SFT VOL. 64 ISSUE 2, 2024, PP. 84–100

Wojciech Wróblewski[a*)], Dorota Seliga[a)]

[a)] *Fire University / Akademia Pożarnicza*
[*] *Corresponding author / Autor korespondencyjny: wwroblewski@apoz.edu.pl*

Safety of Systems Integrating Fire Protection Equipment – Risks, Gaps, Recommendations

Bezpieczeństwo systemów integrujących urządzenia przeciwpożarowe – zagrożenia, luki, rekomendacje

ABSTRACT

Purpose: The purpose of this study is to identify cyber threats associated with systems integrating fire protection devices (SIUP). The analysis includes conducting a comprehensive assessment of potential attack sites (vulnerabilities) and recommendations for building designers and managers to minimise adverse actions.

Project and methods: A detailed review of the literature and cybersecurity standards applicable to fire protection systems, such as NFPA 72, was conducted, from which key points that are vulnerable elements and represent attack surfaces were identified. *The Cybersecurity for Fire Protection Systems* report from a workshop held by the Research Foundation in 2021 was analysed.

Results: Analysis of the collected research material showed that the key points of vulnerability are human factors, software, hardware, wired and wireless connections and system security. In addition, internal threats, i.e. lack of training, malicious action by employees, invasion by unknown software and too much access by security personnel to system components, are also important issues. It has been found that cybercriminals can use various techniques: denial-of- service (DoS) attacks, man-in-the-middle attacks, remote code execution and social engineering, to disrupt systems. To prevent this and minimise the risk of attacks, it is recommended that security configuration guides should be issued, that specialists should be employed and that strategies should be created to increase the resilience of systems integrating fire appliances to cyber attacks. Currently, Polish regulations are mainly based on the technical aspects of SIUP operation, i.e. the installation and operation of alarm systems. There is a lack of relevant legal regulations that directly address the issue of the network and cyber security of these systems.

Conclusions: It is necessary to urgently develop and implement comprehensive legal regulations that would take into account the specificity of the cyber security of fire protection systems in Poland. Future research should also focus on the human factor aspects of SIUP systems security.

Keywords: safety, cyber security, fire protection, system integrating fire protection devices, SIUP, fire protection device

Type of article: original scientific article

Received: 19.11.2024; Reviewed: 02.12.2024; Accepted: 05.12.2024;
Authors' ORCID IDs: W. Wróblewski – 0000-0003-3415-9485; D. Seliga – 0009-0005-1792-4474;
The authors contributed equally to this article;
Please cite as: SFT Vol. 64 Issue 2, 2024, pp. 84–100, https://doi.org/10.12845/sft.64.2.2024.6;

ABSTRAKT

Cel: Celem niniejszego badania jest identyfikacja zagrożeń cybernetycznych związanych z systemami integrującymi urządzenia przeciwpożarowe. Analiza obejmuje przeprowadzenie kompleksowej oceny potencjalnych miejsc ataku (luk) oraz rekomendacje dla projektantów i zarządców budynku służące minimalizacji działań niepożądanych.

Projekt i metody: Przeprowadzono szczegółowy przegląd literatury oraz standardów cyberbezpieczeństwa stosowanych w systemach ochrony przeciwpożarowej, np. NFPA 72. Na ich podstawie zidentyfikowano kluczowe punkty, które są elementami wrażliwymi i stanowią powierzchnię ataku. Przeanalizowano raport *Cybersecurity for Fire Protection Systems* z przeprowadzonych warsztatów zorganizowanych przez Research Foundation w 2021 roku.

Wyniki: Analiza zebranego materiału badawczego wykazała, że kluczowymi punktami podatności są: czynnik ludzki, oprogramowanie, sprzęt, połączenia przewodowe i bezprzewodowe oraz bezpieczeństwo systemowe. Ponadto istotną kwestią są też zagrożenia wewnętrzne – brak szkoleń, złośliwe działanie zatrudnionych, inwazja nieznanego oprogramowania oraz zbyt duży dostęp pracowników ochrony do elementów systemu. Stwierdzono, iż w celu zakłócenia działania systemów cyberprzestępcy mogą wykorzystać różne techniki: ataki DoS, ataki typu *man-in-the-middle*, zdalne wykonanie kodu oraz inżynierię społeczną. Aby temu zapobiec i zminimalizować ryzyko wystąpienia ataków, rekomenduje się obowiązek wydania przewodników

dotyczących konfiguracji zabezpieczeń, zatrudnienie specjalistów, utworzenie strategii mających na celu zwiększenie odporności systemów integrujących urządzenia przeciwpożarowe na cyberataki. Obecnie polskie przepisy opierają się głównie na aspektach technicznych działania SIUP, tj. montażu i eksploatacji systemów alarmowych. Brakuje odpowiednich regulacji prawnych, które bezpośrednio odnosiłyby się do kwestii zabezpieczeń sieciowych i cybernetycznych tych systemów.

Wnioski: Konieczne jest pilne opracowanie i wdrożenie kompleksowych regulacji prawnych, które uwzględniałyby specyfikę cyberbezpieczeństwa systemów ochrony przeciwpożarowej w Polsce. Takie przepisy powinny obejmować nie tylko aspekty techniczne, ale także organizacyjne i proceduralne. Regulacje te muszą być na tyle elastyczne, aby mogły nadążać za szybko zmieniającym się krajobrazem zagrożeń cybernetycznych. W ramach przyszłych badań należy także skupić się na aspektach związanych z czynnikiem ludzkim w kontekście bezpieczeństwa systemów integrujących urządzenia przeciwpożarowe.

Słowa kluczowe: bezpieczeństwo, cyberbezpieczeństwo, ochrona przeciwpożarowa, SIUP, urządzenie przeciwpożarowe

Typ artykułu: oryginalny artykuł naukowy

Przyjęty: 19.11.2024; Zrecenzowany: 02.12.2024; Zaakceptowany: 05.12.2024;
Identyfikatory ORCID autorów: W. Wróblewski – 0000-0003-3415-9485; D. Seliga – 0009-0005-1792-4474;
Autorzy wnieśli równy wkład merytoryczny w powstanie artykułu;
Proszę cytować: SFT Vol. 64 Issue 2, 2024, pp. 84–100, https://doi.org/10.12845/sft.64.2.2024.6;

Introduction

Today's fire protection systems, with advances in technology, have moved from traditional, isolated installations to complex, digitally integrated networks. Increasingly, fire systems and building control systems (BCS) are being combined into a single, integrated whole, allowing them to be monitored and managed in real time. This integration allows data to be exchanged between the various components, enabling them to interact with each other, and automating tasks and creating synergies [1].

This way of managing systems increases the effectiveness of emergency response and enables system functions to be dynamically adapted to changing site conditions.

According to CNBOP-PIB guidelines, a system integrating fire protection devices (referred to as SIUP) is a "tool supporting the control and operation of fire safety systems used in a building. By presenting the collected data in a clear and intuitive manner, it allows supervision of the status and interaction of individual components of the integrated systems and supports the work of the operator in making decisions with their implementation by manually triggering the execution of specific actions" [2].

In Poland, the technical guidelines and standards governing the installation, operation and interoperability of such systems are of key importance for SIUP. Detailed normative documents applicable to these systems in Poland are presented below [2]:

- CNBOP-PIB *Guidelines for the design, installation, commissioning, operation and maintenance of systems integrating fire protection equipment* W-0007:2024 (2nd extended edition, November 2024) SITP WP-05:2024 [3];
- *Design Guidelines for Fire Prevention Equipment Rooms and Service Areas in Buildings. Location, Performance Conditions, Equipment* CNBOP-PIB W-0001:2014 Issue 3 Extended, December 2023 [4];
- National Technical Assessments;
- NFPA 4 – *Standard for Integrated Fire Protection and Life Safety System Testing* [5];
- EN 54-13: *Fire detection and fire alarm systems – Part 13:*

Wprowadzenie

Współczesne systemy ochrony przeciwpożarowej, wraz z rozwojem technologii, przeszły przemianę od tradycyjnych, odizolowanych instalacji do złożonych, cyfrowo zintegrowanych sieci. Coraz częściej systemy pożarowe oraz systemy zarządzania budynkiem (ang. *building control systems*, BCS) są łączone w jedną, zintegrowaną całość, co pozwala na monitorowanie i zarządzanie nimi w czasie rzeczywistym. Dzięki tej integracji zachodzi wymiana danych między różnymi komponentami, umożliwiająca ich wzajemną interakcję, automatyzację zadań oraz uzyskanie efektu synergii [1].

Taki sposób zarządzania systemami zwiększa skuteczność reakcji na sytuacje awaryjne i stwarza możliwość dynamicznego dostosowywania funkcji systemów w zależności od zmieniających się warunków w obiekcie.

Zgodnie z wytycznymi CNBOP-PIB system integrujący urządzenia przeciwpożarowe (SIUP) stanowi „narzędzie wspomagające kontrolę i obsługę zastosowanych w obiekcie budowlanym systemów bezpieczeństwa pożarowego. Poprzez przedstawienie zgromadzonych danych w sposób czytelny i intuicyjny pozwala na nadzór stanu i interakcji poszczególnych komponentów integrowanych systemów oraz wspomaga pracę operatora w podejmowaniu decyzji wraz z ich wdrożeniem poprzez ręczne wywołanie realizacji określonych działań" [2].

W Polsce kluczowe znaczenie dla SIUP mają wytyczne i normy techniczne regulujące kwestie ich instalacji, obsługi oraz współdziałania. Poniżej przedstawiono szczegółowe dokumenty normatywne obowiązujące dla tych systemów w Polsce [2]:

- *Wytyczne projektowania, instalowania, uruchamiania, obsługi i konserwacji systemów integrujących urządzenia przeciwpożarowe* CNBOP-PIB W-0007:2024 (wyd. 2 rozszerzone, listopad 2024) SITP WP-05:2024 [3];
- *Wytyczne Projektowania Pomieszczenia i Miejsca Obsługi Urządzeń Przeciwpożarowych w Budynkach. Lokalizacja, Warunki Wykonania, Wyposażenie* CNBOP-PIB W-0001:2014, wydanie 3 rozszerzone, grudzień 2023 [4];

Compatibility and connectability assessment of system components [6]:
- equipment according to PN-EN 54 (type 1 components),
- external equipment (type 2 components).

On the other hand, the SIUP is also subject to certification, which is defined by regulations relating to construction products, such as Regulation CPR 305/2011 (EU) as well as fire protection regulations, i.e. the Act of 24 August 1991 on fire protection, Polish Journal of Laws 2024, item 275, 1222 [7].

