DOI:10.12845/bitp.35.3.2014.1

ppłk dr inż. **Marek ŻYCZKOWSKI**[1]
prof. dr hab. inż. **Mieczysław SZUSTAKOWSKI**[1]
ppłk dr inż. **Rafał DULSKI**[1]
dr inż. **Mariusz KASTEK**[1]
dr inż. **Wiesław CIURAPIŃSKI**[1]
mgr inż. **Mateusz KAROL**[1]
mgr inż. **Piotr MARKOWSKI**[1]

Przyjęty/Accepted/Принята: 01.09.2013;
Zrecenzowany/Reviewed/Рецензирована: 19.08.2014;
Opublikowany/Published/Опубликована: 30.09.2014;

WYBRANE ZAGADNIENIA OCHRONY INFRASTRUKTURY KRYTYCZNEJ NA PRZYKŁADZIE PORTU MORSKIEGO[2]

Selected Issues Concerning Protection of Key Installations Illustrated on the Example of a Maritime Port

Выбранные вопросы защиты критической инфраструктуры на примере морского порта

Abstrakt
Cel: Celem artykułu jest przybliżenie zagadnień ochrony obiektów infrastruktury krytycznej. Szczególną uwagę zwrócono na zagadnienia ochrony zewnętrznej i monitorowanie obszaru chronionego na przykładzie zabezpieczeń portu morskiego. Na jego terenie można wyróżnić strefy wymagające różnego podejścia do aspektu ochrony, dając w ten sposób pełny obraz systemu ochrony infrastruktury krytycznej obiektów specjalnych.
Wprowadzenie: Obecne zdobycze techniki w zakresie systemów ochrony obiektów infrastruktury krytycznej oferują mnogość rozwiązań z zakresu funkcjonalności i możliwości. Tworząc system bezpieczeństwa obiektu, należy przede wszystkim na poziomie działania procedur bezpieczeństwa zapewnić ich wzajemną komplementarność względem poszczególnych podmiotów je realizujących. W ujęciu systemu ochrony obiektów infrastruktury krytycznej podmiotami realizującymi procedury systemu bezpieczeństwa są zarówno techniczne środki ochrony, jak i służby ochrony. Wymaga to odpowiedniego zarządzania pracą poszczególnych elementów systemu z uwzględnieniem ich możliwości i kompetencji. Ponadto projektowany system ochrony powinien być spójny nie tylko pod względem procedur, lecz również z uwzględnieniem technicznego aspektu działania poszczególnych podsystemów ochrony. W tym celu należy zapewnić integrację poszczególnych podsystemów w centrum nadzoru, które odpowiada za prawidłowy przepływ informacji pomiędzy podmiotami obecnymi w systemie bezpieczeństwa i koordynuje ich pracę.
Wyniki: W artykule zostały przedstawione kluczowe zagadnienia ochrony technicznej obiektów infrastruktury krytycznej w ujęciu ochrony zewnętrznej i wewnętrznej. Autorzy zarysowali podstawowe problemy wykorzystania perymetrycznych czujników specjalnych oraz dalekozasięgowych systemów wizualizacji zdarzeń wspomagających działania służb ochrony fizycznej. Przedstawiono również problematykę systemów integrujących umożliwiających, adekwatną do potrzeb, obsługę systemów ochrony w zakresie BMS w powiązaniu z czujnikami ochrony zewnętrznej.
Wnioski: Na podstawie przeprowadzonej analizy można stwierdzić, iż głównym kryterium doboru elementów systemów ochrony infrastruktury krytycznej jest budżet. Widać wyraźne trendy w wyborze przez inwestorów systemów opartych głównie o detekcję wizualną. Systemy takie, mimo iż oferują wiele funkcjonalności, nie są idealnym rozwiązaniem ze względu na zmienne warunki oświetleniowe. Dodatkowo dają złudne przeświadczenie o ograniczaniu kosztów poprawnie funkcjonującego systemu ochrony. Dlatego kluczowe jest odpowiednie dopasowanie systemu ochrony do potrzeb i wymagań danego obiektu.

Słowa kluczowe: zintegrowane systemy ochrony, infrastruktura krytyczna, system integrujący
Typ artykułu: artykuł przeglądowy

[1] Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego; ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa; mzyczkowski@wat.edu.pl / Military University of Technology in Warsaw, Poland;
[2] Autorzy wnieśli jednakowy wkład w powstanie artykułu / The authors contributed equally to this article;

DOI:10.12845/bitp.35.3.2014.1

Abstract
Aim: The purpose of this article is to expose protection issues of key installations. Specifically, as an illustration, attention is focused on questions concerning the security of a maritime port. Within such a perimeter it is possible to identify a range of zones which require diverse protection measures. In turn, this provides a full image of security measures which need to be harnessed to protect key installations.
Introduction: Current technological advances in the field of security systems for key installations afford a multitude of functional and capability solutions. Creation of a security system requires, at the operational level, a need to ensure compatibility in procedures for those engaged in the realization of protection. Security systems for key installations require the engagement of technical measures as well as the services of security organizations. This requires a suitable management approach to individual elements of the system to maximize capability and competence. Additionally, a proposed security system should be consistent not only in terms of procedures, but also with regard to the technical interaction of each subsystem. To achieve this it is necessary to integrate various subsystems at the control center, which is responsible for co-ordination and proper flow of information between those involved in the security activity.
Results: The paper exposed main technical issues relating to key installation security systems, in context of internal and external security. Authors revealed fundamental problems associated with the use of special perimeter sensors as well as long range visual aids which support the work of security staff. Problems were also highlighted about issues concerning integration of systems which should satisfy requirements of operating BMS security systems in relation to external security sensors.
Conclusions: An analysis reveals that the main criterion for selection of system elements used in the protection of key installations is the budget. Clear trends indicate that, in the main, investors chose systems based on visual detection. Such systems, although offering many features, are not ideal for variable lighting conditions. Additionally, they provide a false conviction of reducing the cost of a properly functioning security system. Therefore, it is vital to adopt a security system which satisfies the needs and requirements of given key installation.

Keywords: integrated security systems, key installations, integrating system
Type of article: review article

Аннотация
Цель: Целью статьи является ознакомление читателей с вопросами защиты объектов критической инфраструктуры. Особенное внимание посвящено вопросам внешней защиты и мониторингу защищаемой территории на примере средств защиты морского порта. Так как на территории такого объекта находятся зоны, требующие различных подходов к вопросу защиты, статья даёт полное представление о системе защиты специальных объектов критической инфраструктуры.
Введение: Современные достижения техники в области систем защиты объектов критической инфраструктуры предлагают множество возможностей и функциональных решений. Создавая систему безопасности объекта, в первую очередь, следует обеспечить взаимодополняемость процедур в отношении отдельных субъектов, которые их реализуют. В данной системе защиты объектов критической инфраструктуры, субъектами реализующими процедуры системы безопасности являются как технические средства защиты, так и сами службы защиты. Такая структура требует соответствующего управления работой отдельных элементов системы с учётом их способностей и компетенций. Кроме того, предложенная система защиты должна быть соответственной не только с точки зрения процедур, но также с учётом технического аспекта работы отдельных подсистем защиты. Для этого следует обеспечить интеграцию отдельных подсистем в центре управления, который отвечает за правильную передачу информаций между субъектами, находящимися в системе безопасности и координирует их работу.
Результаты: В статье были представлены ключевые вопросы технической защиты объектов критической инфраструктуры с точки зрения внешней и внутренней защиты. Авторы коротко охарактеризовали основные проблемы использования специальных периметрических датчиков и систем мониторинга большой дальности, которые поддерживают работу отделов служб физической защиты. Представлена также проблематика интегрирующих систем, которые отвечают потребностям в обслуживании систем защиты в сфере BMS относительно датчиков внешней защиты.
Выводы: На основе проведённого анализа можно сделать вывод, что главным критерием для выбора элементов систем защиты критической инфраструктуры является бюджет. Видны чёткие тенденции при выборе инвесторами систем, основанных, в главной мере, на визуальном обнаружении. Хотя такие системы много функциональны, они не являются идеальным решением в связи с изменчивыми условиями освещения. Кроме того, они создают ложное убеждение в том, что уменьшены затраты на верно функционирующую систему защиты. Таким образом главное, чтобы система защиты соответствовала нуждам и требованиям данного объекта.

