NR 3/2019 maj/czerwiec

Ochrona Mienia i Informacji

Cena 16,90 (w tym 8% VAT), nr ind. 381756

14 Monitoring wizyjny i termowizyjny terenów przygranicznych

20 Sygnalizator SAOZ-PK2 – nowe podejście do sygnalizacji w zewnętrznych systemach sygnalizacji przeciwpożarowych –artykuł Grupy W2

33 Ochrona i obrona baz i obiektów wojskowych

49 Przeglądy DSO i Central Sygnalizacji Pożarowej

NOWY
ZEWNĘTRZNY SYGNALIZATOR
AKUSTYCZNO - OPTYCZNY

www.w2.com.pl

SAOZ-Pk2

NOWA KONSTRUKCJA LAMPY

POŻAR

NIŻSZY POBÓR PRĄDU

SYNCHRONIZACJA CZĘSCI AKUSTYCZNEJ I OPTYCZNEJ

POLSKI PRODUCENT 20 LAT NA RYNKU

ISSN 1732-5951

28 LAT DBAMY O BEZPIECZEŃSTWO LUDZI I MIENIA.

RAJ
INTERNATIONAL

- **KONCEPCJE**
- **PROJEKTY**
- **MONTAŻ**
- **KONSERWACJA**
- **SERWIS**

- **SYSTEMY SYGNALIZACJI POŻARU**
- **DŹWIĘKOWE SYSTEMY OSTRZEGAWCZE**
- **STAŁE URZĄDZENIA GAŚNICZE**
- **SYSTEMY ODDYMIANIA**
- **SYSTEMY SYGNALIZACJI WŁAMANIA**
- **SYSTEMY KONTROLI DOSTĘPU**
- **SYSTEMY TELEWIZJI PRZEMYSŁOWEJ**
- **SYSTEMY OKABLOWANIA STRUKTURALNEGO**
- **INTEGRACJA SYSTEMÓW BEZPIECZEŃSTWA**

RAJ International Sp. z o.o.
ul. Wał Miedzeszyński 552B
03-994 Warszawa
tel. 22 679-92-11
raj-biuro@raj-international.net

www.raj-international.net

Szanowni Czytelnicy,

Ochrona Mienia i Informacji

Trzeci tegoroczny numer Ochrony Mienia i Informacji poświęcamy szeroko rozumianemu bezpieczeństwu publicznemu. Mamy głównie na uwadze różnego rodzaju rozwiązania techniczne i organizacyjne stosowane w służbach, które z racji wykonywanych zadań zobowiązane są do zapewnienia nam obywatelom, a także naszemu państwu warunki do spokojnego i bezpiecznego życia i funkcjonowania. I tak zapewnienie bezpieczeństwa na naszych granicach zewnętrznych wymaga od Straży Granicznej, nie tylko dobrego wyszkolenia zawodowego i czujności podczas wykonywania obowiązków, ale również nowoczesnych systemów technicznych, które wspomogą działania strażników granicznych w trudnych warunkach atmosferycznych, podczas wzmożonego ruchu na przejściach granicznych, podczas prób zorganizowanego przemytu itp. O najnowszych rozwiązaniach technicznych wspomagających pracę Straży Granicznej traktują m.in. artykuły: Monitoring wizyjny i termowizyjny obszarów przygranicznych i Kontrola dostępu oraz Kontrola ruchu osobowego i ruchu towarowego na przejściach granicznych.

Ochrona i obrona obiektów wojskowych podlega regulacjom zapisanym między innymi m.in. w regulaminach: ogólnym SZ RP, działań sił lądowych, a także w normie obronnej SZ RP. Podczas misji zagranicznych ochrona polskich kontyngentów musi obejmować również specyfikę działań wynikających z określonej sytuacji politycznej, geograficznej i militarnej. Problematykę związaną z ochroną i obroną obiektów wojskowy poruszamy w tym numerze, w dwóch aspektach. Po pierwsze prezentując stosowane przez nasze siły zbrojne rozwiązania organizacyjne i techniczne baz wojskowych, tych położonych na terenie kraju oraz tych, które tworzone są w ramach naszych misji zagranicznych naszych. Po drugie przedstawiając wnioski wynikające z wprowadzonej w SZ nowej normy obronnej, która zobowiązuje firmy do dostarczania i instalowania na terenie obiektów wojskowych systemów alarmowych i przeciwpożarowych spełniających określone w tej normie wymagania. Ale ochrona obiektów wojskowych to również ochrona przeciwpożarowa. W bieżącym numerze przedstawiamy pierwszą część prezentacji na temat Wojskowej Ochrony Przeciwpożarowej, skupiając się na jej rysie historycznym i obecnej strukturze organizacyjnej. W kolejnym numerze przedstawimy zadania i obowiązki WOP oraz scharakteryzujemy wojskowe straże pożarne.

Poza tym czytelnik znajdzie w bieżącym numerze rozważania na temat zastosowań Dźwiękowych Systemów Ostrzegawczych na obiektach specjalnych, w których wymaga się zastosowania pewnych specyficznych rozwiązań, na temat tej wybranej grupy systemów ochrony perymetrycznej, jaką z pewnością są systemy doziemne, a także na temat wielu różnych zastosowań dronów w codziennej służbie policji.

Międzynarodowa konferencja techniczno-ochronna Securitech-SW, która odbywała się corocznie w latach 2015–2018, trwale wpisała się w potrzeby Służby Więziennej, jak i w krajobraz Centralnego Ośrodka Szkolenia SW w Kaliszu. Poruszana tematyka konferencji związana była z bieżącymi potrzebami SW, a udział innych służb pozwalał na wzajemną wymianę doświadczeń. Nasza redakcja postanowiła zaprezentować Państwu cykl artykułów, pod ogólnym hasłem „Securitech, wartość pokonferencyjna", w których pragniemy Państwu przedstawić, jak rozwiązania techniczne prezentowane podczas tej konferencji zostały wykorzystane w praktyce. Pierwszy z cyklu artykułów, autorstwa Cezarego Mecwaldowskiego, przedstawia jedno z dedykowanych rozwiązań technicznych, jakie wypracowano i zaprezentowano w trakcie konferencji, pozwalające na szerokie zastosowanie w ochronie obiektów elektronicznych zabezpieczeń krat, wygrodzeń z siatki, włazów i bram Jest to rozwiązanie z urządzeniami bezprzewodowymi.

Poza tym w numerze, jak zawsze wywiady z ciekawymi osobami z branży zabezpieczeń, relacje z konferencji, wystaw i spotkań branżowych, a także kilka ciekawych artykułów firmowych prezentujących najnowsze rozwiązania technologiczne w systemach zabezpieczeń technicznych.

W imieniu zespołu redakcyjnego i własnym życzę Państwu miłej lektury.

Krzysztof Surdyk
Redaktor naczelny

AKTUALNOŚCI I INFORMACJE BRANŻOWE

V Branżowe Spotkanie Kobiet 2019 – Hotel FOLWARK Łochów **4**

Lider Bezpieczeństwa Państwa 2019 – Gala Wręczenia Nagród w Warszawie **6**

XVII Południowa Edycja SPIN2019 w ZAKOPANEM – otwarcie rejestracji dla uczestników **6**

FIRE EXPO SECURITY – 16 Edycja Kongresu Pożarnictwa na PGE Narodowym **7**

CNBOP – Spotkanie Projektantów Systemów Niskoprądowych – prezentacja i omówienie nowości produktowych i systemowych Firmy BOSCH **11**

Historia pierwszej kamery sieciowej na świecie Firmy AXIS **48**

WYWIAD

Wywiad z Panem Konradem Badowskim – Poland, Ukraine & Baltics Business Relationships Manager AXIS Communications – rozmowa Krzysztofa Surdyka **8**

PROJEKTY

Ochrona perymetryczna

SECURITECH, wartość pokonferencyjna. Zabezpieczenia elektroniczne krat, wygrodzeń z siatki, włazów i bram **12**
– artykuł Cezarego Mecwaldowskiego

Zasilacze UPS

Nowe rozwiązania w dziedzinie zasilaczy UPS **37**
– artykuł Firmy IMPAKT S.A.

ZARZĄDZANIE

Monitoring wizyjny i termowizyjny

Monitoring wizyjny i termowizyjny terenów przygranicznych **14**
– artykuł Rafała Rotbluma

Ochrona przeciwpożarowa

Ochrona przeciwpożarowa w Siłach Zbrojnych RP cz. I. Współczesność i tradycje **17**
– artykuł Emila Ćwiklińskiego

Zewnętrzne systemy przeciwpożarowe

Sygnalizator SAOZ-PK2 –nowe podejście do sygnalizacji akustyczno-optycznej w zewnętrznych systemach przeciwpożarowych **20**
– artykuł Firmy W2

Bezpieczeństwo Państwa

Zabezpieczenie infrastruktury krytycznej wymogiem prawidłowego funkcjonowania państwa **22**
– artykuł Firmy MIWI-URMET

Akty prawne ochrony obiektów

Doświadczenia ze stosowania uaktualnionej normy obronnej w Siłach Zbrojnych RP **24**
– artykuł Jacka Popławskiego

Ochrona perymetryczna

Doziemne systemy Ochrony perymetrycznej **28**
– artykuł redakcyjny

Ochrona obiektów wojskowych

Ochrona i obrona baz i obiektów wojskowych **33**
– artykuł Krzysztofa Surdyka

Systemy ochrony granic i przejść granicznych

Kontrola dostępu, ruchu osobowego i towarowego oraz ochrona na przejściach granicznych **43**
– artykuł Damiana Żabickiego

Nowe technologie dla policji

Drony w służbie Policji **46**
– artykuł Damiana Żabickiego

INSTALACJE

Dźwiękowe Systemy Ostrzegawcze

DSO w zastosowaniach specjalnych **40**
– artykuł redakcyjny

PRZEGLĄDY

Przegląd DSO TOA **49**
Przegląd DSO SCHRACK **50**
Przegląd Central Sygnalizacji Pożarowej RAJ **51**
Przegląd Central Sygnalizacji Pożarowej Siemens **52**
Przegląd Central Sygnalizacji Pożarowej SCHRACK **53**
Przegląd Central Sygnalizacji Pożarowej SATEL **54**
Przegląd Central Sygnalizacji Pożarowej MIWI-URMET **55**

OD WYDAWCY

56

REKLAMODAWCY

W2	I okładka, 20–21
RAJ	II okładka, 51
SPIN 2019	3
SECURITECH & DEFENSE 2019	5
PRENUMERATA	15
MIWI-URMET	23, 55
OPTEX	29
PARTNER	41
SPY SHOP	III okładka
SECUREX 2020	IV okładka

17 SPIN

Edycja jesienna - Polska Południowa

Spotkanie Projektantów Instalacji Niskoprądowych

25-26 WRZEŚNIA 2019

Nosalowy Dwór Resort & SPA | Zakopane

www.spin.lockus.pl
www.facebook.com/SPINiSPINExtra

MERCORS.A. zaprasza na prelekcję „Zasilanie urządzeń przeciwpożarowych” poczas 17 edycji Spotkania Projektantów Instalacji Niskoprądowych

mercor®
Współpraca z potencjałem

CENTRALE I ZASILACZE AUTOMATYKI POŻAROWEJ

V BRANŻOWE SPOTKANIE KOBIET 2019

W dniach 13–14 czerwca br firma Schrack Seconet Polska Sp. z o. o. zorganizowała V Jubileuszowe Branżowe Spotkanie Kobiet. W tym wyjątkowym wydarzeniu wzięło udział kilkadziesiąt Pań, reprezentujących firmy z całego kraju – przedstawicielek kadry zarządzającej, projektantek, specjalistek z różnych dziedzin systemów bezpieczeństwa.

Obszar systemów zabezpieczeń obiektów to w większości domena mężczyzn, którzy z reguły są głównymi uczestnikami branżowych spotkań, konferencji, szkoleń czy targów. Kobiety, które wkładają równie wiele wysiłku i pracy, są doskonałymi specjalistami w swoich dziedzinach – projektują, kosztorysują, instalują, a nawet uruchamiają systemy bezpieczeństwa, na co dzień rzadko wysuwają się na pierwszy plan. Schrack Seconet Polska w roku 2015 po raz pierwszy zorganizowała spotkanie, które było dedykowane wyłącznie Paniom – ekspertkom, specjalistkom zaangażowanym w rozwój wymagającej branży systemów zabezpieczeń.

V Branżowe Spotkanie Kobiet odbyło się w tym roku poza Warszawą, w malowniczej okolicy Pałacu i Folwarku w Łochowie.

Rozpoczęło się szkoleniem z wizualnego myślenia, dzięki któremu uczestniczki mogły trochę lepiej poznać siebie i techniki wizualnej komunikacji. Przed wieczorną kolacją Panie miały czas na chwilę relaksu i oderwanie się od codzienności w strefie Wallnes i SPA. Równolegle odbyły się także zajęcia z jogi i zumby.

Pozytywne nastroje podczas spotkania wieczornego pozwoliły na wielogodzinne rozmowy nie tylko okołobiznesowe.

W tegorocznym spotkaniu wzięło udział ponad sześćdziesiąt Pań z 32 firm zlokalizowanych w całej Polsce. Niezależnie od długości współpracy pomiędzy poszczególnymi firmami wielu Paniom to wydarzenie po raz pierwszy dało możliwość spotkania na żywo.

Organizatorzy pragną gorąco podziękować wszystkim Uczestniczkom **V Branżowego Spotkania Kobiet** – 2019 mając jednocześnie nadzieję na spotkanie za rok w jeszcze większym gronie.

SECURITECH & DEFENSE 2019

Konferencja dla wojska

NOWOCZESNE TECHNOLOGIE MILITARNE I CYWILNE

TERMIN: **18–19 września 2019**

MIEJSCE: **Lotnicza Akademia Wojskowa – Dęblin**

Ochrona Mienia i Informacji

www.defense.securitech.edu.pl

UROCZYSTA GALA WRĘCZENIA NAGRÓD „LIDER BEZPIECZEŃSTWA PAŃSTWA 2019”

14 czerwca br. w Centrum Konferencyjnym MON w Warszawie odbyła się uroczysta gala wręczenia nagród w ogólnopolskim konkursie „Lider Bezpieczeństwa Państwa” organizowanym przez Stowarzyszenie Dostawców na Rzecz Służb Mundurowych z siedzibą w Bydgoszczy. Celem konkursu jest nagradzanie osiągnięć polskich przedsiębiorców, realizujących swoją aktywność zawodową w obszarze umacniania istniejącego potencjału bezpieczeństwa narodowego.

W VII edycji Konkursu „Lider Bezpieczeństwa Państwa – 2019” laureatów wyłaniano w dwóch kategoriach: „Produkt” oraz „Innowacyjna firma”. W Kategorii „Produkt” nagrodzone zostały nowatorskie wyroby najwyższej jakości, projekty, jak również usługi, zgłoszone do oceny przez firmy i instytucje, zarejestrowane na terytorium Rzeczpospolitej Polskiej. W kategorii „Innowacyjna firma”, wyróżniono firmy wnoszących wybitny wkład w realizację sprawdzonych, innowacyjnych projektów na rzecz umacniania bezpieczeństwa kraju, nieustających w swoich wysiłkach w zakresie wdrażania innowacji w procesie produkcji i zarządzania.

W tym roku wyłoniono 25 innowacyjnych produktów, które mogą stanowić wyposażenie służb mundurowych oraz 10 firm działających w obszarze szeroko pojętego bezpieczeństwa państwa. Produkty i firmy, nagrodzone zostały prestiżowymi Sta-

tuetkami „Lider Bezpieczeństwa Państwa – 2019”. W Radzie Programowo-Konkursowej pracowali wybitni eksperci i znawcy przedmiotu w zakresie przedstawionej problematyki. Patronat Honorowy nad wydarzeniem objął szef Biura Bezpieczeństwa Narodowego – minister Paweł Soloch.

Pełną relację z tego wydarzenia wraz z listą nagrodzonych osób i firm znajdziecie Państwo na naszej stronie internetowej www.ochrona-mienia.pl

Redakcja

17SPIN

SIEDEMNASTA, POŁUDNIOWA EDYCJA SPOTKANIA PROJEKTANTÓW INSTALACJI NISKOPRĄDOWYCH.
OTWARCIE REJESTRACJI

25.09–26.09.2019r. w hotelu Nosalowy Dwór Resort & SPA, w Zakopanem odbędzie się jesienna edycja Spotkania Projektantów Instalacji Niskoprądowych.

17SPIN to wydarzenie skierowane do profesjonalistów z branży niskich prądów.

Zagadnienia omawiane w trakcie konferencji, podczas specjalistycznych wykładów i prezentacji jak również rozwiązania eksponowane na stoiskach wystawienniczych obejmą szerokie portfolio specjalizacji z branży niskich prądów.

Podczas jesiennej edycji Spotkania Projektantów Instalacji Niskoprądowych, projektanci, producenci, dystrybutorzy i eksperci spotykają się, aby współtworzyć wartościową przestrzeń do konfrontacji opinii i spostrzeżeń na temat najnowszych technologii i rozwiązań branżowych. Praktycy reprezentujący producentów i dostawców omówią efektywne rozwiązania na konkretnych przykładach.

Partnerzy, którzy już potwierdzili swój udział w siedemnastej edycji to: Alter S.A, Apa Group, Assa Abloy, Axxonsoft, BCS, Commscope, Corning, Dallmeier, Dormakaba, GiP, Grupa Romi, Helukabel, Mercor, Optex, Quality7, Roger, Seagate, Smay, Tp-link, Veracomp z marką Extreme Networks, Winkhaus, Yamaha, Zettler.

Po raz pierwszy na SPIN swoje rozwiązania zaprezentują: Alter S.A, Commscope, Dallmeier, Dormakaba, Quality7, Smay, Yamaha.

Wiedzą ekspercką podzielą się: Cezary Mecwaldowski, prowadząc wykład pt. ”Rola projektanta w tworzeniu stanowiska operatora systemu dozoru wizyjnego” oraz Tadeusz Markiewicz prowadząc wykład pt. ”Zagadnienia projektowe związane z nietypowymi aplikacjami systemów detekcji pożaru”.

SPIN daje możliwość bezpośredniego kontaktu, który jest najskuteczniejszym sposobem na rozwój relacji biznesowych, tworzenie nowych projektów oraz zdobywanie wiedzy.

Miejsce: Nosalowy Dwór Resort & SPA, Zakopane
Więcej info: www.spin.lockus.pl,

DZIEŃ Z BEZPIECZEŃSTWEM POŻAROWYM NA PGE NARODOWY. PRZYJDŹ NA KONGRES POŻARNICTWA FIRE SECURITY EXPO 2019

Już 25 lipca 2019, DZIEŃ Z BEZPIECZEŃSTWEM POŻAROWYM na PGE NARODOWY! Nie może Cię zabraknąć! Przyjdź na Kongres Pożarnictwa FIRE SECURITY EXPO 2019! Jedno z najbardziej znanych w Polsce wydarzeń dla projektantów, architektów i specjalistów branży budowlanej poruszające kwestie projektowania i bezpieczeństwa obiektów budowlanych oraz osób w nich przebywających.

W jednym czasie i miejscu – bieżące, najważniejsze i najtrudniejsze problemy ochrony przeciwpożarowej i zabezpieczeń technicznych budynków. Szereg testów, pokazów, warsztatów technicznych. Całodzienna wystawa światowych marek

Wykłady uznanych, wysokiej klasy specjalistów w zakresie projektowania i bezpieczeństwa pożarowego, ekspertów SGSP, CNBOP-PIB, SFPE-SIBP, stowarzyszeń branżowych, uczelni i ośrodków naukowo-badawczych. Liczne case study najbardziej prestiżowych inwestycji budowlanych w kraju. A to wszystko już w lipcu! Podczas największej konferencji pożarowej w kraju! 1000 projektantów, wykonawców i specjalistów ppoż., 250 przedstawicieli dostawców najnowszych technologii i rozwiązań, najbardziej prestiżowe projekty i budowle. Dla pasjonatów pokazy umundurowania i wyposażenia funkcjonariuszy służb od straży, policji po wojsko, a także pokazy ratownictwa medycznego.

Wiodące obszary tegorocznej edycji to: bierna i czynna ochrona przeciwpożarowa; detekcja, sygnalizacja pożarowa, wentylacja i oddymianie, oświetlenie awaryjne, aranżacja przestrzeni biurowych, DSO, monitoring, kontrola i sterowanie systemami bezpieczeństwa, SUG, kontrola dostępu, security, bezpieczeństwo danych, bezpieczeństwo i monitoring: budynków, magazynów, kolei, składowisk/spalarni i lasów, sprzęt i wyposażenie dla Straży Pożarnej, wymagania, wytyczne, normy, operaty pożarowe, kable i przewody, bezpieczeństwo konstrukcji, dachów i fasad, CPR, Ex, Atex, BIM, CDF i wiele innych. **Udział w wydarzeniu jest BEZPŁATNY**

Chcesz wiedzieć więcej? Wejdź na http://www.fire-expo.pl

Reklama

WYWIAD Z PANEM **KONRADEM BADOWSKIM**

W RAMACH SMART CITY FORUM – MARZEC 2019 (POLAND, UKRAINE & BALTICS BUSINESS RELATIONSHIPS MANAGER, AXIS COMMUNICATIONS)

W przestrzeni publicznej, także w branży zabezpieczeń, coraz częściej słyszymy o rozwijaniu inteligentnych miast, czy też smart city. Czy mógłby Pan przybliżyć w skrócie naszym czytelnikom, na czym polega ta idea?