The Regulation of the Minister of Internal Affairs and Administration of 7 June 2010 on fire protection of buildings, other buildings and grounds (Journal of Laws No. 109, item 719 of 22.06.2010) [8] provides a detailed definition of fire protection equipment. In accordance with § 2 para. 1 they are defined as "devices (fixed or semi-permanent, manually or automatically operated) serving to prevent, detect and fight a fire or to limit its effects, in particular: fixed and semi-permanent firefighting and safety devices, inerting devices, devices forming part of the voice alarm system and the fire alarm system, including signalling and alarm devices, fire alarm receiving devices and damage signal receiving devices, evacuation lighting systems, internal hydrants and hydrant valves, external hydrants, pumps in fire pumping stations, fire shut-off dampers, smoke extraction devices, explosion prevention and mitigation devices, smoke curtains and doors, and fire gates and other fire closures, if equipped with control systems, fire electric switches and lifts for rescue teams". Thus, the SIUP links together various systems and equipment (see Figure 1), such as the:
- fire alarm and extinguishing control system: detection of danger and automatic initiation of action, e.g. activation of extinguishing equipment,
- fixed firefighting systems – integration of fixed firefighting systems,
- control system for domestic and fire ventilation dampers – control of ventilation dampers, smoke extraction,
- emergency lighting – to support evacuation by adjusting lighting levels in the building,
- gas detection system – monitoring the level of dangerous gases in the premises,
- access control system – managing access to selected areas of the facility, restricting it to authorised persons
- video surveillance system (VSS/CCTV): visual monitoring of the building.

- Krajowe Oceny Techniczne;
- NFPA 4 – Standard for Integrated Fire Protection and Life Safety System Testing [5];
- PN-EN 54-13: Systemy sygnalizacji pożarowej – Część 13: Ocena kompatybilności możliwości przyłączenia podzespołów systemu [6]:
  - urządzenia zgodne z PN-EN 54 (podzespoły typu 1),
  - urządzenia zewnętrzne (podzespoły typu 2).

Z drugiej strony SIUP obowiązuje też certyfikacja, którą określają przepisy odnoszące się do wyrobów budowlanych, takie jak Rozporządzenie CPR 305/2011 (UE), a także przepisy z zakresu ochrony przeciwpożarowej, tj. ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. 2024, poz. 275, 1222) [7].

W rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz. U. 2020 Nr 109, poz. 719) [8] zawarto szczegółową definicję urządzeń przeciwpożarowych. Zgodnie z § 2 ust. 1 definiuje się je jako „urządzenia (stałe lub półstałe, uruchamiane ręcznie lub samoczynnie) służące do zapobiegania powstaniu, wykrywania, i zwalczania pożaru lub ograniczania jego skutków, a w szczególności: stałe i półstałe urządzenia gaśnicze i zabezpieczające, urządzenia inertyzujące, urządzenia wchodzące w skład dźwiękowego systemu ostrzegawczego i systemu sygnalizacji pożarowej, w tym urządzenia sygnalizacyjno-alarmowe, urządzenia odbiorcze alarmów pożarowych i urządzenia odbiorcze sygnałów uszkodzeniowych, instalacje oświetlenia ewakuacyjnego, hydranty wewnętrzne i zawory hydrantowe, hydranty zewnętrzne, pompy w pompowniach przeciwpożarowych, przeciwpożarowe klapy odcinające, urządzenia oddymiające, urządzenia zabezpieczające przed powstaniem wybuchu i ograniczające jego skutki, kurtyny dymowe oraz drzwi, i bramy przeciwpożarowe i inne zamknięcia przeciwpożarowe, jeżeli są wyposażone w systemy sterowania, przeciwpożarowe wyłączniki prądu oraz dźwigi dla ekip ratowniczych". Zatem SIUP łączy ze sobą różne systemy i urządzenia (zob. ryc. 1), takie jak:
- system sygnalizacji pożarowej i sterowania gaszeniem: detekcja zagrożenia i automatyczne inicjowanie działania np. uruchamianie urządzeń gaśniczych,
- stałe urządzenia gaśnicze: integracja stałych systemów gaśniczych,
- system sterowania klapami wentylacji bytowej i pożarowej: kontrola klap wentylacyjnych, odprowadzenie dymu,
- oświetlenie awaryjne: wsparcie ewakuacji poprzez dostosowanie poziomu oświetlenia w budynku,
- system detekcji gazów: monitorowanie poziomu niebezpiecznych gazów w pomieszczeniach,
- system kontroli dostępu: zarządzanie dostępem do wybranych stref obiektu, ograniczając go dla osób nieupoważnionych,
- system nadzoru wizyjnego (VSS/CCTV): monitorowanie wizualne budynku.

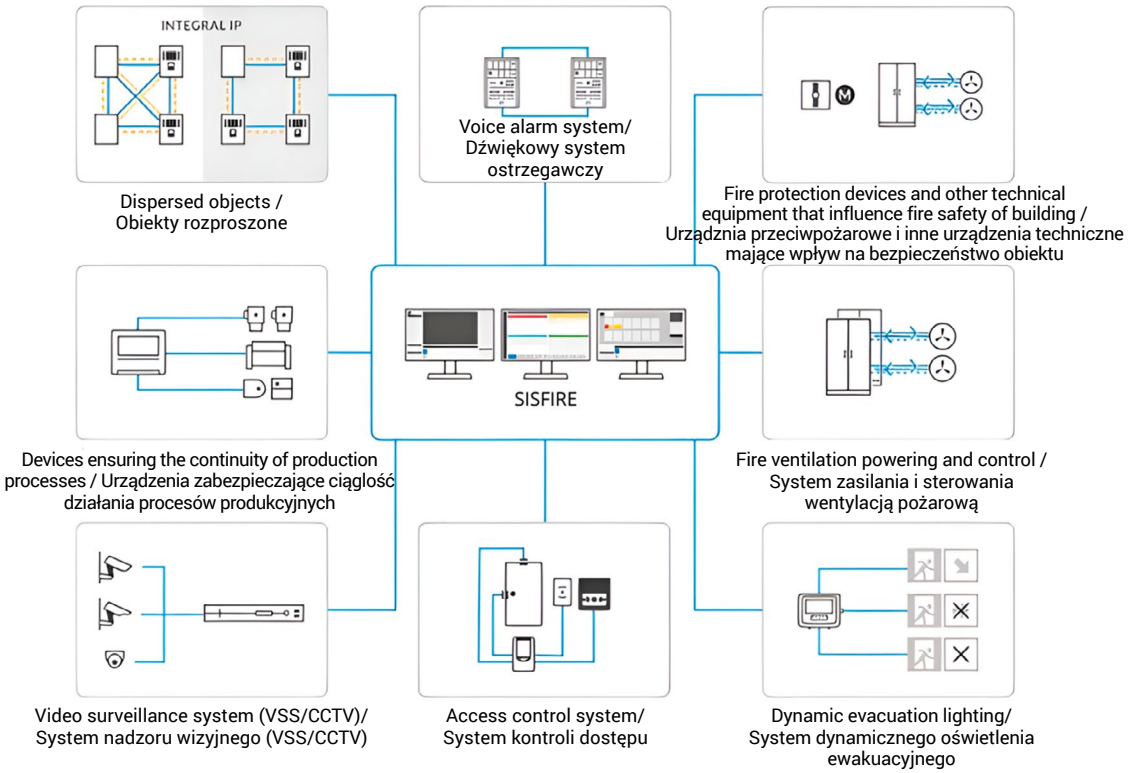

Figure 1. Schematic diagram of the SIS-FIRE fire appliance integration system from manufacturer Schrack Seconet showing interaction with external systems
Rycina 1. Schemat ideowy systemu integrującego urządzenia przeciwpożarowe SIS-FIRE producenta Schrack Seconet przedstawiający współdziałanie z systemami zewnętrznymi
Source / Źródło: K. Kunecki, *Zintegrowany system bezpieczeństwa pożarowego* [2].

An SIUP is an installation enabling [9]:
- manual and automatic control of firefighting equipment and systems,
- verification of the fire alarm signal by other security systems,
- monitoring of the operational status of equipment.

In addition, an SIUP enables the integration of other systems that, although not formally recognised as fire safety systems, affect the level of safety of the facility and its occupants.

The level of safety is also influenced by hardware reliability, which plays a key role in functional safety systems, as required by EN IEC 61508 and sector standards. The safety integrity levels (SIL) defined in the standard specify the requirements for hardware reliability, including the probability of failure on demand and the level of system diagnostics. By implementing redundancy, self-monitoring and real-time failure monitoring mechanisms, the risk of safety-critical failures can be minimised. In the case of SIUP, meeting these requirements directly affects the effectiveness of fire threat detection and response, ensuring high reliability and compliance with applicable standards and regulations.

SIUP stanowi instalację pozwalającą na [9]:
- ręczne i automatyczne sterowanie urządzeniami i systemami przeciwpożarowymi,
- weryfikację sygnału alarmu pożarowego przy pomocy innych systemów bezpieczeństwa,
- monitorowanie stanu pracy urządzeń.

Dodatkowo SIUP umożliwia integrację innych systemów, które – mimo że nie są formalnie uznawane za systemy bezpieczeństwa pożarowego – wpływają na poziom bezpieczeństwa obiektu i osób w nim przebywających.

Na poziom bezpieczeństwa wpływa również niezawodność sprzętowa, która odgrywa kluczową rolę w systemach funkcjonalnego bezpieczeństwa, zgodnie z wymaganiami normy PN-EN IEC 61508 oraz norm sektorowych. Określone w normie poziomy nienaruszalności bezpieczeństwa (ang. *safety integrity level*, SIL) precyzują wymagania dotyczące niezawodności sprzętu, w tym prawdopodobieństwa awarii na żądanie oraz poziomu diagnostyki systemu. Implementacja mechanizmów redundancji, samokontroli i monitorowania awarii w czasie rzeczywistym pozwala na minimalizację ryzyka uszkodzeń krytycznych dla bezpieczeństwa. W przypadku SIUP spełnienie tych wymagań bezpośrednio wpływa na skuteczność detekcji oraz reakcji na zagrożenia pożarowe, zapewniając wysoką niezawodność i zgodność z obowiązującymi normami i przepisami.

Increased integration risks

In integrated building systems, each subsystem, such as firefighting equipment, has dedicated operating algorithms that process inputs and generate output signals to other systems. For example, the fire alarm system (FAS) receives information from various sensors (smoke, temperature, flame, etc.) and then sends signals to the firefighting equipment, the VAS (voice alarm system) and other systems that manage the operation of the building.

The lighting system, in turn, is controlled by light intensity sensors that provide an uninterrupted signal to the energy management and lighting control systems. Due to the technological diversity, information processing requires different algorithms and local processing units. These algorithms can relate to fire protection, general security (such as intrusion monitoring), comfort provision and equipment diagnostics, among other things [1].

However, such systems may be integrated with external networks. The risk of accessing the public Internet then arises. Such a connection increases the risk of cyber threats, which can result in serious consequences, such as the disruption of key life and property protection systems.

Overview of research to date

The topic of cyberterrorism in systems integrating fire protection devices is relatively new and little researched. The lack of extensive literature on the subject reflects its novelty in the field of cyber security.