Ключевые слова: интегрированные системы защиты, критическая инфраструктура, интегрирующая система
Вид статьи: обзорная статья

1. Wprowadzenie

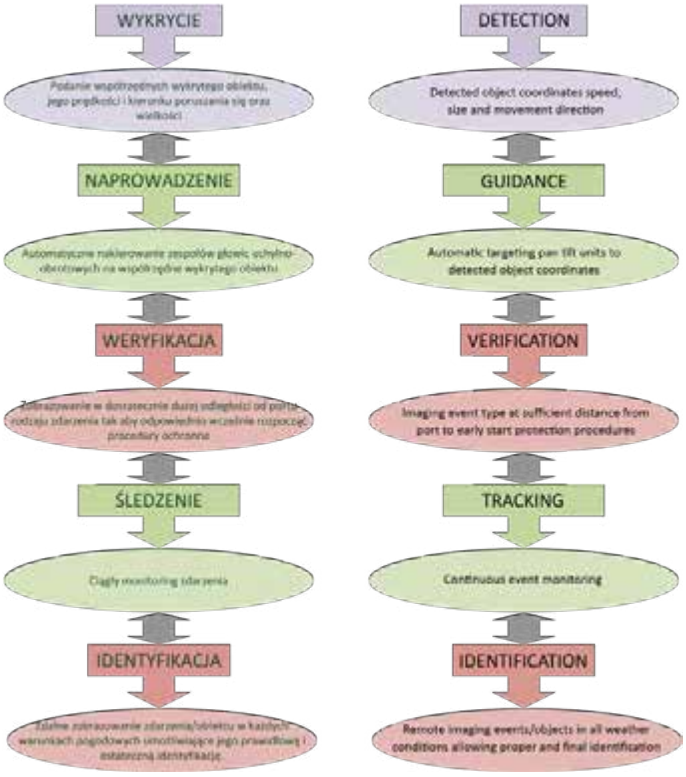
Zintegrowany system bezpieczeństwa obiektu infrastruktury krytycznej powinien opierać się na zatwierdzonym planie ochrony, uwzględniającym współpracę służb działających zgodnie z procedurami bezpieczeństwa przy wykorzystaniu środków technicznych adekwatnych do poziomu zagrożenia. W związku z tym każdy nowo projektowany system ochrony technicznej powinien być skonstruowany w oparciu o najlepsze i najnowocześniejsze standardy ochrony, umożliwiające globalny nadzór nad systemem, oraz powinien być zgodny z wymaganiami kodeksu ISPS [1-3].

System taki poprzez wdrożenie ekonomicznie uzasadnionych, najnowszych rozwiązań technicznych powinien zapewnić:

- ciągły monitoring stref podejścia do obiektów strategicznych, a w szczególności do stref, na które atak wywołałby kumulację strat [4, 5];

- monitoring, skuteczny w każdych warunkach pogodowych [6, 7];
- system zarządzania umożliwiający skuteczne wykorzystanie środków technicznych w warunkach zmiany poziomu bezpieczeństwa.

Rekomendowany przez zespół autorów model zintegrowanego systemu ochrony zakłada korzystanie z rozwiązań pozwalających na zapewnienie spełnienia założeń ochrony. Jak pokazuje praktyka projektowania systemów ochrony obiektów infrastruktury krytycznej, system taki powinien funkcjonować poprzez techniczne wdrożenie procedury (ryc. 1): wykrycia, naprowadzania technicznych systemów zintegrowanych, weryfikacji, śledzenia i identyfikacji zdarzenia.



Ryc. 1. Idea systemu monitorowania i ochrony
Fig. 1. Monitoring and security system diagram
Źródło: Opracowanie własne.
Source: Own elaboration.

Proponowana procedura powinna dotyczyć ochrony każdej części i strefy obiektu, w których każda z funkcji może być realizowana przez różne zespoły czujnikowe, zależnie od skuteczności metod detekcji w danym środowisku.

Według najnowszych stosowanych rozwiązań w opracowywanych technicznych projektach wykonawczych ochrony obiektów infrastruktury krytycznej należy uwzględniać:

- peryferyjne systemy ochrony budowane w oparciu o techniczne systemy ochrony zewnętrznej (PSO);
- systemy ogrodzenia pasywnego lub aktywnego;
- wewnątrzobiektowe systemy sygnalizacji włamania i napadu (SSWiN, I&HAS);
- system kontroli dostępu (SKD, ACC);
- system telewizji dozorowej CCTV;
- centrum zarządzania (nadzoru);
- okablowanie strukturalne (część pasywna i aktywna), wspólne dla wszystkich podsystemów;
- centralny system zegarowy.

2. Koncepcja Centrum Zarządzania

W ramach projektu technicznej integracji systemów bezpieczeństwa obiektu infrastruktury krytycznej wszystkie podsystemy projektowanego Zintegrowanego Systemu Bezpieczeństwa proponuje się objąć jednolitą software'ową platformą integrującą. W swoim zakresie projektowane oprogramowanie integrujące zapewnić musi zespolenie w jeden logiczny system wszystkich elementów obejmujących system detekcji wtargnięć – np. zintegrowanego systemu ochrony obwodowej i zintegrowanego zespołu radarowo-kamerowego, jak również systemu ochrony wewnętrznej. Projektowany system spełnić musi wszystkie wymagania inwestora zgodnie z profilem użytkowania obiektu/terenu, a ponadto wszystkie elementy systemu muszą być zintegrowane na poziomie programowym.

System taki powinien umożliwić:

1. Wspomaganie dowodzenia i zarządzania sytuacjami kryzysowymi w zakresie:
   - wysokospecjalistycznych reguł działania, opartych o procedury bezpieczeństwa wraz z zarządzaniem posiadanymi zasobami;
   - automatyzacji procesów wsparcia operatorów, w zakresie zarządzania i dowodzenia;
   - aktualnego monitoringu wszystkich zasobów dostępnych dla służb ochronnych,
   - możliwości prowadzenia działań dyspozytorskich;
   - optymalizacji tras w zakresie przemieszczania się po obiekcie;
   - szybkiej i niezawodnej łączności bezprzewodowej: fonicznej i wizyjnej z pracownikami służb ochrony.
2. Integrację w ramach jednorodnego systemu dyspozytorskiego cyfrowych oraz analogowych środków łączności radiowej ze środkami łączności stacjonarnej w sytuacjach kryzysowych i wymagających koordynacji pracy wielu osób i służb jednocześnie.
3. Integrację z innymi systemami zainstalowanymi na obiektach, takimi jak: CCTV, I&HAS, ACC oraz innymi systemami specjalistycznymi np. proponowanym do użycia czujnikiem zewnętrznej ochrony obiektu.