Fakt, smart city, czy też inteligentne miasto, stało się ostatnio bardzo modnym określeniem, także w Polsce. Generalnie, moda na język „smart" może minąć, ale sama idea, która się za nim kryje pozostanie, bo odnosi się do odpowiedniego i odpowiedzialnego rozwijania mniejszych i większych miast w warunkach cyfryzacji, internetyzacji, tzw. kultury współdzelenia, przy uwzględnieniu wymogów racjonalnego gospodarowania energią i dbałości o względy ekologiczne.

Uszczegóławiając, są dwie płaszczyzny definiowania – na pierwszej wskazuje się, że smart city to cała usieciowiona infrastruktura, w tym narzędzia, ruchomości, sprzęt ICT, ale i dedykowany software, służąca poprawie lub umacnianiu komfortu życia mieszkańców w wielu wymiarach. Mogą to być rozwiązania do zarządzania dostępem w osiedlach lub w przestrzeni pracy, systemy do śledzenia floty samochodowej, ale też szersze udoskonalenia w zakresie transportu publicznego, mobilności obiektów, czy ludzi w ogóle. W infrastrukturze tej mieści się również cały konglomerat mniejszych lub większych systemów usprawniających i zabezpieczających codzienne nasze funkcjonowanie w miejskim otoczeniu. Możemy zaliczyć do nich, na przykład: automatyzację oświetlenia, nawadniania, bądź gospodarki odpadami, automatyzację stref parkowania, czy obserwacji meteorologicznej lub zanieczyszczeń; a także – wdrażanie sieciowych rozwiązań monitoringu przestrzeni miejskiej, wdrażanie płatności mobilnych za usługi publiczne, albo specjalnych aplikacji do partycypacji obywatelskiej lub promocji lokalnej turystyki; to tylko niektóre z gotowych, dobrych praktyk.

Druga płaszczyzna definiowania smart city odnosi się do – nazwijmy to – wymiaru kulturowego, tzn. do sfery wartości i postaw, jakimi kierują się i wykazują mieszkańcy, tak aby to życie w miejskiej wspólnocie było po prostu lepsze, przyjemniejsze. Innymi słowy, smart city to także przekonanie, że stosowanie nowoczesnych technologii w sferze usług publicznych, że usprawnianie mobilności i ochrona środowiska, ma rację bytu, przy jednoczesnym uwzględnieniu kosztów, a więc np. gotowości do zmiany swoich nawyków, czy ograniczenia swojej prywatności. Trzeba powiedzieć, że w tej swoistej filozofii smart city mieści się pewnego rodzaju zobowiązanie do odpowiedzialnego gospodarowania wspólnym mieniem miejskim. Jak mówią – „sharing is caring".

Jak w takim razie smart city ma się do sfery bezpieczeństwa?

Składową komfortu i jakości życia jest oczywiście poczucie bezpieczeństwa, ale i szereg obiektywnych czynników, budujących realne zaplecze infrastrukturalne. Jako Axis zajmujemy się szeroko pojętym dozorem wizyjnym oraz rozwiązaniami komplementarnymi, np. IP audio, lub radary, więc łatwiej będzie mi odnieść się w tej kwestii do naszego „podwórka". Generalnie, monitoring wraz systemami dostępowymi, sensorami i modułami analitycznymi opartymi na zaawansowanych algorytmach jest jednym z filarów infrastruktury bezpieczeństwa w miastach. Systemy dozoru pozwalają lepiej organizować ruch pojazdów, komunikację w miejskich arteriach i na parkinach; stają się też ważnym elementem bezpieczeństwa obiektów i przestrzeni zamkniętych. Inteligentny monitoring, jako urzeczy-

wistnianie smart city, to przede wszystkim wsparcie w lepszym i skuteczniejszym zabezpieczaniu usług publicznych, zarządzaniu mobilnością i transportem. Zaawansowany monitoring uczestniczy ponadto w automatyzacji przepływów i analiz dużych danych. Smart oznacza więc wykorzystanie dobrodziejstwa ICT do integracji istniejących i nowych systemów monitoringu, także tych niebędących w dyspozycji miasta, tak aby zyskać maksymalnie duży zakres obserwacji. Z doświadczenia w wielu krajach wiemy, że dobrze zintegrowane systemy korzystniej wpływają na zachowanie porządku publicznego – tzn. organy ścigania, ale też służby ochrony, mają większe szanse na wychwycenie zdarzeń i lepsze rozpoznanie sytuacji, co przekłada się na optymalizację prewencji i reakcji.

Ale czy nie jest też tak, że tam, gdzie jest monitoring czujemy się po prostu bezpieczniej?

Oczywiście, przy czym do niedawna pokutowała postawa nieufności względem monitoringu, jako czegoś, co umożliwia śledzenie nas itd. To podejście na zasadzie „uwaga, wielki Brat patrzy" zaczyna się jednak zmieniać. Mieszkańcy polskich miast dostrzegają więcej pozytywów z obecności kamer w miejscach publicznych, np. parkach, czy w obiektach zamkniętych typu galerie handlowe, parkingi podziemne, kluby. Świadomość obserwacji danych miejsc zniechęca również do wandalizmu i innych niepożądanych zachowań. Jeśli mamy korelować poczucie bezpieczeństwa z dozorem wizyjnym w kontekście smart city to można powiedzieć, że dzięki zastosowaniu monitoringu miasto, a w zasadzie określone jego przestrzenie, stają się bardziej dostępne, żywe, i łatwiej się po nich poruszać.

Jakie innowacyjne technologie dozoru mogą więc znaleźć zastosowanie w „inteligentnych miastach"?

Może zacznę z nieco innej strony. Branża dozoru nieustannie się rozwija i co róż poszczególni producenci próbują zaskoczyć czymś nowym. Rzecz jednak w tym, by te innowacje – do wykorzystania także na użytek smart city – nie były „sztuką dla sztuki", tylko realnym krokiem w przód. W Axis stawiamy więc na takie R&D, które faktycznie przyczynią się do unowocześnienia jakiegoś rozwiązania, albo stworzenia urządzenia, bądź komponentu technologicznego realnie podnoszącego jakość, funkcjonalność, elastyczność, czy też ekonomię systemów dozoru.

Schodząc do konkretów – technologia Sharpdome, dla przykładu, umożliwia uzyskanie tej samej optymalnej ostrości obrazu i pełnej wierności scen we wszystkich pozycjach. To odpowiedź na ograniczenia konwencjonalnej kamery kopułkowej, która zniekształca obraz. Sharpdome zapewnia wyraźną identyfikację obiektów nawet o 20 ° powyżej horyzontu kamery, dzięki czemu kamery z tą technologią nadają się również do nierównego terenu. Inna technologia – Zipstream – zmniejsza zapotrzebowanie na przepustowość i zasoby pamięci o nawet 50%, a tym samym pozwala na oszczędności. Technicznie polega to na tym, że sceny zawierające interesujące szczegóły są nagrywane w pełnej rozdzielczości, natomiast pozostałe obszary są filtrowane. Ważne szczegóły ułatwiające prace wyjaśniające lub dochodzeniowe, takie jak twarze, tatuaże czy tablice rejestracyjne, są izolowane i zachowywane, z kolei mniej ważne obszary, jak białe ściany, trawniki i roślinność są wygładzane. Kolejna nasza technologia – Lightfinder – pozwala uzyskać kolorowy obraz w pełnej rozdzielczości, z niewielkim rozmyciem, w niemal całkowitej ciemności, także obiektów w ruchu. Nie mogę nie wspomnieć tu też o najnowszej generacji procesorów Axis, czyli ARTPEC7. To kość własnej produkcji, oparta na własnym patencie, której potężne możliwości obliczeniowe zwiększają każdą funkcjonalność monitoringu, także w obszarze tzw. analityki brzegowej, która staje się obecnie kluczowa. Nowy procesor pozwala na uzyskiwanie obrazu o jeszcze lepszej jakości, optymalizuje cyberochronę dozoru, ale też zwiększa możliwości integracji systemów.

Obok tych wymienionych jest oczywiście cały zasób technologii do takich zastosowań jak: rozpoznawanie twarzy, rozpoznawanie tablic rejestracyjnych, dozór w pojazdach, zliczanie osób, ochrona przed wtargnięciem, obserwacja termowizyjna, detekcja dźwięku, monitoring środowiska, czy detekcja radarowa. Wszystkie one mogą tworzyć kompleksowe mega-systemy.

Może Pan podać przykład działania takich kompleksowych systemów – kamer w połączeniu z czujnikami?

Weźmy standardowy czujnik ruchu, lub detektor radarowy podłączony do określonej platformy – w razie jakiegoś incydentu, zdarzenia mogą uruchomić kamerę, która z kolei przekaże dane do centrum operacyjnego, w którym jest podejmowana określona reakcję. Na tym samym obszarze, możemy mieć czujnik środowiskowy, który uruchomi kamerę wizyjną lub termowizyjną, co pozwoli szybko zidentyfikować pożary lub wycieki, a następnie wysłać ostrzeżenia, powodujące dalsze działania. Gdy rozważa się zakres i skalę integracji czujników – od termicznego do ruchu, od atmosferycznego po wizyjne – sposoby ich łączenia są nieskończone.

A jeśli jesteśmy przy radarach – to warto wspomnieć, że pozwalają one także ograniczać do minimum liczbę fałszywych alarmów, a te przekładają się na codzienne funkcjonowanie miast. Każdy fałszywy alarm odciąga uwagę od prawdziwych zagrożeń, co wiąże się przecież z niepotrzebnym kosztem, ale też pewną uciążliwością dla mieszkańców. Radary dostarczają ponadto ważne informacje dotyczące wykrytych obiektów, których nie są w stanie dostarczyć kamery, takie jak położenie, czy prędkość. Inwestycja w taką radarową detekcję ruchu, w myśl filozofii smart city, to inwestycja nie tylko w bezpieczeństwo, ale też przejaw gospodarnego podejścia.

Czy mógłby Pan podać przykłady miast, które wprowadzają tego typu innowacje w zakresie dozoru właśnie na rzecz smart city?

Wiele ciekawych rozwiązań wdraża się w USA, Kanadzie, Holandii, czy w Szwecji. Cały czas obserwujemy dobre praktyki, ale też wsłuchujemy się w potrzeby samorządów, także w Polsce. Podam dwa przykłady działań modernizacyjnych, stricte związanych z monitoringiem – Łódź i Atlanta. W pierwszym przypadku, zaprojektowano nowy system w taki sposób, by można było uruchomić kilka centrów operacyjnych oraz kilkanaście punktów oglądowych. Dodatkowo, dokonano integracji nowego systemu z realizowanym równolegle systemem monitoringu wizyjnego ITS w Zarządzie Dróg i Transportu w Łodzi. Obecnie, miasto posiada 444 kamer, z których obraz przekazywany jest płynnie i bezpiecznie do operatorów oraz udostępniany służbom miejskim, Policji i Straży Miejskiej, a wkrótce również Straży Pożarnej. Atlanta uruchomiła z kolei projekt Operation Shield. Polega on – podobnie jak w Łodzi, choć na wiele większą skalę – na zaawansowanej integracji systemów dozoru wizyjnego, będących w dyspozycji prywatnych i publicznych podmiotów, i utworzeniu jednego centrum dowodzenia. Zaprojektowano solidną i elastyczną

platformę operacyjną, która jest w stanie obsłużyć i połączyć ponad 10 000 kamer różnych marek o różnej charakterystyce i funkcjonalności.

Tego typu wdrożenia będą standardem „inteligentnych miast" w niedalekiej przyszłości. Oczywiście, całodobowy monitoring oparty na podsystemach podmiotów publicznych i prywatnych, operatorów transportowych, firm, centr handlowych, wreszcie osiedli mieszkaniowych, będzie możliwy i skuteczny, jeśli cały proces współdzielenia danych będzie odpowiednio zabezpieczony, także na poziomie czynnika ludzkiego. Ale to już inny temat.

Smart city to także dbałość o ekosystem. Jak branża dozoru podchodzi do kwestii zrównoważonego rozwoju ?

Trudno mi odpowiadać za całą branżę, ale Axis mocno inwestuje w ekologię produkcji. Od pewnego czasu systematycznie włączamy do naszego cyklu dostaw rozwiązania typu „green design". To produkty oparte na materiałach i substancjach pochodzących z recyklingu.

Koordynacją tych działań zajmuje się w ramach firmy Axis Green Design Group. To specjalnie powołany dział, który wypracował wytyczne dotyczące ekoinnowacji, korespondujące z wytycznymi ONZ w zakresie zrównoważonego rozwoju. Regulują one m.in.: dobór materiałów, optymalizację projektowania podzespołów i całego systemu produkcji, a także sposoby dalszej utylizacji.

Dla przykładu, w praktyce wygląda to tak, że Axis stworzył własną listę materiałów i substancji zabronionych w produkcji, zarówno tych już prawnie zakazanych, jak i tych, które są dozwolone, ale oddziałują negatywnie na środowisko i pewnie lada moment zakazane zostaną. Na liście są m.in. plastyfikatory i bromowane, lub chlorowane środki zmniejszające palność.

Axis ma też na uwadze jakość powietrza. Wraz z partnerami pracujemy nad czujnikami środowiskowymi – o których wspominałem już wcześniej. Zależy nam na technologiach, gotowych do obrazowania termicznego i identyfikacji strat energii cieplnej w budynkach. Nie da się wyczerpać tutaj całego tematu ekologii, ale myślę, że w tym aspekcie wyprzedzamy konkurencję.

Czy w związku z wdrażaniem idei smart city nie widzi Pan zagrożeń dla prywatności mieszkańców miast?

Wróćmy do początku – smart city w praktyce ma upraszczać życie, ale trzeba powiedzieć jasno – trudno budować „miasta inteligentne", jeśli nie uczynimy ich najpierw bezpieczniejszymi, i to w wielu wymiarach. Jeśli mówimy to monitoringu wizyjnym jako ważnym elemencie infrastruktury bezpieczeństwa miasta – jego funkcjonalność nie może naruszać granic prywatności, ale nie możemy wykluczyć, jak bardzo byśmy się nie starali od strony hardware'u i software'u, że ktoś te granice przekroczy. Duża tu rola władz państw i miast, by pomagali dobrym prawodawstwem, skutecznym jego wdrażaniem, a także edukacją. Podsumowując, zagrożenia dla prywatności oczywiście są, tak jak w każdej branży na styku ICT – internet – człowiek. Ważne, aby na poziomie poszczególnych interesariuszy – od producenta, usługodawcy, przez użytkownika po instytucje rządowe i samorządowe – była odpowiednia wola, by tym zagrożeniom przeciwdziałać. Zatem, rozwój w stylu smart musi być rozwojem odpowiedzialnym, czyli takim, który ma gwarantować równowagę między poszczególnymi potrzebami, prawami i obowiązkami w miejskiej społeczności.

Krzysztof Surdyk
Ochrona Mienia i Informacji
Redaktor naczelny
Euro-Media sp.z o.o.
02-786 Warszawa, ul. Rosoła 10A
t. 606 911 071
e-mail: k.surdyk@ochrona-mienia.pl

Reklama

Dlaczego ta kamera
nie jest zwykłą kamerą?

AXIS P3717-PLE Network Camera

Ponieważ AXIS P3717-PLE to są właściwie cztery kamery. Ponieważ zamiast jednej, jest wyposażona w cztery zmiennogniskowe głowice, które można elastycznie pozycjonować w dowolnym kierunku. Dzięki temu, możemy uzyskać widok czterech, różnych scen jednocześnie. Dodatkowo, AXIS P3717-PLE została wyposażona w zdalny zoom i ustawienie ostrości oraz 360-stopniowe oświetlenie w podczerwieni. Można uzyskać dowolną kombinację: panoramiczny 360-stopniowy widok ogólny, kombinację widoków ogólnych oraz szczegółowe zbliżenia, nawet w całkowitej ciemności... kupując tylko jedno urządzenie w przystępnej cenie. Wszystko to dzięki temu, że AXIS P3717-PLE nie jest zwykłą kamerą - to są aż cztery wysokiej jakości kamery w jednej.

www.axis.com/products/axis-p3717-ple

AXIS COMMUNICATIONS

KONFERENCJA PROJEKTANTÓW SYSTEMÓW NISKOPRĄDOWYCH

W dniach 11–12 czerwca br. firma Bosch Security Systems zorganizowała konferencję-spotkanie projektantów systemów niskoprądowych. W tym roku konferencja odbyła się w Centrum Naukowo-Badawczym Ochrony Przeciwpożarowej w Józefowie k. Warszawy.

Podczas spotkania przedstawiono nowości produktowe i systemowe Bosch'a, a odrębne sesje poświęcone zostały narzędziom wspierającym projektowanie systemów bezpieczeństwa.

Uczestnikom konferencji zaprezentowano między innymi takie tematy jak: projektowanie systemów wideo detekcji dymu i ognia z przykładami wdrożeń Bosch'a, programy wspierające projektowanie kamer CCTV w kontekście norm zobrazowania i skuteczności inteligentnej analityki obrazu, wykorzystanie cech centrali DSO Paviro w dużych oraz rozproszonych instalacjach nagłośnienia ewakuacyjnego, scenariusze integracji systemów bezpieczeństwa za pomocą Building Integration System (BIS), wytyczne do planowania i instalacji czujek kanałowych.

Przy współpracy z CNBOP, uczestnikom spotkania zaprezentowano przykłady testów laboratoryjnych, którym poddawane są produkty Bosch do celów certyfikacyjnych, takie jak: odporność czujek pożarowych i głośników DSO na wibracje i udar czy test odporności na wysoką temperaturę głośników pożarowych w porównaniu do głośników komercyjnych,

Wykładowcy z CNBOP omówili również najnowsze zagadnienia normatywne związane z certyfikacją urządzeń oraz projektowaniem systemów bezpieczeństwa pożarowego w obiektach, a w tym m.in.: porównanie szybkości detekcji czujek punktowych oraz kamer do wykrywania pożarów, uzgadnianie projektów SSP i DSO w kontekście certyfikacji i dopuszczeń, w obszarze ochrony przeciwpożarowej, a także nowe wymagania w zakresie projektowania DSO.

Uczestnicy mieli również możliwość zapoznania się ze sprzętem demonstracyjnym firmy Bosch, prezentowanym podczas konferencji.

SECURITECH, WARTOŚĆ POKONFERENCYJNA.
Zabezpieczenia elektroniczne krat, wygrodzeń z siatki, włazów i bram

Międzynarodowa konferencja techniczno-ochronna Securitech, która odbywała się corocznie w latach 2015–2018, trwale wpisała się w potrzeby Służby Więziennej, jak i w krajobraz Centralnego Ośrodka Szkolenia SW w Kaliszu. Z roku na rok, poprzez dyskusje specjalistów ze Służby Więziennej z przedstawicielami producentów urządzeń i systemów, ekspertami i naukowcami, pozwoliły na wypracowanie oraz zaprezentowanie dedykowanych, nowoczesnych rozwiązań technicznych. Poruszana tematyka konferencji związana była z bieżącymi potrzebami SW, a udział innych służb pozwalał na wzajemną wymianę doświadczeń. Artykuł przedstawia jedno z dedykowanych rozwiązań technicznych, jakie wypracowano i zaprezentowano w trakcie konferencji, pozwalające na szerokie zastosowanie w ochronie obiektów i nie tylko. Jest to rozwiązanie z urządzeniami bezprzewodowymi.

Zabezpieczenia elektroniczne zakładów karnych i aresztów śledczych wymagają odmiennego podejścia w projektowaniu[1]. Rozpatruje się nie tylko możliwość wtargnięcia intruza na teren, do obiektu, pomieszczenia, ale także sytuację odwrotną, kiedy to osadzeni mogą próbować ucieczki z pomieszczenia, obiektu lub terenu. Wytyczne[2] zawierają informację o strefach ochrony, oraz minimalnych wymaganiach technicznych ich zabezpieczania. Jak w każdym systemie zabezpieczeń elektronicznych oczekiwana jest możliwie najszybsza reakcja systemu na występujące zagrożenie, powiadomienie funkcjonariuszy ochrony w czasie umożliwiającym im skuteczną reakcję. Podążając za wspominanymi wytycznymi urządzenia najczęściej projektuje się na granicy stref ochronnych, jak najbliżej miejsc przebywania stałego lub czasowego osadzonych.

Fot. 1.
Źródło: zaanstad.nieuws.nl

Rynek oferuje obecnie szeroką gamę urządzeń[3] o coraz lepszych parametrach, pozwalających na zastosowanie różnych urządzeń w podobnych warunkach. Istotną rolę w ich wyborze pełni wiedza i doświadczenie projektanta, możliwości instalacji, warunki architektoniczne, środowiskowe itp. W niektórych rozwiązaniach urządzenia bezprzewodowe w systemach zabezpieczeń elektronicznych uzyskują przewagę nad rozwiązaniami przewodowymi na przykład, kiedy:

- okablowanie narażone jest na uszkodzenie (np. ruchome siatki, wygrodzenia, kraty, bramy itp.) lub sabotaż,
- występuje zagrożenie przepięciami z wyładowań atmosferycznych lub innych wynikających z różnicy potencjału (szczególnie przy dużej liczbie konstrukcji metalowych jak wygrodzenia z siatki lub concertiny, kraty, bramy itp.),
- występują częste zmiany funkcjonalne w obiekcie, wymagające przenoszenia urządzeń detekcyjnych,
- wykorzystuje się detektory do lokalizacji obiektów, pojazdów, przedmiotów, osób itp.