As a result of digital transformation, cyber attacks aimed at stealing data or disrupting key services are on the rise. A study on the Shodan.io platform (a search engine for Internet-connected devices) found 43,500 building management systems (BCS) vulnerable to cyber threats. Similarly, fire protection systems that were previously less vulnerable to attacks are becoming increasingly exposed to cyber threats through connections to BCSs, IoT and other publicly available platforms [10].

To address these challenges, 16 NFPA standards, including NFPA 72 [11] (National Fire Alarm and Signaling Code®), incorporate cyber security guidelines covering hardware, software, data paths and physical protection of systems. The latest edition introduces security levels (SL1–SL3) tailored to the severity of cyber threats. Despite the introduction of these guidelines, knowledge of system vulnerabilities remains limited.

Research to date on cyber security in the context of fire protection systems indicates a lack of comprehensive analyses of the risks posed by their complex integration into systems [12]. While component-specific security guidelines exist (NFPA 72, UL 2572), there is a lack of consistent standards that take into account the specifics of fire protection systems and their connection to external networks.

To bridge this gap, the Fire Protection Research Foundation, an NFPA affiliate, has launched a study on cyber vulnerabilities in fire protection systems. The report, sponsored by ASHE, Procter and Gamble and Telgian, offers an overview of the standards, assesses vulnerabilities and risks, and provides strategies for mitigation.

Wzrost ryzyka związanego z integracją

W zintegrowanych systemach budynkowych każdy podsystem (np. urządzenia gaśnicze) posiada dedykowane algorytmy działania, które przetwarzają dane wejściowe i generują sygnały wyjściowe do innych systemów. Na przykład, system sygnalizacji pożarowej (SSP) odbiera informacje z różnych czujników (dymu, temperatury, płomienia itp.), a następnie przesyła sygnały do urządzeń gaśniczych, systemu DSO (dźwiękowych systemów ostrzegawczych) oraz innych systemów zarządzających funkcjonowaniem budynku.

Z kolei system oświetleniowy jest kontrolowany przez sensory natężenia światła, które dostarczają nieprzerwany sygnał do systemów zarządzania energią i sterowania oświetleniem. Ze względu na zróżnicowanie technologiczne przetwarzanie informacji wymaga stosowania różnych algorytmów i lokalnych jednostek przetwarzających. Algorytmy te mogą dotyczyć m.in. ochrony przeciwpożarowej, bezpieczeństwa ogólnego (jak monitorowanie włamań), zapewnienia komfortu użytkownikom obiektu oraz diagnostyki urządzeń [1].

Powyższe systemy mogą być zintegrowane z zewnętrznymi sieciami. Pojawia się wtedy ryzyko związane z dostępem do publicznego Internetu. Takie połączenie zwiększa ryzyko zagrożeń cybernetycznych, co może skutkować poważnymi konsekwencjami, takimi jak zakłócenia pracy kluczowych systemów ochrony życia i mienia.

Przegląd dotychczasowych badań

Temat cyberterroryzmu w systemach integrujących urządzenia przeciwpożarowe jest stosunkowo nowy i mało zbadany. Stan ten zdaje się potwierdzać brak obszernej literatury przedmiotu.

W wyniku transformacji cyfrowej rośnie liczba cyberataków mających na celu kradzież danych lub zakłócenie kluczowych usług. Badanie na platformie Shodan.io (wyszukiwarka dla urządzeń podłączonych do Internetu) wykazało obecność 43,5 tys. systemów zarządzania budynkiem (BCS) narażonych na cyberzagrożenia. Podobnie, systemy ochrony przeciwpożarowej, które wcześniej były mniej podatne na ataki, stają się coraz bardziej narażone na cyberzagrożenia przez połączenia z systemami BCS, IoT i innymi publicznie dostępnymi platformami [10].

Aby sprostać opisanym wyżej wyzwaniom, 16 norm NFPA, w tym NFPA 72 [11] (ang. *National Fire Alarm and Signaling Code®*), uwzględnia wytyczne dotyczące zabezpieczeń cybernetycznych, obejmujące sprzęt, oprogramowanie, ścieżki transmisji danych oraz fizyczną ochronę systemów. W najnowszej edycji wprowadzono poziomy zabezpieczeń (SL1–SL3) dostosowane do stopnia zagrożeń cybernetycznych. Mimo powstania tych wytycznych, wiedza na temat słabości systemów pozostaje ograniczona.

Dotychczasowe badania nad cyberbezpieczeństwem w kontekście systemów ochrony przeciwpożarowej wskazują na brak kompleksowych analiz zagrożeń wynikających z ich złożonej integracji z systemami [12]. Choć istnieją wytyczne dotyczące bezpieczeństwa dla poszczególnych komponentów (NFPA 72, UL 2572), nie ma spójnych standardów uwzględniających specyfikę systemów przeciwpożarowych i ich połączenia z zewnętrznymi sieciami.

W celu zapełnienia tej luki Fire Protection Research Foundation, afiliat NFPA, rozpoczął badanie nad podatnością systemów przeciwpożarowych na zagrożenia cybernetyczne. Raport,

Purpose of the article

The purpose of this article is to analyse the security of systems integrating fire protection equipment, including the identification of threats and security gaps in these systems, and to develop recommendations for increasing the level of protection of these systems against terrorist attacks.

To achieve the above objective, it is necessary to find answers to the following research problems:

- What are the most common threats to systems integrating fire appliances in terms of reliability and cyber security?
- What security gaps can be identified in existing systems integrating fire protection equipment?
- What recommendations can be made to strengthen the protection of these systems against cyber attacks?

Methodology

The research methodology of this study is based on a comprehensive survey of the literature, existing standards and available reports on the cyber security of systems integrating fire protection devices (SIUP).

Document analysis and literature review methods were used to identify threats and vulnerabilities in these systems, as well as to compare current standards to determine the most effective security practices.

Fire alarm systems are considered fundamental building safety systems, reducing the likelihood of injury and loss of life, and limiting damage caused by fire, smoke and heat [13].

Design and installation must be carried out by qualified professionals who are certified and comply with the specific regulations and standards set out by the aforementioned organisations. Increasingly, fire alarm systems are being integrated with other building automation solutions and security systems to help minimise the effects of fire by facilitating evacuation and preventing the spread of fire [13].

Current research, however, does not encompass complete safety assessments of integrated fire protection systems. It mainly focuses on the development of more advanced and reliable solutions, such as automatic fire alarm systems using cyber-physical technologies that use various sensors to collect physical data and use them to control this system [14], the use of microcontrollers to monitor and remotely control fire protection components in nuclear power plants [15], and the development of intelligent fire detection systems, for educational facilities, that integrate a variety of sensors and communication technologies [16].

Although these studies show efforts to improve fire protection systems through integration and advanced technologies, the current state of knowledge does not provide a comprehensive safety assessment for fully integrated systems.

sponsorowany przez ASHE, Procter and Gamble oraz Telgian, zawiera przegląd norm, ocenę podatności i zagrożeń oraz strategie ich łagodzenia.

Cel artykułu

Celem artykułu jest analiza bezpieczeństwa systemów integrujących urządzenia przeciwpożarowe, z uwzględnieniem identyfikacji zagrożeń oraz luk w zabezpieczeniach tych systemów, a także opracowanie rekomendacji dotyczących zwiększenia poziomu ochrony tychże systemów przed atakami terrorystycznymi.

Aby osiągnąć powyższy cel, konieczne jest znalezienie odpowiedzi na następujące problemy badawcze:

- Jakie zagrożenia dla systemów integrujących urządzenia przeciwpożarowe w kontekście ich niezawodności i cyberbezpieczeństwa występują najczęściej?
- Jakie luki w zabezpieczeniach można zidentyfikować w istniejących systemach integrujących urządzenia przeciwpożarowe?
- Jakie rekomendacje można opracować w celu wzmocnienia ochrony tych systemów przed cyberatakami?

Metodologia

Metodologia badań niniejszego opracowania opiera się na kompleksowym przeglądzie literatury, istniejących standardów i dostępnych raportów dotyczących cyberbezpieczeństwa systemów integrujących urządzenia przeciwpożarowe.

Metody analizy dokumentów i literatury zostały wykorzystane do identyfikacji zagrożeń i słabych punktów w tych systemach, a także do porównania obecnych standardów w celu określenia najbardziej skutecznych praktyk bezpieczeństwa.

Systemy sygnalizacji pożaru są uważane za fundamentalne systemy bezpieczeństwa w budynkach, zmniejszające prawdopodobieństwo obrażeń, utraty życia i ograniczające szkody spowodowane przez ogień, dym i ciepło [13].

Projektowanie i czynności instalacyjne muszą być wykonywane przez wykwalifikowanych specjalistów, którzy posiadają odpowiednie certyfikaty. Powinny być zrealizowane zgodnie ze szczegółowymi przepisami i normami określonymi przez przywołane wcześniej organizacje. Coraz częściej systemy sygnalizacji pożaru są zintegrowane z innymi rozwiązaniami automatyki budynkowej i systemami bezpieczeństwa, co sprzyja minimalizowaniu skutków pożaru poprzez ułatwienie ewakuacji i zapobieganie rozprzestrzenianiu się ognia [13].

Aktualne badania nie przedstawiają jednak pełnych ocen bezpieczeństwa zintegrowanych systemów ochrony przeciwpożarowej. Skupiają się głównie na rozwijaniu bardziej zaawansowanych i niezawodnych rozwiązań, takich jak automatyczne systemy sygnalizacji pożaru wykorzystujące technologie cyber-fizyczne, które zbierają dane fizyczne za pomocą różnych czujek i używają ich do sterowania tym systemem [14]. Powstają również opracowania poświęcone zastosowaniu mikrokontrolerów do monitorowania i zdalnego sterowania komponentami ochrony przeciwpożarowej w elektrowniach jądrowych [15], a także rozwojowi inteligentnych systemów wykrywania pożaru dla obiektów

Literature review and analysis of standards

The method used is to review existing norms, guidelines and standards for the cyber security of fire systems, particularly those that have been integrated with building management systems (BCS).

The analysis included the following documents:

- NFPA 72 – National Fire Alarm and Signaling Code – a key standard for alarm systems, including fire alarm systems. It provides guidance on cyber security, including hardware, software and physical security requirements [11].
- NIST 800-82 – Guide to Industrial Control Systems (ICS) Security – guidelines for protecting industrial control systems, which includes fire systems. This standard provides security strategies for IT/OT networked systems, which are key to protecting SIUP [17].
- UL 2900-2-3 – Standard for Software Cybersecurity for Network-Connectable Products – Life Safety and Signaling Systems – standards for software security and network device security [18].

Analysis of research reports

The method involved analysing published reports, in particular research by the Fire Protection Research Foundation (FPRF) and other industry organisations that provide data on cyber threats to SIUP systems.

Based on the report *Cybersecurity for Fire Protection Systems* [12] the main risks associated with the integration of fire systems with external systems and potential security vulnerabilities that can be exploited by cybercriminals are identified. The document also includes the results of a workshop with industry experts, where the main risks were identified and appropriate strategies were proposed.

