszek – 0009-0009-5059-3426; Z. Czaplińska-Paszek – 0000-0003-2429-8262;

Procentowy wkład merytoryczny: S. Paszek – 90%; Z. Czaplińska-Paszek – 10%;

Proszę cytować: Safety & Fire Technology 2026, 1, 210–222, <https://doi.org/10.12845/sft.67.1.2026.10>;

Artykuł udostępniany na licencji CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>).

Introduction

The National Rescue and Firefighting System (KSRG) [1, art. 1, para. 1], [2] in Poland includes e.g. organisational units of the National Fire Service (PSP, professional, uniformed and equipped with special equipment [3, art. 1]) and their collaborating Volunteer Fire Service (OSP) units. The OSP units operate as associations [4–5], in which properly trained members conduct rescue and firefighting operations in the form of civil defence [6], thus socially dependent on other professional or private responsibilities in their availability.

The Kendrick extrication device (KED) is designed for full-length spinal immobilisation and patient extraction. At present, the device is not a primary piece of rescue equipment pursuant to the R1 standard [7], however it often is an optional supplement.

In recent years, the tendency towards gradual abandonment of its use is becoming increasingly clear. It is also noticeable in changing qualified first aid procedures (KPP) prepared by the Headquarters of the State Fire Service. In the 2010 training curriculum it was still listed a spinal immobilisation device [8]. However, the KED application provision is not present in later editions of the qualified first aid training curriculum of 2023 [9] or 2025 [10]. The very design of the device enables application to a patient in the seated position, so it is the most often used to secure patients after traffic accidents during evacuation from a wrecked vehicle. After evacuating the patient and transferring it to medical rescue teams (ZRM) [11, art. 15 para. 1, pts. 1, 2] that will transport the patient to the hospital, the KED from the ambulance is normally given to the rescue team “in exchange”, in the same manner as e.g. the spinal board. Often, when the patient does not need to be extracted from the wrecked vehicle by firefighters, evacuation using the KED is conducted by ZRM directly. Evacuation without equipment is quicker, because proper application of the KED requires specific time and effective cooperation of at least two persons. For that reason, already at the stage of arrival to the patient, a quick decision on further organisation of

Wstęp

Krajowy system ratowniczo-gaśniczy (KSRG) [1, art. 14, ust. 1], [2] w Polsce tworzą m.in. jednostki organizacyjne Państwowej Straży Pożarnej (PSP, będącej zawodową, umundurowaną i wyposażoną w specjalistyczny sprzęt formacją [3, art. 1]) oraz współpracujące z nią ochotnicze straże pożarne (OSP). OSP działają w formie stowarzyszenia [4–5], w którym członkowie po odpowiednim przeszkoleniu realizują działania ratowniczo-gaśnicze w ramach obrony cywilnej [6], a więc społecznie, zależnie od swojej dostępności wynikającej z innych obowiązków zawodowych czy prywatnych.

Kamizelka Kendricka jest urządzeniem służącym do unieruchomienia kręgosłupa na całej jego długości oraz do ewakuacji poszkodowanych. Obecnie urządzenie to nie jest podstawowym elementem wyposażenia ratowniczego według standardu R1 [7], jednak często stanowi jego opcjonalne uzupełnienie.

W ostatnich latach coraz wyraźniejsza staje się tendencja do stopniowej rezygnacji z jej wykorzystywania. Można to też zauważyć w zmieniających się procedurach z zakresu kwalifikowanej pierwszej pomocy (KPP) opracowywanych przez Komendę Główną PSP. W programie szkolenia z 2010 r. wskazywano ją jeszcze jako jeden z przyrządów do unieruchamiania kręgosłupa [8]. Zapis o wykorzystywaniu KED nie pojawia się natomiast w kolejnych edycjach programu szkolenia KPP z lat 2023 [9] i 2025 [10]. Sama budowa kamizelki umożliwia jej założenie u poszkodowanego w pozycji siedzącej, dzięki czemu najczęściej stosowana jest do zabezpieczenia ofiar wypadków komunikacyjnych podczas ich ewakuacji z waku pojazdu. Po ewakuacji pacjenta i przekazaniu go pod opiekę zespołów ratownictwa medycznego (ZRM) [11, art. 15 ust. 1 pkt 1 i 2], które będą transportować go do szpitala, zwyczajowo KED z karetki jest oddawana na stan zastępu „na wymianę”, na tej samej zasadzie co np. deska ortopedyczna. Niejednokrotnie, gdy nie ma konieczności wydobywania poszkodowanego z waku pojazdu przez strażaków, ewakuację z wykorzystaniem KED prowadzą bezpośrednio ZRM.

evacuation operations is required. When selecting the evacuation method, the person in charge of rescue operations (KDR) or their designated person in charge of medical rescue operations (KMDR) must also consider the technical conditions and access to the patient, as well as the forces and resources available. In addition, the condition of the patient will often influence the decision on further operations, i.e. whether providing aid is required after accessing the patient, followed by preparation for evacuation, or whether immediate evacuation is required, followed by rescue operations [12]. In addition, the KDR or KMDR must evaluate if rescuers will be really enabled to apply the KED in hard to reach and confined space of the wrecked vehicle, considering that for proper application of the KED following guidelines, the patient must be reached by two rescuers. Interestingly, regardless of whether the patient will be evacuated using the KED or without equipment, the patient's prognosis of later neurological changes remain similar [13]. In addition, evacuation without equipment is more effective in securing the cervical spine in vertical and sagittal plane than evacuation with the KED [14]. Only in protection from rotary mobility of the cervical spine, the KED gains advantage over evacuation without equipment [15–16]. Considering the need to use hydraulic tools to access the patient in technical rescue, the application of the KED, which often brings no clear benefits to the patient, becomes an unnecessary equipment burden. It can additionally impede operational logistics and the course and coordination of the entire rescue mission. Consequently, the abandonment of the KED could streamline the KDR or KMDR decision-making process to select the evacuation method. The person in charge of operations will not have to focus on selecting the optimum variant, increasing the attention available for other matters potentially more important at the given moment, and key decisions for the coordination of the entire rescue mission.

Material and methods

This study was conducted to determine the actual frequency of practical application of the KED in fire protection units and the main reasons, why rescuers are reluctant to apply it for patient evacuation from a vehicle. In addition, considering the changes to the State Fire Service training curriculum that occurred during the gathering of materials for this study, the purpose of the authors was also to evaluate the validity of excluding the KED from the current qualified first aid training curriculum for the Fire State Service. For that purpose, the survey questionnaire was prepared in Google Forms and made available from August 2022 to March 2026.