Bezprzewodowy system można szybko dostosować, przenieść urządzenia detekcyjne w inne miejsca. Takie opisywane urządzenia zawierające akcelerometr trójosiowy i żyroskop należą do grupy urządzeń perymetrycznych, instalowanych na granicy stref ochronnych, jak wygrodzenia, bramy, kraty, włazy itp. Pozwalają precyzyjnie określić miejsce powstania alarmu, a przy zintegrowaniu z systemem dozoru wizyjnego na jego szybką, zdalną weryfikację. W porównaniu do detektorów opartych o inne zjawiska fizyczne, urządzenia te pozwalają uniknąć wzbudzenia alarmu przez owady, ptaki czy inne zwierzęta.

[1] „Zabezpieczenia techniczno-ochronne zakładów karnych i aresztów śledczych" C. Mecwaldowski, Euromedia 2014

[2] Wytyczne Dyrektora Generalnego Służby Więziennej nr 4/2013

[3] „Więzienie obiekt pod specjalnym nadzorem" C. Mecwldowski SEC&AS 5/2017

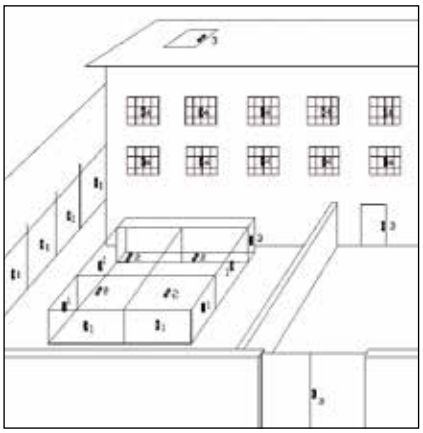
Detektory montowane bezpośrednio na kratach lub siatkach, pozwalają wykryć:

- uderzenia o kraty, siatki,
- próby przecięcia lub piłowania,
- wygięcia, przemieszczenia,
- otwarcie bram, krat, przejść.

W przypadku zastosowania detektora na kracie okiennej w zakładzie karnym, należy utrudnić do niego dostęp, na przykład poprzez:

- zastosowanie siatki drobnooczkowej po stronie wewnętrznej,
- zastosowanie krat koszowych (wygrodzeniowych, wewnętrznych) w celi przed ścianą z oknem będącą jednocześnie ścianą zewnętrzną budynku, graniczącą bezpośrednio z terenem poza więzieniem.

Opisywane rozwiązanie pozwala identyfikować zagrożenie z konkretnego okna/kraty, co przy zastosowaniu innych detektorów wiąże się z całą linią okien/krat lub ścianą objętą zasięgiem czujki. Przykład jak wiele jest miejsc instalacji detektorów bezprzewodowych przedstawia rysunek 1. Urządzenia pozwalają na zabezpieczenie stalowych krat okiennych (4) i siatek stalowych lub ogrodzeń przęsłowych, zarówno w poziomie (2) jak i pionie (1) np. w zastosowaniu ochronnym placów spacerowych, przejść na terenie obiektu zabezpieczonych od góry siatkami lub kratami stalowymi. Urządzenia te zapewniają także detekcję otwarcia włazów, drzwi, krat i bram (3). Uzyskuje się w ten sposób precyzyjną lokalizację wystąpienia alarmu związaną z adresowalnym detektorem (właz, krata okienna, krata przejściowa, drzwi, przęsło płotu lub brama itp.) Urządzenia przeznaczone są do pracy w warunkach zewnętrznych (IP67). System posiada automatyczną funkcję kontroli komunikacji bezprzewodowej,



Rysunek 1. Przykład zastosowania detektorów bezprzewodowych w zakładzie karnym
Źródło: opracowanie własne

Fot. 2.
Źródło: Chelm.naszemiasto.pl

stanu detektorów i baterii, której żywotność wynosi do 8 lat.

Możliwości zastosowania opisywanego systemu są znacznie większe niż tylko zabezpieczenie perymetryczne obiektu. Inne ciekawe zastosowania, to:

Bezprzewodowy system dozoru osadzonych podczas konwoju. Urządzenie odbiorcze może być instalowane w pojeździe konwojowym lub mocowane zaczepami do ramienia konwojenta/dowódcy konwoju (mocowane na ramieniu, ponieważ miejsce to nie powoduje przesłonięcia ciałem wbudowanych w urządzenie anten, a także z uwagi na stosowane kamizelki ochronne). Identyfikatory elektroniczne – tagi bezprzewodowe (zapinane opaskami lub wszyte w odzież skarbową) posiadają konwojowani osadzeni. Oddalenie się osadzonego od pojazdu konwojowego lub konwojentów na określoną odległość, wywołuje alarm. System posiada możliwość nadzoru drzwi w pojeździe konwojowym, poza ewentualnym alarmem otwarcia również rejestr otwarcia/zamknięcia.

Bezprzewodowy system nadzoru osadzonych podczas pobytu w więzieniu lub w pracy. System pozwala na kontrolę czy osadzeni, którzy powinni być od siebie izolowani w czasie odbywania aresztu lub kary pozbawienia wolności, nie kontaktują się bezpośrednio ze sobą. Osadzeni wyposażeni w identyfikatory elektroniczne – tagi (zapinane opaskami lub wszyte w odzież skarbową), system umożliwia rejestrowanie gdzie poruszają się, generować alarm po przekroczeniu dozwolonej odległości między osadzonymi np. podczas korzystania z telefonów samoinkasujących, przemieszczania się po terenie więzienia, przebywania na placach spacerowych lub w pracy. System posiada możliwość bezprzewodowego nadzoru drzwi/przejść/okien w oddziale, poza ewentualnym alarmem otwarcia również rejestr otwarcia/zamknięcia, miejsc przebywania osadzonych na terenie zakładu.

Bezprzewodowy system rejestracji czynności patrolowych. Umożliwia rejestrowanie czynności realizowanych przez funkcjonariuszy w patrolu na terenie jednostki.

Bezprzewodowy system lokalizacji obiektów (pojazdów, przedmiotów, narzędzi itp.) do różnych zastosowań np. w miejscach pracy osadzonych, w halach produkcyjnych itp. Umożliwiają alarmowanie w przypadku zmiany położenia zabezpieczanego przedmiotu, pojazdu.

Opisywane rozwiązania posiadają możliwość integracji z innymi systemami zabezpieczeń elektronicznych. Duża liczba danych, jakie można pozyskać z systemu pozwala na różnorodne zastosowanie analityczne, poza bezpośrednim zastosowaniem w alarmowaniu. Dostępna jest także opcja automatycznej integracji z autonomicznym dronem przeznaczonym do ochrony obiektu[4]. Z opracowanych rozwiązań korzystają również inne służby, w tym wojsko.

kpt. mgr inż. Cezary Mecwaldowski
St. wykładowca Zakładu Szkolenia Ochronnego Centralnego Ośrodka Szkolenia Służby Więziennej w Kaliszu

[4] „Bezprzewodowe zabezpieczenie obiektu zintegrowane z autonomicznym dronem, jako system ochrony obwodowej" P. Piasecki, P. Łuków, Zabezpieczenia 1/2018

MONITORING WIZYJNY I TERMOWIZYJNY TERENÓW PRZYGRANICZNYCH

Na przestrzeni ostatnich lat, można zaobserwować bardzo intensywny rozwój technologii wizyjnych w instalacjach monitoringowych. Jeszcze kilka lat temu, prym wiodły prymitywne kamery analogowe, których jakość pozwalała, co najwyżej na bardzo ogólny ogląd sytuacji. Od kilku lat widać bardzo szybko postępujące zmiany, zarówno jeśli chodzi o samą technologię jak i wykorzystanie tego typu systemów.

Warto na samym początku opisu zwrócić uwagę na to, z jakich kluczowych elementów składa się typowy system monitoringu wizyjnego, gdyż należy pamiętać o tym, że sama kamera, jest ważnym, ale nie jedynym istotnym elementem takiego systemu. Równie ważnym, jak kamera jest rejestrator obrazu.

Współczesne rejestratory oferują znacznie więcej aniżeli samą możliwość rejestracji obrazu lub jego podglądu na żywo. Wyposażone w funkcje analityczne najczęściej pozwalają na prowadzenie prostych analiz w czasie rzeczywistym. Jednocześnie, analizy typu detekcja ruchu czy wtargnięcia lub przekroczenie linii, oferowane są również, jako część składowa oprogramowania samych kamer. Trzeba jednak zwrócić uwagę na to, iż o ile wydźwięk marketingowy takich rozwiązań jest bardzo duży, to do ich profesjonalnego zastosowania, jakim jest wykorzystanie operacyjne przez różnego rodzaju formacje i służby, wymagane jest zastosowanie znacznie bardziej zaawansowanych technologii, gwarantujących wysoką skuteczność działania przy zachowania minimalnego poziomu fałszywych alarmów. Najnowsze systemy wykorzystujące sztuczną inteligencję, opartą o sieci neuronowe i tzw. *deep learning,* rewolucjonizują w tym momencie podejście do monitoringu wizyjnego, nie tylko oferując funkcjonalności opisane poniżej, ale przede wszystkim zmieniając kompletnie perspektywę wykorzystania takich systemów. W większości przypadków, do tej pory mieliśmy do czynienia z użytkowaniem monitoringu *post factum.* Sprawiało to, że narzędzie takie nadawało się w dużej mierze do zbierania materiału dowodowego z już zaistniałej sytuacji. Wraz z nadejściem wspomnianej rewolucji, otrzymujemy możliwość reagowania w czasie rzeczywistym i realnego przeciwdziałania zagrożeniom, a nie jedynie ich dokumentowania.

Prowadzenie dozoru wizyjnego terenów przygranicznych, dokonując możliwie ogólnego podziału, można określić, jako: monitoring wizyjny bezpośrednio związany z przejściami granicznymi oraz monitoring terenów przygranicznych tzw. zielonej granicy, z uwzględnieniem szczególnego przypadku granicy morskiej.

Kwestia dozoru wizyjnego przejść granicznych i połączeń drogowych do nich prowadzących, rozpatrywana pod kątem rozwiązań możliwych do zastosowania, przypomina instalacje stosowane w tzw. *inteligentnych miastach (smart city).*

Poczynając od samych przejść granicznych, najnowocześniejsze rozwiązania pozwalają na odczytywanie numerów tablic rejestracyjnych, porównywanie ich z bazą danych pojazdów poszukiwanych lub weryfikację z bazą CEPIK za pomocą rozpoznawania marki, modelu i koloru pojazdu. Co ważne dostępne są na rynku systemy niewymagające do tych funkcjonalności specjalizowanych kamer *ANPR* sparowanych z kamerami *overview,* co w bardzo istotny sposób przyczynia się do zmniejszenia kosztów infrastrukturalnych. Do przygotowania takiej instalacji wystarczy, zatem zwykła kamera IP z filtrem polaryzacyjnym oraz komputer/rejestrator z odpowiednim oprogramowaniem. Taki punkt kamerowy można również wyposażyć w funkcję rozpoznawania twarzy osób kierujących pojazdami wraz ze zliczaniem pasażerów w pojeździe. Jednocześnie te samo narzędzie, można zintegrować na przykład ze skanerem paszportów i dokonywać na bieżąco porównywania zdjęć z dokumentów z wizerunkami osób legitymujących się nimi.

Co więcej, w niektórych, systemach możliwe jest również rozpoznawanie osób z częściowo zasłoniętymi twarzami, poprzez czarne okulary, kominiarki, czy na przykład makijaż maskujący, oszukujący większość standardowych rozwiązań tego typu systemów. Oczywiście, baza osób poszukiwanych może być na bieżąco aktualizowana w czasie rzeczywistym, również z wykorzystaniem słabszej jakości zdjęć, np. pochodzących właśnie z monitoringu.

Docelowo, tego typu analiza będzie mogła być zintegrowana na przykład z będącą obecnie w fazie projektowania *chmurą obliczeniową* Policji.

W przypadku większych przejść granicznych przydatnymi funkcjami mogą okazać się analizy przepływu pojazdów, ich klasyfikacja ze względu na rodzaj pojazdu (np. samochód osobowy, ciężarowy, dostawczy itd.). Wyniki tych analiz, wykorzystywane są w czasie rzeczywistym do sterowania urządzeniami infrastruktury drogowej oraz generowania informacji do systemów digital signage, informujących

Fot. 1. Monitoring wizyjny na przejściu granicznym
Źródło: strazgraniczna.pl

lub nakazujących kierowcom odpowiednie zachowanie. Dzięki temu możliwe jest upłynnienie przepływu samochodów i osób na zatłoczonych przejściach granicznych, poprzez właściwe sterowanie ruchem. Co więcej, możliwe jest również informowanie kierowców o długości kolejek i czasie oczekiwania, co w znaczący sposób wpływa na ich komfort oraz możliwość planowania podróży.

Zupełnie inny zakres funkcjonalności potrzebny jest do dozorowania terenów tzw. zielonej granicy. Po pierwsze należy tutaj wyróżnić dwa główne scenariusze zastosowań.

Pierwszy z nich to zastosowanie stacjonarne, podobne do klasycznej ochrony obwodowej. Mamy tutaj do czynienia z pasem terenu, który pokrywamy zasięgiem widzenia kamer. W dłuższych scenach, trudnym terenie i przy często występujących niekorzystnych warunkach atmosferycznych sensownym staję się wykorzystanie kamer termowizyjnych. Są one niestety wielokrotnie droższe od kamer rejestrujących zakres fal widzialnych oraz bardziej kłopotliwe w serwisie. Dodatkowo, do dyspozycji w kamerach termowizyjnych jest z reguły znacznie niższa rozdzielczość,

Fot. 2. Wytrzymałe kamery wizyjne ze zintegrowaną funkcja analizy wideo
Źródło: Systemy wizyjne

co przekłada się na ich częste zestawianie w parze z klasycznymi kamerami wizyjnymi. Takie zestawy dostarczają strumienie wideo, które można nałożyć na siebie i otrzymać bardzo czytelny obraz niezależnie od warunków atmosferycznych czy oświetleniowych. Z uwagi jednak na wspomnianą cenę, nie jest to powszechnie wykorzystywane rozwiązanie.

Znacznie tańszym systemem, może okazać się połączenie zwykłej kamery IP, wyposażonej w nowoczesny, czuły przetwornik i dobrej jakości obiektyw o dużej jasności i zoomie, z oświetlaczem laserowym. Tego typu systemy, wykorzystywane na przykład na lotniskach, dobrze sprawdzają się nawet na dystansach kilku kilometrów, jednak w porównaniu z termowizją, są znacznie bardziej podatne na zakłócenia powodowane przez warunki atmosferyczne.

W przypadku systemów stacjonarnych, bardzo dobrym rozwiązaniem jest wykorzystanie analizy wideo pozwalającej na pełną klasyfikację obiektów znajdujących się w obserwowanej scenie. Dzięki temu, jesteśmy w stanie określić czy dozorowany pas terenu przekracza człowiek, czy na przykład zwierzę. W zależności od założeń operacyjnych możliwe jest

natychmiastowe wykorzystanie komunikacji głosowej lub świetlnej skierowanej w stronę osoby naruszającej obszar chroniony, wzywając ją do zaniechania próby przekroczenia tego obszaru. Co więcej, dzięki możliwości mapowania sceny z kamery, możliwa jest w czasie rzeczywistym, wizualizacja na wirtualnych mapach, dokładnej ścieżki przemieszczania się osoby naruszającej strefę oraz automatyczna

Reklama

WAKACYJNA OFERTA!

Zamów prenumeratę
dwumiesięcznika

Ochrona Mienia i Informacji

86 zł
Wersja drukowana

PROMOCJA WAŻNA DO 1.09.2019

a otrzymasz ROCZNIK 2018* GRATIS!

* Rocznik 2018 w wersji drukowanej. Oferta dotyczy prenumeraty rocznej.

prenumerata@mediafachowe.pl
22 535 32 29
www.czasopismo.net

Fot. 3. Dron na uwięzi
Źródło: Nextron.pl

koordynacja działań funkcjonariuszy podejmujących interwencję (podawanie aktualnej pozycji osoby podejrzanej wraz z podglądem obrazu na żywo na urządzeniach mobilnych z danych kamer).

Nieco innymi prawami rządzi się monitoring wizyjny realizowany doraźnie. Tutaj w wykorzystaniu najlepiej sprawdzają się mobilne maszty z kamerami, zarówno zwykłymi jak i termowizyjnymi oraz coraz lepsze pod kątem zdolności operacyjnych bezzałogowe statki powietrzne, wyposażone w głowice obserwacyjne z dużym przybliżeniem, najczęściej składające się z dwóch omawianych rodzajów kamer.

Co do samych dronów, jest to zdecydowanie temat na osobną serię artykułów. W tym przypadku warto przyjrzeć się szczególnie jednemu ich rodzajowi, a mianowicie dronom na uwięzi. Przewód łączący takiego drona ze stacją bazową, może mieć nawet kilkaset metrów długości i zapewniać zarówno komunikację przewodową jak i również stałe źródło zasilania, co sprawia, że taki dron w zasadzie nie ma ograniczenia, co do czasu lotu. Dodatkowo istnieją takie konstrukcje wielowirnikowców, które są niemalże niesłyszalne już przy odległościach rzędu 100 metrów, co sprawia, że mogą być z powodzeniem wykorzystywane nawet do prowadzenia wielogodzinnych, obserwacji.

Najnowsze systemy analityczne, wykorzystujące sztuczną inteligencję, pozwalają na skuteczny dozór stref, również na ruchomym obrazie, z jakim mamy do czynienia przy strumieniach wideo generowanych przez głowicę obserwacyjną drona. Sprawia to, że tego typu statki powietrzne, są bardzo ciekawą alternatywą dla standardowych mobilnych punktów obserwacyjnych, choć oczywiście, w przypadku bardzo trudnego terenu, czy złych warunków pogodowych, mają swoje istotne ograniczenia.

Odrębną kategorią monitorowania terenów przygranicznych jest kwestia granicy morskiej. Z uwagi na specyfikę obiektów i odległości, na jakich prowadzona ma być detekcja, stosuje się tutaj systemy, takie na przykład, jak wprowadzony kilka lat temu do służby Zautomatyzowany System Radarowego Nadzoru. W nim również występuje element monitoringu wizyjnego w postaci kamer przystosowanych do operowania przy bardzo niskim poziomie oświetlenia oraz kamer termowizyjnych, jednak podstawą działania jest radar do wykrywania celów nawodnych.

Na zakończenie, należy wspomnieć jeszcze o trzech bardzo istotnych kwestiach, bez których opisane wyżej przykładowe możliwości, są w zasadzie bezużyteczne.

Po pierwsze, to skuteczne zabezpieczenie systemu. Abstrahując od jakości analiz oferowanych przez różnych producentów, najistotniejszym elementem każdego z systemów monitoringu jest kwestia podejścia producenta do zabezpieczenia systemu przed ingerencją osób z zewnątrz. Pod tym względem, już w przedbiegach należałoby odrzucić wszelkie systemy wykorzystujące do analizy zasoby sprzętowe, znajdujące się w chmurze producenta. Istnieje jedynie garstka „zachodnich" producentów oferujących wysoki poziom szyfrowania danych przy jednoczesnym prowadzeniu analizy na sprzęcie znajdującym się lokalnie lub serwerowni, w sztabie. Warto wspomnieć, że wśród nich znajduje się kilka polskich firm, których jakość produktów niejednokrotnie przewyższa nawet powszechnie cenione systemy izraelskie.

Po drugie, to możliwość zdalnego przesyłu strumieni wideo. Jest ona szczególnie istotna w przypadku monitoringu tzw. zielonych granic. Dzięki zaawansowanemu transkodingowi obrazu istnieje możliwość przesyłania strumieni wideo w jakości full HD, nawet przy łączach o przepustowości 32kbps. Tym samym możliwe jest zbudowanie centralnej stacji monitorowania z podglądem obrazu na żywo z wielu kamer w oparciu o łącza, realizowane na przykład przez routery komunikujące się w technologii 3G/LTE lub poprzez łącza satelitarne. Jednocześnie warto zwrócić uwagę na sam rodzaj kodeku wykorzystywanego do kodowania obrazu. Niektórzy producenci oprogramowania stosują swoje własne kodeki, które nie tylko zwiększają wydajność transmisji, ale również zapewniają dodatkowy poziom bezpieczeństwa przesyłanego i zapisywanego materiału.