Results

Identification of risks

In order to understand the safety of systems integrating fire protection devices (SIUP), it is crucial to define the term hazard precisely. A threat refers to a situation or factor that has the potential to cause undesirable or negative events. In cyber security, a threat represents a potential danger to the digital infrastructure. Such incidents pose a serious risk to an organisation, potentially leading to financial and reputational losses [19].

edukacyjnych, które integrują różnorodne czujniki i technologie komunikacyjne [16].

Chociaż wspomniane badania pokazują wysiłki na rzecz ulepszania systemów ochrony przeciwpożarowej poprzez integrację i zaawansowane technologie, obecny stan wiedzy nie zapewnia wszechstronnej oceny bezpieczeństwa dla w pełni zintegrowanych systemów.

Przegląd literatury i analiza norm

Zastosowana metoda polega na przeglądzie istniejących norm, wytycznych i standardów dotyczących cyberbezpieczeństwa systemów pożarowych, w szczególności tych, które zostały zintegrowane z systemami zarządzania budynkiem (BCS).

Analiza obejmowała następujące dokumenty:

- NFPA 72 – National Fire Alarm and Signaling Code – kluczowy standard dotyczący systemów alarmowych, w tym systemów sygnalizacji pożaru. Zawiera wytyczne dotyczące cyberbezpieczeństwa, w tym wymogi zabezpieczeń sprzętowych, programowych i fizycznych [11].
- NIST 800-82 – Guide to Industrial Control Systems (ICS) Security – wytyczne dotyczące ochrony systemów sterowania przemysłowego, co obejmuje również systemy pożarowe. Standard ten zawiera strategie zabezpieczeń dla systemów podłączonych do sieci IT/OT, które są kluczowe dla ochrony SIUP [17].
- UL 2900-2-3 – Standard for Software Cybersecurity for Network-Connectable Products – Life Safety and Signaling Systems – standardy zabezpieczenia oprogramowania i bezpieczeństwa urządzeń sieciowych [18].

Analiza raportów badawczych

Metoda ta obejmowała analizę opublikowanych raportów, w szczególności badań prowadzonych przez Fire Protection Research Foundation (FPRF), oraz inne organizacje branżowe, które dostarczają danych na temat cyberzagrożeń w systemach SIUP.

Na podstawie raportu pt. *Cybersecurity for Fire Protection Systems* [12] zidentyfikowano główne zagrożenia związane z integracją systemów pożarowych z systemami zewnętrznymi oraz potencjalne luki w zabezpieczeniach, które mogą być wykorzystane przez cyberprzestępców. Dokument ten zawiera również wyniki warsztatów przeprowadzonych z udziałem ekspertów branżowych, gdzie zidentyfikowano główne zagrożenia i zaproponowano odpowiednie strategie.

Wyniki

Identyfikacja zagrożeń

W celu zrozumienia bezpieczeństwa systemów integrujących urządzenia przeciwpożarowe kluczowe jest precyzyjne zdefiniowanie pojęcia „zagrożenie". Zagrożenie oznacza sytuację lub czynnik, który potencjalnie może wywołać zdarzenia niepożądane lub negatywne. W cyberbezpieczeństwie zagrożenie stanowi potencjalne niebezpieczeństwo dla infrastruktury cyfrowej. Takie incydenty stanowią poważne ryzyko dla organizacji, w postaci możliwych strat finansowych i utraty reputacji [19].

The network perimeter is a key element of the infrastructure, encompassing all points where the fire alarm system connects to other networks or systems and exchanges data with external devices. Connection points (system interfaces, connection points) are particularly vulnerable to attacks and are often a strategic target for malicious activity.

The first document, NFPA 72, is a standard that sets out guidelines for the design, installation, testing, maintenance and operation of fire alarm and alarm communication systems. It considers fire detection technologies, integration with building automation and procedures for regular testing and maintenance of systems.

In the 2022 edition, the scope has been expanded to include guidance on cyber security and remote access to systems. In the 2025 edition, Chapter 11 has been supplemented with specific requirements for the protection of fire alarm systems against cyber attacks, introducing three levels of protection [11]:

- SL1: for wired interfaces not using the Internet Protocol,
- SL2: for wireless interfaces not using the Internet Protocol and for wired and wireless Internet interfaces not connected to publicly accessible networks,
- SL3: for wired and wireless Internet interfaces connected to publicly accessible networks.

The second standard is UL 2900-2-3 on Software Cybersecurity for Networked Products – Part 2–3: *Detailed Requirements for Security Signaling and Life Safety Systems*, is a standard developed by Underwriters Laboratories (UL). The document defines tests, such as vulnerability analysis, penetration testing and risk assessment, to detect and address weaknesses in software and hardware. The standard covers three levels of security, from basic (L1) to advanced (L3), taking into account security management processes and the product lifecycle. It is a key element for manufacturers seeking to ensure their systems are highly resilient to cyber threats [18].

The most recent document is NIST Special Publication 800-82 Revision 3, *Guide to Operational Technology (OT) Security*, and provides detailed guidance on protecting operational technology (OT) such as industrial control systems, building automation and transportation. It extends coverage to OT in the broadest sense, including devices and physical systems connected to networks, taking into account current threats and vulnerabilities. It includes specific security profiles tailored to different levels of risk and integrates requirements from NIST SP 800-53 Rev. 5. The main objectives of the publication are to secure OT systems against cyber attacks, reduce operational risk and ensure business continuity in critical infrastructures [17].

The final report of the 2021 study distinguishes key cyber vulnerabilities of integrated systems, which includes six elements (see Figure 2):

Obwód sieci stanowi kluczowy element infrastruktury, obejmujący wszelkie punkty, w których system sygnalizacji pożaru łączy się z innymi sieciami lub systemami oraz wymienia dane z zewnętrznymi urządzeniami. Miejsca połączeń (interfejsy systemowe, punkty połączenia) cechują się szczególną podatnością na ataki i często stanowią strategiczny cel działań niepożądanych.

Pierwszy dokument – NFPA 72 – to standard określający wytyczne dotyczące projektowania, instalacji, testowania, konserwacji i eksploatacji systemów sygnalizacji pożarowej oraz komunikacji alarmowej. Uwzględnia technologie detekcji pożaru, integrację z automatyką budynkową, a także procedury regularnego testowania i utrzymania systemów.

W edycji z 2022 r. rozszerzono zakres o wytyczne dotyczące cyberbezpieczeństwa oraz zdalnego dostępu do systemów. W edycji z 2025 r. rozdział 11 uzupełniono o konkretne wymagania dotyczące ochrony systemów sygnalizacji pożarowej przed atakami cybernetycznymi, wprowadzając trzy poziomy zabezpieczeń [11]:

- SL1: dla przewodowych interfejsów niekorzystających z protokołu internetowego,
- SL2: dla bezprzewodowych interfejsów niekorzystających z protokołu internetowego oraz dla przewodowych i bezprzewodowych interfejsów internetowych niepołączonych z publicznie dostępnymi sieciami,
- SL3: dla przewodowych i bezprzewodowych interfejsów internetowych połączonych z publicznie dostępnymi sieciami.

Drugi standard – UL 2900-2-3 – dotyczy cyberbezpieczeństwa oprogramowania dla produktów podłączonych do sieci. Część 2–3: *Szczegółowe wymagania dla systemów sygnalizacji bezpieczeństwa i ochrony życia* to norma opracowana przez Underwriters Laboratories (UL). Dokument definiuje testy, takie jak analiza podatności, testy penetracyjne i ocena ryzyka, mające na celu wykrycie i eliminację słabości w oprogramowaniu i sprzęcie. Standard obejmuje trzy poziomy zabezpieczeń, od podstawowego (L1) do zaawansowanego (L3), z uwzględnieniem procesów zarządzania bezpieczeństwem i cyklu życia produktów. Jest kluczowym elementem dla producentów dążących do zapewnienia wysokiej odporności swoich systemów na zagrożenia cybernetyczne [18].

Ostatnim dokumentem jest NIST Special Publication 800-82 Revision 3, *Guide to Operational Technology (OT) Security*, który dostarcza szczegółowych wytycznych dotyczących ochrony technologii operacyjnych (OT), takich jak systemy sterowania przemysłowego, automatyka budynkowa i transport. Rozszerza zakres na szeroko pojęte OT, w tym urządzenia i systemy fizyczne połączone z sieciami, uwzględniając aktualne zagrożenia i podatności. Zawiera konkretne profile bezpieczeństwa dostosowane do różnych poziomów ryzyka oraz integruje wymagania z NIST SP 800-53 Rev. 5. Główne cele publikacji to zabezpieczenie systemów OT przed cyberatakami, redukcja ryzyka operacyjnego i zapewnienie ciągłości działania w krytycznych infrastrukturach [17].

W raporcie końcowym badań z 2021 r. wyróżnia się kluczowe podatności cybernetyczne systemów zintegrowanych, które obejmują sześć elementów (zob. ryc. 2).

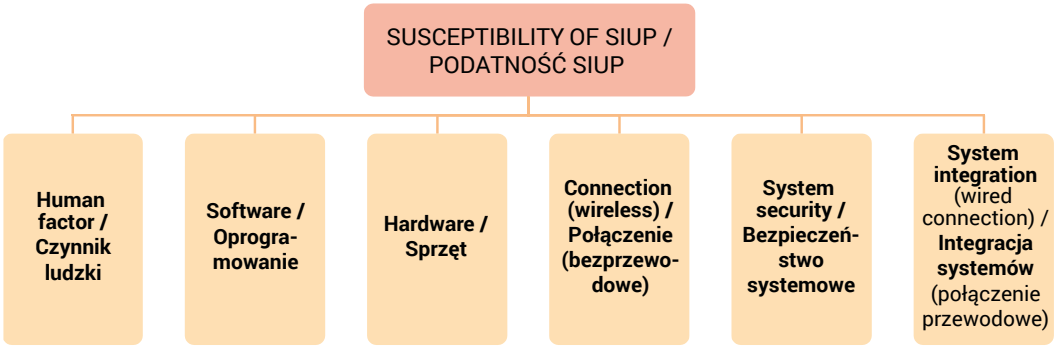

Figure 2. Vulnerable elements of systems integrating fire protection (SIUP)
Rycina 2. Elementy SIUP podatne na zagrożenia
Source: Own elaboration based on [17].
Źródło: Opracowanie własne na podstawie [17].

When it comes to the human element, the reliability of suppliers and technicians responsible for installing and maintaining systems is important. Failure to control access to systems, as well as the potential creation of "backdoors" by technicians or manufacturers, are significant risks. Additionally, the failure to change default passwords and the risk of malicious actions by rogue individuals (e.g. industrial espionage) increases the vulnerability of systems to unauthorised access and manipulation. As required by the NIS 2 Directive, key entities, including suppliers, should implement cyber security risk management mechanisms, including access control, supplier verification and elimination of default passwords. The directive emphasises multi-component authentication, regular audits and incident reporting to minimise the risk of malicious activity [26].