Bezprzrządowa ewakuacja trwa krócej, gdyż prawidłowe założenie KED wymaga określonego czasu i wprawnej współpracy co najmniej dwóch osób. Z tego powodu już na samym etapie dotarcia do poszkodowanego należy podjąć szybką decyzję odnośnie do dalszej organizacji działań w zakresie ewakuacji osoby ratowanej. Kierujący działaniem ratowniczym (KDR) lub wyznaczony przez niego kierujący medycznym działaniem ratowniczym (KMDR), decydując o sposobie ewakuacji, musi uwzględnić dodatkowo techniczne warunki i możliwości wykonania dostępu do poszkodowanego, a także dostępne siły i środki. Ponadto stan samego poszkodowanego będzie niejednokrotnie wpływał na decyzję o kolejności działań, tj. czy ze względu na jego bezpieczeństwo konieczne będzie udzielenie pomocy po wykonaniu dostępu i następnie przygotowanie go do ewakuacji, czy też konieczna będzie niezwłoczna ewakuacja, a dopiero potem prowadzenie działań ratowniczych [12]. Dodatkowo KDR lub KMDR musi ocenić, czy ratownicy będą mieli realne możliwości wykorzystania KED w trudnodostępnych oraz ciasnych przestrzeniach wraku pojazdu, biorąc pod uwagę, że w celu prawidłowej, zgodnej z zaleceniami aplikacji KED, do poszkodowanego musi dotrzeć dwóch ratowników. Co ciekawe, bez względu na to, czy poszkodowany będzie ewakuowany przy pomocy KED, czy też bezprzrządowo, jego rokowania w kontekście późniejszych zmian neurologicznych pozostają zbliżone [13]. Co więcej, bezprzrządowa ewakuacja lepiej zabezpiecza kręgosłup szyjny w płaszczyźnie poprzecznej oraz strzałkowej w porównaniu z ewakuacją z wykorzystaniem KED [14]. Jedynie w kontekście zabezpieczania przed obrotową ruchomością kręgosłupa szyjnego KED zyskuje przewagę nad ewakuacją bezprzrządową [15–16]. Uwzględniając konieczność wykorzystania narzędzi hydraulicznych w ramach ratownictwa technicznego w celu dotarcia do poszkodowanego, stosowanie KED, która często nie przynosi wyraźnych korzyści dla poszkodowanego, staje się zbędnym obciążeniem sprzętowym. Może dodatkowo utrudniać logistykę działań oraz przebieg i koordynację całej akcji ratowniczej. Rezygnacja z KED może zatem usprawnić proces decyzyjny KDR lub KMDR w zakresie wyboru techniki ewakuacji. Osoba kierująca działaniem nie będzie musiała koncentrować się na wyborze optymalnego wariantu, dzięki czemu będzie mogła poświęcić większą uwagę innym, potencjalnie istotniejszym w danym momencie kwestiom oraz decyzjom kluczowym dla koordynacji całego działania ratowniczego.

Materiał i metody

Niniejsze badanie zostało przeprowadzone w celu określenia faktycznej częstotliwości praktycznego wykorzystywania KED w jednostkach ochrony przeciwpożarowej oraz głównych przyczyn, które sprawiają, że ratownicy niechętnie decydują się na jej użycie w celu ewakuacji poszkodowanych z pojazdu. Dodatkowo, uwzględniając zmiany w programie kształcenia PSP, które nastąpiły na etapie zbierania materiału do niniejszej pracy, celem autorów stała się także ocena zasadności pominięcia kamizelki KED w aktualnym programie szkolenia KPP dla PSP. W tym celu przygotowano kwestionariusz ankiety w formularzu Google, udostępniony w okresie od sierpnia 2022 r. do marca 2026 roku.



Figure 1. QR code to the survey
Rycina 1. QR kod prowadzący do ankiety

Source: Own elaboration.
Źródło: Opracowanie własne.

The survey was addressed to State Fire Service officers and Volunteer Fire Service members that qualified first aid in collaboration with the National Medical Rescue System. The questionnaire included nine questions on the practical use of the KED in the incident scene. The respondents were informed of the purpose of the study and by completing and submitting the form, they consented to the publication of its results. The form was distributed to an anonymous group of respondents using social media. It was addressed to members of groups gathering persons in professional or voluntary service of fire protection units. Next, current scientific evidence on the application of the KED was gathered to analyse the survey results.

Results

In accordance with *The principles of organisation of medical rescue of the KSRG* [17, pt. 5.4.], the principles of acquisition of rescuer qualifications are defined in the regulation of the minister in charge of internal affairs for the State Fire Service and in the regulation of the minister of health in for Volunteer Fire Service rescuers. As mentioned earlier, in 2023, during the gathering of materials for this study, qualified first aid procedures were updated in the State Fire Service and the KED was no longer listed as spinal immobilisation device [9–10]. However, in the analogical regulation of the minister of health on qualified first aid, applicable to the Volunteer Fire Service rescuer training, the example of use of the KED is also included in the current version [18].

Among the surveyed firefighters ($N = 210$), a vast majority, more than 80%, were Volunteer Fire Service members, while one fifth of them were fully professional State Fire Service officers. In addition, one fourth of the people surveyed had medical rescuer education, thus competencies far beyond the qualified first aid standard. More than 57% of respondents had experience of serving as KDR, thus the competence to make decisions on the tactics of such operations, evacuation and equipment application in the incident scene.

Ankiętę skierowano do funkcjonariuszy PSP oraz członków OSP udzielających KPP w ramach współpracy z Systemem Państwowego Ratownictwa Medycznego. Kwestionariusz zawierał dziewięć pytań dotyczących praktycznego wykorzystania KED na miejscu zdarzenia. Uczestnicy badania zostali poinformowani o celu badania, a poprzez wypełnienie i przesłanie formularza wyrazili zgodę na publikację jego wyników. Formularz został rozesłany do anonimowej grupy respondentów za pomocą mediów społecznościowych. Adresatami byli członkowie grup skupiających osoby pełniące zawodową bądź ochotniczą służbę w jednostkach ochrony przeciwpożarowej. Następnie zgromadzono aktualne doniesienia naukowe z zakresu stosowania KED, by na ich podstawie przeanalizować wyniki przeprowadzonej ankiety.

Wyniki

Zgodnie z *Zasadami organizacji ratownictwa medycznego KSRG* [17, pkt 5.4.] zasady nabywania uprawnień ratownika w PSP określa rozporządzenie ministra właściwego do spraw wewnętrznych, zaś w przypadku ratowników w OSP – rozporządzenie ministra zdrowia. Jak wspomniano wcześniej, w 2023 r., a więc w trakcie zbierania materiału do niniejszej pracy, nastąpiła zmiana procedur KPP w PSP, w ramach której KED nie wymieniano już jako urządzenia służącego do unieruchomienia kręgosłupa [9–10]. Natomiast w analogicznym rozporządzeniu ministra zdrowia w sprawie KPP, mającym zastosowanie w szkoleniu ratowników OSP, przykład wykorzystywania KED jest zawarty także w wersji aktualnej [18].

W grupie przebadanych strażaków ($N = 210$) zdecydowaną większość, bo ponad 80%, stanowią członkowie OSP, natomiast niemal jedną piątą funkcjonariusze PSP. Dodatkowo niespełna jedna czwarta badanych osób posiada wykształcenie ratownika medycznego, a więc kompetencje znacznie przekraczające standard KPP. Ponad 57% respondentów ma doświadczenie w pełnieniu funkcji KDR, a co za tym idzie, kompetencje decyzyjne na miejscu zdarzenia w zakresie taktyki działań, decyzji o ewakuacji oraz wykorzystywanego sprzętu.