Ostatnim elementem, najistotniejszym z punktu widzenia całości systemu bezpieczeństwa terenów przygranicznych, jest integralność i modułowość rozwiązania. Szczególną uwagę należy tutaj zwrócić na *wybór oprogramowania*, które z jednej strony będzie zapewniało możliwie najlepszą skuteczność analiz wideo, ale z drugiej, będzie platformą pozwalającą na zautomatyzowanie i integrację procesów, związanych nie tylko z samą obsługą wideo czy pozostałej infrastruktury bezpieczeństwa (skanery rentgenowskie, czujniki materiałów niebezpiecznych itp.), mogącą stanowić realne wsparcie w zarządzaniu operacyjnym w przypadku wystąpienia zagrożenia. Najlepsze systemy są w stanie obsłużyć wszystkie niezbędne z punktu widzenia bezpieczeństwa, urządzenia sterowalne elektronicznie występujące na wyposażeniu danych jednostek, przy zachowaniu uniwersalności i jednorodności swojego interfejsu wraz z modułową budową i niezawodnością działania. Możliwość rozbudowy w przyszłości oraz łatwość integracji z powstającymi centralnymi systemami, również jest niezwykle istotna.

Podsumowując, systemy wizyjne i termowizyjne w ochronie obszarów przygranicznych czeka w najbliższych latach bardzo duży rozwój. Zupełnie osobnym zagadnieniem, są prawne aspekty funkcjonowania tego typu systemów, ale jak to zwykle bywa, i w tym przypadku ustawodawca nie do końca nadąża z regulacjami prawnymi za rozwojem technologii. W tym miejscu po raz kolejny pojawia się kwestia bezpieczeństwa zabezpieczenia danych oraz kwestia prawnego wykorzystania danych. Bezpieczeństwo to, na najwyższym poziomie, zapewnia jedynie garstka producentów. Pozostaje, więc mieć nadzieję, że nasza prywatność nie będzie ponad miarę naruszana, a równowaga pomiędzy bezpieczeństwem państwa, a naszą prywatnością oparta będzie nie tylko o dobrze funkcjonujące i przemyślane obwarowania prawne, ale również, a może przede wszystkim, o zdrowy rozsądek osób zarządzających i wykorzystujących systemy monitorujące, na co dzień.

Rafał Rotblum
Ekspert w dziedzinie fizycznej i technicznej ochrony obiektów

OCHRONA PRZECIWPOŻAROWA W SIŁACH ZBROJNYCH RP

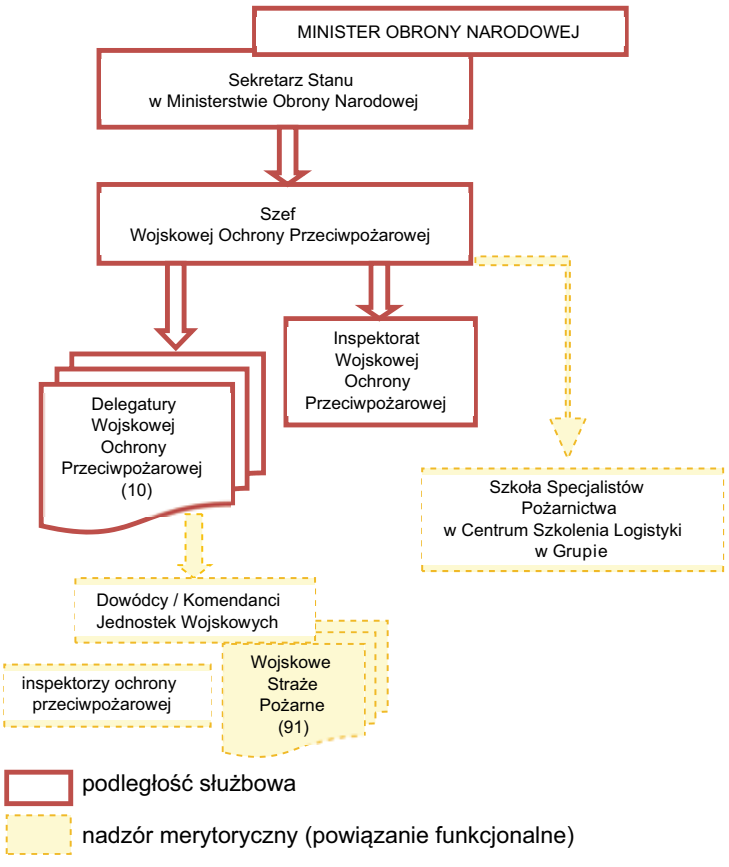
Część I. Współczesność i tradycje

Wojskowa Ochrona Przeciwpożarowa sprawuje w imieniu Ministra Obrony Narodowej instytucjonalny nadzór nad przestrzeganiem przepisów o ochronie przeciwpożarowej (na takich samych zasadach jak Państwowa Straż Pożarna w kraju) oraz wykonuje zadania w zakresie organizowania i prowadzenia działań ratowniczych w czasie walki z pożarami, a także likwidacji innych miejscowych zagrożeń. Zgodnie z § 3 ust. 1 rozporządzenia Ministra Obrony Narodowej z dnia 24 sierpnia 1992 r. w sprawie zasad i trybu wykonywania zadań przez Wojskową Ochronę Przeciwpożarową WOP tworzą:

1) **Szef WOP i podległy mu Inspektorat WOP,**
2) **szefowie delegatur WOP i podległe im delegatury WOP,**
3) **wojskowe straże pożarne.**

W skład struktury etatowej Wojskowej Ochrony Przeciwpożarowej wchodzi Inspektorat Wojskowej Ochrony Przeciwpożarowej w Warszawie oraz 10 delegatur Wojskowej Ochrony Przeciwpożarowej. Siedziby i właściwość terytorialną Szefa WOP i podległych mu Szefów Delegatur WOP określono następująco:

1. Szef Wojskowej Ochrony Przeciwpożarowej z siedzibą w **Warszawie** – właściwy dla obszaru całej Polski .
2. Szef Delegatury Wojskowej Ochrony Przeciwpożarowej z siedzibą w:
   Bydgoszczy – właściwy dla obszaru województwa kujawsko-pomorskiego i łódzkiego;
   Gdyni – właściwy dla obszaru województwa pomorskiego;
   Krakowie – właściwy dla obszaru województwa małopolskiego, śląskiego i świętokrzyskiego;
   Lublinie – właściwy dla obszaru województwa lubelskiego i podkarpackiego;
   Olsztynie – właściwy dla obszaru województwa warmińsko-mazurskiego i podlaskiego;
   Poznaniu – właściwy dla obszaru województwa wielkopolskiego;



Struktura organizacyjna

Szczecinie – właściwy dla obszaru województwa zachodniopomorskiego;
Warszawie – właściwy dla obszaru województwa mazowieckiego;
Wrocławiu – właściwy dla obszaru województwa dolnośląskiego i opolskiego;
Zielonej Górze – właściwy dla obszaru województwa lubuskiego.

Zasadnicze zadania

Wojskowa Ochrona Przeciwpożarowa wykonując zadania Państwowej Straży Pożarnej posiada legitymację prawną w obszarze swojego oddziaływania, tj. w komórkach i jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych do podejmowania określonych działań mających na celu zapewnienie odpowiedniego poziomu ochrony przeciwpożarowej w resorcie obrony narodowej, a w szczególności w Siłach Zbrojnych RP.

Do zadań wykonywanych w poszczególnych obszarach należą w szczególności sprawowanie nadzoru nad przestrzeganiem przepisów przeciwpożarowych, poprzez:

a) rozpoznawanie zagrożeń pożarowych i innych miejscowych zagrożeń

w komórkach i jednostkach podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych. Zadanie to realizowane jest w oparciu o prowadzone czynności kontrolno-rozpoznawcze z zakresu ochrony przeciwpożarowej w komórkach i jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych. Czynności kontrolno–rozpoznawcze z zakresu ochrony przeciwpożarowej wykonywane są przede wszystkim na podstawie rocznych planów kontroli szefów Delegatur WOP, zatwierdzanych przez Szefa Wojskowej Ochrony Przeciwpożarowej. Ponadto mogą być wykonywane z inicjatywy Szefa WOP lub szefa delegatury WOP, na polecenie sądu, prokuratora lub Najwyższej Izby Kontroli, jak również na zlecenie dowódcy (kierownika) komórki lub jednostki organizacyjnej podległej Ministrowi Obrony Narodowej lub przez niego nadzorowanej.

Realizacja czynności kontrolno-rozpoznawczych należy do podstawowych zadań delegatur WOP. Rocznie wykonywanych jest średnio 220–250 czynności kontrolno-rozpoznawczych z zakresu ochrony przeciwpożarowej jednostek i instytucji resortu obrony narodowej.

b) wydawanie decyzji administracyjnych: o wstrzymaniu robót (prac), ćwiczeń, o zakazie używania maszyn i urządzeń oraz środków transportu, a także eksploatacji terenów, obiektów i pomieszczeń lub ich części. Szefowie delegatur WOP w ramach rozpoznawania zagrożeń pożarowych w oparciu o prowadzone czynności kontrolno-rozpoznawcze, posiadają legitymację prawną do wydawania pokontrolnych decyzji administracyjnych. Uprawienia te wynikają z § 3 ust. 5 rozporządzenia Ministra Obrony Narodowej w sprawie zasad i trybu wykonywania zadań przez Wojskową Ochronę Przeciwpożarową, w myśl którego w postępowaniu administracyjnym, w sprawach związanych z wykonywaniem zadań i kompetencji WOP, jeżeli inne przepisy nie stanowią inaczej, organem właściwym jest szef delegatury WOP na terenie swojego działania.

Przedmiotowe decyzje wydawane są w związku ze stwierdzeniem w użytkowanych budynkach istniejących nieprawidłowości będących podstawą do uznania tych budynków za zagrażające życiu ludzi.

c) wyrażanie stanowiska w sprawach zgodności wykonania obiektu budowlanego z projektem budowlanym oraz z wymaganiami ochrony przeciwpożarowej, poprzez prowadzenie czynności kontrolno-rozpoznawczych w trybie określonym w art. 56 Prawa budowlanego (tzw. odbiory techniczne w związku ze zgłoszeniem przez inwestorów zakończenia budowy obiektów budowlanych i zamiarze przystąpienia do ich użytkowania).

d) uzgadnianie ekspertyz technicznych i wystąpień dotyczących rozwiązań zamiennych i zastępczych, dotyczących innego sposobu spełnienia wymagań przepisów ochrony przeciwpożarowej oraz przepisów techniczno-budowlanych. Szefowie delegatur Wojskowej Ochrony Przeciwpożarowej wykonując zadania organów administracji uzgadniają (postanowieniami wg przepisów KPA), rozwiązania zamienne lub zastępcze wynikające z przedstawionych ekspertyz technicznych oraz wniosków i wystąpień.

e) opiniowanie dokumentacji (np. programów inwestycyjnych) pod względem zgodności z wymaganiami przepisów ochrony przeciwpożarowej. W ramach prowadzonej działalności Wojskowa Ochrona Przeciwpożarowa opiniuje pod względem ochrony przeciwpożarowej programy inwestycji, minimalne wymagania organizacyjno-użytkowe oraz inną dokumentację, taką jak: plany zagospodarowania przestrzennego kompleksów, projekty urządzania obozowisk, wnioski dot. zmiany sposobu użytkowania obiektów.

Wojskowa Ochrona Przeciwpożarowa sprawuje nadzór nad 1450-cioma jednostkami i instytucjami wojskowymi oraz

25 000 obiektów budowlanych. Rocznie wykonuje ok. 200 czynności kontrolno-rozpoznawczych, opiniuje 210 programów inwestycji oraz minimalnych wymagań org.– użytkowych i uzgadnia wiele ekspertyz technicznych. Ponadto, Szef WOP jest zarządzającym obszarem bezpieczeństwa pożarowego Podsystemu Bezpieczeństwo w Systemie Funkcjonalnym Ochrona i Przetrwanie Wojsk w zakresie określenia wymagań dotyczących uzyskiwania zdolności w tym obszarze przez Siły Zbrojne RP.

Historia i tradycje Wojskowej Ochrony Przeciwpożarowej

Już w latach 1920–1921 w Departamencie VIII Budownictwa istniał samodzielny Wydział Przeciwpożarowy. W okresie 1921–1925 sprawy przeciwpożarowe przejął Referat Budownictwa. Następnie po reorganizacji w 1925 r. dziedzinę tę przeniesiono do Referatu Budowy i Utrzymania. Od 1931 r., w związku z przekazaniem Intendenturze zagadnień konserwacji budynków, ochrona przeciwpożarowa podporządkowana została Departamentowi Intendentury. Od 1936 r. do wybuchu wojny służba przeciwpożarowa podlegała Dowództwu Obrony Przeciwlotniczej, zarówno na szczeblu

Ministerstwa Spraw Wojskowych, jak i Okręgu. Referat Przeciwpożarowy funkcjonował samodzielnie.

Po drugiej wojnie światowej ochrona przeciwpożarowa w wojsku utworzona została w pionie służby kwaterunkowo-eksploatacyjnej rozkazem Naczelnego Dowództwa WP nr 70 z dnia 06.05.1945 r. W okresie tym odczuwano brak doświadczonej kadry. W wyniku wspólnych przedsięwzięć szkoleniowych Wojska i Związku Straży Pożarnych odbudowano ze zniszczeń obiekty Szkoły Oficerów Pożarnictwa przy ul. Słowackiego 52/54 w Warszawie i przeszkolono na rocznym kursie 31 oficerów zawodowych wojska, po czym skierowano ich do służby na stanowiska o specjalności pożarniczej. Do 1948 r. zorganizowano straże pożarne w składnicach, jednostkach lotniczych i na poligonach oraz w niektórych jednostkach wojskowych. Następnie, na potrzeby wojska, w Centralnym Ośrodku Szkolenia Kwatermistrzowskiego w Poznaniu zorganizowano szkolenie pożarnicze. Dynamikę rozwoju poszczególnych dziedzin ochrony przeciwpożarowej odnotowano w drugiej połowie lat 60-tych. Powołano samodzielny ośrodek szkolenia w Lublinie, uaktualniono przepisy przeciwpożarowe w wojsku. Realizacja zadań następnie odbywała się w oparciu o ustawę o ochronie przeciwpożarowej z 12.06.1975 r.

Kierownictwo i nadzór nad ochroną przeciwpożarową sprawował Główny Kwatermistrz, jako organ centralny. Realizację zadań powierzono Szefowi Służby Zakwaterowania i Budownictwa, który posiadał fachową komórkę w postaci Wydziału Ochrony Przeciwpożarowej. W okręgach wojskowych kierownictwo i nadzór nad ochroną przeciwpożarową sprawowali dowódcy OW, którzy zadania wykonywali przez swoich zastępców. Kwatermistrz OW realizował zadania ochrony przeciwpożarowej poprzez Szefa Służby Zakwaterowania i Budownictwa, któremu podlegały Rejonowe Zarządy Kwaterunkowo-Budowlane (WRZKB). Szef Służby i szef WRZKB następnie przez fachowe dwu-trzyosobowe wydziały Ochrony Przeciwpożarowej. Szef Sztabu i szef Służb Technicznych OW, pomimo obowiązków w tym zakresie, nie dysponowali już specjalistycznymi organami. W Rodzajach Sił Zbrojnych kierownictwo i nadzór nad ochroną przeciwpożarową sprawował Dowódca RSZ. Tu również obowiązywał wieloszczeblowy system kierowania i nadzoru.

Podstawę prawną do zmiany i wyeliminowania niedoskonałości w funkcjonowaniu ochrony przeciwpożarowej w wojsku dała ustawa z dnia 24.08.1991 r. o ochronie przeciwpożarowej i ustawa z dnia 24.08.1991 r. o Państwowej Straży Pożarnej oraz akty wykonawcze. Ponadto podstawą do współczesnej organizacji i funkcjonowania dziedziny, jaką jest wojskowa ochrona przeciwpożarowa stanowiło prawo międzynarodowe zawarte w protokołach dodatkowych Konwencji Genewskiej odnoszących się do ochrony formacji cywilnych w czasie konfliktów zbrojnych. Przeobrażenia w ochronie przeciwpożarowej w kraju w 1991 r. doprowadziły do likwidacji komórek organizacyjnych ochrony przeciwpożarowej w poszczególnych Ministerstwach i powstania Państwowej Straży

Pożarnej na mocy ustawy z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej, która ponadto dawała legitymację prawną do powołania Wojskowej Ochrony Przeciwpożarowej a wydane na jej podstawie rozporządzenie Ministra Obrony Narodowej z dnia 24 sierpnia 1992 r. w sprawie zasad i trybu wykonywania zadań przez Wojskową Ochronę Przeciwpożarową określiło następujące jednostki organizacyjne WOP:

1) Szef WOP i podległy mu Inspektorat WOP;
2) szefowie okręgowi WOP i podległe im okręgowe inspektoraty WOP;
3) szefowie delegatur okręgowych inspektoratów WOP i podległe im delegatury;
4) wojskowe straże pożarne.

W wyniku reorganizacji Sił Zbrojnych

RP z dniem 1 kwietnia 2002 r. dokonano zmian w strukturach organizacyjnych Wojskowej Ochrony Przeciwpożarowej. Rozformowano istniejące dotąd Okręgowe Inspektoraty WOP, a Delegatury Okręgowych Inspektoratów WOP przeformowano w Delegatury Wojskowej Ochrony Przeciwpożarowej. W ramach tych zmian utworzono obecne 10 Delegatur WOP.

Mł. Brygadier Emil Ćwikliński
Starszy Specjalista
Inspektorat Wojskowej Ochrony Przeciwpożarowej

SYGNALIZATOR SAOZ-PK2 – NOWE PODEJŚCIE DO SYGNALIZACJI AKUSTYCZNO-OPTYCZNEJ W ZEWNĘTRZNYCH SYSTEMACH PRZECIWPOŻAROWYCH

Firma W2 chcąc sprostać oczekiwaniom klientów, opracowała nowy sygnalizator akustyczno-optyczny SAOZ-Pk2 do zastosowań w zewnętrznych oraz wewnętrznych systemach przeciwpożarowych.

SAOZ-Pk2 jest zmodyfikowaną wersją, znanego od kilku lat sygnalizatora SAOZ-Pk. Wprowadzone zmiany dotyczą parametrów sygnalizatora oraz jego funkcjonalności. Obudowa sygnalizatora SAOZ-Pk2 jest identyczna pod względem gabarytu i kształtu do obudowy SAOZ-Pk. W korpusie sygnalizatora zmienione zostało położenie mikroprzełącznika, który w nowej wersji jest sześciopozycyjny. Kluczowa modyfikacja polega na zastosowaniu nowego typu lampy błyskowej zbudowanej w oparciu o diody LED.

Urządzenie zostało przebadane zgodnie z normą EN 54-3:2001+A1:2002+A2:2006 dla sygnalizatorów akustycznych oraz zgodnie z normą EN 54-23:2010 dla sygnalizatorów optycznych. Zgodność urządzenia z wymogami została potwierdzona przez Certyfikat oraz Świadectwo Dopuszczenia wydane przez CNBOP-PIB.

Tabela 1. Porównanie parametrów oraz funkcji SAOZ-Pk2 i SAOZ-Pk.

Parametr/ funkcja	SAOZ-Pk	SAOZ-Pk2
Napięcie zasilania [V]	16 – 32,5	20 – 32,5
Pobór prądu w stanie alarmowania [mA]	< 450	< 100 < 50*
Rodzaj środowiska pracy	B	
Kategoria urządzenia	O	
Źródło dźwięku	Przetworniki piezoceramiczne	
Natężenie dźwięku w odl. 1 m	>110 dB	
Liczba syren	4	
Obniżony poziom głośności	Tak, o 10 dB	Tak, o 6 dB
Źródło światła	palnik ksenonowy	diody LED
Barwa światła	czerwona	W zależności od wersji lampy błyskowej: barwa czerwona, biała lub na zmianę czerwona i biała
Czas trwania błysku [ms]	~0,5	~190
Liczba błysków na minutę	34	33
Tryb obniżonego obszaru pokrycia	Nie	Tak
Opóźnienie wyłączenia lampy błyskowej	Nie	Tak, tylko przy zastosowaniu wyłącznika WSD-1
Obsługa wyłącznika WSD-1	Tak	
Synchronizacja	tylko część akustyczna	część akustyczna i optyczna
Współpracująca puszka instalacyjna	PIP-3AN	

* dotyczy aktywnego trybu obniżonego obszaru pokrycia i obniżonego poziomu głośności

Sygnalizacja akustyczna

Zasada działania sygnalizacji akustycznej w SAOZ-Pk2 nie uległa zmianom. Tak samo jak w SAOZ-Pk użytkownik ma możliwość wyboru jednego z czterech wzorów syren alarmowych oraz aktywowania trybu obniżonego poziomu głośności. Wyboru wzoru syreny alarmowej oraz uruchomienie trybu obniżonego poziomu głośności dokonuje się za pomocą trzech mikroprzełączników. Syreny alarmowe generowane są przez dwa przetworniki piezoceramiczne. Natężenie dźwięku mierzone z odległości 1m wynosi powyżej 110 dB dla syreny pożarowej. Przy aktywnej funkcji obniżonego poziomu głośności, natężenie dźwięku maleje o 6 dB.

Sygnalizacja optyczna

Obwód odpowiedzialny za sygnalizację optyczną przeszedł kompleksową modernizację. Przede wszystkim nowa lampa błyskowa została zbudowana w oparciu o diody LED. Zmiana ta ma wpływ na walory estetyczne, parametry błysku oraz parametry elektryczne.