Zastosowanie takiego zintegrowanego systemu zapewni wysoką jakość działania, zwiększanie bezpieczeństwa i obniżanie kosztów operacyjnych.

Uwaga 1: System taki musi zapewnić wspomaganie zarządzania wszystkimi podsystemami, takimi jak alarmy, kontrola dostępu i wideo oraz wszystkimi zasobami, takimi jak straż i jednostki mobilne.

Uwaga 2: System musi być skonfigurowany tak, aby działał bezpośrednio z czujnikami, takimi jak kamery, czujki alarmowe czy punkty kontroli dostępu. Gorszym rozwiązaniem jest realizacja zadań poprzez zindywidualizowane systemy zarządzania dla poszczególnych roz-

DOI:10.12845/bitp.35.3.2014.1

wiązań, takich jak systemy zarządzania wideo czy systemy kontroli dostępu. Sposób konfiguracji poszczególnych podsystemów zależy głównie od specyficznych wymogów obiektu.

Wówczas tak zorganizowany i koordynowany system zapewnia autonomiczny nadzór w wybranych obszarach, zastępując ochronę i mobilne jednostki, a tym samym obniża on koszty utrzymania ochrony.

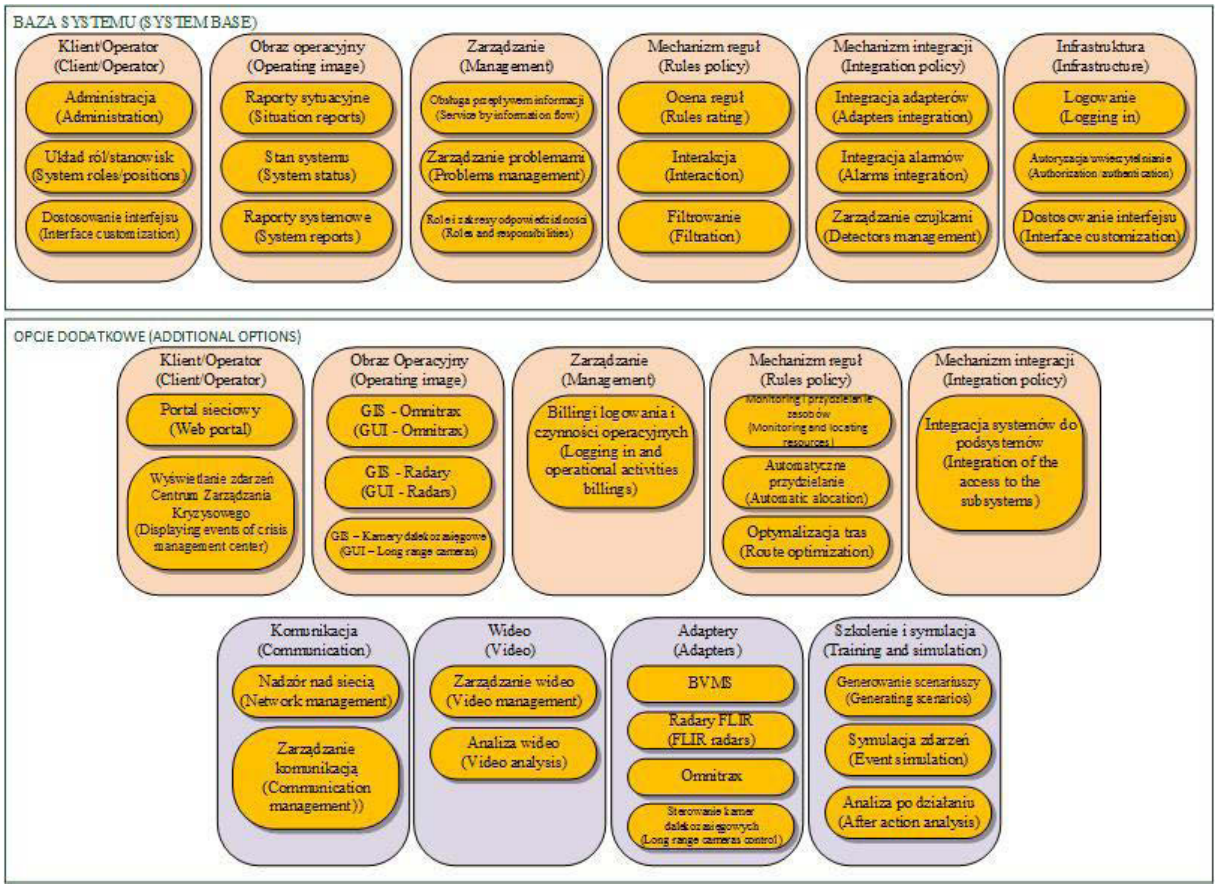
2.1. Opis architektury systemu integrującego i metod integracji podsystemów

Jak opisano wcześniej, system integrujący powinien być software'ową platformą umożliwiającą budowę zintegrowanych systemów dowodzenia i kontroli. Oznacza to, że istnieje możliwość skonfigurowania go do obsługi szerokiego zakresu podsystemów z różnymi interfejsami, począwszy od pojedynczych czujników, np. pojedyncza kamera telewizji przemysłowej, do kompletnych systemów złożonych z wielu czujników. Przykłady takich rozwiązań można spotkać w systemach ochrony obiektów, takich jak lotniska, porty morskie, rafinerie, wymagających współpracy z kilkoma tysiącami czujników, setkami klientów i tysiącami zgłoszeń na godzinę.

System, według obecnych trendów programistycznych, powinien wykorzystywać trzy warstwy modelu architektury SOA (*Service-Oriented Architecture*): warstwę źródła danych, warstwę usług oraz warstwę klienta.

Ponadto jako produkt długookresowy powinien być łatwy w utrzymaniu i umożliwiać modyfikację oraz rozbudowę konstrukcji. Warto, aby system posiadał architekturę modułową umożliwiającą konserwację części systemu, wymianę poszczególnych podsystemów, jak również testowanie wybranych fragmentów systemu bez konieczności wyłączania systemu z użytkowania. Jako modelowe oprogramowanie integrujące powinien być także napisany na bazie standardowych komponentów, co pozwala na ograniczenie ilość kodu do utrzymania. W związku z powyższym system umożliwić powinien również zarządzanie danymi urządzeń (w rozumieniu uwspólniania danych) i rejestrację zdarzeń w jednym środowisku aplikacji systemu integrującego.

System integrujący zapewnia przepływ informacji pomiędzy użytkownikami w oparciu o świadomość sytuacji operacyjnej poprzez zarządzanie zasobami systemu (nie tylko urządzeniami aktywnymi tj. czujki, kontrolery, kamery, bramki, itp..), ustalenie zadań i zakresów odpowiedzialności poszczególnych osób objętych systemem bezpieczeństwa, jak również monitorowanie i zarządzanie zasobami ludzkimi. System musi zapewniać bezpieczeństwo przepływu informacji do poszczególnych użytkowników i obejmować swym zakresem służby ochronne oraz policję, straż pożarną, pogotowie ratunkowe, służby antyterrorystyczne i inne służby publiczne (energetyka, gaz, kanalizacja, itp.).