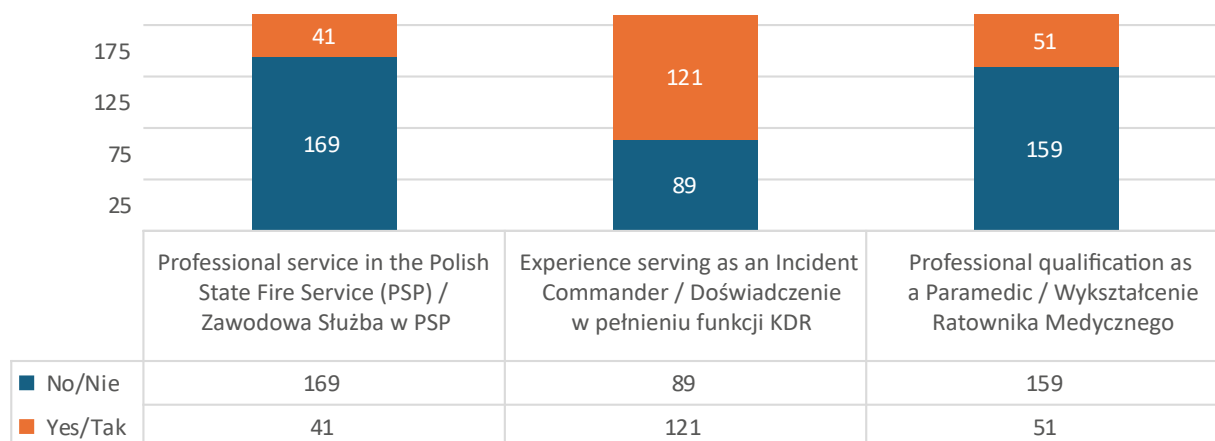


Figure 2. Characteristics of the study group
Rycina 2. Charakterystyka badanej grupy

Source: Own elaboration.
 Źródło: Opracowanie własne.

Among the firefighters surveyed, almost two thirds had more than 5 years of experience, while every third responded could boast of at least 10 years in service. In addition, as much as 85% of the respondents had more than 3 years of experience in the fire service, which means that the qualified first aid course curriculum of the State Fire Service were updated during their service and that they had pre-2023 experience. The firefighters of the KSRG are required to complete a 66-hour qualified first aid course that required additional recertification every 3 years. Among the firefighters surveyed, almost two thirds had their last recertification before the update to the qualified first aid training curriculum for the State Fire Service in 2023, while three fourths participated in recertification in the 2022–2025 period. That enabled the assumption that respondents had adequate experience and substantive preparation to provide high level aid, based on regular professional development and practical training. Nonetheless, as few as 9% of the firefighters surveyed correctly decoded the MBLHT acronym that specified the order of fastening of KED straps (middle strap, bottom strap, legs strap, head strap, top strap) and as many as 80% admitted that acronym was completely unknown to them.

Spośród badanych strażaków niemal dwie trzecie ma ponad 5-letnie doświadczenie, natomiast co trzeci z pytanych może się pochwalić co najmniej 10-letnią służbą. Ponadto aż 85% respondentów ma powyżej trzech lat doświadczenia w straży pożarnej, co oznacza, że zmiany w programie kursu KPP dla PSP miały miejsce już w trakcie ich służby oraz że mają doświadczenie sprzed 2023 r. Strażacy w KSRG są zobowiązani do ukończenia 66-godzinnego kursu KPP, który dodatkowo wymaga recertyfikacji co trzy lata. Pośród ankietowanych strażaków niemal dwie trzecie ostatnią recertyfikację przechodziło przed zmianą programu szkolenia KPP dla PSP w 2023 roku, natomiast aż trzy czwarte brało udział w recertyfikacji w latach 2022–2025. Dzięki temu możemy przyjąć założenie, że respondenci posiadają odpowiednie doświadczenie oraz merytoryczne przygotowanie do udzielania pomocy na wysokim poziomie, wynikające z regularnego doskonalenia zawodowego i praktycznego szkolenia. Pomimo tego zaledwie 9% ankietowanych strażaków prawidłowo rozszyfrowało akronim MBLHT określający kolejność zapinania pasów mocujących KED (ang. *middle strap, bottom strap, legs strap, head strap, top strap*), a aż 80% przyznaje, że ten akronim nie jest im w ogóle znany.

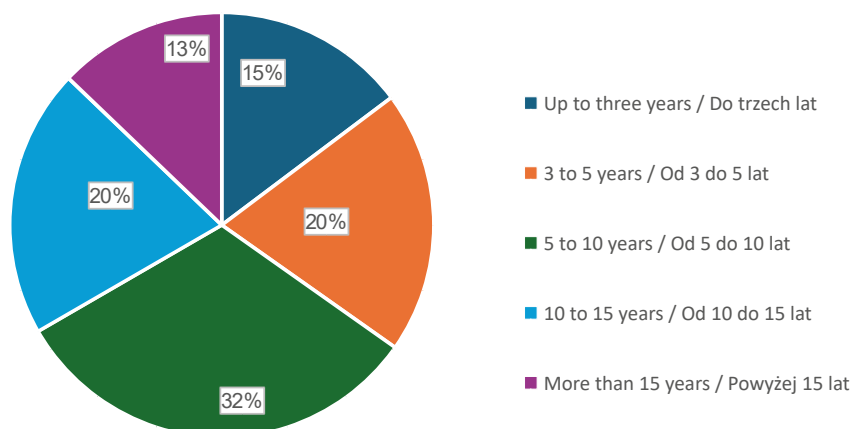


Figure 3. Length of service in National Rescue and Firefighting Units
Rycina 3. Staż służby jednostkach KSRG

Source: Own elaboration.
 Źródło: Opracowanie własne.

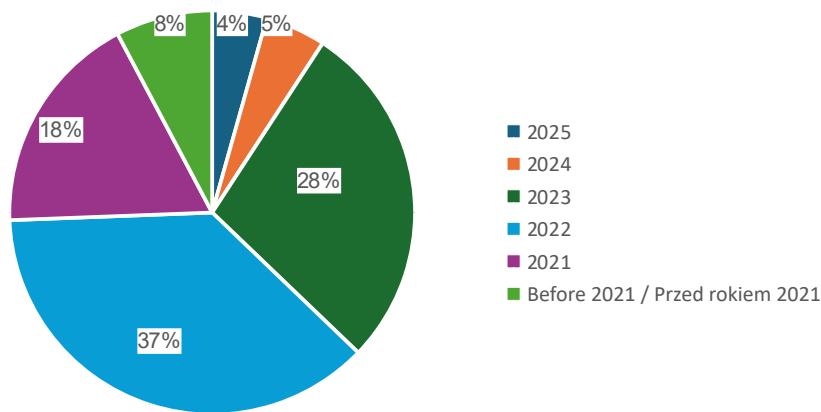


Figure 4. Date of the last recertification of the qualified first aid course
Rycina 4. Termin ostatniej recertyfikacji kursu KPP

Source: Own elaboration.

Źródło: Opracowanie własne.

Moreover, a vast majority of them admitted that they had never used the KED during operations (60%) and as few as 16% declared to have used it in the previous year. Slightly more than one fourth of the rescuers had last used the KED within the previous 3 years, i.e. one time in the entire recertification period.

The answers to the question on the frequency of use of the KED were comparable, because as few as one third of respondents believed to use the KED more than once per 10 years. Regular use of the KED at least one per half a year was only admitted by 12% and at least once per month by only 2% of all rescuers surveyed.