Estetyka

Wpływ na walory estetyczne ma przede wszystkim klosz, pod którym zamontowany jest układ generujący światło błyskowe. Zmiana ta polega na zmniejszeniu transparentności klosza, dzięki czemu zamaskowany został obwód lampy błyskowej. Sygnalizatory SAOZ-Pk2 dostępne są w trzech wersjach wykonania lampy błyskowej. Pierwszy rodzaj lampy będzie emitować światło o barwie czerwonej zgodnie z Rozporządzeniem MSWiA z dn. 27 kwietnia 2010 r. (Dz.U. 2010 nr 85 poz. 553). W tej

konfiguracji klosz będzie koloru czerwonego. Drugi rodzaj sygnalizacji optycznej to błysk o barwie białej, klosz będzie koloru białego. Trzeci typ sygnalizacji optycznej polega na generowaniu impulsu świetlnego na zmianę o barwie czerwonej i białej. W tym przypadku fabrycznie zostanie zamontowany klosz biały.

Parametry optyczne

W poprzedniej wersji sygnalizatora za źródło światła wykorzystany został palnik ksenonowy, jego zmiana na diody LED zaowocowała osiągnięciem lepszych parametrów optycznych i elektrycznych. Zmienił się m. in. czas trwania błysku, który w przypadku palnika ksenonowego wynosił ~0,5 ms, w nowej lampie czas trwania błysku wynosi ~0,19 s. Nowością w SAOZ-Pk2 jest funkcja umożliwiająca zmniejszenie obszaru pokrycia. Funkcje tą można aktywować ustawiając mikroprzełącznik LP w pozycji ON, wówczas bryła fotometryczna dla barwy czerwonej jest mniejsza niż w SAOZ-Pk, jednocześnie zmniejsza się pobór prądu. W trybie pełnego obszaru pokrycia bryła fotometryczna jest większa. Dla sygnalizatorów, gdzie impuls błyskowy ma barwę białą, bryła fotometryczna jest większa niż dla błysku o barwie czerwonej.

Parametry elektryczne

Istotną zmiana jest znaczne zmniejszenie poboru prądu. Całkowity pobór prądu przez SAOZ-Pk2 w trybie pełnej głośności i pełnego obszaru pokrycia nie przekracza 100 mA, dzięki czemu nie ma potrzeby stosowania dodatkowych źródeł zasilania, kiedy budowane są sieci paru sygnalizatorów, a wydajność prądowa central wynosi np. 0,5 A. W sytuacji, kiedy użytkowni uruchomi funkcję obniżonego poziomu głośności i zmniejszonego obszaru pokrycia, pobór prądu przez urządzenie nie będzie przekraczać 50 mA.

Nowe f unkcje

Nowością w SAOZ-PK2 jest możliwość synchronizacji zarówno części akustycznej jak i optycznej. W przypadku SAOZ-Pk synchronizowana była tylko część akustyczna. Zasada działania synchronizacji nie uległa zmianie, to znaczy że do budowy sieci sygnalizatorów potrzebna jest dodatkowa linia podłączana do zacisku „S" sygnalizatora. Impuls synchronizacyjny nadawany jest przez urządzenie o najwyższym priorytecie, czyli pracujące w trybie „Master". Pozostałe urządzenia w sieci muszą być ustawione w trybie „Slave", tryb pracy sygnalizatora konfigurowany jest jednym mikroprzełącznikiem. Zachowanie zasady działania linii synchronizacyjnej daje możliwość budowania sieci z różnego typu sygnalizatorów np. SAOZ-Pk, SA-K7N, SA-K5N.

Ostatni przełącznik umożliwia aktywowanie opóźnienia wyłączenia lampy błyskowej. Funkcja ta zadziała tylko wtedy, kiedy do zacisku sygnalizatora zostanie podłączony wyłącznik sygnału akustycznego (WSD-1). Opóźnienie wyłączenia lampy błyskowej, polega na generowaniu światła błyskowego przez 2 minuty od momentu wyłączenia sygnału akustycznego. Po upływie tego czasu nie będzie emitowany ani sygnał akustyczny ani sygnał optyczny. W celu ponownego uruchomienia sygnalizacji akustyczno-optycznej należy odłączyć zasilanie i po kilkunastu sekundach ponownie doprowadzić do zacisków sygnalizatora napięcie zasilające.

Reklama

ZABEZPIECZENIE INFRASTRUKTURY KRYTYCZNEJ WYMOGIEM PRAWIDŁOWEGO FUNKCJONOWANIA PAŃSTWA

Przez ochronę infrastruktury krytycznej należy rozumieć wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom, ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków lub innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

Aby uchronić się od zagrożeń spowodowanych przez klęski żywiołowe czy celowe działanie człowieka (sabotaż, terroryzm, ...), **infrastrukturę należy zabezpieczyć za pomocą elektronicznych systemów bezpieczeństwa**.

Najlepszą ochronę infrastruktury krytycznej zapewni dedykowana do tego typu zadań **inteligentna Platforma monitoringu wizyjnego Arkiv**. Platforma ta jest w pełni zintegrowana z systemem bezpieczeństwa **ProtegeGX**. Zarówno Arkiv, jak i ProtegeGX zbudowane są w oparciu o serwery posiadające zaawansowane mechanizmy gwarantujące ich bezawaryjne działanie. Cenne dane możemy zabezpieczyć za pomocą macierzy dyskowej RAID. Jeżeli zabezpieczany obiekt cechuje się szczególną ważnością, czy wrażliwością zalecane jest wykorzystanie funkcji nadmiarowego serwera (serwera failover). Aby system działał najefektywniej, należy dążyć do maksymalnej automatyzacji. Właśnie z tego względu serwery CCTV posiadają wbudowane zaawansowane funkcje analityki wideo, które potrafią automatycznie wykryć ogień bądź dym na którejkolwiek z kamer znajdujących się w systemie. Potrafią również **rozpoznać twarz poszukiwanej osoby, tablice rejestracyjne pojazdów, wykryć obiekty przecinające wcześniej zdefiniowane wirtualne linie, lub monitorować obecność w zdefiniowanych strefach zagrożeń i wiele innych**. Operator systemu zostaje zaalarmowany o zaistniałych zdarzeniach. Arkiv dzięki zapisowi metadanych razem z materiałem wideo umożliwia w ułamku sekundy odszukanie zdarzenia również w nagraniach. Podczas sytuacji kryzysowej niedopuszczalny jest tradycyjny sposób przeglądania danych. Ślęczenie przed monitorem i przeglądanie dostępnego materiału w poszukiwaniu interesującego nas zdarzenia może trwać niemal w nieskończoność i niebezpiecznie opóźniać podjęcie stosownych działań zaradczych. W systemie Arkiv wskazujemy jedynie wytyczne do wyszukiwania, a wyniki otrzymujemy natychmiast w formie miniatur. Nikogo nie trzeba chyba przekonywać, że w sytuacji zagrożenia najważniejszy jest czas. Im szybciej operator znajdzie zdarzenie, tym więcej czasu służby będą miały na jego opanowanie, lub zapobieżenie jego skutkom. Platforma monitoringu wizyjnego Arkiv jest kompatybilna ze znakomitą większością kamer IP dostępnych na rynku oraz jako jeden z nielicznych systemów ma możliwość przejęcia strumieni wideo zarówno z rejestratorów IP jak i analogowych. Powyższe cechy pozwalają zastosować Arkiv w istniejących już systemach, które nie posiadają tak zaawansowanych funkcjonalności. Znakomitym uzupełnieniem funkcjonalności Arkiva **jest ProtegeGX. System bezpieczeństwa łączący w sobie cechy systemu antywłamaniowego, kontroli dostępu, zarządzającego windami, oraz posiadającego funkcje automatyki budynkowej, rejestracji czasu pracy, rejestracji gości.** System ten przewyższa swoimi możliwościami produkty konkurencji, może się poszczycić wieloma zadowolonymi użytkownikami z różnych branż i krajów. Dzięki zastosowaniu kart dostępu w najbezpieczniejszym, dostępnym w tym momencie standardzie Desfire, możemy być pewni, że niepowołane osoby nie dostaną się niezauważone na teren zabezpieczanego obiektu. Aby system działał zgodnie z założeniami, nie możemy zapomnieć również o elementach detekcyjnych najwyższej jakości. Platforma Protrege GX bardzo chętnie łączona jest z barierami podczerwieni i mikrofalowymi włoskiego producenta Mitech.

Pełna synergia Arkiv i ProtegeGX umożliwia prawidłowe zabezpieczenie najważniejszych obiektów. Systemy komunikują się ze sobą dzięki czemu możliwe jest maksymalne wykorzystanie ich potencjału i jeszcze szybsze wykrycie zagrożenia. System telewizji przemysłowej otrzymując informację o naruszeniu strefy w SSWiN, może skierować uwagę operatora, automatycznie pokazując obraz kamery powiązanej ze strefą, lub wywołać odpowiedni preset kamery obrotowej mającej w zasięgu ww. strefę. ProtegeGX może z kolei pobierać materiał wideo z systemu Arkiv. Jeżeli w obiekcie nastąpi alarm lub siłowe otwarcie drzwi, operatorowi automatycznie zostaną wyświetlone najistotniejsze dla niego informacje. Dostanie precyzyjną informację gdzie doszło do naruszenia systemu oraz zostanie wyświetlony obraz na żywo, natomiast w osobnym oknie pojawi się nagranie z chwili zdarzenia. Co istotne, zarówno Arkiv jak i Protege są systemami skalowalnymi, co oznacza, że inwestycję można realizować etapami, a koszty z nią związane rozłożyć w czasie.

Tylko przez łączne zastosowanie systemów Arkiv i ProtegeGX, delikatny i skomplikowany system naczyń połączonych, jakim jest infrastruktura krytyczna, może być właściwie zabezpieczony i chroniony. **Zaawansowana technologia Arkiv i ProtegeGX umożliwia szybką reakcję i pełną ochronę zasobów, obiektów, urządzeń czy instalacji mających podstawowe znaczenie dla prawidłowego i harmonijnego funkcjonowania gospodarki, państwa i życia jego obywateli.**

Tomasz Białek
Inżynier ds. Zintegrowanych Systemów Bezpieczeństwa

Miwi Urmet Sp. z o.o.
91-341 Łódź, ul. Pojezireska 90a
tel. 42 616 21 00
e-mail: miwi@miwiurmet.pl

ICTProtegeGX®

Jeden zintegrowany system dla bezpieczeństwa i automatyki obiektu.

- Kontrola Dostępu
- System Sygnalizacji Włamania i Napadu
- Telewizja Przemysłowa
- Rejestracja Gości
- Zarządzanie windami
- Rejestracja Czasu Pracy
- Interkom (komunikacja)
- Automatyka Budynku

oraz szerokie możliwości integracji z systemami zewnętrznymi

Miwi Urmet Sp. z o.o.

91-341 Łódź,
ul. Pojezierska 90A
tel. 42 616 21 00
miwi@miwiurmet.pl

www.miwiurmet.pl

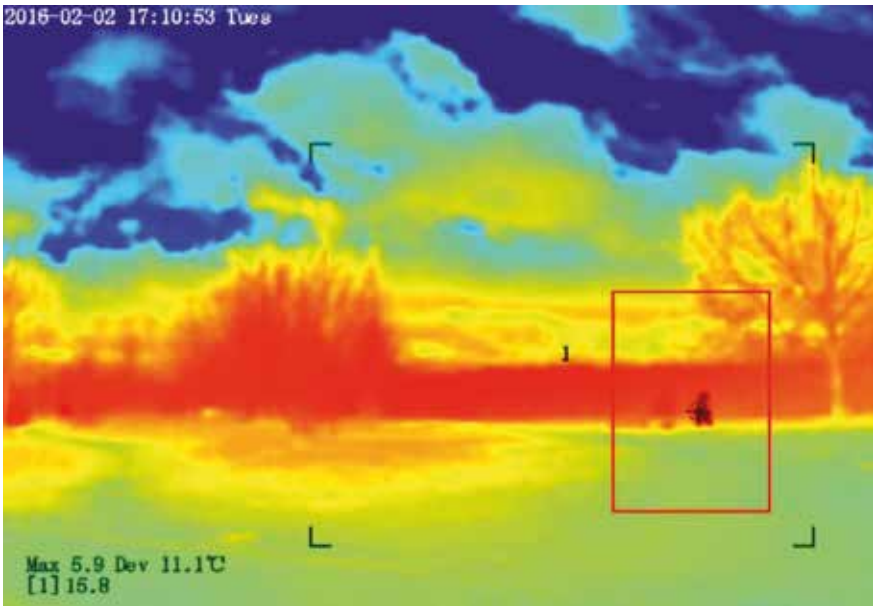
DOŚWIADCZENIA ZE STOSOWANIA UAKTUALNIONEJ NORMY OBRONNEJ W SIŁACH ZBROJNYCH RP

Artykuł ten jest próbą omówienia NO-04-A004-1 2016, która z dużym opóźnianiem została wprowadzona do realizacji w wojsku. Została oparta o wymagania NO PN-EN 50131-2-2: 2009, która już została wprowadzona w środowisku cywilnym w sierpniu 2009 r. Jednak obserwacja realizacji inwestycji oraz projektów, które są realizowane w wojsku dają podstawę sądzić, że wiedza wynikająca z tych aktów jest niewystarczająca. Należy ją jak najszerzej prezentować i rozpowszechniać informacje o rozwiązaniach, które powinny być stosowane w wojsku.

Człowiek, który dotychczas chronił koszary i sprzęt bojowy będzie zastępowany technicznymi systemami wspomagającymi ochronę. Tylko nowoczesne technologie we współpracy z wyspecjalizowanymi służbami ochronnymi są w stanie sprostać zadaniu i na właściwym poziomie chronić obiekty i sprzęt wojskowy, a także podejmować działania uprzedzające w przypadku zaistnienia zagrożenia. Ochrona koszar, sprzętu bojowego i wyposażenia wojskowego w warunkach pokoju i działań bojowych jest ważnym zadaniem, ale nie stała się priorytetem w bieżącej działalności wojska.

Aby umożliwić zastosowanie nowych technologii w ochronie obiektów wojskowych dokonano aktualizacji przyjętej wcześniej normy i od dnia 05.05.2016 r., zgodnie z zatwierdzoną decyzją Nr 98/MON Ministra Obrony Narodowej z dnia 14 kwietnia 2016 r. (Dz. Urz. Min. Obr. Nar. poz. 58) wszystkie nowo budowane oraz już funkcjonujące systemy powinny spełniać wymagania zaktualizowanej normy.

Wymagania Norm Obronnych z serii NO-04-A004 Obiekty wojskowe – Systemy alarmowe w wielu miejscach znacznie różnią się od zapisów z aktualnych Polskich Norm dotyczących systemów alarmowych. Jest to bardzo ważne dla firm składających ofertę instytucji wojskowej. W wielu wypadkach zamawiający w wojskowych mundurach opierają się na



Fot. 1. Obraz z kamery termowizyjnej
Źródło: Novuscctv.com

niejawnych dokumentach, do których wykonawcy nie mają dostępu. Oprócz tego część wymagań zawartych w Normach Obronnych nie ma swoich odpowiedników w aktualnych normach „cywilnych", co komplikuje projektowanie i dobór elementów ochrony dla wojska. Zdecydowana większość urządzeń oferowanych na rynku ochrony jest klasyfikowana wg norm „cywilnych", a ich parametry mieszczą się – jeśli są odpowiedniej klasy – w wymaganiach militarnych. Problemy dotyczą zwłaszcza:

- klasyfikacji środowiskowej urządzeń – pokrycie z normami cywilnymi jest tylko częściowe,
- wymagań, co do zasilania – nie ma w aktualnych „cywilnych" normach odpowiednika zapisów wojskowych. W normach obronnych są zapisy szczątkowe, w których powielono wymagania z około 1996 roku z wycofanych w 2009 roku norm „cywilnych" z serii 08390,
- poziomów dostępu do programowania i odczytu danych z urządzeń stosowanych w ochronie – brak tu korelacji z normami PN.
- brakuje w Normach Obronnych wymagań: dotyczących współpracy zabezpieczeń mechanicznych z elektronicznymi systemami ochrony.
- nie określono w NO wymagań dotyczących obudów urządzeń w klasach szczelności, odporności na wodę i uderzenia (klasyfikacja IP i IK).
- nie sprecyzowano wymagań systemów bezprzewodowych – wymagania w NO dla przycisków napadowych – zwanych w normie pilotami – w grupie ostrzegaczy napadowych są ogólnikowe i mogą wprowadzać w błąd,
- nie określono precyzyjnie wymagań dla zabezpieczenia mechanicznych, budowlanych i organizacyjnych centrów monitoringu – wymagania wojskowe mieszczą się w kilku zdaniach.

Jednak analiza powyższego dokumentu i doświadczenie skłania mnie do postawienia tezy, że większość obiektów wojskowych w myśl normy cywilnej PN-EN-50131 powinna być zaprojekto-

wana i wykonana, **wg stopnia trzeciego** (zgodnie z normą cywilną), co w mojej ocenie jest wystarczającym poziomem dla zabezpieczenia większości obiektów wojskowych.

Dokonując oceny aktualnej Normy Obronnej producenci i dystrybutorzy, a także instalatorzy systemów alarmowych wskazują różne niedoprecyzowane kwestie ściśle związane ze rodzajem systemów czy też urządzeń, które ich dotyczą.

Przykładem może być kwestia wykorzystania kamer termowizyjnych na obiektach wojskowych i obiektach infrastruktury krytycznej. To kolejny trudny temat związany z ochroną zewnętrzną tego typu obiektów. Trudny, ponieważ słabo opisany w normach. Dotyczy to zarówno Polskiej/Europejskiej Normy PN-EN 50131-1:2009, Normy PN-EN 62676-1-1:2014, jak i innych powiązanych z nią norm, które nie wspominają nawet słowem o kamerach termowizyjnych stosowanych w systemach ochrony.

Można mieć zastrzeżenia do nowej Normy Obronnej serii NO-04-A004 z 2016 roku, ale jej zaletą jest fakt, że w jakikolwiek sposób wspomina i stara się znormalizować wykorzystywanie wspomnianych wyżej technologii w ochronie obiektów wojskowych. ***Według Normy Obronnej kamery termowizyjne na obiektach wojskowych mogą być wykorzystywane na dwa sposoby***:

- do weryfikacji sygnałów alarmowych czujek zewnętrznych,
- jako odrębne urządzenie alarmowe przy wykorzystaniu wizyjnej detekcji ruchu.

Odnośnie weryfikacji sygnałów alarmowych w części 4 Normy Obronnej dotyczącej urządzeń zewnętrznych zapisano: *„W strefie ochrony zewnętrznej bezpośredniej oraz w strefie ochrony zewnętrznej obwodowej należy integrować zewnętrzne systemy alarmowe z telewizyjnymi systemami nadzoru w celu natychmiastowej weryfikacji generowanych sygnałów alarmowych przez urządzenia alarmowe zainstalowane w tych strefach”.*

Więcej na temat sposobu integracji można znaleźć w części 7 dotyczącej telewizyjnych systemów nadzoru. Jest to istotny zapis dotyczący sposobu współpracy telewizyjnego systemu nadzoru z systemem alarmowym: *„… Powyższa weryfikacja powinna się odbywać na zasadzie przełączenia obrazu z miejsca zdarzenia na monitor alarmowy z jednoczesnym rozpoczęciem rejestracji zdarzenia z tzw. „prealarmem”. System powinien być skonfigurowany w taki sposób, aby odtworzył obraz obszaru, w którym wystąpił alarm począwszy od momentu 5 s przed jego powstaniem. …”.* Podano również wymóg, że kamery termowizyjne stosowane na obiektach wojskowych muszą mieć rozdzielczość nie mniejszą niż 320x240 pikseli. W mojej ocenie opis ten jest niewystarczający i może stać się źródłem rozbieżności pomiędzy zleceniodawcą a wykonawcą.

Z kolei w części 4 Normy Obronnej w wymaganiach dotyczących czujek stosowanych w strefie ochrony zewnętrznej obwodowej, w tablicy 2 podano, że kamery światła dziennego mogą być wykorzystywane w systemach wizyjnej detekcji ruchu na odległość maksymalną 80 m, a kamery termowizyjne na odległość do 450 m.

Z powyższych zapisów dla specjalistów wypływają określone wnioski, w tym między innymi, że:

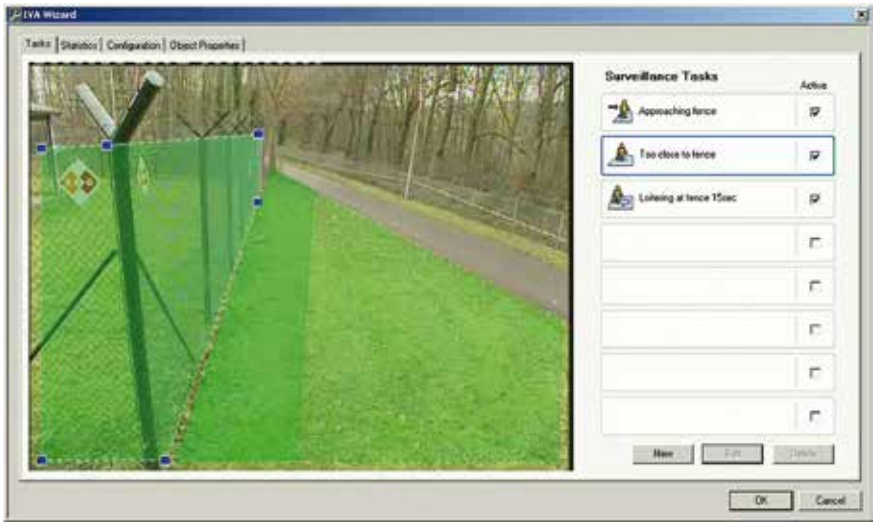
- do weryfikacji sygnałów alarmowych nie jest możliwe zastosowanie kamer umieszczonych na głowicach PT, a muszą to być kamery stacjonarne;
- kamery termowizyjne, ze względu na fakt, że promieniowanie termiczne jest słabiej tłumione przez atmosferę (mgła, kurz, opady itp.) mogą być wykorzystywane na większe odległości niż kamery światła dziennego;
- można przyjąć, że maksymalne odległości, na jakie można stosować kamery (wizyjne i termowizyjne) do weryfikacji sygnałów alarmowych, są takie same, jak wyżej podane graniczne odległości (w cz. 4 Normy Obronnej), dla maksymalnej detekcji kamer, wykorzystywanych w systemach detekcji ruchu.