Ryc. 2. Moduły i funkcje systemu integrującego
Fig. 2. Integrating system modules and functions
Źródło: Opracowanie własne.
Source: Own elaboration.

2.2. Opis funkcjonalności możliwych do wykorzystania w trakcie użytkowania systemu

Zintegrowana platforma bezpieczeństwa przeznaczona do ochrony obiektów infrastruktury krytycznej obejmować powinna między innymi:

1. Zintegrowany system zarządzania sensorami oraz podsystemami funkcjonalnymi (radary, system perymetryczny, system wizyjny, system BMS, itp.).
2. Zintegrowany system wsparcia dowodzenia akcją i sytuacją kryzysową obejmujący:
   – podsystem zarządzania zasobami, w tym aplikację w rozwiązaniach przestrzennych (terenach rozległych) „swój-obcy";
   – podsystem zarządzania ćwiczeniami – możliwość zaprogramowania systemu tak, aby symulował sytuację alarmową z określonymi parametrami (zakres, czas, przebieg, częstotliwość itp.);
   – podsystem zarządzania bezpieczeństwem – gdzie w sytuacjach alarmowych system podpowiada operatorowi procedury, wskazuje dostępne zasoby, automatycznie informuje wskazany personel, realizuje automatycznie określone procedury itp.;
   – podsystem zarządzania łącznością, w tym moduł dyspozytorski oraz integrujący wszystkie radiowe i przewodowe środki łączności;
   – aplikacje klienckie systemu na urządzenia przenośne wykorzystywane przez służby w terenie – umożliwiające wymianę z operatorami danych dotyczących zdarzeń i zleceń.
3. Moduł raportów umożliwiający Administracji i Zarządowi tworzenie wszelkiego rodzaju statystyk, zestawień służących do monitorowania i optymalizowania systemu bezpieczeństwa.

Dodatkowo system integrujący pozwalać powinien na elastyczność i etapowość procesów wdrażania poszczególnych elementów, wynikających z założeń inwestycyjnych, jak również operacyjnych w ramach integracji istniejących i nowo powstających systemów ochronnych oraz wsparcie przy zmianach procedur bezpieczeństwa wynikających z kolejnych etapów i nowo wprowadzanych podsystemów.

Jako wymóg podstawowy należy traktować orientację o stanie obiektu, aktualnej sytuacji ochrony i funkcjonowaniu systemu poprzez:

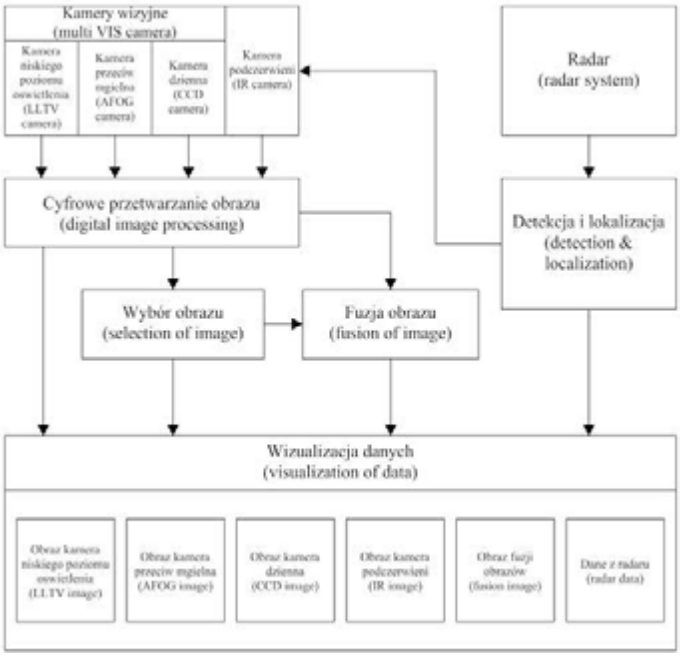
- jednolity dla wszystkich użytkowników obraz sytuacji operacyjnej w oparciu o aktualną wizję z kamer oraz aktywne podkłady syntetyczne;
- gwarancję natychmiastowej łączności fonicznej dzięki pełnej integracji z systemami telefonii stacjonarnej, komórkowej oraz radiotelefonii np. Tetra;
- dystrybucję stanu sytuacji operacyjnej i obrazów wideo do wszystkich użytkowników: stacjonarnych, mobilnych i internetowych.

2.3. Centrum Nadzoru

Budowa stanowiska zintegrowanego w pomieszczeniu Centrum Nadzoru – głównym i zapasowym, zapewni interaktywną obsługę wszystkich podsystemów poprzez kombinację wizualizacji stanów systemu, stanów alarmowych, zdarzeń alarmów technicznych i systemu podpowiedzi na zaistniałe zdarzenia wraz z wizualizacją ich na wydzielonych ekranach w postaci map synoptycznych i zrzutów z obrazów poszczególnych kamer systemu wizyjnego.

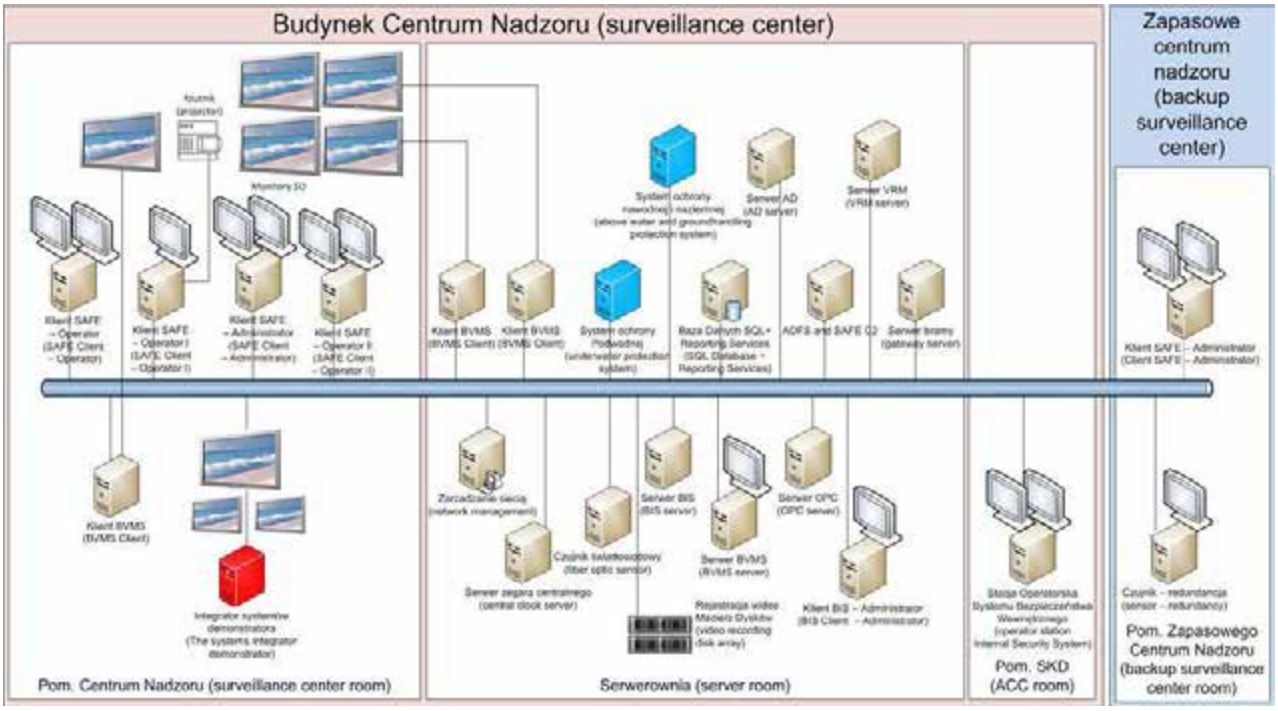
Propozycję konfiguracji architektury systemu ochrony obiektu infrastruktury krytycznej przedstawiono na przykładzie portu morskiego (ryc. 4).