The software of fire protection systems also shows numerous vulnerabilities. Unchanged standard passwords and infrequent updates make these systems more vulnerable to attacks. A lack of adequate updates results in security vulnerabilities being left behind, which can be exploited by cybercriminals to take control of the system or disrupt its operation.

In the context of equipment, mobile devices that lack adequate physical security while accessing building management systems (BMS) or other systems are a significant problem. An additional risk factor is the failure to keep fire protection equipment up to date with the latest security features, which increases its vulnerability to cyberattacks.

Wireless connections represent another source of risk. Remote access codes allowing intervention in the system, such as in remote maintenance functions, can be intercepted by unauthorised persons. Furthermore, the connection of systems to open or unsecured networks, set up by technicians without proper IT oversight, creates the possibility of unauthorised access. Additionally, failure to update embedded software (e.g. in radio systems) can lead to network security breaches.

System security is vulnerable to security misconfigurations, which can result in open access to unauthorised individuals. In addition, these systems are susceptible to denial-of-service (DoS) attacks, which can disrupt their normal operation by overloading the network or blocking access.

Jeśli chodzi o element ludzki, istotne znaczenie ma wiarygodność dostawców oraz techników odpowiedzialnych za instalację i konserwację systemów. Niedopatrzenia w zakresie kontroli dostępu do systemów, a także potencjalne tworzenie „tylnych drzwi" przez techników lub producentów stanowią istotne zagrożenie. Dodatkowo, brak zmiany domyślnych haseł oraz ryzyko szkodliwych działań ze strony nieuczciwych osób (np. szpiegostwo przemysłowe) zwiększa podatność systemów na nieautoryzowany dostęp i manipulacje. Zgodnie z wymogami dyrektywy NIS2, podmioty kluczowe, w tym dostawcy, powinny wdrożyć mechanizmy zarządzania ryzykiem cyberbezpieczeństwa, obejmujące kontrolę dostępu, weryfikację dostawców oraz eliminację domyślnych haseł. Dyrektywa kładzie nacisk na wieloskładnikowe uwierzytelnianie, regularne audyty i zgłaszanie incydentów, aby minimalizować ryzyko działań szkodliwych [26].

Oprogramowanie systemów ochrony przeciwpożarowej również wykazuje liczne podatności. Niezmieniane standardowe hasła, rzadkie aktualizacje sprawiają, że systemy te są bardziej narażone na ataki. Brak odpowiednich aktualizacji skutkuje pozostawieniem luk bezpieczeństwa, które mogą być wykorzystane przez cyberprzestępców do przejęcia kontroli nad systemem lub zakłócenia jego funkcjonowania.

W kontekście sprzętu, istotnym problemem są urządzenia przenośne, które nie posiadają odpowiednich zabezpieczeń fizycznych i jednocześnie mają dostęp do systemów zarządzania budynkiem (BMS) lub innych systemów. Dodatkowym czynnikiem ryzyka jest brak bieżącej aktualizacji sprzętu ochrony przeciwpożarowej o najnowsze zabezpieczenia, co zwiększa jego podatność na ataki cybernetyczne.

Połączenia bezprzewodowe stanowią kolejne źródło zagrożeń. Zdalne kody dostępu umożliwiające interwencję w systemie (np. w zdalnych funkcjach konserwacji) mogą zostać przejęte przez osoby niepowołane. Ponadto, połączenie systemów z otwartymi lub niesekwestrowanymi sieciami, instalowanymi przez techników bez odpowiedniego nadzoru IT, stwarza możliwość nieuprawnionego dostępu. Dodatkowo, brak aktualizacji oprogramowania wbudowanego (np. w systemach radiowych) może prowadzić do naruszenia bezpieczeństwa sieci.

System integrations highlight additional risks arising from the inter-integration of life safety systems with other critical building systems. These interconnections mean that the compromise of one system can lead to the disruption to others, thus significantly increasing risk. The lack of adequate safeguards in gateways integrating fire systems with other building systems, the use of insecure protocols and the lack of separation between systems only compound the potential risks.

Internal cyber security threats to building and life safety systems are also a very important issue. These include:

- lack of training – low level of awareness of cyber threats;
- human factor – malicious actions or disgruntled employees; practices of third-party vendors that do not comply with cyber security policies, physical access to systems being gained by unauthorised individuals;
- invasion – introduction of software with a "backdoor", introduction of own private equipment into the network;
- the level of protection – access that is broader than required for the performance of duties (excessive access) or lack of adequate screening of contractors and their employees.

The third edition of *Protecting Against Terrorism* [20] highlights the different types of attacks that can threaten the security of systems. Among these are:

- Man-in-the-middle (MitM) attacks involving the interception of communications between system components by unauthorised individuals who can modify transmitted data. Such actions can trigger false alarms or block warning signals, compromising the effectiveness of the threat response.
- Remote code execution (RCE) – allows cybercriminals to take remote control of a system, enabling them to disable or modify its functions. The consequences of such an attack pose a direct threat to life and property, as they can prevent a security system from functioning properly.
- Radio frequency jamming (RF jamming) – fire protection systems often use radio data transmission between components. Radio frequency jamming attacks can block the transmission of key information in real time, leading to delays in evacuation or lack of alarm response.
- Physical intrusion – unauthorised access to control panels and alarm equipment through physical manipulation (e.g. direct access to control panels) can allow control of the fire protection system to be taken over. The lack of adequate physical safeguards, such as access control to vital components, significantly increases the risk of such incidents.

In areas where fire systems connect to IP networks or contain ports to connect external devices, the risk of unauthorised access increases, potentially leading to system disruption or damage with significant safety implications [12].

Bezpieczeństwo systemowe jest narażone na zagrożenia związane z niewłaściwą konfiguracją zabezpieczeń, co może skutkować otwarciem dostępu do osób nieautoryzowanych. Ponadto, systemy te są podatne na ataki typu Denial of Service (DoS), które mogą zakłócić ich normalne działanie poprzez przeciążenie sieci lub blokowanie dostępu.

Integracje systemów uwidaczniają dodatkowe ryzyka wynikające z połączenia systemów ochrony życia z innymi krytycznymi systemami budynkowymi. Połączenia te powodują, że naruszenie działania jednego systemu może prowadzić do zakłóceń w innych, co znacząco zwiększa ryzyko. Brak odpowiednich zabezpieczeń w bramkach integrujących systemy pożarowe z pozostałymi systemami budynkowymi, stosowanie niepewnych protokołów oraz brak separacji między systemami tylko potęgują potencjalne zagrożenia.

Bardzo istotną kwestią są również zagrożenia wewnętrzne cyberbezpieczeństwa dla systemów budynkowych i systemów bezpieczeństwa życia. Do nich zalicza się:

- brak szkoleń – niski poziom świadomości w zakresie zagrożeń cybernetycznych;
- czynnik ludzki – złośliwe działania lub niezadowoleni pracownicy; praktyki zewnętrznych dostawców, które są niezgodne z polityką bezpieczeństwa cybernetycznego, uzyskanie fizycznego dostępu do systemów przez nieautoryzowane osoby;
- inwazja – wprowadzenie oprogramowania z „tylnymi drzwiami", wprowadzenie prywatnego własnego sprzętu do sieci;
- poziom ochrony – dostęp o szerszym zakresie niż wymagany do pełnienia obowiązków (nadmierny dostęp) czy brak odpowiedniego sprawdzenia kontrahentów i ich pracowników.

W trzecim wydaniu publikacji *Protecting Against Terrorism* [20] wyróżnione są różne rodzaje ataków, które mogą zagrozić bezpieczeństwu systemów. Wśród nich znajdują się:

- ataki typu *man-in-the-middle* (MitM) polegające na przechwytywaniu komunikacji pomiędzy elementami systemu przez osoby nieuprawnione, które mogą modyfikować przesyłane dane. Takie działania mogą wywoływać fałszywe alarmy lub blokować sygnały ostrzegawcze, co zagraża skuteczności reakcji na zagrożenie.
- Zdalne wykonanie kodu (ang. *remote code execution*, RCE) pozwala cyberprzestępcom na przejęcie zdalnej kontroli nad systemem, umożliwiając im jego wyłączenie lub modyfikację funkcji. Skutki takiego ataku stanowią bezpośrednie zagrożenie dla życia i mienia, ponieważ mogą zablokować właściwe działanie systemu ochrony.
- Zakłócanie częstotliwości radiowych (ang. *RF jamming*) – systemy ochrony przeciwpożarowej często wykorzystują radiową transmisję danych między komponentami. Ataki zakłócające częstotliwości radiowe mogą blokować przekazywanie kluczowych informacji w czasie rzeczywistym, co prowadzi do opóźnień w ewakuacji lub braku reakcji alarmowej.
- Fizyczne włamania – nieautoryzowany dostęp do paneli kontrolnych i urządzeń alarmowych przez manipulację

fizyczną (np. bezpośredni dostęp do paneli sterujących) może umożliwić przejęcie kontroli nad systemem ochrony przeciwpożarowej. Brak odpowiednich zabezpieczeń fizycznych, takich jak kontrola dostępu do istotnych komponentów, znacznie zwiększa ryzyko takich incydentów.

W obszarach, gdzie systemy pożarowe łączą się z sieciami IP lub zawierają porty umożliwiające podłączenie zewnętrznych urządzeń, zwiększa się ryzyko nieautoryzowanego dostępu, który potencjalnie może prowadzić do zakłócenia pracy systemu lub uszkodzeń o istotnych skutkach dla bezpieczeństwa [12].

Gaps in standards and security

Testing the vulnerability of systems integrating fire protection equipment to terrorist threats is an important part of ensuring the security of critical infrastructure. These systems, as part of critical facilities, can be potential targets for terrorist attacks, requiring a comprehensive approach to risk assessment and implementation of protective measures [21–22].

An interesting aspect is the use of the scenario method to assess terrorist threats to strategic facilities, including fire protection systems. It involves creating scenarios consisting of terrorist threat options and response plans for physical protection systems [21].

At the same time, research indicates that terrorist groups are increasingly interested in industrial control systems, which may also include fire protection systems [21]. A comprehensive approach to this issue is necessary to ensure effective protection of critical infrastructure against potential terrorist attacks [21–23].

The analyses of standards and cyber security reports carried out have revealed significant shortcomings in the security of fire protection systems. The most noticeable problems include the following areas [12]:

- cyber security rules – lack of consistent policies on key aspects of security, such as:
  - equipment inventory, network diagrams and system configurations,
  - authentication and password management,
  - assigning responsibility for system maintenance,
  - updating hardware, software and network connection documentation,
  - defining supply chain and technical support requirements,
  - requirements for the integration of external systems and subsystems,
  - development and maintenance of authentication processes.
- security functions – security requires constant monitoring and updating of security functions that protect systems from unauthorised access and other threats;
- integration and commissioning – all policies and procedures should be analysed and adapted after the integration of new systems;
- maintaining the desired level of security – software updates are not always deployed as soon as they are released, increasing the risk of security vulnerabilities;
- training for technical and non-technical staff – training is

Luki w standardach i zabezpieczeniach

Badania podatności systemów integrujących urządzenia przeciwpożarowe na zagrożenia terrorystyczne są istotnym elementem zapewnienia bezpieczeństwa infrastruktury krytycznej. Systemy te, jako część kluczowych obiektów, mogą być potencjalnym celem ataków terrorystycznych, co wymaga kompleksowego podejścia do oceny ryzyka i wdrażania środków ochronnych [21–22].