Należy dodać, że czwarty arkusz Normy Obronnej NO-04-A004 Obiekty wojskowe. Systemy alarmowe, ***zawiera unikalne dla projektantów w Polsce informacje na temat projektowania ochrony zewnętrznej obiektów***. Normy PN-EN dotyczą, bowiem tylko systemów alarmowych wewnątrz obiektów z uwzględnieniem tego, że część urządzeń może być montowana na zewnątrz. W normie NO-04-A004-4: 2016 jest podany podział na cztery strefy ochrony:

- peryferyjna – poza ogrodzeniem, zwykle niewyposażona w urządzenia alarmowe, wymagany pas o szerokości 25 m bez zasłaniającej roślinności,
- zewnętrzna obwodowa – obszar między ogrodzeniem zewnętrznym a wewnętrznym – systemy ogrodzeniowe, nadziemne i podziemne,
- zewnętrzna bezpośrednia – obszar o szerokości 15 m przyległy do budynków, gdzie montowane są zarówno systemy alarmowe, jak i kamery,
- wewnętrzna – obszar wewnątrz budynków razem ze wszystkimi otworami, gdzie montuje się systemy ochrony elektronicznej.

Wprowadzone są pojęcia dotyczące telewizyjnych systemów nadzoru i telewizyjnych systemów nadzoru z wizyjną detekcją ruch.

Ochrona strefy peryferyjnej. W strefie peryferyjnej nie należy instalować urządzeń alarmowych w czasie pokoju. W strefie tej utrzymuje się pas 25 m wolny od wysokich zarośli, krzewów i traw, umożliwiający wgląd w teren przyległy do



Fot. 2. Ochrona obwodowa
Źródło: Secural

chronionego obiektu. Pasa tego nie utrzymuje się w przypadku, gdy strefa ochrony peryferyjnej obejmuje obszar niebędący terenem wojskowym.

Ochrona strefy zewnętrznej obwodowej. W strefie zewnętrznej obwodowej następujących obiektów wojskowych kategorii I, m.in. stanowisk dowodzenia poziomu strategiczno–operacyjnego, stanowisk dowodzenia i naprowadzania Sił Powietrznych, baz, składnic oraz składów, w których przechowuje się uzbrojenie, amunicję, materiały wybuchowe, bomby, rakiety, granaty, torpedy itp. należy stosować, co najmniej dwa niezależne urządzenia lub systemy alarmowe działające w oparciu o różne zjawiska fizyczne – np. w układzie.: system naziemny i system ogrodzeniowy, system ogrodzeniowy i system podziemny, system naziemny i system podziemny lub dwa systemy naziemne. W strefie zewnętrznej obwodowej pozostałych obiektów wojskowych kategorii I powinno się stosować pojedyncze urządzenia lub systemy alarmowe naziemne, podziemne lub ogrodzeniowe. Systemy alarmowe ogrodzeniowe należy instalować na ogrodzeniach wewnętrznych (w przypadku, gdy występują dwa ogrodzenia).

System alarmowy w strefie zewnętrznej obwodowej powinien wykrywać:

- poruszanie się w chronionej strefie,
- sabotaż urządzeń i linii dozorowych systemu alarmowego.

Ponadto systemy alarmowe powinny sygnalizować użycie ostrzegacza napadowego.

Ochrona strefy zewnętrznej bezpośredniej. W strefie zewnętrznej bezpośredniej należy stosować pojedyncze urządzenie lub systemy alarmowe naziemne, podziemne lub ogrodzeniowe. Przy wyborze urządzeń wchodzących w skład poszczególnych systemów należy brać pod uwagę ich zasięgi dostosowane do wielkości ochranianych budynków lub rejonów. Zainstalowane w strefie zewnętrznej bezpośredniej urządzenia powinny współpracować z telewizyjnymi systemami nadzoru, jako weryfikacja powstałych zdarzeń alarmowych. NO-04-A004-1: 2016, określa się następujące rodzaje czynności, jakie powinien wykrywać system alarmowy w strefie zewnętrznej bezpośredniej:

- poruszanie się w chronionej strefie,
- sabotaż urządzeń systemu alarmowego.

Ponadto systemy alarmowe powinny sygnalizować użycie ostrzegacza napadowego.

Ochrona strefy wewnętrznej. W strefie wewnętrznej należy instalować dwa oddzielne urządzenia, które swoje działanie opierają na dwóch niezależnych od siebie zjawiskach fizycznych (np. czujka mikrofalowa i czujka podczerwieni).

Określa się następujące rodzaje czynności, jakie powinien wykrywać system alarmowy w strefie wewnętrznej:

- otwarcie drzwi, okien i innych zamknięć chronionej strefy,
- penetrację okien i innych zamknięć chronionej strefy bez ich otwierania,
- poruszanie się w chronionej strefie,
- sabotaż urządzeń systemu alarmowego.

Ponadto systemy alarmowe powinny sygnalizować użycie ostrzegacza napadowego.

Proces dostosowania do nowych Norm Obronnych jest długotrwały i kosztowny, jednak bez jego realizacji bądź zastąpienia jej przez inny dokument nie będzie możliwy jakościowy skok w dziedzinie ochrony obiektów wojskowych. Obecnie w tym procesie dostosowawczym konieczne jest trzymanie się następujących **ogólnych zasad budowy systemów alarmowych** wg normy obronnej NO-04-A004-1 2016:

Zasada nr 1: Ochronę rejonów, terenów, obiektów i pomieszczeń jednostek wojskowych należy zawsze rozpoczynać od budowy systemów alarmowych w strefie ochrony wewnętrznej poprzez instalację systemu alarmowego, czyli system, który będzie wykrywał i sygnalizował niebezpieczeństwo wynikające z niewłaściwej pracy urządzeń systemu alarmowego. Ponadto należy zaplanować wykonanie w I kolejności elementy tego systemu w pomieszczeniach podlegających szczególnej ochronie. Naliczenia ilościowe urządzeń zawarto w NO-04-A004 arkusz 3.

Zasada nr 2: W dalszej kolejności planować rozrzedzanie tego systemu, zabezpieczając strefę ochrony zewnętrznej bezpośredniej i/lub zewnętrznej obwodowej, w których stosuje się elementy systemów ochrony zewnętrznej określone w NO-04-A004 ark. 4. W uzasadnionych przypadkach, o ile istnieje taka możliwość, instaluje się urządzenia do prowadzenia obserwacji terenów przyległych do obiektów wojskowych (w strefie peryferyjnej) na kierunkach zagrożonych największą penetracją i występowania innych zagrożeń.

Zasada nr 3: Nadzór nad wszystkimi sygnałami, informacjami o stanie systemów i urządzeń alarmowych w obiekcie wojskowym sprawuje lokalne centrum nadzoru (LCN) – alarmowe centrum odbiorcze. Zaleca się tam, gdzie jest możliwe i ekonomicznie uzasadnione tworzenie Garnizonowych Centrów Monitorowania Alarmów (GCMA) i prowadzenie nadzoru nad wszystkimi obiektami wojskowymi garnizonu z wykorzystaniem jednego scentralizowanego punktu monitorującego sygnały alarmowe.

Zasada nr 4: Każda rozbudowa systemu powiązana z zabezpieczeniem kolejnych pomieszczeń, budynków powinna być połączeniem z LCN lub GCMA i uaktualnieniem dokumentacji z nią związanej, w tym dokumentacji powykonawczej. Biorąc pod uwagę powyższe oraz fakt, że instalacje alarmowe stanowią integralną część obiektu budowlanego (tak jak np. instalacja elektryczna, wodociągowa itp.) wszelką budowę i rozbudowę instalacji alarmowych należy prowadzić w taki sposób, jak inwestycja budowlana poprzez wprowadzenie zadania do Planu Inwestycji Budowlanych, czyli każda nawet najmniejsza rozbudowa systemu musi być traktowana, jako inwestycja i realizowana poprzez ww. plan.

Zasada nr 5: Centrale alarmowe oraz inne urządzenia decyzyjno-nadzorujące pracę systemu alarmowego powinny znajdować się w pomieszczeniach LCN, GCMA, sił ochronnych lub służb dyżurnych w miejscach, w którym pełniona jest całodobowa służba. To wskazuję nam w sposób jednoznaczny, gdzie należy umieścić LCN.

Zasada nr 6: Każde urządzenie alarmowe (czujka alarmowa, ostrzegacz napadowy) powinno być włączone do wejścia centrali alarmowej rozróżnianego, jako jedna linia alarmowa celem jednoznacznej identyfikacji miejsca zdarzenia alarmowego.

Zasada nr 7: Wewnętrzne czujki alarmowe instalowane w magazynach broni, amunicji, granatów, materiałów wybuchowych oraz innych magazynach i pomieszczeniach wymagających szczególnej ochrony powinny być rozmieszczone w taki sposób, aby swoim polem detekcji obejmowały całą chronioną powierzchnię pomieszczeń, wykluczając powstawanie tzw. „martwych pól". W wielu projektach zadań inwestycyjnych projektanci zapominają o tym wymogu, co powoduję, że niejako z zasady osłabia się ochronę tego ważnego elementu.

Zasada nr 8: Zewnętrzne urządzenia alarmowe powinny posiadać parametry funkcjonalne, które nie będą zakłócać pracy innych urządzeń będących w wyposażeniu obiektów wojskowych oraz nie

Fot. 3. Symboliczna baza wojskowa (do ochrony)
Źródło: Archiwum Allegro

będą utrudniać wykonywania zadań przez personel obiektów wojskowych.

Zasada nr 9: W przypadku dublowania torów transmisji, uszkodzenie każdego z nich ma powodować alarm w LCN (GCMA, Oddalonym Centrum Monitorowania).

Nowoprojektowane i modernizowane systemy powinny spełniać odpowiednie funkcje określone w ww. zaktualizowanej normie, umożliwiając wykrywanie intruzów, przetwarzanie informacji, zgłaszanie alarmów i ich obsługiwanie. Nowe systemy wspomagające ochronę, stosowane do ochrony obszarów, rejonów, terenów, obiektów i pomieszczeń wojskowych ***powinny spełniać pięć podstawowych warunków***:

- wykorzystywać w pełni parametry techniczne czujek zastosowanych do ochrony zadanego rejonu, obszaru, pomieszczenia;
- nie przeszkadzać oraz nie dezorganizować codziennej pracy personelu w chronionym obszarze, rejonie, terenie, obiekcie lub pomieszczeniu;
- zapewniać integrację z istniejącymi systemami sygnalizacji zagrożeń (np. pożarowego) oraz stanowić uzupełnienie innych rodzajów środków zabezpieczających zgodnie z obowiązującymi przepisami,
- funkcjonować poprawnie przy: wilgotności powietrza od 5 do 95%, temperaturze od –40°C do + 50°C dla czujek montowanych w strefie ochrony zewnętrznej obwodowej i bezpośredniej, w temperaturze od –25°C do + 40°C dla czujek montowanych wewnątrz nieogrzewanych pomieszczeń (magazynów), od –10°C do + 40°C dla czujek montowanych wewnątrz ogrzewanych pomieszczeń (magazynów), nie mieć szkodliwego wpływu na zdrowie ludzi przebywających w chronionym obszarze, obiekcie lub pomieszczeniu, w których są one zamontowane. System alarmowy instalowany w pomieszczeniach (magazynach), w których przechowuje się środki tworzące mieszaniny wybuchowe palnych gazów i par cieczy z powietrzem – powinny być przeciwwybuchowe i iskrobezpieczne oraz zabezpieczone pod względem przeciwpożarowym.

Artykuł opisuje tylko niektóre różnice w NO i normach cywilnych. Tych różnic jest znacznie więcej. Te odmienności są widoczne i NO nie nadąża za zmianami w technice ochrony. Proces ten jest bardzo dynamiczny. Zmiany legislacyjne NO są bardzo czasochłonne i już w momencie ich nowelizacji są przestarzałe. Wydaje się koniecznym zmiana podejścia do tego problemu i przyjęcie nowych, bardziej efektywnych rozwiązań.

W mojej ocenie należałoby przejąć długofalowy plan modernizacji systemów ochrony obiektów wojskowych w oparciu o nowo opracowany dokument, który byłby przyjęty po szerokiej konsultacji wojska i wykonawców i który powinien zawierać wybrane nowoczesne rozwiązania dostosowane do potrzeb wojska, eliminujące stare i nieefektywne rozwiązania, które wciąż w wojsku funkcjonują.

Jest to tym bardziej konieczne, że wojsko nie posiada na chwilę obecną racjonalnych procedur, które wpływałby na jakość realizowanych inwestycji. Brak jest np. wyspecjalizowanej komórki, która oceniałaby projekty realizowanych inwestycji ochronnych w wojsku. Wojsko oddało to w prywatne ręce i niektóre firmy realizujące inwestycje wykorzystują tę okoliczność, proponując rozwiązania techniczne nie zawsze nowoczesne lub niedostosowane optymalnie do potrzeb wojska, stosując kryteria zysku ekonomicznego, a nie faktycznego zaspokajanie potrzeb w zakresie ochrony obiektów wojskowych.

Wojsko wydatkuję znaczne kwoty na realizację zadań ochronnych przez Specjalistyczne Uzbrojone Formacje Ochronne (SUFO). Zastosowanie w szerszym zakresie techniki w ochronie obiektów pozwoli ograniczyć te wydatki w perspektywie ok 10 lat, o blisko 50%.

Daje się jednak zauważyć, że problemy realizacji zadań ochronnych w wojsku, i jego rzeczywiste potrzeby w tym zakresie, ciągle nie wzbudzają większego zainteresowania decydentów. Dotychczasowy system i unormowania prawne pozostają bez zmian. Nie dostosowano struktur do zmieniających się zadań, nie opracowano nowych procedur i rozwiązań. Koszty ochrony wciąż rosną, a w związku z odnotowywanym zwiększeniem kosztów pracy, będą osiągały jeszcze większe kwoty.

Jedyną drogą na ograniczenie tych wydatków jest stworzenie nowych unormowań prawnych i przygotowanie kadr, które będą mogły racjonalizować te wydatki. Wdrożenie według nowych pomysłów, nowych inwestycji oraz przygotowanie zmiany sytemu realizacji zadań ochrony fizycznej np. poprzez stworzenie zależnej od wojska wyspecjalizowanej formacji ochronnej, pozwoli w przyszłości na podniesienie na wyższy poziom realizacji zadań ochrony obiektów, a także zmniejszenie finalnego kosztu realizacji zadań ochronnych w Wojsku Polskim.

Jacek Popławski
były oficer IWsp SZ RP

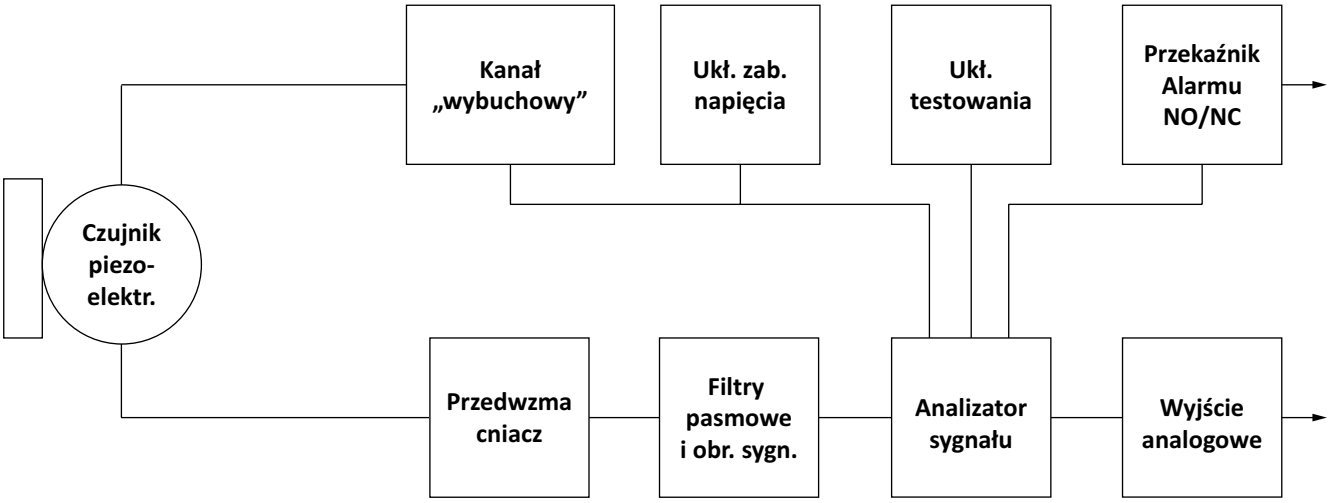
DOZIEMNE SYSTEMY OCHRONY PERYMETRYCZNEJ

Systemy ochrony perymetrycznej (obwodowej) montowane pod ziemią, na płocie lub wzdłuż niego, w ścianach budynków itp. mają wykryć intruza zanim jeszcze podejdzie do chronionego obiektu. Współcześnie znana jest duża ilość liniowych i kierunkowych detektorów wszelkiego typu: podczerwieni, radarowych, przewodowych, sejsmicznych itd. Wieloletnie doświadczenie pozwoliło na stworzenie systemów, które przy bardzo skutecznym wykrywaniu naruszenia chronionego terenu, praktycznie zmniejszają do minimum liczbę fałszywych alarmów. Do najbardziej rozpowszechnionych technologii ochrony przestrzennej należą: systemy monitoringu wizyjnego (CCTV) i czujki radarowe. Połączenie tych technologii z detektorami umieszczonymi wzdłuż/wokół chronionej strefy daje jeszcze lepsze efekty, pozwalając na praktyczne wyeliminowanie fałszywych alarmów i dokładną lokalizację miejsca wtargnięcia intruza z dokładnym określeniem jego osoby, włącznie. W dalszym ciągu tej publikacji, chcemy skupić się na jednym z rodzajów systemów ochrony perymetrycznej, jakim są systemy montowane pod ziemią, nazywane doziemnymi, podziemnymi lub zakopywanymi. Do najbardziej popularnych doziemnych systemów zewnętrznej ochrony obwodowej należą systemy przedstawione poniżej.

System sejsmiczny.

System sejsmiczny, zwany inaczej geofonicznym stanowi element zewnętrznej ochrony obwodowej. Tworzą go czujki wibracyjne, które reagują na wstrząsy. Detektory rozmieszcza się pod ziemią wzdłuż kabla, którego zadaniem jest przekazywanie sygnałów do centrali systemu alarmowego. Czujka wykrywa i sygnalizuje drgania charakterystyczne dla pojawienia się intruzów. Można by wymienić bardzo wiele typów rozwiązań czujek wibracyjnych. W zastosowaniach praktycznych należy rozgraniczyć ww. klasyczne czujki wibracyjne (popularne) od czujek wibracyjnych tzw. sejsmicznych, o bardzo skomplikowanej budowie. Czujki wibracyjne i sejsmiczne realizują funkcję wynikającą z analizy drgań, stąd i ich skomplikowana budowa w szczególności tych wyższej klasy (sejsmicznych z układem mikroprocesorowym). Działanie czujek wibracyjnych i opcjonalnie sejsmicznych może być oparte na różnych rozwiązaniach zależnie od potrzeb. Przy ich konstrukcji wykorzystywane są różnego rodzaju przetworniki, np. elektrodynamiczne, fotoelektryczne czy piezoelektryczne.

Sejsmiczny system ochrony perymetrycznej z wykorzystaniem czujek wibracyjnych jest szczególnie zalecany do stosowania w terenie silnie pofałdowanym, w miejscach oddalonych od ruchu. W systemach tych, wykorzystywane są bezobsługowe czujniki sejsmiczne z przetwornikiem piezoelektrycznym, specjalnie zaprojektowane do pracy pod powierzchnią gruntu. Czujnik zawiera element czuły na wstrząsy w postaci przetwornika piezoceramicznego, zamkniętego szczelnie w chroniącej go obudowie z tworzywa sztucznego, odpornego na działanie substancji chemicznych i organicznych występujących w gruncie. Czujnik jest całkowicie bezobsługowy, nie zawiera żadnych aktywnych podzespołów elektronicznych, dzięki czemu jest niewrażliwy na wszelkie awarie i uszkodzenia natury elektrycznej. System jest wrażliwy na zakłócenia typu pulsacyjnego, które mogą być wynikiem działania urządzeń nawadniających np. fontanny, pompy o ruchu posuwisto-zwrotnym itp. Dla jego poprawnej pracy ważne może być usytuowanie wylotów rynien. W pobliżu owocujących sadów (spadające owoce) system może powodować fałszywe alarmy. W miejscach o dużym ruchu, dla poprawności działania systemu wymagane jest zastosowanie tzw. przeciw-fazy, czyli dodatkowego obwo-



Rys. 1. Schemat czujki sejsmicznej z przetwornikiem piezoceramicznym
Źródło: opracowanie M, Szulc, A. Rosiński.