Głównym założeniem budowy zintegrowanego stanowiska nadzoru jest minimalizacja osób niezbędnych do sterowania poszczególnymi, odrębnymi podsystemami. Zintegrowane stanowisko operatorskie skonstruowane powinno być tak, aby zapewnić maksymalną sprawność służb ochrony w realizowaniu zadań. Jako moduł główny systemu projektuje się uwspólnianie interfejsu opracowanego połączenia cech i funkcjonalności poszczególnych czujników systemu ochrony. Na schematach blokowych (ryc. 3 i 5) przedstawiono podstawowe funkcjonalności realizowane przez czujniki wchodzące w skład systemu ochrony portu morskiego. Na ryc. 5 zobrazowano schemat działania algorytmów odpowiedzialnych za analizę danych z kamer oraz pozostałych czujników wchodzących w skład systemu. Wizualizacja danych pomiarowych za pomocą algorytmów fuzji została zminimalizowana, przy zachowaniu pełnej informacji potrzebnej operatorowi systemu do prawidłowej reakcji na zaistniałe zdarzenia. Na ryc. 3 zobrazowano schemat działania algorytmów odpowiedzialnych za analizę danych z radaru oraz powiązanych. Przedstawiono zestaw danych, które zostają wyświetlone na pulpicie operatora.

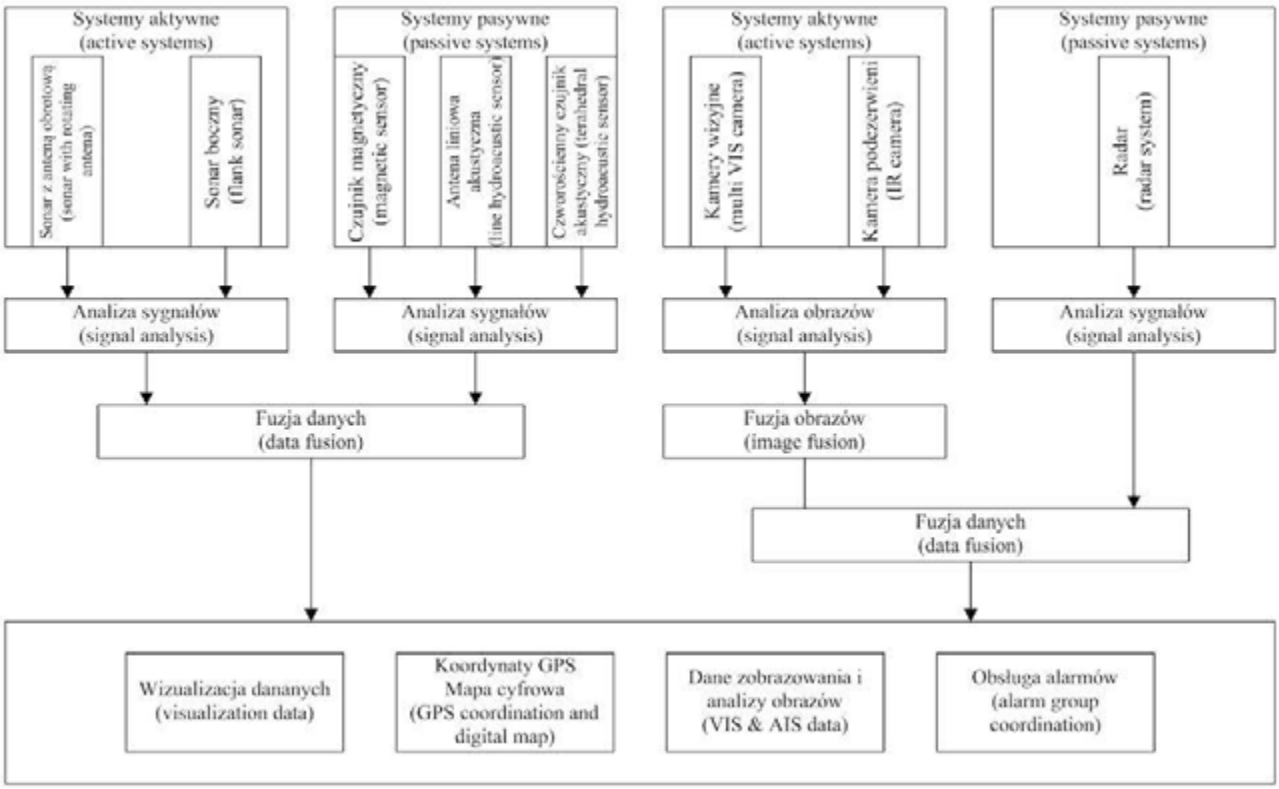


Ryc. 3. Funkcje systemu detekcji radarowo-kamerowej w systemie ochrony portu morskiego
Fig. 3. Features of radar-camera detection system protection system seaport
Źródło: Opracowanie własne.
Source: Own elaboration.

DOI:10.12845/bitp.35.3.2014.1



Ryc. 4. Architektura urządzeń systemu zarzadzania ochroną obiektów infrastruktury krytycznej portu morskiego
Fig. 4. Management architecture of critical infrastructure seaport protection system
Źródło: Opracowanie własne.
Source: Own elaboration.



Ryc. 5. Funkcje czujnikowych systemów aktywnych i pasywnych w systemie ochrony portu morskiego
Fig. 5. Sensor features of active and passive systems in seaport security
Źródło: Opracowanie własne.
Source: Own elaboration.

3. Koncepcja okablowania strukturalnego i centralnego systemu zegarowego

Okablowanie strukturalne dla systemów zabezpieczeń ma być wydzieloną instalacją niezależną od pozostałej części sieci LAN obiektów. Musi zawierać odrębne okablowanie poziome, szkieletowe i punkty dystrybucyjne. W celu wyodrębnienia przyłączy dla urządzeń zabezpieczeń należy zastosować kable skrętkowe w kolorze innym niż okablowanie komputerowe. Zalecany jest kolor zielony (nie należy stosować kabli w powłoce pomarańczo-

wej lub szarej). Komponenty użyte do budowy systemu okablowania strukturalnego (szafy 19", panele 19", kable skrętkowe) muszą pochodzić od jednego producenta i muszą być oznaczone wspólnym logo systemu okablowania dedykowanego dla systemów zabezpieczeń.

System okablowania strukturalnego ma zapewnić warstwę fizyczną, co najmniej klasy E (kategorii 6) według najnowszych standardów PN-EN 50173, ISO/IEC 11801, ANSI/TIA/EIA 568, gwarantującą niezawodne działanie aplikacji 10GBase-T (10 Gbit/s) według EN 50173-99-1, ISO/IEC TR 24750, TIA-TSB-155. Dla podwyższenia niezawodności należy zastosować łącza zbudowane z kabla skrętkowego kategorii 6A zakończonego złączami kategorii 6. Dla połączeń światłowodowych należy użyć komponentów jednomodowych SM.