Co więcej, również zdecydowana większość spośród nich przyznaje, że nigdy nie wykorzystywała KED podczas działań (60%), a zaledwie 16% deklaruje jej użycie w ciągu ostatniego roku. Nieco ponad jedna czwarta ratowników po raz ostatni wykorzystywała KED na przełomie ostatnich trzech lat, a więc jeden raz w całym okresie recertyfikacji.

W pytaniu o częstotliwość stosowania KED odpowiedzi są porównywalne, bowiem zaledwie co trzeci respondent uważa, że korzysta z KED częściej niż raz na 10 lat. Do regularnego wykorzystywania KED przynajmniej raz na pół roku przyznaje się zaledwie 12%, a przynajmniej raz w miesiącu już tylko 2% spośród wszystkich ankietyowanych ratowników.

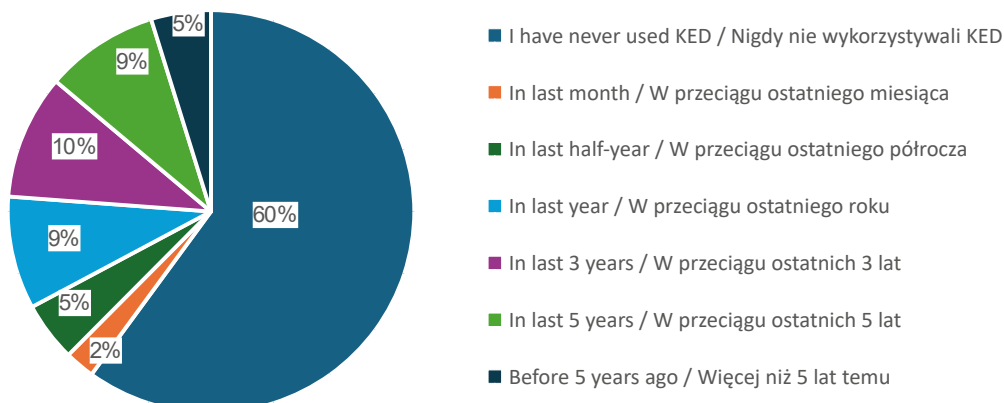


Figure 5. Comparison of respondents in the context of the approximate time that has passed since the last practical use of KED
Rycina 5. Porównanie respondentów w kontekście orientacyjnego czasu, który upłynął od ostatniego praktycznego wykorzystywania KED

Source: Own elaboration.

Źródło: Opracowanie własne.

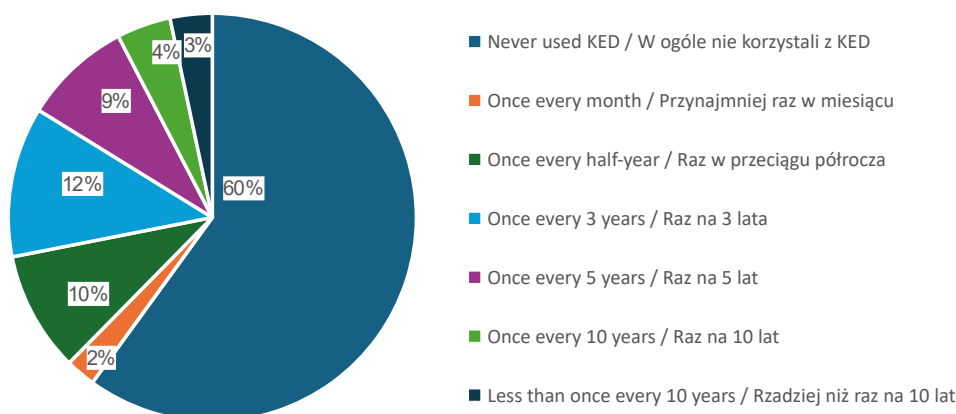


Figure 6. Comparison of respondents in the context of the frequency of practical use of KED

Rycina 6. Porównanie respondentów pod względem częstotliwości praktycznego wykorzystywania KED

Source: Own elaboration.

Źródło: Opracowanie własne.

In the final question, asking to determine the cause of the declining interest in the KED, the firefighters surveyed could select any number of answers from the six variants proposed. The reasons differed, because none of the arguments clearly convinced a vast majority of the firefighters surveyed. It is worth noting that almost half of them admitted not to have the KED in their fire engines. Almost as much answers indicated that the main reason for the reluctance to use this type of equipment was the excessively long time required for proper application. Almost one third believed that the subject equipment was used so rarely due to the lack of proficiency in using it. Exactly 30% of the firefighters doubted whether after evacuating and transferring a patient to ZRM they would receive another KED from the ambulance as part of equipment rotation. The same number of respondents believed that one of the main reasons that the subject equipment was used rarely was the requirement to assign as many as two rescuers to one patient, as specified in the operating instructions by the manufacturer of the device [19]. In addition, almost 14% of the firefighters surveyed did not at all regard the KED as effective means of spinal immobilisation.

W ostatnim pytaniu, które dotyczyło określenia przyczyny spadającego zainteresowania KED, ankietowani strażacy mogli wytypować dowolną liczbę odpowiedzi spośród sześciu proponowanych wariantów. Powody są zróżnicowane, gdyż żaden z argumentów nie przekonał jednoznacznie większości ankietowanych strażaków. Na uwagę zasługuje to, że niemal połowa z nich przyznaje, iż w ogóle nie posiada KED na wyposażeniu wozów bojowych. Prawie tyle samo odpowiedzi wskazywało, że głównym powodem niechęci do wykorzystywania tego typu sprzętu jest zbyt długi czas potrzebny do jego prawidłowego założenia. Ponad jedna trzecia uważa, że brak biegłości w stosowaniu omawianego ekwipunku sprawia, że jest on tak rzadko wykorzystywany. Również 30% strażaków podaje w wątpliwość, czy po ewakuowaniu poszkodowanego, który zostanie przekazany pod opiekę ZRM, otrzymają z karetki inną KED w ramach rotacji sprzętu. Taka sama liczba ankietowanych uważa, że jednym z głównych powodów rzadkiego decydowania się na korzystanie z omawianego ekwipunku jest konieczność oddelegowania aż dwóch ratowników do jednego poszkodowanego – co zostało określone w instrukcji obsługi producenta urządzenia [19]. Dodatkowo niemal 14% badanych strażaków w ogóle nie wierzy w skuteczność działania KED w zakresie unieruchamiania kręgosłupa.