OPTEX
Sensing Innovation

JUŻ 40 LAT JESTEŚMY ŚWIATOWYM LIDEREM DETEKCJI

Założona w 1979 roku firma OPTEX specjalizuje się w technologiach detekcji. Dzięki temu jesteśmy w stanie sprostać wymaganiom różnych branż, od automatyki drzwiowej i przemysłowej, po branżę security i ochronę kluczowych zasobów środowiskowych. Historia firmy zaczęła się 40 lat temu w Japonii. OPTEX szybko pojawił się w Ameryce Północnej i Południowej, Europie, na Bliskim Wschodzie oraz w Azji. Firma ma obecnie siedziby w 12 krajach i jest reprezentowana w 80.
Naszym celem jest dostarczanie innowacyjnych i wysoce niezawodnych rozwiązań detekcji.

40th
OPTEX GROUP

Więcej informacji na www.optex-europe.com/pl

OCHRONA WEWNĘTRZNA | OCHRONA ZEWNĘTRZNA | DETEKCJA POJAZDÓW | LICZENIE PRZEPŁYWU LUDZI | KONTROLA DOSTĘPU

du „odejmującego" sygnały zakłócające. System sejsmiczny nie toleruje mocno wilgotnego podłoża (wysoki poziom wód gruntowych lub woda opadowa odprowadzana na chroniony teren). Za to świetnie nadaje się pod aleje żwirowe. Jest najczęściej stosowany do ochrony samotnych siedlisk.

Dzięki swej wysokiej czułości czujniki mogą pracować na głębokości do 60 cm, gdzie nie oddziałują już niekorzystne warunki atmosferyczne i nie występują gryzonie. Ponadto czujniki zakopane na takiej głębokości nie przeszkadzają w normalnych pracach ogrodowych ani konserwacji powierzchni (np. wymiany nawierzchni asfaltowej) – można je wykonywać bez ryzyka uszkodzenia czujników.

Fot. 1. Rozmieszczenie czujek sejsmicznych
Źródło: atline.pl.

Zabetonowane systemy ochrony obwodowej

Wyróżniliśmy te systemy nie ze względu na rodzaj czujników (wykorzystuje się tu np. czujniki sejsmiczne z przetwornikiem piezoelektrycznym), a dla podkreślenia ich szczególnego zastosowania. Zabetonowane systemy ochrony doskonale sprawdzają się w wykrywaniu intruzów poruszających się po betonowym podłożu, np. w miejscach takich jak okolice drzwi i okien domostwa lub ścieżki między budynkami. Instalacja czujek pod betonową powłoką nawierzchni uniemożliwia dostrzeżenie i ominięcie lub zniszczenie urządzenia. Osobliwe położenie kabli sensorycznych pod powłoką betonową umożliwia poruszanie się po danej powierzchni nie tylko osób, ale i kilkutonowych pojazdów, nie zmniejszając jednocześnie wrażliwości czujek i nie wpływając negatywnie na skuteczność systemu alarmowego.

Niezaprzeczalną zaletą systemów zabetonowanych jest ich niewidzialność dla potencjalnego intruza. Dodatkowo, ich instalacja jest maksymalnie uproszczona dzięki często fabrycznie okablowanym modułom, przeznaczonym do ochrony obszaru o powierzchni jednego do czterech metrów kwadratowych. Istnieje oczywiście możliwość ich łączenia w celu kompletnego zabezpieczenia żądanego perymetru.

Systemy zabetonowane stosuje się do ochrony stref strategicznych, takich jak obszary przed drzwiami i pod oknami oraz podjazdów i ścieżek prowadzących do budynków. Dzięki temu, że system taki instalowany jest pod betonem, nie zakłóca on estetyki chronionego obszaru.

W systemach tych stosuje się zwykle specjalne czujniki piezoceramiczne, które są umieszczone na płycie pod posadzką oraz pokryte betonem (jastrychem). Czujniki wykrywają ciśnienie wytwarzane przez osobę przechodzącą przez chroniony obszar lub stojącą na nim. Chociaż znajdują się one pod grubą warstwą betonową oraz wytrzymują obciążenia wielu ton, czujniki wyczuwają nawet najlżejsze kroki. Czujniki te, są całkowicie bezobsługowe i nie są narażone na awarie elektryczne, ponieważ nie zawierają żadnych aktywnych podzespołów elektronicznych.

Fot. 2. Przykład montażu zabetonowanego systemu z czujnikami piezoelektrycznymi
Źródło: atline.pl.

System z kablem sensorycznym

System elektromagnetycznej detekcji ruchu (Passive Magnetic Field Detection) jest oparty na zasadzie detekcji anomalii magnetycznych. Wykonany jest z dwóch specjalnych kabli ekranowanych, ułożonych równolegle i zakopanych na głębokości kilkudziesięciu centymetrów (zwykle 15 ÷ 25 cm) pod powierzchnią ziemi na granicy chronionego obszaru. Odległość miedzy kablami wynosi zwykle około 2,0 m, a długość jednego odcinka nie prze-

kracza 200 m. Zwykle kable tak się układa, aby zamknąć obwodowo strefę kontrolowaną dookoła chronionego terenu.

W ekranach kabli wykonane są w równomiernych odstępach otwory, które umożliwiają: w przypadku jednego kabla emitowanie promieniowania elektromagnetycznego, generowanego przez płynący w nim prąd, a w przypadku drugiego kabla – odbieranie promieniowania elektromagnetycznego emitowanego przez pierwszy kabel. Odebrane promieniowanie indukuje w drugim kablu napięcie, będące źródłem informacji dla procesorów analizy sygnału.

Kable są podłączone obustronnie do specjalnych urządzeń nadawczo – odbiorczych, które zarazem mogą stanowić początek kolejnego odcinka kabli. Urządzenia te generują przepływ prądu w pierwszym kablu oraz odbierają i analizują prąd indukowany w drugim kablu.

Pojawienie się intruza w strefie detekcyjnej (szerokości około 3 ÷ 6 m) zakłóca rozkład pola magnetycznego. Analizie podlegają następujące parametry:

a) zmiana amplitudy, która jest zależna od masy intruza;
b) zmiana częstotliwości, która jest zależna od prędkości ruchu intruza;
c) czas występowania zmiany, przy czym wzorce czasu dla naruszenia strefy przez człowieka są wstępnie zaprogramowane.

Te trzy wielkości dostatecznie definiują rodzaj naruszenia, aby ustrzec się fałszywych alarmów w skutku przebiegnięcia małego zwierzęcia lub ekstremalnie złej pogody. Kiedy dojdzie do przekroczenia wszystkich trzech zadanych wartości progowych, system generuje sygnał alarmowy. Bariera może skutecznie chronić od powierzchni ziemi do około 4 metrów wysokości. Podział całego obwodu na 100 … 200-metrowe odcinki pozwala szybko określić numer sektora, w którym nastąpiło naruszenie. Jednocześnie trzeba dodać, że w systemach o stałych parametrach generowanego pola elektromagnetycznego możliwe jest tylko wykrycie zakłócenia. Natomiast w przypadku impulsowej charakterystyki generowanego pola elektromagnetycznego możliwe jest, za pomocą bardziej złożonych układów analizy odebranego sygnału, w miarę dokładne określenie miejsca pojawienia się intruza.

Kabel sensoryczny (używana jest również nazwa sensorowy) może być zakopany w podłożu (również pod betonem, asfaltem itp.), dzięki czemu jest całkowicie niewidoczny dla potencjalnego intruza,

Fot. 4. Idea działania systemu perymetrycznego doziemnego z kablem sensorycznym
Źródło: Senstar Corp.

który na drodze obserwacji obiektu z zewnątrz nie jest w stanie wykryć istnienia systemu ochrony obwodowej i zawczasu przygotować planu ataku. Dodatkowo zainstalowany pod ziemią system jest odporny na przypadkowe uszkodzenia, bezpośredni wpływ warunków atmosferycznych (np. szybkich zmian temperatury), a także nie szpeci architektury chronionego obiektu.

Kable sensoryczne znajdują zastosowanie w konfiguracjach rozpoczynających się od pojedynczych odcinków (np. monitorowanie drogi dojazdowej i sygnalizowanie zbliżających się pojazdów i ludzi), przez niewielkie obiekty (np. posesje prywatne, ośrodki wypoczynkowe, obiekty magazynowe, zakłady karne), aż do rozległych obszarów wymagających wielokilometrowych pasów ochronnych (zakłady przemysłowe, pasy graniczne). Możliwe są dwa podstawowe warianty dozoru:

- dozór obszaru zamkniętego, gdzie kabel ułożony jest np. wzdłuż płotu chronionego obiektu w kształcie zamkniętej pętli (co pozwala m.in. na dwukierunkowe zasilanie i komunikację);
- dozór odcinka, gdzie początek pierwszego i koniec ostatniego odcinka nie łączą się ze sobą pozwalając na monitoring np. pasów granicznych.

Zasada działania systemu w obu przypadkach jest identyczna. Informacje dotyczące stanów alarmowych z poszczególnych odcinków dozoru zbierane są przez komputer PC z zainstalowanym odpowiednim oprogramowaniem. Na ekranie monitora istnieje możliwość obserwacji mapy synoptycznej chronionego terenu z zobrazowanym stanem poszczególnych odcinków. System posiada regulację czułości pozwalającą wyeliminować sygnały powodowane np. przez zwierzęta. Przeciwwskazaniem dla systemu opartego na kablu sensorycznym jest przejazd ciężkiego sprzętu np.; ciężarówki, sprzęt budowlany itp. Kabel, stosowany, jako czujnik, jest bardzo wrażliwy na drgania i nacisk. Można go umieszczać prawie wszędzie, a jedynym ograniczeniem w stosowaniu, ze względu na konieczność płytkiego umieszczenia w ziemi, są miejsca przejazdu ciężkich pojazdów. Pod powierzchniami utwardzonymi konieczne jest, w celu zachowania czułości, zwielokrotnienie ułożenia kabla.

System światłowodowy

Bardziej zaawansowanym technologicznie rozwiązaniem jest system wykorzystujący, jako sensor kabel światłowodowy. W działaniu oraz sposobach wykorzystywania podobny jest do systemu z kablem sensorowym. Światłowody mogą być układane w ziemi, bezpośrednio na chronionym podłożu lub na specjalnej siatce zwiększającej szerokość strefy wykrywania.

Światłowody znalazły szerokie zastosowanie w ochronnych systemach podłożowych, ponieważ reagują na nacisk wywierany na ich zewnętrzną powłokę ochronną. Ułożony w ziemi, na głębokości kilku centymetrów, kabel światłowodowy doskonale reaguje na nacisk powodowany przez przechodzącego człowieka. W skutek spoistości gleby nacisk ten jest wykrywany nawet w odległości kilkunastu centymetrów od kabla, dzięki czemu nie ma konieczności układania go zbyt gęsto.

Centrala systemu transmituje przez włókno światłowodu promień światła laserowego. Wibracja lub nacisk, spowodowany ruchem intruza, powoduje przesunięcia w odebranym świetle na końcu światłowodu, w stosunku do wzorca promienia laserowego. Jeżeli zmiany parametrów transmisji przekroczą wartości progowe, zaprogramowane, jako kryteria alarmu, zostanie wygenerowany sygnał alarmu. Zastosowanie analizy spektralnej lub interferometrycznej odbieranego sygnału daje możliwość regulacji czułości detekcji, przez co uzyskuje się mniejszą podatność na zakłócenia i eliminuje fałszywe alarmy. Podkreślić należy bardzo prostą konfigurację, łatwość instalacji oraz bardzo wysoką skuteczność ochronną i odporność na próby oszukania systemu. Może być on stosowany wszędzie, gdzie wymagane jest wykrycie niepożądanej obecności.

Zakopany w ziemi kabel światłowodowy wykrywa ruch i jest całkowicie odporny na wszelkie zakłócenia elektromagnetyczne, świetlne, radiowe itd. Ponieważ światłowód nie przewodzi sygnału elektrycznego, można go bezpiecznie mocować w pobliżu linii energetycznych, systemów radarowych, a jego odporność

chemiczna predysponuje go również do zastosowań w środowisku agresywnym chemicznie i zagrożonym wybuchem.

Powyższe cechy tworzą z niego efektywny system wykrywania naruszeń stref chronionych, najczęściej zaskakując potencjalnego intruza, gdyż zamaskowany kabel światłowodowy nie jest możliwy do wykrycia za pomocą obecnie istniejących przyrządów. Jedyną niedogodnością jest warunek mówiący, iż miejsca utwardzenia terenu należy planować wraz z systemem.

Systemy wykorzystujące światłowód detekcyjny mogą być montowane w postaci modułów składających się z mat zakopywanych w ziemi. Maty ze światłowodem można założyć pod piaskiem, żwirem lub pod nawierzchnią brukowaną. W momencie, kiedy intruz nadepnie na taką matę, nastąpi ugięcie kabla, przy jednoczesnej zmianie intensywności przesyłanego światła. Zmiana ta jest rozpoznawana przez moduł detekcyjny, który jest sercem całego systemu. Moduł porównuje strumień światła z wyjścia przewodu detekcyjnego z poziomem sygnału, który jest wprowadzany do wejścia przewodu detekcyjnego. Zmiana natężenia światła powoduje zadziałanie przekaźnika, a tym samym alarm. Oczywiście przewód detekcyjny musi być odpowiednio zabezpieczony. W tym celu stosuje się gumowe osłony, które chronią przewód przed mechanicznym uszkodzeniem.

System impedancyjny

Kablowy system impedancyjny, zwany inaczej systemem pojemnościowym wykrywa zbliżanie się intruza do rozłożonych kabli dzięki pomiarowi i analizie impedancji. Kable, między którymi powstaje strefa wykrywania, umieszczane są płytko pod ziemią. Mogą być przykryte asfaltem lub betonem. Długość kabli w jednym sektorze chronionym, w zależności od producenta systemu, może wynosić do 100 m lub nawet do 300 m. Zasilanie kabli i pełna kontrola zmian impedancji dokonywane są przez komputer PC ze specjalistycznym oprogramowaniem, które pozwala na identyfikację miejsca przejścia intruza i zobrazowanie tego na mapie synoptycznej. System jest szczególnie polecany tam, gdzie duże powierzchnie terenu chronionego muszą być utwardzone. Stopień skuteczności systemu impedancyjnego nie zależy od rodzaju nawierzchni, pod którą są umieszczone kable (trawa, beton, klinkier, asfalt itp.).

Przykład połączenia systemu doziemnego z systemami obserwacji przestrzennej

W przypadku konieczności kompleksowego monitorowania obszarów, odosobnionych obiektów np. infrastruktury krytycznej, obiektów wojskowych, ale w szczególności do wykorzystania przez Straż Graniczną do ochrony granic, zachodzi potrzeba zastosowania kilku różnych systemów ochrony obwodowej, które będą się wzajemnie uzupełniały gwarantując niezawodną ochronę. Takim rozwiązaniem jest, stworzona prze jednego z producentów, kombinacja sieci rozproszonych, inteligentnych sensorów sejsmicznych zdolnych do wykrywania osób i pojazdów oraz sensorów obrazowych (zestaw kamera dzienno-nocna i termalna) powiązanych systemem kratowej łączności lokalnej typu MESH[1]. Każdy sensor pracuje niezależnie od pozostałych, posiada własne źródło zasilania, odbiornik GPS i moduły łączności radiowej. Możliwości sensorów wsparte systemami łączności lokalnej (między sensorami sejsmicznymi i obrazowymi) i odległej (miedzy sensorami obrazowymi i stanowiskiem operatora systemu) zapewniają operatorowi systemu w centrum zarządzania pełną informację o zdarzeniach w monitorowanym obszarze/obiekcie. Pozwala to na podjęcie stosownej, przewidzianej na okoliczność ochrony przed intruzami akcję. Np. w przypadku Straży Granicznej można we właściwe miejsce skierować wieżowe systemy rozpoznania, wysłać patrol interwencyjny lub rozpoznawczy czy bezzałogowy aparat latający.

Tego typu rozwiązania ochrony perymetrycznej charakteryzują się takimi cechami, jak: otwartą architekturą systemu, dużą mobilnością użytkową, niskim współczynnikiem niepożądanych alarmów, możliwością konfiguracji ad hoc, którą łatwo można dostosować do właściwości terenu i chronionych obiektów. Ze względu na brak możliwości bieżącego kontrolowania sensorów doziemnych, rozmieszczonych zwykle na dużym obszarze, sensory systemu wyposażone są często w czujniki zmiany położenia. Stąd jakakolwiek zmiana pozycji urządzeń po instalacji w terenie skutkuje wysłaniem do operatora systemu sygnału sabotaż.

Fot. 5. Czujnik sejsmiczny
Źródło: ATLine. Nowoczesne systemy alarmowe

Wykorzystano m.in.:
1. W. Szulc, A. Rosiński, Wybrane możliwości detekcyjne czujek wibracyjnych i sejsmicznych stosowanych w SSWiN, Logistyka nr 6/2015
2. https://www.weber-systems.pl/show.php/2/1/11/8
3. D. Żabicki, Czujki dedykowane do ochrony obwodowej, D. Żabicki, Czujki dedykowane do ochrony obwodowej, Ochrona Mienia i Informacji
4. Systemy ochrony zewnętrznej, https://www.alkam-security.pl/systemy-ochrony-zewnetrznej/
5. Zakopywane systemy ochrony obwodowej, http://atline.pl/oferta/sisma-ca-1/
6. Zabetonowane systemy alarmowe, http://atline.pl/kategorie-oferta/zabetonowane-systemy-ochrony/

Redakcja

[1] radiowe sieci lokalne o strukturze kratowej (*mesh network*), w których poszczególne urządzenia radiowe mogą retransmitować dane przesyłane przez inne urządzenia radiowe sieci.

OCHRONA I OBRONA BAZ I OBIEKTÓW WOJSKOWYCH

Ochrona i obrona baz i obiektów wojskowych w RP

Obiekt wojskowy to element infrastruktury obronnej obejmujący wszystkie stacjonarne (a w wyjątkowych wypadkach także ruchome) obiekty i urządzenia, które zgodnie ze swym przeznaczeniem służą do zaspokajania potrzeb sił zbrojnych, a w szczególności dowodzenia, bytowania, szkolenia i przemieszczania wojsk. Tych obiektów w Polsce jest ponad tysiąc, w tym ochranianych – 350 i zalicza się do nich również bazy wojskowe.

Podstawową formą ochrony obiektów użytkowanych przez Siły Zbrojne RP jest bezpośrednia ochrona fizyczna. Powinna ona stanowić pewien spójny i w pełni zdolny do reakcji system, gotowy do realizacji wielu zadań w ekstremalnych warunkach, także w trybie alarmowym. W skład tych sił wchodzą wszystkie siły ochronne jednostki wojskowej lub kilku jednostek, jeżeli stacjonują w kompleksie (garnizonie) służby dyżurne oraz warty: warty wojskowe, warty OWC oraz warty wystawiane poprzez SUFO. Specjalistyczne Uzbrojone Formacje Ochrony (SUFO) – chronią 52,5% obiektów wojskowych, Oddziały Wart Cywilnych (OWC) – 44,5%, oraz przez żołnierzy – ok. 3%.

Służbę wartowniczą i ochronną organizuje się w oparciu o system posterunków i patroli. Ze względu na sposób pełnienia służby na posterunkach rozróżnia się następujące posterunki stałe i posterunki ruchome. W zależności od miejsca pełnienia służby na posterunkach rozróżnia się posterunki zewnętrzne i wewnętrzne, natomiast ze względu na czas pełnienia służby posterunki dzieli się na dwuzmienne, trzyzmienne i doraźne[1].

Pod względem prawnym kwestia ochrony fizycznej wojsk została uregulowana (teoretycznie) również w odniesieniu do hipotetycznego okresu zagrożenia wojennego i wojny: obiekty wojskowe w czasie pokoju są chronione przez SUFO i OWC, a po ogłoszeniu mobilizacji, wprowadzeniu stanu wojennego lub w czasie wojny – SUFO są militaryzowane i nadal wykonują zadania ochrony, można też zmilitaryzować inne specjalistyczne uzbrojone formacje ochronne przedsiębiorców. Od OWC ochronę przejmują wojskowe pododdziały ochrony i obrony obiektów. Natomiast obiekty kategorii I są szczególnie ochraniane w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa oraz w czasie wojny przez jednostki zmilitaryzowane specjalnie tworzone w tym celu na podstawie odrębnych przepisów (par. 5.5 rozporządzenia)[2]. Szczególna ochrona obiektów jest przygotowywana i prowadzona z udziałem Sił Zbrojnych RP, policji, PSP oraz formacji obrony cywilnej, z zastrzeżeniem par. 4 ust. 3 pkt 8, par. 7 ust. 2 pkt 5 i ust. 3 pkt 4 (par. 5.6 rozporządzenia)[3].