Interesującym aspektem jest wykorzystanie metody scenariuszowej do oceny zagrożeń terrorystycznych dla obiektów strategicznych, w tym systemów przeciwpożarowych. Polega ona na tworzeniu scenariuszy składających się z wariantów zagrożeń terrorystycznych oraz planów reakcji systemów ochrony fizycznej [21].

Jednocześnie badania wskazują na rosnące zainteresowanie grup terrorystycznych systemami kontroli przemysłowej, co może obejmować również systemy przeciwpożarowe [21]. Kompleksowe podejście do tego zagadnienia jest niezbędne dla zapewnienia skutecznej ochrony infrastruktury krytycznej przed potencjalnymi atakami terrorystycznymi [21–23].

Przeprowadzone analizy norm oraz raportów dotyczących cyberbezpieczeństwa ujawniły istotne niedociągnięcia w zabezpieczeniach systemów ochrony przeciwpożarowej. Najbardziej zauważalne problemy obejmują następujące obszary [12]:

- zasady bezpieczeństwa cybernetycznego – brak spójnych polityk dotyczących kluczowych aspektów bezpieczeństwa, takich jak:
  - inwentaryzacja urządzeń, schematy sieci i konfiguracje systemu,
  - zarządzanie uwierzytelnianiem i hasłami,
  - przydzielanie odpowiedzialności za konserwację systemów,
  - aktualizacja dokumentacji sprzętu, oprogramowania i połączeń sieciowych,
  - określenie wymagań dotyczących łańcucha dostaw oraz wsparcia technicznego,
  - wymogi dotyczące integracji systemów zewnętrznych oraz podsystemów,
  - rozwój i utrzymanie procesów związanych z uwierzytelnianiem;
- funkcje bezpieczeństwa – bezpieczeństwo wymaga stałego monitorowania i aktualizacji funkcji ochronnych, które zabezpieczają systemy przed nieautoryzowanym dostępem oraz innymi zagrożeniami;
- integracja i uruchamianie – wszystkie zasady i procedury powinny być analizowane i dostosowywane po integracji nowych systemów;

essential for both technical staff and those responsible for management, administration and contracting;
- education and awareness – raising awareness of cyber security in the fire and life safety industry.

Fire systems manufacturer Honeywell has issued security patches for two serious vulnerabilities affecting the Internet server used in Notifier alarm systems. Gjoko Krstic, a researcher at Applied Risk, discovered that the NOTI-FIRE-NET server (NWS-3) has vulnerabilities that allow authentication bypass (CVE-2020-6972) and information disclosure (CVE-2020-6974) [24].

The NOTI-FIRE-NET interface allows several smart fire panels to be linked together on a single network, and a web server allows remote access to this network, providing insight into event history, device status and other information. It was discovered that an unauthorised attacker could access the control panel by manipulating the server response and changing the message from "FAILURE" to "SUCCESS" [23].

The second vulnerability relates to the predictable name of the database backup file, which contains sensitive data such as usernames and passwords. Downloading this file allows full access to the alarm system [24].

According to the Applied Risk report, these vulnerabilities are rated as medium to high, but the DHS (Department of Homeland Security) and CISA (Cybersecurity and Infrastructure Security Agency) agencies classify them as critical. Honeywell has released firmware update 4.51 to patch these vulnerabilities. The company also recommends isolating systems from the Internet, using VPNs for remote connections and setting strong passwords [24].

Recommendations

On the basis of the analyses carried out and in the light of current standards and regulations, it is crucial to implement a series of measures to ensure the highest levels of functional safety system safety and reliability.

First and foremost, absolute adherence to the requirements set out in EN IEC 61508 is essential. Adherence to these standards ensures that systems are designed and implemented in accordance with industry best practice, which has a significant impact on their reliability and efficiency. Defining and achieving an appropriate security integrity level through a thorough risk analysis will allow the requirements for equipment reliability, including the probability of on-demand failures and the level of system diagnostics, to be set precisely [25]. Implementing redundancy, self-monitoring and real-time failure monitoring mechanisms is

- utrzymanie pożądanego poziomu bezpieczeństwa
- aktualizacje oprogramowania nie zawsze są wdrażane natychmiast po ich wydaniu, co zwiększa ryzyko wystąpienia luk w zabezpieczeniach;
- szkolenia dla personelu technicznego i nietechnicznego – szkolenia są niezbędne zarówno dla pracowników technicznych, jak i dla osób odpowiedzialnych za zarządzanie, administrację oraz zawieranie kontraktów;
- edukacja i świadomość – zwiększenie świadomości w branży przeciwpożarowej i bezpieczeństwa życia w zakresie cyberbezpieczeństwa.

Producent systemów pożarowych Honeywell wydał poprawki zabezpieczające dla dwóch poważnych podatności dotyczących serwera internetowego używanego w systemach alarmowych Notifier. Gjoko Krstic, badacz z Applied Risk, odkrył, że serwer NOTI-FIRE-NET (NWS-3) posiada luki pozwalające na obejście autoryzacji (CVE-2020-6972) oraz ujawnienie informacji (CVE-2020-6974) [24].

Interfejs NOTI-FIRE-NET umożliwia łączenie kilku inteligentnych paneli przeciwpożarowych w jednej sieci, a serwer internetowy – dalny dostęp do tej sieci, dając wgląd w historię zdarzeń, status urządzeń i inne informacje. Odkryto, że nieautoryzowany atakujący może uzyskać dostęp do panelu administracyjnego, manipulując odpowiedzią serwera i zmieniając komunikat z „FAILURE" na „SUCCESS" [23].

Druga podatność dotyczy przewidywalnej nazwy pliku kopii zapasowej bazy danych, który zawiera wrażliwe dane, takie jak nazwy użytkowników i hasła. Pobranie tego pliku umożliwia pełny dostęp do systemu alarmowego [24].

Zgodnie z raportem Applied Risk, luki te oceniono jako średnie i wysokie, ale agencje DHS (ang. *Department of Homeland Security*, Departament Bezpieczeństwa Wewnętrznego) i CISA (ang. *Cybersecurity and Infrastructure Security Agency*, Agencja Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury) klasyfikują je jako krytyczne. Honeywell udostępnił aktualizację firmware'u 4.51, aby załatać te podatności. Firma zaleca także izolowanie systemów od internetu, korzystanie z VPN w przypadku zdalnych połączeń oraz ustawienie silnych haseł [24].

Rekomedacje

Na podstawie przeprowadzonych analiz oraz w świetle obowiązujących norm i przepisów kluczowe jest wdrożenie szeregu działań mających na celu zapewnienie najwyższego poziomu bezpieczeństwa i niezawodności systemów funkcjonalnego bezpieczeństwa.

Przede wszystkim niezbędne jest bezwzględne przestrzeganie wymagań określonych w normie PN-EN IEC 61508. Stosowanie się do tych standardów gwarantuje, że systemy są projektowane i realizowane zgodnie z najlepszymi praktykami branżowymi, co znacząco wpływa na ich niezawodność i efektywność. Określenie i osiągnięcie właściwego poziomu nienaruszalności bezpieczeństwa (SIL) poprzez dokładną analizę ryzyka pozwoli precyzyjnie ustalić wymagania dotyczące niezawodności sprzętu, w tym prawdopodobieństwa awarii na żądanie i poziomu

essential to minimise the risk of critical failures. In the case of SIUP, meeting these requirements directly increases the effectiveness of fire detection and response.

Based on the *Cybersecurity for Fire Protection Systems* report, the remaining recommendations are based on three issues:

- security configuration guides and best practices,
- guidelines and standards for systems hardening,
- default assumption of no trust in third parties.

The first area emphasises three critical aspects. First and foremost is ensuring that installers and maintenance personnel have access to appropriate guides and best practices for security configuration. It is also crucial to implement a training programme that not only conveys knowledge of procedures, but also explains the rationale behind particular processes. In addition, it is essential to employ specialists with diverse skills who have both technical and operational knowledge of the systems they work with.

As part of the guidelines and standards, the configuration of fire protection systems is required to comply with security standards that facilitate the adequate protection of workstations.

The final point about lack of trust draws attention to the fact that access to systems is controlled and protected and that documentation should be kept internally, without external systems. Likewise, it is imperative to ensure that the working environment of employees with remote access is secure.

In the US, strategies are also being recommended to increase the resilience of fire protection systems against cyber attacks. These strategies focus on five key areas: raising awareness of cyber threats, fostering dialogue and cross-sector collaboration, implementing best practices for cyber protection, updating security codes and standards, and developing education and training programmes [12].

The results clearly indicate the need for action at several levels:

1. Updating safety standards – existing standards need to be adapted to the changing risk landscape, particularly taking into account new risks arising from the integration of fire systems.
2. Training of technical staff – it is necessary to raise awareness of cyber threats among companies installing and operating SIUP systems. Technical staff should be adequately trained in cyber security best practices.
3. Further research – it was recommended that empirical research be continued, which will include testing SIUP systems in real-world conditions to better understand the effectiveness of the proposed safeguards.

In addition, it will be appropriate to conduct comprehensive security audits of existing SIUP systems to identify potential gaps and vulnerabilities. It is also necessary to develop cyber security incident response plans that take into account the specifics of fire systems and the potential consequences of their failure.

They also highlight the need for closer collaboration between SIUP system manufacturers, cyber security experts and emergency services to develop a holistic approach to protecting these critical systems.

It is also important to consider cyber security aspects from the design and implementation stage of new SIUP systems. This

diagnostyki systemu [25]. Wdrożenie mechanizmów redundancji, samokontroli oraz monitorowania awarii w czasie rzeczywistym jest niezbędne do minimalizacji ryzyka krytycznych uszkodzeń. W przypadku SIUP spełnienie tych wymagań bezpośrednio zwiększa skuteczność detekcji i reakcji na zagrożenia pożarowe.

W oparciu o raport pt. *Cybersecurity for Fire Protection Systems*, pozostałe rekomendacje opierają się na:

- przewodnikach dotyczących konfiguracji zabezpieczeń oraz najlepszych praktykach,
- wytycznych i standardach dotyczących hartowania systemów,
- domyślnym założeniu braku zaufania do stron trzecich.

Pierwszy obszar kładzie nacisk na trzy krytyczne aspekty. Przede wszystkim jest to zapewnienie instalatorom i konserwatorom dostępu do odpowiednich przewodników oraz najlepszych praktyk w zakresie konfiguracji zabezpieczeń. Kluczowe jest również wdrożenie programu szkoleń, który nie tylko przekazuje wiedzę o procedurach, ale również podaje uzasadnienie poszczególnych procesów. Ponadto niezbędne jest zatrudnianie specjalistów o zróżnicowanych umiejętnościach, którzy posiadają zarówno wiedzę techniczną, jak i operacyjną na temat systemów, z którymi pracują.