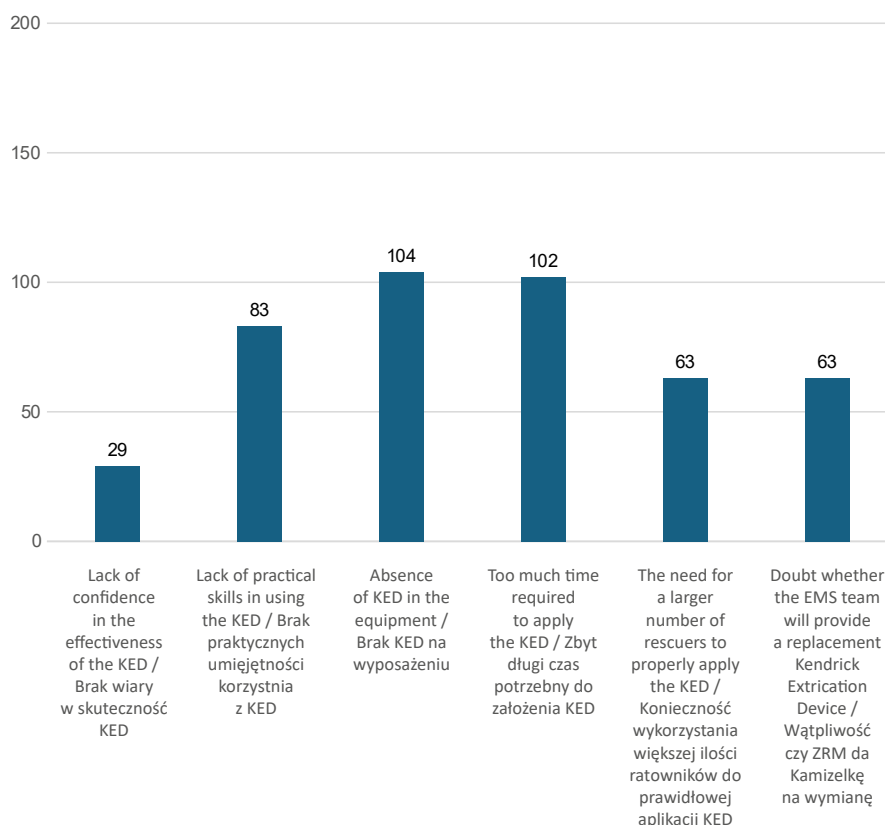


Figure 7. Main reasons for avoiding KED in National Rescue and Firefighting Units

Rycina 7. Główne powody unikania kamizelki Kendricka w KSRG

Source: Own elaboration.

Źródło: Opracowanie własne.

Cooperation with medical rescue units in Poland and abroad

In the place of incident, the cooperation between the firefighters and ZRM is essential [20]. The qualification to use the KED should be mastered by both of these units. For that specific reason, a similar survey was also conducted among ZRM members [21]. It established that also in that target group, the experience in the practical use of the KED is scarce and almost half of respondents never encountered it during medical rescue operations. Regarding the reasons for such state of affairs, similar to KSRG firefighters, ZRM members stated above all the long time required for proper application of the KED. In addition, ZRM members believed that the firefighters were primarily responsible for patient evacuation, so if it had been completed without KED, it was the decision and responsibility of the rescuers in charge of the operations. That is in perfect correspondence with the findings of this study, based on which more than half of respondents do not at all have the subject equipment in store. Similar results were also presented by studies conducted abroad. For example, in the Middle East a low level of proficiency in practical use of the KED in pre-hospital conditions was demonstrated by rescue units [22]. This is not an isolated case, because also in the USA, in the Howard County, a study was conducted, of which the results confirmed significant deficiencies in the operating knowledge of the KED in medical rescuers and firefighters [23].

Współpraca z jednostkami ratownictwa medycznego w Polsce i za granicą

Na miejscu zdarzenia bardzo ważna jest współpraca pomiędzy strażakami a ZRM [20]. Umiejętność korzystania z KED powinna być domeną obu tych podmiotów. Z tego właśnie powodu podobne badanie zostało przeprowadzone również wśród członków ZRM [21]. Ustalono wówczas, że także w tej grupie docelowej doświadczenie w praktycznym wykorzystywaniu KED jest znikome, a niemal połowa ankietowanych w ogóle nie miała z nią do czynienia podczas udzielania medycznych czynności ratunkowych. Jeśli zaś chodzi o powody takiego stanu rzeczy, to podobnie jak strażacy KSRG, członkowie ZRM wskazują przede wszystkim na długi czas potrzebny do prawidłowej aplikacji KED. Członkowie ZRM uważali ponadto, że w głównej mierze to właśnie strażacy odpowiadają za ewakuację poszkodowanych, zatem jeżeli była ona prowadzona bez wykorzystywania KED, stanowiło to decyzję i odpowiedzialność ratowników prowadzących działania. To doskonale koresponduje z ustaleniami powziętymi w niniejszym badaniu, z których wynika, iż ponad połowa ankietowanych w ogóle nie posiada omawianego sprzętu na wyposażeniu. Podobne wyniki prezentują również badania przeprowadzone za granicą. Przykładowo, na Bliskim Wschodzie również udowodniono niski poziom umiejętności w praktycznym użytkowaniu KED w warunkach przedszpitalnych przez jednostki ratownicze [22]. Nie jest to odosobniony przypadek, ponieważ także w USA,

Benefits and hazards of using the Kendrick Extrication Device

In turn, when comparing evacuation with the KED and evacuation without equipment using the Rautek manoeuvre, another weakness of the former is the deterioration of respiratory function in patients immobilised using it, in addition to the aforementioned difficulties with spinal immobilisation in the transverse and sagittal plane [12]. This is because the stress on the chest due to the tight fastening of the KED (essential for its effectiveness) may cause additional pain in the patient, in particular if the patient has suffered blunt injuries to the chest. Consequently, the device may impede the patient's breathing, which may have a critical impact on the further prognosis [24–25]. Also if the patient managed to exit wreck alone, as long as the patient is ambulatory, the chance to survive and recover is higher than with preventative immobilisation using the KED or cervical collar [26]. Another challenge is related to the requirement to assign a greater number of people than to evacuation using the Rautek manoeuvre. This, in turn, requires additional training [27] in communication and cooperation in the application of the KED. Although the essence of all rescue operations is joint training and coordination of the team so that every not only member perfectly knew their own tasks, but also could predict the next move of other rescuers providing qualified first aid [28], due to the rare use of the KED in real rescue operations, maintaining proficiency in using it would require assigning significant training time. Such sessions would take place at the expense of training in other life-saving procedures, much more frequently used in practice. In addition, the time demand listed as one of the main reasons to abandon the use of the KED by the respondents is also justified by literature, which states the adverse impact of delayed arrival of injured patients to the rescue department [29–30].

In turn, the KED is endorsed by the International Commission for Mountain Emergency Medicine and the Terrestrial Rescue Commission of the International Commission for Alpine Rescue, which recommended it [31] for use to evacuate injured mountaineers from difficult-to-access mountain crevices and glaciers [32]. However, in the review of scientific evidence on the use of the subject equipment in traffic accidents, a positive opinion on the Kendrick Extrication Device occurred only once, in the study conducted by French scientists. They proved a positive impact of the KED in connection with trochanteric belt to secure the pelvis during evacuation from the vehicle [33]. Finally, however, in Polish conditions hard numerical data leave no delusions – based on the data collected from the National Medical Command Support System made available by the National Medical Rescue Monitoring Centre, in the 2017–2022 period ZRM interventions using the KED were incidental [34]. In addition, in these cases the KED was mostly used in the alternative variant, for pelvic girdle immobilisation, and not as expected, for its primary design purpose, for

w hrabstwie Howard, przeprowadzono badanie, którego wyniki potwierdziły znaczące braki w zakresie znajomości obsługi KED przez ratowników medycznych i strażaków [23].