Instalowane okablowanie strukturalne musi posiadać deklarację zgodności z najnowszymi normami dotyczącymi okablowania strukturalnego oraz systemów zabezpieczeń. Dla zapewnienia elastyczności system musi umożliwiać swobodną rozbudowę oraz rekonfigurację.

Obecnie w ramach dowolnego projektu ochrony przewiduje się utworzenie zintegrowanego sieciowego systemu bezpieczeństwa zbudowanego w oparciu o szereg podsystemów. Każdy z tych serwerów opracowuje zespół danych, które zapisywane są w urządzeniach rejestrujących za pomocą znaczników czasu. Aby sprawnie zarządzać zapisanym materiałem archiwalnym i móc prawidłowo przypisać zdarzenie do jego zapisu weryfikacyjnego dowolnego podsystemu, należy zastosować system zegara centralnego. W związku z tym, że jest to system sieciowy zamknięty, proponuje się wykorzystanie własnego sieciowego serwera czasu. Umożliwi on ujednolicenie czasu systemowego na wszystkich urządzeniach, a ponadto zabezpieczy system bezpieczeństwa przed nieuprawnionym wejściem hackerskim w powiązania sieciowe, gdyby system korzystał z zewnętrznych serwerów czasu.

4. Przykładowa koncepcja typowego peryferyjnego systemu ochrony w oparciu o architekturę portu morskiego (PSO)

Zgodnie z opisem wymagań na wielobranżowy zintegrowany system ochrony portu morskiego [8, 9] proponuje się system, który ma zawierać:

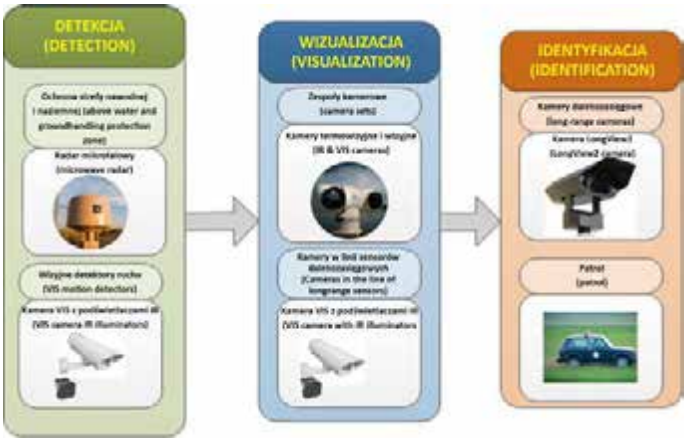
- Czujniki ochrony nawodnej, w skład których wchodzą:
  a. kamery wizyjne, termowizyjne dalekozasięgowe do zobrazowania powierzchni;
  b. radary mikrofalowe do wykrywania obiektów na powierzchni strefy chronionej,
- Czujniki ochrony podwodnej, do których zaliczają się:
  a. aktywny sonar wysokiej częstotliwości do wykrywania obiektów podwodnych oraz analizy kadłubów wpływających jednostek;
  b. podwodne pasywne bariery akustyczne i magnetyczne do wykrycia oraz lokalizacji obiektów naruszających strefę bezpieczeństwa portu.
- Czujniki ochrony naziemnej strefy brzegowej portu morskiego, w skład których wchodzą:
  a. kamery wizyjne, termowizyjne dalekozasięgowe do zobrazowania chronionej strefy naziemnej;
  b. radary mikrofalowe do wykrywania obiektów na obszarze naziemnym strefy chronionej.

W projekcie morskim, ze względu na jego charakter, zakłada się użycie następujących urządzeń do budowy peryferyjnego systemu ochrony (PSO) w celu detekcji próby wtargnięć na obszar chroniony:

- wytworzenie wirtualnych nawodnych i naziemnych stref detekcji (związanych ze swoim położeniem z granicą obszaru portu morskiego strefy przybrzeżnej) przez radary mikrofalowe zakresu 35 lub 77 GHz. Ryc. 6 przedstawia koncepcję połączenia i funkcje elementów składowych systemu ochrony strefy naziemnej i nawodnej systemu;
- nadzór strefy chronionej z wykorzystaniem zespołu radarowego za pomocą kamer z oświetlaczami w zakresie bliskiej podczerwieni 940 nm, rozstawionymi w miejscu związanym z umiejscowieniem radarów. Kamery wyposażone będą w inteligentną analizę ruchu w obrazie umożliwiającą wytworzenie strefy detekcji i będą generowały sygnał alarmu w momencie prób ich przekroczenia.

Identyfikacja zdarzeń wykrytych za pomocą czujników mikrofalowych i zweryfikowanych przez zespoły kamerowe ma odbywać się za pomocą:

- dalekozasięgowych kamer niskiego poziomu oświetlenia z funkcją anty-FOG, LLTV oraz panoramy;
- przejazdu Patrolu SOL na zidentyfikowane miejsce wtargnięcia.



Ryc. 6. Koncepcja nawodnego i naziemnego systemu ochrony portu morskiego
Fig. 6. Concept of above and underwater seaport surveillance system
Źródło: Opracowanie własne.
Source: Own elaboration.

5. Przykładowy system ogrodzenia aktywnego

Na wielobranżowy zintegrowany system ochrony proponuje się zestaw, który ma zawierać co najmniej:

- monitoring całej strefy ogrodzenia obiektowego np. za pomocą czujnika światłowodowego [10-13];

DOI:10.12845/bitp.35.3.2014.1

- monitoring otwartych, szczególnych stref zastrzeżonych za pomocą nadzoru kamerowego z detekcją ruchu dot. części terenu newralgicznego.

Wizualizacja zdarzeń strefy wewnętrznej zapewniona musi być przez zestawy kamerowe na głowicy uchylno-obrotowej (kamery wizyjne z podświetlaczami). Identyfikacja zdarzeń zdetekowanych w strefach objętych ogrodzeniem, a nieobjętych zasięgiem np. przez radary mikrofalowe następować musi przez:

- kamery niskiego poziomu oświetlenia stałopozycyjne i na głowicach uchylno-obrotowych;
- czujnik światłowodowy mocowany na ogrodzeniu portu;
- przejazd patrolu na zidentyfikowane co do położenia miejsce na terenie.

Ryc. 7. Koncepcja systemu ochrony części obiektowej objętej ogrodzeniem
Fig. 7. Concept of seaport fenced area surveillance system
Źródło: Opracowanie własne.
Source: Own elaboration.

Podstawą organizacji systemu ochrony obwodowej obiektu infrastruktury krytycznej, ze względu na podniesienie skuteczności systemu zintegrowanego, jest detekcja prób wtargnięcia intruza na teren przez forsowanie ogrodzenia. Ryc. 7 przedstawia koncepcję połączenia i funkcje elementów składowych systemu ogrodzenia aktywnego. W grupie czujników ogrodzeniowych rozumianych jako bariery mechaniczno-elektroniczne, jak również czujników elektronicznych montowanych na ogrodzeniu, ze względu na elastyczność układania i parametry detekcji, wyróżniają się czujniki światłowodowe. Ich główną zaletą jest to, iż nie wymagają budowania infrastruktury strefowego zbierania sygnałów elektrycznych. Współczesne rozwiązania czujników światłowodowych umożliwiają detekcję zaburzenia (oddziaływanie masy powyżej 20 kg na ogrodzenie) na odcinku 40 km z rozdzielczością 5 metrów. Dlatego w wielu rozwiązaniach koncepcji ochrony obiektów infrastruktury krytycznej wstępnie proponujemy użycie tego elementu jako podstawowego czujnika ochrony obwodowej.