W ramach wytycznych i standardów wymaga się, aby konfiguracja systemów ochrony przeciwpożarowej była zgodna ze standardami bezpieczeństwa, które ułatwiają odpowiednie zabezpieczenie stacji roboczych.

Ostatni punkt dotyczący braku zaufania zwraca uwagę na to, iż dostęp do systemów jest kontrolowany i chroniony, a dokumentacja powinna być przechowywana w sposób wewnętrzny, bez udziału zewnętrznych systemów. Należy upewnić się, że środowisko pracy pracowników posiadających zdalny dostęp jest zabezpieczone.

W Stanach Zjednoczonych rekomenduje się również strategie mające na celu zwiększenie odporności systemów ochrony przeciwpożarowej na cyberataki. Strategie te koncentrują się na pięciu kluczowych obszarach: podnoszeniu świadomości o zagrożeniach cybernetycznych, wspieraniu dialogu i współpracy międzysektorowej, wdrażaniu najlepszych praktyk w zakresie ochrony przed cyberzagrożeniami, aktualizacji kodeksów i norm bezpieczeństwa oraz rozwoju programów edukacyjnych i szkoleniowych [12].

Wyniki jednoznacznie wskazują na konieczność podjęcia działań na kilku poziomach:

1. Aktualizacja standardów bezpieczeństwa – należy dostosować istniejące normy do zmieniającego się krajobrazu zagrożeń, w szczególności uwzględniając nowe zagrożenia wynikające z integracji systemów pożarowych.
2. Szkolenie personelu technicznego – konieczne jest zwiększenie świadomości zagrożeń cybernetycznych wśród firm instalujących i obsługujących systemy SIUP. Personel techniczny powinien być odpowiednio przeszkolony w zakresie najlepszych praktyk dotyczących cyberbezpieczeństwa.
3. Dalsze badania – zarekomendowano kontynuowanie badań empirycznych, które obejmą testowanie SIUP w rzeczywistych warunkach, aby lepiej zrozumieć skuteczność proponowanych zabezpieczeń.

approach should become the industry standard, ensuring that security is an integral part of the system and not an add-on introduced after the fact.

In addition, the recommendations mention the creation of a central centre for the exchange of information on threats and cyber security incidents specific to SIUP systems. Such a centre could serve as a platform for quickly responding to new threats and sharing experiences in neutralising them.

Recommendations for Poland

Another key finding is the lack of adequate legal regulations in Poland that directly address the problem of the cyber security of fire protection systems. Unlike other countries, where there are detailed regulations for securing fire protection systems, Poland does not have comprehensive regulations or standards that would mandate the implementation of advanced cyber security measures in fire systems.

Systems integrating fire protection devices, by their very nature, are installed for security in critical infrastructure facilities. Thus, they should also be subject to the Critical Infrastructure Act and the aforementioned NIS 2 Directive. The NIS 2 Directive imposes cyber security obligations, meaning that SIUP systems must be secured against both physical and digital threats. The Critical Infrastructure Act, on the other hand, requires these systems to be designed and maintained to the highest standards of reliability and security, such as those set out in EN IEC 61508. Meeting these requirements is not only a legal obligation, but also crucial to ensuring effective detection and response to fire threats. Regular audits and updates to the SIUP are essential to maintain regulatory compliance and to minimise the risk of failure.

Current regulations mainly focus on the technical aspects of fire systems, such as the installation and operation of alarm systems, but there are no uniform rules governing the network and cyber security of these systems.

In the new *Guidelines for the design, installation, commissioning, operation and maintenance of systems integrating fire protection equipment*, security issues are presented in general terms. According to them, it is advisable to implement redundancy mechanisms and to secure systems against physical and cyber threats, thus minimising the risk of disruption. SIUPs should operate in accordance with international standards such as ISO 27002, which

Ponadto stosowne będzie przeprowadzenie kompleksowych audytów bezpieczeństwa istniejących SIUP w celu identyfikacji potencjalnych luk i słabości. Konieczne jest również opracowanie planów reagowania na incydenty cyberbezpieczeństwa, które uwzględniałyby specyfikę systemów pożarowych i potencjalne skutki ich awarii.

Podkreśla się w tym miejscu również konieczność nawiązania ściślejszej współpracy między producentami SIUP, ekspertami ds. cyberbezpieczeństwa i służbami ratowniczymi w celu wypracowania holistycznego podejścia do ochrony tych krytycznych systemów.

Istotne jest także uwzględnienie aspektów cyberbezpieczeństwa już na etapie projektowania i wdrażania nowych SIUP. Taki podejście powinno stać się standardem w branży, dzięki czemu zabezpieczenia staną się integralną częścią systemu, a nie dodatkiem wprowadzanym po fakcie.

Dodatkowo zalecenia mówią o utworzeniu centralnego ośrodka wymiany informacji o zagrożeniach i incydentach cyberbezpieczeństwa specyficznych dla SIUP. Taki ośrodek mógłby służyć jako platforma do szybkiego reagowania na nowe zagrożenia i dzielenia się doświadczeniami w zakresie ich neutralizacji.

Rekomendacje dla Polski

Kolejnym kluczowym wnioskiem jest brak w Polsce odpowiednich regulacji prawnych, które bezpośrednio odnosiłyby się do problemu cyberbezpieczeństwa systemów ochrony przeciwpożarowej. W przeciwieństwie do innych krajów, gdzie istnieją szczegółowe regulacje dotyczące zabezpieczania systemów przeciwpożarowych, w naszym kraju nie ma kompleksowych przepisów ani standardów, które nakładałyby obowiązek implementacji zaawansowanych środków cyberbezpieczeństwa w systemach pożarowych.

Systemy integrujące urządzenia przeciwpożarowe ze względu na swoją specyfikę są montowane dla bezpieczeństwa w obiektach infrastruktury krytycznej. Zatem powinny podlegać również ustawie o infrastrukturze krytycznej oraz wspomnianej wcześniej dyrektywie NIS 2. Dyrektywa NIS 2 nakłada obowiązki w zakresie cyberbezpieczeństwa, co oznacza, że SIUP powinny być zabezpieczone zarówno przed zagrożeniami fizycznymi, jak i cyfrowymi. Natomiast ustawa o infrastrukturze krytycznej wymaga, aby systemy te były projektowane i utrzymywane zgodnie z najwyższymi standardami niezawodności i bezpieczeństwa, takimi jak określone w normie PN-EN IEC 61508. Spełnienie tych wymagań jest nie tylko obowiązkiem prawnym, ale także kluczowym dla zapewnienia skutecznej detekcji i reakcji na zagrożenia pożarowe. Regularne audyty i aktualizacje SIUP są niezbędne dla utrzymania zgodności z przepisami oraz dla minimalizacji ryzyka awarii.

Obecne przepisy koncentrują się głównie na technicznych aspektach działania systemów pożarowych, takich jak montaż i eksploatacja systemów alarmowych, ale brak jest jednolitych przepisów regulujących kwestie zabezpieczeń sieciowych i cybernetycznych tych systemów.

W nowych *Wytycznych projektowania, instalowania, uruchamiania, obsługi i konserwacji systemów integrujących urządzenia*

guarantees the integrity and security of transmitted data while protecting access to critical infrastructure [26]. It is essential to equip the systems with independent sources of emergency power to enable them to function in the event of a power failure, as well as to implement real-time monitoring and protection functions. In addition, access to the systems must be adequately secured through multi-level user authorisation and control.

However, due to the nature of the document, guidelines are a supporting tool to facilitate compliance with statutory requirements or good practice, but unfortunately they are not in themselves binding and their use is not mandatory. This loophole poses a serious threat to the security of buildings equipped with SIUP. It makes these systems vulnerable to potential cyber attacks. The lack of adequate legal protection means that the fire safety systems in these buildings could be breached by malicious actors, potentially threatening the safety of occupants and the integrity of the structures themselves.

It is therefore necessary to urgently develop and implement comprehensive legal regulations that would take into account the specificity of the cyber security of fire protection systems in Poland. Such regulations should cover not only technical but also organisational and procedural aspects, ensuring a holistic approach to the problem. These regulations must be flexible enough to keep up with the rapidly changing landscape of cyber threats.

Limitations and future research

The main limitations of this study are that it is based on an analysis of literature and reports, without direct testing of SIUPs. The results are based on the available data, which may not cover all aspects of the risks, especially in terms of emerging technologies. The lack of direct empirical testing means that future research is needed. Such research should focus on conducting practical tests of SIUPs in controlled environments to verify theoretical assumptions and identify potential security vulnerabilities. It is also important to broaden the scope of research to include an analysis of new threats related to rapidly developing technologies that may affect the security of SIUP.

In addition, it is necessary to develop standardised methods to assess and compare the effectiveness of different security solutions, enabling a more precise definition of best practices in the protection of SIUP systems.

This standardisation should cover not only technical aspects, but also organisational and legal procedures. It is worth considering the creation of an international cooperation framework for the exchange of threat information and best practices, which will contribute to increasing the overall security level of SIUPs worldwide.

przeciwpożarowe kwestie bezpieczeństwa przedstawione są w sposób ogólny. Zgodnie z nimi wskazane jest wdrożenie mechanizmów redundancji oraz zabezpieczenie systemów przed zagrożeniami fizycznymi i cybernetycznymi, co pozwala na minimalizację ryzyka zakłóceń. SIUP powinny działać zgodnie z międzynarodowymi normami, takimi jak ISO 27002, co gwarantuje integralność i bezpieczeństwo przesyłanych danych, jednocześnie chroniąc dostęp do infrastruktury krytycznej [26]. Istotne jest wyposażenie systemów w niezależne źródła zasilania awaryjnego, które umożliwiają ich funkcjonowanie w przypadku zaniku napięcia, a także realizacja funkcji monitorowania i ochrony w czasie rzeczywistym. Dodatkowo dostęp do systemów musi być odpowiednio zabezpieczony przez wielopoziomową autoryzację i kontrolę użytkowników.

Jednak ze względu na charakter dokumentu wytyczne są narzędziem pomocniczym, ułatwiającym spełnianie wymagań ustawowych lub stosowanie dobrych praktyk. Niestety same w sobie nie mają charakteru wiążącego i ich wdrażanie nie jest obligatoryjne. Ta luka prawna stanowi poważne zagrożenie dla bezpieczeństwa budynków wyposażonych w SIUP. Sprawia ona, że systemy te są podatne na potencjalne cyberataki. Brak odpowiedniej ochrony prawnej oznacza, że systemy bezpieczeństwa pożarowego w tych budynkach mogą zostać naruszone przez złośliwe podmioty, potencjalnie zagrażając bezpieczeństwu mieszkańców i integralności samych konstrukcji.