Korzyści i zagrożenia wynikające ze stosowania kamizelki Kendricka

Porównując ewakuację z wykorzystaniem KED z ewakuacją bezprzyrządową przy pomocy rękoczynu Rauteka, należy zauważyć, że oprócz wspomnianych wcześniej trudności z unieruchomieniem kręgosłupa w płaszczyźnie poprzecznej i strzałkowej, na niekorzyść KED przemawia również pogorszenie czynności oddychowej u pacjentów [12]. Dzieje się tak, ponieważ ucisk wywołany na klatkę piersiową przez ciasne zapięcie KED (będące niezbędnym elementem wpływającym na jej skuteczność) może u poszkodowanego powodować dodatkowe dolegliwości bólowe, tym bardziej, jeżeli doznał on tępych urazów w obrębie klatki piersiowej. W konsekwencji kamizelka może utrudniać mu oddychanie, co może mieć krytyczny wpływ na dalsze rokowania [24–25]. Także sytuacja samodzielnego opuszczenia wraku przez poszkodowanego, o ile jest w stanie sam się poruszać, przekłada się na większe szanse przeżycia i powrotu do zdrowia niż prewencyjne unieruchomienie przy pomocy KED czy kołnierza ortopedycznego [26]. Kolejne wyzwanie wiąże się z koniecznością zaangażowania większej liczby osób niż podczas ewakuacji przy zastosowaniu chwytu Rauteka. To z kolei wymaga prowadzenia dodatkowych szkoleń [27] w zakresie komunikacji oraz współpracy przy zakładaniu KED. Wprawdzie istotą wszystkich działań ratowniczych jest wspólne szkolenie i zgrzywanie zespołu, tak aby każdy z jego członków doskonale znał nie tylko swoje zadania, ale także przewidywał następny ruch pozostałych ratowników udzielających KPP [28], jednak rzadkie wykorzystywanie KED w rzeczywistych działaniach ratowniczych powoduje, że utrzymanie biegłości w jej stosowaniu wymagałoby znacznego nakładu czasu szkoleniowego. Takie zajęcia odbywałyby się kosztem trenowania innych procedur ratujących życie, które o wiele częściej miałyby wykorzystanie w praktyce. Dodatkowo czasochłonność, wskazywana przez ankietowanych jako jeden z głównych powodów rezygnacji z użycia kamizelek, znajduje uzasadnienie w literaturze, w której podkreśla się niekorzystny wpływ opóźnionego dotarcia pacjentów urazowych do oddziału ratunkowego [29–30].

Pochlebnie na temat KED wypowiadają się natomiast Międzynarodowa Komisja Górskiej Medycyny Ratunkowej oraz Komisja ds. Ratownictwa Naziemnego Międzynarodowej Komisji Ratownictwa Alpejskiego, udzielając jej rekomendacji [31] do wykorzystywania w przypadku konieczności ewakuacji poszkodowanych alpinistów z trudno dostępnych szczelin górskich oraz lodowców [32]. Jednakże w przeglądzie dowodów naukowych dotyczących użycia omawianego urządzenia w wypadkach komunikacyjnych pozytywna opinia na temat kamizelki Kendricka pojawiła się tylko raz – w badaniu przeprowadzonym przez francuskich naukowców. Udowodnili oni bowiem pozytywny wpływ KED w połączeniu z pasem krętarzowym na zabezpieczenie miednicy podczas ewakuacji z pojazdu [33]. Ostatecznie jednak w warunkach polskich twarde dane liczbowe nie pozostawiają złudzeń – według

spinal immobilisation. This is an additional confirmation that the frequency of use of the KED in real operations could decrease over time, often because both the firefighters and ZRM members lack proficiency in operating it.

Discussion

Based on the presented results, it has been found that the KED is used sporadically and that the respondents that actually have had the opportunity to use it in practice have only done it incidentally. Furthermore, in existing scientific evidence, it was postulated multiple times that despite the numerous positive aspects, such as protection of the spine from rotary mobility, easier evacuation from difficult-to-access areas and more stable protection of the pelvis when using a strap to immobilise it, the risk of the eventual consequences of improper use could be more severe for the patients. For that specific reason, evacuation with the KED does not always improve the prognosis of the patients and sometimes could even aggravate the injuries, deteriorate the overall condition of the patient by intensifying hypoxia and other potential injuries that the device does not protect the patient from. They include for example the increased mobility of the cervical spine in the sagittal and vertical plane. Moreover, the KED does not prevent further neurological complications better than evacuation without equipment. In addition, evacuation using the KED is much more resource-consuming, which in some cases may also have a negative impact on the patient's prognosis. In addition, contrary to quick evacuation, it requires assigning a greater number of personnel, which could be completing other tasks at the same time. Obviously, when handling patients injured in a traffic accident, whose condition often deteriorates drastically, both the time and the forces and resources saved during the mission may determine its success.

Conclusions

To conclude, despite the multiple advantages of the KED, the authors recommend far-reaching caution in using it, because the potential risk arising from improper use, in particular by teams that do not use it in their daily operations, could outweigh the potential benefits. For these particular reasons the authors agree with the decision of the Headquarters of the State Fire Service to remove the KED mention from the qualified first aid course

informacji zgromadzonych w Systemie Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego udostępnionych przez Krajowe Centrum Monitorowania Ratownictwa Medycznego w latach 2017–2022 interwencje ZRM z użyciem KED były incydentalne [34]. Dodatkowo w przypadkach tych KED wykorzystywana była najczęściej w wariantcie alternatywnym do unieruchomienia w obrębie obręczy biodrowej, a nie jak mogłoby się wydawać – zgodnie z jej podstawowym konstrukcyjnym założeniem – do unieruchomienia w obrębie kręgosłupa. To dodatkowo potwierdza, że KED może z upływem czasu stawać się urządzeniem coraz rzadziej wykorzystywanym w realnych działaniach, często z tego powodu, że zarówno strażakom, jak i członkom ZRM zwyczajnie brakuje biegłości w jej obsłudze.

Dyskusja

Na podstawie zaprezentowanych wyników ustalono, iż KED jest wykorzystywana sporadycznie, a ci z ankietowanych, którzy w istocie mieli możliwość jej praktycznego użycia, czynili to jedynie epizodycznie. Co więcej, w istniejących dowodach naukowych wielokrotnie postulowano, że pomimo wielu pozytywnych aspektów, takich jak zabezpieczenie kręgosłupa przed ruchomością obrotową, ułatwienie ewakuacji z trudnodostępnych miejsc oraz stabilniejsze zabezpieczenie miednicy podczas wykorzystywania pasa do jej unieruchomienia, ryzyko ewentualnych konsekwencji wynikających z jej nieumiejętnego użycia może być dla pacjentów o wiele poważniejsze. Z tego właśnie powodu ewakuacja z wykorzystaniem KED nie zawsze poprawia rokowania pacjentów, a momentami może nawet nasilać obrażenia, pogarszając ogólny stan poszkodowanego poprzez narastającą hipoksję oraz ewentualne inne obrażenia, przed którymi kamizelka pacjenta nie chroni. Są nimi na przykład zwiększona ruchomość kręgosłupa szyjnego w płaszczyźnie strzałkowej oraz poprzecznej. KED nie zabezpiecza również przed dalszymi powikłaniami neurologicznymi lepiej niż ewakuacja bezprzyrządowa. Ponadto ewakuacja przy pomocy KED jest o wiele bardziej czasochłonna, co w niektórych przypadkach może również negatywnie wpływać na rokowania poszkodowanego. Dodatkowo w odróżnieniu od szybkiej ewakuacji, wymaga zaangażowania większej liczby personelu, który w tym czasie mógłby realizować inne zadania. Oczywiście jest, że w przypadku postępowania z poszkodowanymi w wypadku komunikacyjnym, których stan nierzadko ulega diametralnemu pogorszeniu, zarówno czas, jak i dostępne siły oraz środki zaoszczędzone podczas trwania akcji mogą przesądzić o jej powodzeniu.