Same czujniki światłowodowe budowane są w różnych konfiguracjach, ale zapewniają bardzo wysoki poziom detekcji, ponadto są rozwiązaniami dyskretnymi, ekonomicznymi i elastycznymi w konfigurowalności stref ochrony. Na obecnym etapie rozwoju technologicznego możemy mówić o światłowodowych czujnikach ochrony obwodowej: polaryzacyjnych, z wykorzystaniem światłowodowych siatek Bragga, jak również interferometrycznych. Najlepszym rozwiązaniem, stosowanym w obiektach typu więzienia, lotniska i rafinerie w Australii, USA, EU, jest czujnik interferometryczny, który pokazuje zmiany natężenia światła w czujnikowym światłowodzie jednomodowym dochodzącego do detektorów optycznych z całego toru światłowodu czujnikowego. Układ czujnika sygnalizuje zaistnienie sygnału alarmu wywołanego poruszaniem się ogrodzenia oraz dokonuje pomiaru różnicy czasowej, dojścia sygnałów zaburzeń do odpowiednich detektorów w przeciwstawnych torach optycznych. Pomiar różnicy czasów umożliwia wyznaczenie miejsca tego zdarzenia z dużą, opisaną wyżej, rozdzielczością.

Zgodnie z założeniami zastosowanie światłowodowej detekcji wielokilometrowej na ogrodzeniu wyeliminuje potrzebę budowy skomplikowanej infrastruktury elektronicznej. Ponadto wymienione rozwiązania umożliwiają równoległe prowadzenie w kablu sensorycznym dodatkowych włókien światłowodowych, które z powodzeniem mogą być wykorzystane np. dla potrzeb telewizji dozorowej. W ramach użycia na obiektach specjalnych jego podstawową zaletą jest to, iż nie emituje żadnego promieniowania i jest pod tym względem bezpieczny – np. neutralny dla atmosfery wybuchowej. W związku z powyższym ochrona obwodowa, obejmująca ogrodzenie ciągłe zamontowane na gruncie, powinna być zapewniona przez takiego typu czujnik. W komercyjnym wydaniu produkowany jest on przez kilka firm. Zaawansowana technologicznie analiza sygnału w czujniku tego typu umożliwia określenie lokalizacji powstania zakłócenia (z dokładnością do ok. 20 metrów) i określenie jego typu. Określenie typu oznacza możliwość rozpoznania zakłócenia wywołanego przez wiatr, burze, samolot, ptaki czy małe zwierzęta i niezgłaszanie alarmu w takim przypadku, jak również rozpoznanie, że źródłem zakłócenia jest np. wtargnięcie człowieka lub zwierzęcia o określonej wadze i zgłoszenie tego faktu jako alarm. Możliwe jest również rozróżnienie, czy alarm wywołany jest próbą sforsowania ogrodzenia albo próbą niszczenia opłotowania. Fizycznie światłowód powinien być instalowany na ogrodzeniu o dobrej jakości, zgodnej z wymogami normatywnymi. Odcinek, w którym światłowód funkcjonuje jako czujnik, wyznaczany jest tylko przez jeden kabel światłowodowy, który nie musi być doprowadzony ponownie do Centrum Nadzoru. Długość tego odcinka może wynosić obecnie maksymalnie 40 km i pomiędzy sterownikami system nie wymaga instalacji żadnych innych elementów elektronicznych i doprowadzania zasilania. Dzięki temu instalacja jest szybka, prosta i tania w utrzymaniu. Ponadto czujnik umożliwia dowolne kształtowanie stref ochrony w zależności od wymagań, od ukształtowania ogrodzenia i sposobu rozłożenia czujnika na nim. Strefy programuje się software'owo już po instalacji i można je dowolnie kształtować zgodnie z wymogami administratora w celu odpowiedniego obrazowania sytuacji alarmowych w zintegrowanym systemie ochrony. Dodatkowym atutem takiego rozwiązania jest to, że przy wykorzystaniu go jako typowego medium telekomunikacyjnego może być dowolnie kształtowane przy zmianach w systemie ogrodzenia terenu portu, a wymagana korekta software'owa

Światłowodowy kabel czujnikowy / fiber optic sensor cable

Ryc. 6. Przykładowy sposób instalacji czujnika światłowodowego na ogrodzeniu
Fig. 6. Installation example of optical fiber sensor on fence
Źródło: Opracowanie własne.
Source: Own elaboration.

nie stanowi wyzwania dla przeszkolonego administratora systemu. Jak widać na ryc. 6, zainstalowany kabel czujnikowy jest bardzo dyskretny.

Dodatkowo opcjonalnie istnieje możliwość wprowadzenia redundancji czujnika światłowodowego rozpostartego na parkanie technicznym poprzez zakopanie drugiego światłowodu w linii ogrodzenia. To dodatkowo wprowadza możliwość bardziej skutecznego wykrywania prób wykonania podkopów pod ogrodzeniem. Naprawa kabla czujnikowego jest w tym przypadku taka sama jak naprawa światłowodowego kabla telekomunikacyjnego i przywraca sprawność systemu w stu procentach. Jak wspomniano wcześniej, system światłowodowy umożliwia wirtualne, programowo zmieniane w dowolnym momencie, zakładanie stref. Każda ze stref ochrony objętej czujnikiem światłowodowym może znajdować się, zgodnie z założonymi procedurami, w stanie aktywnym wyłączonym z eksploatacji (tam, gdzie wymagane było prowadzenie czujnika w strefie otwartej), w stanie tzw. „cichego czuwania", jak również w stanie zdezaktywowanym, o czym decyduje operator. Dlatego system umożliwia czasową, w trybie rzeczywistym, dezaktywację określonych stref oraz bram w przypadku ich otwarcia przez obsługę. Może to działać tak samo jak uprawnione otwarcie drzwi w systemie kontroli dostępu. System światłowodowy posiada zaimplementowane w swoim sterowniku procedury autotestowania w formie ciągłego monitoringu sygnału z czujnika, co wynika z natury jego działania. Jednym z objawów ich funkcjonowania jest wskazywanie w czasie rzeczywistym faktu wystąpienia uszkodzenia kabla czujnikowego i wskazania jego miejsca. Opisany rodzaj czujnika należy do grupy czujników ogrodzeniowych i mimo częstych błędnych informacji posiada parametry detekcji zgodne z tego typu klasą urządzeń, tzn. mniej niż jeden fałszywy alarm na strefę (zakładana w systemach ochrony około 100 m) w miesiącu. Ponadto system charakteryzuje się długim czasem *Mean Time Between Failures* (MTBF) powyżej > 40,000 godzin (około 5 lat). Należy wówczas wykonać konserwację systemu i krótki czas naprawy *Mean Time to Repair* (MTTR) < 2 godzin.