Konieczne jest zatem pilne opracowanie i wdrożenie kompleksowych regulacji prawnych, które uwzględniałyby specyfikę cyberbezpieczeństwa systemów ochrony przeciwpożarowej w Polsce. Takie przepisy powinny obejmować nie tylko aspekty techniczne, ale także organizacyjne i proceduralne, zapewniając holistyczne podejście do problemu. Regulacje te muszą być na tyle elastyczne, aby mogły nadążać za szybko zmieniającym się krajobrazem zagrożeń cybernetycznych.

Ograniczenia i przyszłe badania

Główne ograniczenia niniejszych badań wynikają z tego, że są one oparte na analizie literatury i raportów, bez bezpośredniego testowania SIUP. Wyniki bazują na dostępnych danych, które mogą nie obejmować wszystkich aspektów zagrożeń, szczególnie w przypadku nowo pojawiających się technologii. Brak bezpośrednich testów empirycznych oznacza konieczność przyszłych badań.Takie badania powinny skupić się na przeprowadzeniu praktycznych testów SIUP w kontrolowanych środowiskach, aby zweryfikować teoretyczne założenia i zidentyfikować potencjalne luki w zabezpieczeniach. Istotne jest również rozszerzenie zakresu badań o analizę nowych zagrożeń związanych z dynamicznie rozwijającymi się technologiami, które mogą wpływać na bezpieczeństwo SIUP.

Ponadto konieczne jest opracowanie standardowych metod oceny i porównywania skuteczności różnych rozwiązań zabezpieczających, co umożliwiłoby bardziej precyzyjne określenie najlepszych praktyk w dziedzinie ochrony SIUP.

Standaryzacja ta powinna obejmować nie tylko aspekty techniczne, ale również procedury organizacyjne i prawne. Warto rozważyć stworzenie międzynarodowych ram współpracy w zakresie

Future research should also focus on the human factors aspect of SIUP security. This includes analysing methods for training personnel operating the systems, developing effective incident response procedures and investigating psychological aspects of user behaviour that may affect the security of the systems.

wymiany informacji o zagrożeniach i najlepszych praktykach, co przyczyni się do podniesienia ogólnego poziomu bezpieczeństwa SIUP na całym świecie.

W ramach przyszłych badań należy także skupić się na aspektach związanych z czynnikiem ludzkim w kontekście bezpieczeństwa SIUP. Powinny objąć analizę metod szkolenia personelu obsługującego systemy, opracowanie skutecznych procedur reagowania na incydenty oraz badanie psychologicznych aspektów zachowań użytkowników, które mogą wpływać na bezpieczeństwo systemów.

Literature / Literatura

[1] Stępkowski R., *Integracja systemów bezpieczeństwa w budynkach wysokich i wysokościowych. Wpływ na ochronę przeciwpożarową obiektu*, https://ela.pl/wp-content/uploads/2019/09/Ryszard-St%C4%99pkowski-wyk%C5%82ad-2.pdf [dostęp: 31.10.2024].

[2] Kunecki K., *Zintegrowany system bezpieczeństwa pożarowego* w: Materiały pokonferencyjne z Ogólnopolskich Dni Ochrony Przeciwpożarowej w dniach 9–10.10.2024.

[3] *Wytyczne projektowania, instalowania, uruchamiania, obsługi i konserwacji systemów integrujących urządzenia przeciwpożarowe* CNBOP-PIB W-0007:2024 (wyd. 2 rozszerzone, listopad 2024) SITP WP-05:2024.

[4] *Wytyczne projektowania pomieszczenia i miejsca obsługi urządzeń przeciwpożarowych w budynkach. Lokalizacja, warunki wykonania, wyposażenie* CNBOP-PIB W-0001:2014 wydanie 3 rozszerzone, grudzień 2023.

[5] NFPA 4 – Standard for Integrated Fire Protection and Life Safety System Testing.

[6] PN-EN 54-13: Systemy sygnalizacji pożarowej – Część 13: Ocena kompatybilności możliwości przyłączenia podzespołów systemu.

[7] Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz.U. 2024, poz. 275, 1222).

[8] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. 2010 Nr 109, poz. 719).

[9] Zapała R., *System integrujący urządzenia przeciwpożarowe w systemach kontroli rozprzestrzeniania dymu i ciepła. Praktyczne aspekty sterowania, zasilania i integracji*, „Rynek Instalacyjny" 2020, 5, https://www.rynekinstalacyjny.pl/artykul/systemy-ppoz/43379,system-integrujacy-urzadzenia-przeciwpozarowe-w-systemach-kontroli-rozprzestrzeniania-dymu-i-ciepla-praktyczne-aspekty-sterowania-zasilania-i-integracji [dostęp: 30.10.2024].

[10] Hutchison V., Brackett J., *Cybersecurity and fire protection,* May 13, 2021, PE, SASHE, CHFM, https://www.hfmmagazine.com/articles/4177-cybersecurity-and-fire-protection [dostęp: 30.10.2024].

[11] NFPA 72 – National Fire Alarm and Signaling Code.

[12] Chevreaux J., Owen P., Donaldson K., Bright K., Largen A., Meiselman D., Kirsanova K., Borinski M., Uribe A., *Cybersecurity for Fire Protection Systems, Final Report*, M.C. Dean, Inc. Tysons, VA, USA, JesResearch fundation, REsearch for the NFPA Mission, September 2021.

[13] Sinopoli J., *Chapter 9 – Fire Alarm and Mass Notification Systems, in: Smart Buildings Systems for Architects, Owners and Builders*, Elsevier, Oxford 2010.

[14] Shulga T., Nikulina Yu., *Decision Support System for Fire Alarm Design*, w: *Society 5.0: Human-Centered Society Challenges and Solutions*, A. Kravets, A. Alexander, M.Sh. Bolshakov, M. Shcherbakov, https://doi.org/10.1007/978-3-030-95112-2_33, Springer International Publishing, 2022, 407–416.

[15] Behera R.P., Murali N., Satya Murty S.A.V, *Development of Tele-Alarm and Fire Protection system using Remote Terminal Unit for Nuclear Power Plant*, w: *International Conference on Robotics, Automation, Control and Embedded Systems (RACE)* 2015, https://doi.org/10.1109/RACE.2015.7097289.

[16] Dasig D.D., *Design and in Prototype Implementation of Fire Detection and Intelligent Alarm System, Proc. of the Intl. Conf. on Advances in Computing, Control and Networking – ACCN*, Institute of Research Engineers and Doctors, USA 2015.

[17] NIST 800-82 – Guide to Industrial Control Systems (ICS) Security.

[18] UL 2900-2-3 – Standard for Software Cybersecurity for Network-Connectable Products – Life Safety and Signaling Systems.

[19] D'Ambrosio N., Perrone G., Romano S.P., *Including insider threats into risk management through Bayesian threat graph networks*, Computers & Security" 2023, 103410, https://doi.org/10.1016/j.cose.2023.103410.

[20] *Protecting Against Terrorism Third Edition*, Centre for the Protection of National Infrastructure.

[21] Azarenko O., Shevchenko R., Diviziniuk M., Shevchenko O., Honcharenko Yu., *Methods of assessing terrorist threats to strategic facilities of the state*, Critical Infrastructure Security and Industrial Control Systems, 2023.

[22] Theodora L., *Critical Infrastructure Security and Industrial Control Systems*, Social Science Research Network, 2010, https://dx.doi.org/10.2139/ssrn.1692827.
[23] Shvetsov A.V., Shvetsov M.A., Gromov V.N., Balalaev A.S., Shvetsova S.V., Sharov V.A., Kozyrev V. A., *Trends of Modern Terrorism in the Metro Systems of the World*, "European Journal for Security Research", 2018, 1, 149–156, https://doi.org/10.1007/s41125-018-0037-9.
[24] Kovacs E., *Vulnerabilities Allow Hackers to Access Honeywell Fire Alarm Systems*, February 24, 2020 https://www.securityweek.com/vulnerabilities-allow-hackers-access-honeywell-fire-alarm-systems/ [dostęp: 30.10.2024].
[25] PN-EN 61508: Bezpieczeństwo funkcjonalne układów sterowania
[26] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.

WOJCIECH WRÓBLEWSKI, PH.D. – an assistant professor at the Fire University's Institute of Internal Security where holds the position of the Head of Postgraduate Studies on Managing Cybersecurity in the Public Sector. He conducts research on public security, civil protection, humanitarian aid and contemporary threats such as hybrid warfare, cybersecurity, terrorist threats and counterterrorism systems. He is also working on the use of artificial intelligence in civil protection and emergency management. Author of numerous scientific publications analysing the threats and challenges of homeland security and security engineering.

DOROTA SELIGA – a master's student in safety engineering at the Fire University. She completed engineering studies in fire safety at the Main School of Fire Service and bachelor's studies in internal security at the Cardinal Stefan Wyszyński University. She works at DEKK Fire Solutions, a company dealing with active fire protection, gaining experience in designing and implementing security solutions. She is a member of the Management Board of the District Branch of the Association of Volunteer Fire Brigades of the Republic of Poland in Piaseczno, where she is involved in fire safety activities. She constantly expands her knowledge through industry training and participation in conferences devoted to modern security technologies.

DR WOJCIECH WRÓBLEWSKI – adiunkt w Instytucie Bezpieczeństwa Wewnętrznego Akademii Pożarniczej, gdzie pełni funkcję Kierownika Studiów Podyplomowych – Zarządzanie Cyberbezpieczeństwem w Sektorze Publicznym. Prowadzi badania w zakresie bezpieczeństwa publicznego, ochrony ludności, pomocy humanitarnej oraz współczesnych zagrożeń, takich jak wojna hybrydowa, cyberbezpieczeństwo, zagrożenia terrorystyczne i systemy antyterrorystyczne. Pracuje również nad wykorzystaniem sztucznej inteligencji w ochronie ludności i zarządzaniu kryzysowym. Jest autorem licznych publikacji naukowych analizujących zagrożenia i wyzwania związane z bezpieczeństwem wewnętrznym i inżynierią bezpieczeństwa.

DOROTA SELIGA – studentka studiów magisterskich na kierunku inżynieria bezpieczeństwa w Akademii Pożarniczej. Ukończyła studia inżynierskie na kierunku bezpieczeństwo pożarowe w Szkole Głównej Służby Pożarniczej oraz studia licencjackie na kierunku bezpieczeństwo wewnętrzne na Uniwersytecie Kardynała Stefana Wyszyńskiego. Pracuje w firmie DEKK Fire Solutions zajmującej się aktywną ochroną przeciwpożarową, zdobywając doświadczenie w projektowaniu i wdrażaniu rozwiązań bezpieczeństwa. Jest członkiem Zarządu Oddziału Powiatowego Związku Ochotniczych Straży Pożarnych RP w Piasecznie, gdzie angażuje się w działania na rzecz bezpieczeństwa pożarowego. Stale poszerza swoją wiedzę poprzez szkolenia branżowe oraz udział w konferencjach poświęconych nowoczesnym technologiom bezpieczeństwa.