Wnioski

Podsumowując, pomimo wielu zalet KED, autorzy zalecają daleko idącą ostrożność w jej stosowaniu, gdyż potencjalne ryzyko wynikające z jej nieumiejętnego wykorzystywania – zwłaszcza wśród załóg, które nie mają z nią na co dzień styczności – może przewyższać potencjalne korzyści. Z tych właśnie powodów autorzy przychylają się do stanowiska Komendy Głównej PSP w zakresie wycofania wzmianki na temat KED z programu kursu KPP dla

curriculum for State Fire Service officers and recommend the Ministry of Health to act similarly in the qualified first aid course curriculum for civilian use, including for Volunteer Fire Service firefighters. The authors believe that within the 66-hour course curriculum, it may be difficult to schedule time to train procedures that are relatively rarely used in practice and that could be an additional hazard to the patient's prognosis in certain situations. The additional time, thus saved within the qualified first aid course, could be used to improve techniques of evacuation without equipment. As demonstrated, it yields similar effects for the patient, while causing less complications in coordinating operations in the place of incident. In addition, the authors recommend that the persons designing rescue equipment consider the need to develop new equipment that could replace the KED, better suited to contemporary patient evacuation and immobilisation challenges.

funkcjonariuszy PSP, rekomendując podobne przedsięwzięcie także dla Ministerstwa Zdrowia w ramach programu kursu KPP dla środowiska cywilnego, w tym strażaków OSP. Autorzy są zdania, że w ramach programu 66-godzinnego kursu trudno może być zaplanować czas na trening procedur, które stosunkowo rzadko mają przełożenie na praktykę oraz w określonych sytuacjach mogą stanowić dodatkowe zagrożenie dla rokowania pacjenta. Czas zaoszczędzony w ten sposób w ramach kursu KPP mógłby zostać wykorzystany na doskonalenie technik ewakuacji bezprzryadowej. Ta, jak udowodniono, daje porównywalne efekty dla pacjenta, a zarazem mniej komplikuje organizację akcji prowadzonej na miejscu wypadku. Ponadto autorzy zalecają, aby osoby zajmujące się projektowaniem sprzętu ratowniczego uwzględniły konieczność opracowania nowego oprzyrządowania, które mogłoby stać się następcą KED, lepiej dostosowanym do dzisiejszych wyzwań związanych z ewakuacją i unieruchamianiem poszkodowanych.

List of abbreviations

KDR	person in charge of rescue operation
KED	Kendrick Extrication Device
KMDR	person in charge of medical rescue operations
KPP	Qualified first aid
KSRG	National Rescue and Firefighting System
MBLHT	acronym of the order of fastening straps in the Kendrick Extrication Device (Middle strap, Bottom strap, Legs strap, Head strap, Top strap)
OSP	Volunteer Fire Service
PSP	State Fire Service
ZRM	medical rescue team

Wykaz skrótów

KDR	kierujący działaniem ratowniczym
KED	kamizelka Kendrick'a
KMDR	kierujący medycznym działaniem ratowniczym
KPP	kwalifikowana pierwsza pomoc
KSRG	krajowy system ratowniczo-gaśniczy
MBLHT	akronim opisujący kolejność zapinania pasów w Kamizelce Kendricka (ang. <i>Middle strap, Bottom strap, Legs strap, Head strap, Top strap</i>)
OSP	ochotnicza Straż Pożarna
PSP	Państwowa Straż Pożarna
ZRM	zespół ratownictwa medycznego

AI Use Statement

The authors declare that no artificial intelligence tools were used in the preparation of this article to generate text, analyses, graphics, or other elements of the publication.

The authors take full responsibility for the content of the publication, including the scientific accuracy, interpretation of results, and the final editing of the manuscript.

According to the journal's editorial policy, the uncritical copying of AI-generated content and its inclusion in a publication without proper critical analysis, verification, and revision by the author is prohibited.

Oświadczenie dotyczące wykorzystania AI

Autorzy oświadczają, że w procesie przygotowania niniejszego artykułu nie korzystano z narzędzi opartych na sztucznej inteligencji do generowania treści, analiz, grafik ani innych elementów publikacji.

Autorzy ponoszą pełną odpowiedzialność za treść publikacji, w tym za poprawność merytoryczną, interpretację wyników oraz redakcję tekstu.

Zgodnie z polityką redakcyjną czasopisma zabronione jest bezrefleksyjne kopiowanie treści wygenerowanych przez narzędzia AI oraz pozostawianie ich w publikacji bez krytycznej analizy, weryfikacji i redakcji przez autorów.