Podsumowując, system światłowodowy w budowanym zintegrowanym systemie bezpieczeństwa umożliwi/zapewni:

- wymagane funkcjonalności jako czujnik ochrony obwodowej,
- ekonomiczność rozwiązania; czujnik jest układem liniowym o rozłożonej czułości, więc w przeciwieństwie do każdego innego rozwiązania nie wymaga instalowania żadnego układu centrali/podcentrali w trakcie ogrodzenia i w granicach wyznaczanych stref, co powoduje, iż nie trzeba budować infrastruktury technicznej typu studzienki kanalizacyjne, skrzynki na elementy elektroniczne wymagające ogrzewania oraz układy zabezpieczające tory transmisyjne i zasilające od wyładowań atmosferycznych,
- elastyczność i konfigurowalność rozwiązania; czujnik tego typu może posiadać całkowitą długość około 40 km, w związku z tym umożliwi zabezpieczenie całości ogrodzenia. Zapewni ponadto możliwość przesunięcia go w ramach zmian w czasie przyszłego użytkowania, w tym umożliwi wydłużenie go.

6. Wnioski

Z naszej dotychczasowej praktyki wynika, iż największe problemy z organizacją zintegrowanych systemów ochrony infrastruktury krytycznej pojawiają się w obszarze budżetu. Potencjalnych inwestorów nie stać na dobrze zaplanowany i technicznie nowoczesny system wykorzystujący najnowsze zdobycze wiedzy i techniki. System, który jednocześnie będzie dopasowany do warunków środowiskowych, adekwatny do założeń ochrony i odpowiedni do funkcji, które musi spełnić. W wybranym zakresie brakuje w chwili obecnej kompleksowych rozwiązań ochrony. Tam, gdzie to zapoczątkowano, główny nacisk położono na rozwinięcie systemów, którym autorzy celowo nie poświęcili większej uwagi, tzn. organizacji kontroli dostępu, wewnątrzobiektowej ochronie alarmowej czy telewizji dozorowej. Ponadto niewielki zasób fachowej literatury w języku polskim oraz ograniczone zasoby angielskojęzyczne powodują trudności w dostosowaniu systemu do wymagań bezpieczeństwa stawianych obiektom infrastruktury krytycznej.

Inwestorzy zachęceni przez dystrybutorów możliwościami detekcji obrazowej starają się zastąpić tą techniką cały system ochrony. Dlatego na polskim rynku pojawiły się rozwiązania bazujące na detekcji w obrazie,

DOI:10.12845/bitp.35.3.2014.1

tak przecież wrażliwej na zmiany warunków oświetlenia, oraz na wykorzystaniu kamer megapikselowych, co jak wiadomo, pociąga za sobą koszty związane z archiwizacją materiału wideo. Kluczowe więc z punktu widzenia autorów jest wdrożenie, nawet etapowo, zintegrowanego wielosensorowego systemu dopasowanego do wymagań danego obiektu systemu ochrony zbudowanego na software'owym systemie integrującym zorientowanym na zarządzanie informacją, a tym samym zasobami ludzkimi.

7. Podsumowanie

W artykule przedstawiono wymagania projektowe oraz najważniejsze funkcjonalności nowoczesnych systemów ochrony w aspekcie ochrony obiektu infrastruktury krytycznej – portu morskiego. Zaprezentowana została koncepcja zintegrowanego systemu ochrony obiektów infrastruktury krytycznej. Na bazie doświadczeń nabytych podczas projektowania systemów ochrony różnych obiektów infrastruktury krytycznej w artykule szczególną uwagę zwrócono na procedury działania systemu bezpieczeństwa oraz na przepływ informacji pomiędzy podsystemami w zintegrowanym systemie ochrony.

Literatura

1. Zdanowicz W., *Ochrona żeglugi i portów morskich (część I)*, „Zabezpieczenia" Issue 6, 2009.
2. Zdanowicz W., *Ochrona żeglugi i portów morskich (część II)*, „Zabezpieczenia" Issue 1, 2010.
3. Stateczny A., Kazimierski W., Wawrzyniak N., *Analiza funkcjonalności geoinformatycznego systemu ochrony portu*, „Archiwum Fotogrametrii, Kartografii i Teledetekcji" Vol. 23, 2012, 397-406.
4. Ciurapiński W., Dulski R., Kastek M., Szustakowski M., Bieszczad G., Życzkowski M., Trzaskawka P., *Data fusion concept in multispectral system for perimeter protection of stationary and moving objects*, „Electro-Optical and Infrared Systems: Technology and Applications VI" Vol. 7481, 748111, 2009.
5. Vokorokos L., Chovanec M., Latka O., *Security of Distributed Intrusion Detection System Based on Multisensor Fusion*, 6th International Symposium on Applied Machine Intelligence and Informatics (SAMI), 2008, 19-24.
6. Kastek M., Dulski R., Życzkowski M., Szustakowski M., Ciurapiński W., Firmanty K., Pałka N., Bieszczad G., *Multisensor systems for security of critical infrastructures – Concept, data fusion, and experimental results*, International Symposium on Photoelectronic Detection and Imaging 2011: Advances in Infrared Imaging and Applications, Vol. 8193, 81933X, 2011.
7. Szustakowski M., Ciurapiński W., Życzkowski M., Pałka N., Kastek M., Dulski R., Bieszczad G., Sosnowski T., *Multispectral system for perimeter protection of stationary and moving objects*, „Electro-Optical and Infrared Systems: Technology and Applications VI" Vol. 7481, 74810D, 2009.
8. Życzkowski M., Pałka N., Trzciński T., Dulski R., Kastek M., Trzaskawka P., *Integrated radar-camera security system – experimental results*, "Radar Sensor Technology XV" Vol. 8021, 80211U, 2011.
9. Giompapa S., Gini F., Farina A., Graziano A., Croci R., Distefano R., *Maritime border control multisensor system*, "Aerospace and Electronic Systems Magazine" Vol. 24 Issue 8.
10. Życzkowski M., Szustakowski M., Ciurapiński W., Pałka N., Kastek M., *Integrated optoelectronics security system for critical infrastructure protection*, "Przegląd Elektrotechniczny" Vol. 86 Issue 10, 2010, 157-160.
11. Maki M.C., *Fiber optic fence sensor developments*, "Aerospace and Electronic Systems Magazine" Vol. 19 Issue 2.
12. Zyczkowski M., *Intruder localization and identification in fiber optic systems,* "Optics and Photonics for Counterterrorism and Crime Fighting IV" Vol. 7119, 71190L, 2008.
13. Zyczkowski M., Ciurapinski W., *Fibre optic sensor with disturbance localization in one optical fibre*, O"ptical Sensing Technology and Applications" Vol. 6585, 2007.

ppłk dr inż. Marek Życzkowski – adiunkt w zakładzie systemów optoelektronicznych Instytutu Optoelektroniki Wojskowej Akademii Technicznej

prof. dr hab. inż. Mieczysław Szustakowski – kierownik zespołu systemów bezpieczeństwa i analizy zagrożeń w Instytucie Optoelektroniki Wojskowej Akademii Technicznej

ppłk dr inż Rafał Dulski – adiunkt w zakładzie techniki podczerwieni i termowizji Instytutu Optoelektroniki Wojskowej Akademii Technicznej

dr inż. Mariusz Kastek – adiunkt w zakładzie techniki podczerwieni i termowizji Instytutu Optoelektroniki Wojskowej Akademii Technicznej

dr inż. Wiesław Ciurapiński – kierownik zakładu systemów optoelektronicznych Instytutu Optoelektroniki Wojskowej Akademii Technicznej

mgr inż. Mateusz Karol – doktorant w Instytucie Optoelektroniki Wojskowej Akademii Technicznej

mgr inż. Piotr Markowski – doktorant w Instytucie Optoelektroniki Wojskowej Akademii Technicznej