Literature / Literatura

- [1] Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (t.j. Dz.U. 2025 poz. 188).
- [2] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 17 września 2021 r. w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego (Dz.U. 2021 poz. 1737).
- [3] Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (t.j. Dz.U. 2025 poz. 1312).
- [4] Ustawa z dnia 17 grudnia 2021 r. o ochotniczych strażach pożarnych (Dz.U. 2021 poz. 2490).
- [5] Ustawa z dnia 7 kwietnia 1989 r. – Prawo o stowarzyszeniach (Dz.U. 1989, Nr 20 poz. 104).
- [6] Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907).
- [7] *Zasady Organizacji Ratownictwa Medycznego w KSRG – załącznik nr 3: Sprzęt ratownictwa medycznego*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2026.
- [8] *Program kursu w zakresie kwalifikowanej pierwszej pomocy dla strażaków Państwowej Straży Pożarnej – Treści kształcenia: pkt. 10 10. Urazy mechaniczne i obrażenia – złamania, zwichnięcia, skręcenia, krwotoki, obrażenia klatki piersiowej, brzucha, kręgosłupa, głowy i kończyn*, Biuro Szkolenia Komendy Głównej Państwowej Straży Pożarnej, Warszawa 2010.
- [9] *Program szkolenia w zakresie kwalifikowanej pierwszej pomocy dla strażaków Państwowej Straży Pożarnej*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2023.
- [10] *Program szkolenia KPP MSWiA dla Państwowej Straży Pożarnej*. Departament Zdrowia Ministerstwa Spraw Wewnętrznych i Administracji, Warszawa 2025.
- [11] Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz.U. 2006 poz. 1410 z późn. zm.).
- [12] *Zasady organizacji ratownictwa medycznego w KSRG. Załącznik nr 1 Procedury ratownicze z zakresu kwalifikowanej pierwszej pomocy – Procedura 1. Sekwencja założeń taktycznych w ratownictwie medycznym*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2026.
- [13] Misasi A, Ward J.G, Haan J.M. et al., *Prehospital Extrication Techniques: Neurological Outcomes Associated with the Rapid Extrication Method and the Kendrick Extrication Device*, „The American Surgeon” 2018;84(2), 248–253, <https://doi.org/10.1177/000313481808400233>.
- [14] Engsberg J.R., Standeven J.W., Shurtleff T.L. et al., *Cervical spine motion during extrication*, „J Emerg Med.” 2013, 44(1), 122–127, <https://doi.org/10.1016/j.jemermed.2012.02.082>.
- [15] Bucher J., Dos Santos F., Frazier D., et al., *Rapid Extrication versus the Kendrick Extrication Device (KED): Comparison of Techniques Used After Motor Vehicle Collisions*, „West J Emerg Med.” 2015, 16(3), 453–458, <https://doi.org/10.5811/westjem.2015.1.21851>.
- [16] Howell J.M. et al., *A practical radiographic comparison of short board technique and Kendrick extrication device*, „Annals of Emergency Medicine” 1989, 18, 9, 943–946, [https://doi.org/10.1016/S0196-0644\(89\)80458-5](https://doi.org/10.1016/S0196-0644(89)80458-5).
- [17] *Zasady Organizacji Ratownictwa w KSRG, Część V: Ratownictwo Medyczne, Poziom Podstawowy*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2026.
- [18] *Załącznik nr 1: Ramowy program szkolenia z kwalifikowanej pierwszej pomocy, część III: Treści nauczania i umiejętności wynikowe, pkt. 10. Urazy mechaniczne i obrażenia – złamania, zwichnięcia, skręcenia, krwotoki, obrażenia klatki piersiowej, brzucha, kręgosłupa, głowy i kończyn*, Obwieszczenie Ministra Zdrowia z dnia 24 lutego 2021 w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Zdrowia w sprawie kursu w zakresie kwalifikowanej pierwszej pomocy (Dz.U. 2021 poz. 411).
- [19] FREN0 Users Manual Model 125 pub. No. 234-1754-02 April 2001, <https://www.manualslib.com/manual/1776826/Ferno-125.html>.
- [20] Gałązkowski R., Pawlak A., Pszczółowski K., *Rola jednostek Krajowego Systemu Ratowniczo-Gaśniczego w funkcjonowaniu systemu Państwowego Ratownictwa Medycznego w rejonach wiejskich w Polsce*, „Bezpieczeństwo i Technika Pożarnicza” 2014, 34, 2, 15–26.
- [21] Paszek S., *Ocena częstotliwości praktycznego wykorzystywania Kamizelki Kendrica na podstawie odpowiedzi udzielonych przez członków Zespołów Ratownictwa Medycznego*, „Anestezjologia i Ratownictwo” 2025, 19, 160–155.
- [22] Jadgal N., Nikravan Mofrad M., Jamsahar M. et al., *The Clinical Skills of Emergency Medical Service (EMS) Personnel Regarding Spinal Immobilization of Trauma Victims: A Cross-Sectional Study*, „Arch Acad Emerg Med.” 2020, 9(1), e3, <https://doi.org/10.22037/aaem.v9i1.928>.
- [23] Bouland A.J. et al., *Assessing Attitudes toward Spinal Immobilization*, „Journal of Emergency Medicine” 2013, 45, 4, e117–e125, <https://doi.org/10.1016/j.jemermed.2013.03.046>.
- [24] Rasal Carnicer M., Juguera Rodríguez L., Vela de Oro N. et al., *Differences in lung function after the use of 2 extrication systems: a randomized crossover trial*, „Emergencias” 2018, 30(2), 115–118.
- [25] Ay D., Aktaş C., Yeşilyurt S. et al., *Effects of spinal immobilization devices on pulmonary function in healthy volunteer individuals*, „Ulus Travma Acil Cerrahi Derg.” 2011, 17(2), 103–107, <https://doi.org/10.5152/eajem.2016.32757>.
- [26] Shafer J. et al., *Cervical Spine Movement During Extrication*, „Annals of Emergency Medicine” 2008, 51, 4, 551, <https://doi.org/10.1016/j.jemermed.2012.02.082>.
- [27] Ersson A., Lundberg M., Wramby C.O. et al., *Extrication of entrapped victims from motor vehicle accidents: the crew concept*, „European Journal of Emergency Medicine” 1999, 6(4), 341–347, <https://doi.org/10.1097/00063110-199912000-00012>.
- [28] Wyrozębski M., *The Organization of Activities in a Qualified First Aid Team on the Example of the State Fire Service. Preliminary Research Report*, „Safety & Fire Technology” 2025, 66, 2, 24–38, <https://doi.org/10.12845/sft.66.2.2025.2>.
- [29] Brown J.B., Rosengart M.R., Forsythe R.M. et al., *Not all pre-hospital time is equal: Influence of scene time on mortality*, „Journal of Trauma and Acute Care Surgery” 2016, 81(1), 93–100, <https://doi.org/10.1097/ta.0000000000000999>.

- [30] Wilmink A.B.M., Samra G.S., Watson L.M. et al., *Vehicle entrapment rescue and pre-hospital trauma care*, "Injury" 1996, 21, 21–25, [https://doi.org/10.1016/0020-1383\(95\)00162-X](https://doi.org/10.1016/0020-1383(95)00162-X).
- [31] Winterberger E., Jacomet H., Zafren K. et al., *The Use of Extrication Devices in Crevasse Accidents: Official Statement of the International Commission for Mountain Emergency Medicine and the Terrestrial Rescue Commission of the International Commission for Alpine Rescue Intended for Physicians, Paramedics, and Mountain Rescuers*, "Wilderness & Environmental Medicine" 2008, 19(2), 108–110, <https://doi.org/10.1580/07-WEME-CO-1012.1>.
- [32] Pasquier M., Spichiger T., Zen-Ruffinen G. et al., *Stabilization of the Kendrick Extrication Device During Winching Air*, "Medical Journal" 2013, 32, 6, 350–351, <https://doi.org/10.1016/j.amj.2013.04.021>.
- [33] Reynard F.A., Flaris A.N., Simms E.R. et al., *Kendrick's extrication device and unstable pelvic fractures: Should a trochanteric belt be added? A cadaveric study*, "Injury" 2016, 47, 3, 711–716, <https://doi.org/10.1016/j.injury.2016.01.028>.
- [34] Paszek S., *Analiza ilościowa oraz praktyczne wykorzystanie kliniczne kamizelki Kendricka w zespołach ratownictwa medycznego na podstawie danych z Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego w latach 2017–2022*, "Anestezjologia i Ratownictwo" 2024, 18, 178–185.

SŁAWOMIR PASZEK, M.SC. – research and teaching assistant at the Department of Emergency Medicine of the Medical University of Warsaw. Instructor at the Medical Rescue Training Centre in the National Medical Rescue Monitoring Centre of LPR. Medical rescuer and medical dispatcher for many years. Member of the European Resuscitation Council.

ZOFIA CZAPLIŃSKA-PASZEK, M.D. – physician in specialty training in Anaesthesiology and Intensive Care. Graduate of the Faculty of Medicine of the Medical University of Warsaw.

MGR SŁAWOMIR PASZEK – asystent naukowo-dydaktyczny Zakładu Medycyny Ratunkowej Warszawskiego Uniwersytetu Medycznego. Instruktor Centrum Szkolenia Ratownictwa Medycznego w Krajowym Centrum Monitorowania Ratownictwa Medycznego LPR. Wieloletni Ratownik Medyczny oraz Dyspozytor Medyczny. Członek European Resuscitation Council.

LEK. ZOFIA CZAPLIŃSKA-PASZEK – lekarz w trakcie specjalizacji w Anestezjologii i Intensywnej Terapii. Absolwent Wydziału Lekarskiego Warszawskiego Uniwersytetu Medycznego.

sft.cnbop.pl