W hipotetycznej operacji militarnej na terenie kraju wystąpi wiele obiektów stacjonarnych o znaczeniu taktycznym i operacyjnym. Będą to obiekty rozlokowane czasowo, jak np. bazy logistyczne, a także obiekty stałe, np. składy, magazyny, zakłady zbrojeniowe, infrastruktura komunikacyjna, energetyczna i inne.

Zapewnienie odpowiedniego poziomu bezpieczeństwa tych obiektów będzie istotnym elementem operacji obronnej. Przestrzenny charakter przyszłych działań zbrojnych poszerza zakres działań ochronno-obronnych, które nie będą jedynie działaniami przeciw-dywersyjnymi. Obiekty ważne z punktu widzenia obronności mogą być również celem działania oddziałów wydzielonych przeciwnika, desantów powietrznych, grup rajdowych, czy nawet grup uzbrojonych, dążących do ich przejęcia w stanie nienaruszonym. Wymusza to potrzebę organizowania ochrony i obrony obiektów, jako systemu działań i traktowania ich, jako zespołu wzajemnie uzupełniających się przedsięwzięć, takich jak rozbudowa fortyfikacyjna, działanie na przedpolach, czy działania manewrowe. Przewaga poszczególnych elementów tego systemu będzie zależeć w głównej mierze od rodzaju obiektu, poziomu zagrożenia oraz sił i środków przewidzianych do jego ochrony lub obrony.

Siły wyznaczone do obrony takich obiektów będą pochodzić z wojsk operacyjnych, obrony terytorialnej oraz pozamilitarnych ogniw obronnych, np. straży przemysłowych i obiektowych czy policji. Jednak główny ciężar działań w tym zakresie powinny wziąć na siebie pododdziały ochrony i obrony obiektów, takie

Fot. 1. Fragment bazy lotniczej
Źródło: Panic PL

[1] Dz.U.2007.126.876 ROZPORZĄDZENIE MINISTRA OBRONY NARODOWEJ z dnia 21 czerwca 2007 r. w sprawie szczegółowych zadań pełnomocników ochrony oraz szczególnych wymagań w zakresie ochrony fizycznej jednostek organizacyjnych podległych MON lub przez niego nadzorowanych, § 7. 1

[2] Wytyczne ministra obrony narodowej z 20 grudnia 2004 r. w sprawie ogólnych wymagań przygotowania i prowadzenia szczególnej ochrony obiektów kategorii I. Wyd. drugie. Szt. OT Wewn. 1/2005, s. 7.

[3] Ibidem

jak batalion ochrony i obrony obiektów (booo).

Gwoli uczciwości warto zauważyć, że wśród specjalistów z branży ochrony, a także wśród samych wojskowych trwają dyskusje, co do skuteczności rozwiązań przyjętych w zakresie obrony i ochrony obiektów wojskowych, i to zarówno w warunkach pokojowych, jak i w czasie ewentualnego konfliktu zbrojnego (patrz. [4]).

Ochrona fizyczna jednostki organizacyjnej, w zależności od jej kategorii i charakteru, powinna być uzupełniona technicznymi środkami wspomagającymi ochronę, do których zalicza się: systemy i urządzenia alarmowe, systemy sygnalizacji włamania i napadu (SSWiN) — zewnętrzne i wewnętrzne, systemy telewizji przemysłowej (CCTV) — zewnętrzne i wewnętrzne, systemy kontroli dostępu (SKD), łączność wartowniczą i służb dyżurnych (przewodową, radiową lub radiotelefoniczną) itp.[5] Systemy alarmowe zastosowane w ochronie obiektów powinny posiadać deklarację zgodności ich wykonania w odpowiedniej klasie, natomiast urządzenia wykorzystane do ich budowy — odpowiednie certyfikaty lub świadectwa kwalifikacyjne. Systemy i urządzenia powinny spełniać parametry określone w normie obronnej NO-04-A004 — „Obiekty wojskowe. Systemy alarmowe."

Ochrona baz w misjach pokojowych i stabilizacyjnych.

Podczas prowadzenia stabilizacyjnych i pokojowych misji wojskowych, siły zbrojne muszą zapewnić ochronę i obronę swoich czasowych lub stałych baz wojskowych. W dzisiejszych konfliktach asymetrycznych, szczególnie w rejonach zurbanizowanych, potencjalne zagrożenie dla takich baz może czaić się wszędzie. Ataki na bazy prowadzące do ranienia i śmierci żołnierzy lub personelu cywilnego powodują obniżenie ich morale i prowadzą do obniżenia poziomu realizowanych zadań. Dlatego pewna i skuteczna ochrona baz jest zadaniem o charakterze egzystencjalnym.

Z raportu opracowanego na polecenie Sekretarza Generalnego ONZ wynika, że

Fot. 2. Baza sił pokojowych
Źródło: schmittys-life.de

od 1948 służąc pod flagą ONZ, w wyniku różnego rodzaju 943 aktów agresji, straciło życie ponad 3500 żołnierzy i cywilów. Tylko w ciągu ostatnich lat, od 2013 do 2017 roku zginęło 195 osób, w znacznej części przypadków w wyniku na ataków na bazy i obozy misji oenzetowskich.

Dlatego wg zaleceń ONZ baza musi być chroniona z wykorzystaniem możliwie najlepszych środków ochrony fizycznej i technicznej. Poza tym kierownictwo organizacji wychodzi z założenia, że bezpieczeństwo bazy nie może być zabezpieczone bez działań aktywnych. Sama baza powinna być swego rodzaju *centrum bezpieczeństwa.* Natomiast wokół bazy rozciągać powinna się jasno określona *strefa bezpieczeństwa* obejmująca kilka kilometrów dróg, wiosek i obozów IDP[6], których ludność powinna wiedzieć, że znajdują się w strefie, w której obowiązuje „zero tolerancji", jeżeli chodzi o obecność uzbrojonych osób lub grup. Żołnierze ONZ powinni używać wszystkich dostępnych środków taktycznych w celu uzyskania pełnej dominacji na tym obszarze, a w tym m.in.: nocne operacje bojowe, piesze patrole, zajęcie stacjonarnych (ukrytych/rozproszonych) pozycji w ciągu dnia i nocy w celu uniemożliwienia przemieszczania w rejonie chronionym bazy grup przestępczych, ekstremistycznych lub terrorystycznych.

W praktyce, oprócz zagrożeń, polegających na wtargnięciu na teren bazy intruzów, zorganizowanych grup przestępców lub terrorystów, bardzo często bazy misji pokojowych lub stabilizacyjnych podlegają ostrzałowi artyleryjskiemu, rakietowemu lub z broni strzeleckiej. Tego typu atakom można przeciwdziałać przede wszystkim poprzez wcześniejsze rozpoznanie planów potencjalnego przeciwnika (operacje wywiadowcze). Bardzo pomocne są nowe rozwiązania technologiczne. Jednym z nich są akustyczne detektory wystrzałów.

Akustyczne detektory wystrzałów zaprojektowane zostały początkowo, jako wyposażenie dodatkowe dla lepszej ochrony wojsk, przez działanie, jako swego rodzaju Combat Multiplier[7], dzięki któremu możliwe jest utrzymanie taktycznej przewagi nad przeciwnikiem i zachowanie życia własnych żołnierzy. Detektory tego typu pozwalają na zarejestrowanie i wykrycie wystrzału, ale również na lokalizację miejsca, z którego padł. System akustycznej detekcji wystrzałów składa się z wielu macierzy akustycznych, rozmieszczonych na obszarze wokół bazy, wykrywających fale dźwiękowe generowane po wystrzale z broni strzeleckiej, odpaleniu pocisków rakietowych (RPG) i pocisków moździerzowych i pozwala na

[4] R. Radziejewski, Ochrona obiektów wojskowych w świetle uregulowań prawnych, Kwartalnik Bellona, nr 4/2012

[5] Dz.U.2007.126.876 ROZPORZĄDZENIE MINISTRA OBRONY NARODOWEJ z dnia 21 czerwca 2007 r. w sprawie szczegółowych zadań pełnomocników ochrony oraz szczególnych wymagań w zakresie ochrony fizycznej jednostek organizacyjnych podległych MON lub przez niego nadzorowanych, § 8. 1

[6] IDP – Internally Displaced Person czyli osoba wewnętrznie przesiedlona w ramach własnego kraju, przesiedleńca.

[7] force multiplication lub force/combat multiplier – w naukach wojskowych zwielokrotnianie siły lub mnożnik siły odnosi się do czynnika lub kombinacji czynników, które dają danemu ugrupowaniu wojskowemu lub konkretnemu rodzajowi uzbrojenia (lub innemu rodzajowi sprzętu) zdolność do osiągnięcia większych możliwości bojowych, niż bez niego. Konieczne zwiększenie zdolności bojowych wymagane do uzyskania takiej samej efektywności działań bez stosowania tego czynnika, nazywany jest współczynnikiem mnożenia/zwielokrotnienia. Na przykład, jeśli pewna technologia, taka jak GPS, umożliwia osiągnięcie takich samych rezultatów bojowych, przy siłach pięciokrotnie mniejszych niż, bez stosowania tej technologii, to mnożnik wynosi pięć. Takie oszacowania są wykorzystywane do uzasadnienia kosztów inwestycji w technologię rozumianą, jak mnożnik zdolności bojowych.

wykrywanie, dokładną identyfikację i lokalizację miejsca wystrzału w czasie rzeczywistym. Systemy detekcji akustycznej wystrzałów umożliwiają również zobrazowanie zarejestrowanej sytuacji ogniowej wokół ochranianego obiektu. Pozwala to na ochronę personelu ochranianego obiektu i przeprowadzenie natychmiastowej odpowiedzi ogniowej.

Akustyczne detektory wystrzałów, ze względu na wykrywanie dźwięków o różnym charakterze mogą z powodzeniem być wykorzystywane w misjach pokojowych. Rozlokowane wokół baz, obozów uchodźców ochranianych przez siły ONZ lub wzdłuż linii rozgraniczenia wrogich sił mogą stanowić dobrą ochronę personelu wojskowego i cywilnego bazy lub osób zgromadzonych w obozie. Mogą również dostarczyć dowodów naruszenia reżimu przerwania ognia przez skonfliktowane strony.

Dla przykładu, w ciągi 30 godzin pracy, w rejonie posterunku sił ONZ, SIERRA-SIERRA, położonym w górach wokół Sarajewa w Bośni, system akustycznej detekcji wystrzałów wykrył i zarejestrował 92 wystrzały. Ustalono, że 56% z nich pochodziło ze strony serbskiej, a 44% ze strony bośniackiej. Informacje te zostały wykorzystane w negocjacjach między walczącymi stronami, celem przerwania aktywności ogniowej na tym obszarze.

Inteligentne bazy.

Przeznaczenie baz wojskowych i realizacja przez nie określonych zadań, ulega w ostatnim czasie poważnym zmianom. W przeszłości bazy stanowiły punkt wyjściowy do przeprowadzania operacji wojskowych, czy to stabilizacyjno-pokojowych, czy też bojowych, służąc przede wszystkim, jako tzw. „safe havens – bezpieczne przystanie" przed zagrożeniami, stanowiąc jednocześnie ochronę zagrożonego terytorium. Jednak obecnie rola tych baz znacznie wzrosła i stanowią one dzisiaj część wielopłaszczyznowej przestrzeni zmagań wojennych, zarówno tych fizycznych, jak i toczonych w cyberprzestrzeni. Nowe zadania wiążą się przede wszystkim z zaawansowanymi technologiami cyfrowymi i związane są z nowoczesnymi operacjami wojskowymi, takimi jak: zaopatrzenie sił mobilnych, naprawa krytycznych elementów uzbrojenia (zanim te ulegną ostatecznemu zniszczeniu), przetwarzanie ogromnej ilości danych, ich analiza i zobrazowanie w jednym miejscu, itp. Bazy wojskowe stanowią istotny element działań wojsk, szczególnie w operacjach zagranicznych. Istotnym elementem zwiększającym ich bezpieczeństwo, możliwości operacyjne i oszczędności finansowe związane z ich działaniami, są technologie sztucznej inteligencji, które jako pierwsze są na razie stopniowo wprowadzane w bazach NATO i USA. Po pierwszych doświadczeniach widać, że *inteligentne bazy* są kluczem do jutrzejszych działań operacyjnych sił zbrojnych.

Specjaliści doszli do wniosku, że obsługa i ochrona baz wojskowych, które faktycznie są szczególnego rodzaju miastami, może być realizowana z wykorzystaniem zaawansowanych platform cyfrowych, które coraz powszechniej wprowadzane są w tzw. *inteligentnych miastach (smart city)*. I faktycznie *inteligentne miasta*, w których w ciągu ostatnich 10 lat, planiści miejscy wdrożyli szereg nowych technologii (różnego rodzaju sensory, inteligentny monitoring, analiza danych i aplikacje na smartfony itp.), posłużyły, jako swego rodzaju modelowy wzorzec dla stworzenia *inteligentnych baz* wojskowych.

Tworzone w ten sposób *„inteligentne bazy"*, mogą gwarantować sobie niezawodność funkcjonowania i skuteczną ochronę, na znacznie wyższym niż dotąd poziomie, co z pewnością przełożyłoby się na większą skuteczność wykonania zadań w ramach misji wojskowych.

W istocie *inteligentna baza*, to integracja innowacji technologicznych i procesowych, które poprawiają wydajność, efektywność i wygodę w zarządzaniu zasobami i działaniami tej instalacji wojskowej, a także w zarządzaniu jej kompleksową obroną i ochroną. Innymi słowy, *inteligentna baza* integruje inteligentne technologie i praktyki w zakresie nowoczesnych rozwiązań energetycznych, mobilnych, budowlanych i naprawczych, a także obronę fizyczną bazy z ochroną techniczną, wykorzystując najnowsze rozwiązania z dziedziny technicznych środków bezpieczeństwa.

Inteligentne technologie pozwalają na ich zastosowanie zarówno w niewielkich obozach wojskowych, jak i w dużych bazach przeznaczonych dla kilku tysięcy personelu wojskowego, dużej ilości sprzętu i uzbrojenia. Pozwalają również na ich adaptację do specyfiki misji wojskowej, dopasowane do konkretnej bazy, a adresowane są do czterech następujących filarów jej działalności:

- Transport i logistyka – *inteligentna baza* przekształca sposób, w jaki przemieszczamy ludzi i towary, od systemu transportu wewnątrz i na zewnątrz bazy do łańcucha dostaw;
- Zdrowie i kondycja – nowe technologie w rewolucyjny sposób poprawiają warunki życia i pracy w bazie wojskowej;
- Technika i obiekty bazy – *inteligentna baza* w optymalny sposób zarządza energią, wodą, środowiskiem i obiektami budowlanymi na swoim terenie, a także zapewnia pełny serwis instalacji wojskowych:
- Bezpieczeństwo i rozpoznanie wojskowe (wywiad) – *inteligentna baza* dysponuje rozwiniętą siecią różnego rodzaju czujników (sensorów), dzięki czemu jej system ochrony i obrony można nazwać aktywnym, reaktywnym (wobec najmniejszych zagrożeń)

Fot. 3. Amerykańska baza morska w Keflavik (Islandia)
Źródło: Pinterest

Fot. 4. Żołnierz ONZ na posterunku
Źródło: TVP Tygodnik

i dostosowanym do zagrożeń, z jakimi może spotkać się personel bazy.

Stosowanie inteligentnych technologii w bazach wojskowych jest więcej niż hipotetyczne. Niektóre amerykańskie bazy za granicą niedawno otworzyły inteligentne elektrownie słoneczne, które pozwalają im działać niezależnie od lokalnej sieci elektroenergetycznej, co jest krytyczną możliwością w sytuacji awaryjnej. Inne eksperymentują z pojazdami bez kierowcy, aby przetransportować rannych żołnierzy przez teren bazy do punktów medycznych.

Bazy wojskowe w strefach konfliktu, zlokalizowane często w sąsiedztwie wiosek lub małych miast, często narażone są na niespodziewane ataki terrorystyczne, szczególnie w godzinach nocnych. Dlatego bazy chronione są nie tylko przez żołnierzy, ale przez cały zestaw technicznych środków ochrony, takich jak: CCTV, radary, urządzenia elektro-optyczne, termowizyjne itp. Czujniki sejsmiczne stosowane, jako część tej kompleksowej ochrony obiektu, monitorują tzw. martwe punkty oraz zapewniają skrytą i zamaskowaną ochronę dróg podejścia, sygnalizując zbliżającego się do bazy intruza, na podstawie drgań spowodowanych jego krokami. W przypadku, kiedy intruz przedostał się na teren bazy, stwarzając zagrożenie dla jej personelu, połączone w sieć inteligentne kamery wyodrębniłyby nieproszonego gościa. W najgorszym przypadku inteligentna baza mogłaby odizolować odgłosy strzałów i przekazać informacje o ich lokalizacji służbom dyżurnym w bazie. Alert może zostać wysłany do smartfonów wszystkich osób, powiadamiając ich o aktywnej strzelaninie, wskazując obszary, których należy unikać. Funkcjonariusze bazy będą mogli natychmiast zablokować wrażliwe miejsca (stanowiska dowodzenia, szpitale itp.). Stosowane są rozwiązania, które ponadto wyłączają systemy obwodowej ochrony sejsmicznej w ciągu dnia, ograniczając liczbę fałszywych alarmów, a uruchamiają w warunkach nocnych, kiedy personel bazy śpi.

Oprócz bezpieczeństwa i oszczędności technologia może poprawić życie w bazie:

- Czujniki, które potrafią odróżnić pracowników bazy od tymczasowego personelu i odwiedzających, mogą pomóc w zarządzaniu zatorami podczas porannych godzin szczytu lub dużych imprez publicznych, takich jak pokazy lotnicze;
- Technologia wytwarzania przyrostowego, pozwala bazom używać druku 3D w celu szybszej i tańszej naprawy i wymiany części, które mogą być produkowane na miejscu;
- Czujniki w pojemnikach na śmieci i na półkach sklepów spożywczych w bazie mogą pomóc personelowi zajmującemu się zarządzaniem odpadami w zarządzaniu zbiorami i automatyzować zamówienia zapasów sklepowych;
- Innowacyjne technologie budowy i planowania urbanistycznego mogą pomóc bazom zaprojektować zabudowę obszarów o różnym przeznaczeniu, a także uniknąć kosztów środowiskowych poprzez identyfikację miejsc, których nie można zmienić.

Chociaż technologia sprawia, że bazy wojskowe stają się bardziej wydajne pod względem ekonomicznym czy bezpieczniejsze ze względu na zastosowane środki techniczne, to jednak stosowanie tych wszystkich inteligentnych urządzeń niesie ze sobą określone ryzyko. W *inteligentnych miastach* były już przypadki, że hakerzy zainfekowali inteligentne urządzenia wirusami; przejęli systemy zamków hotelowych za pomocą oprogramowania ransomware[8] i zastosowali wobec urządzeń wykorzystujących Internet rzeczy (IoT), ataki typu DDoS[9].

W zastosowaniach militarnych, wprowadzenie dużej liczby bezprzewodowych czujników i połączenie ich z najważniejszymi, wrażliwymi częściami składowymi dużej instalacji wojskowej, może wydawać się być sprzeczne z obowiązującymi w siłach zbrojnych, zasadami bezpieczeństwa. Wątpliwości mogą być podnoszone zwłaszcza przez dowódców wojskowych, którzy z względów oczywistych stawiają bezpieczeństwo ponad wygodą i oszczędnościami.

Jednak luki w zabezpieczeniach systemowych można łatwo zmniejszyć, zmieniając domyślne hasła i szyfrując strumienie danych. Wymogi dot. bezpieczeństwa informacyjnego będą oczywiście wymagać czegoś więcej niż dobrych praktyk i haseł. Konieczne będzie rygorystyczne testowanie nowych urządzeń, zanim będą mogły zostać użyte. Ale to nie powinno być przeszkodą dla ich wdrożenia. Modernizacja i aktualizacja starzejących się instalacji baz wojskowych za pomocą inteligentnych technologii w celu lepszej ochrony żołnierzy i członków ich rodzin, jest tego warta.

Wykorzystano m.in.:
1. R. Radziejewski, Ochrona obiektów wojskowych w świetle uregulowań prawnych, Kwartalnik Bellona, nr 4/2012
2. https://peacekeeping.un.org/sites/default/files/improving_security_of_united_nations_peacekeepers_report.pdf
3. Łada, Specyfika ochrony fizycznej obiektów wojskowych, Studia Kaliskie, http://www.pwsz.kalisz.pl/wp-content/uploads/2015/02/studia-tom-5-norm.pdf
4. https://militarium.net/ochrona-i-obrona-obiektow-w-warunkach-konfliktu-militarnego/
5. Smart military bases, https://www2.deloitte.com/us/en/pages/public-sector/articles/byting-the-bullet-smart-military-bases.html

Krzysztof Surdyk
Redaktor naczelny

[8] Ransomware (inne określenie: oprogramowanie szantażujące; ang. ransomware – zbitka słów ransom „okup" i software „oprogramowanie") – typ szkodliwego oprogramowania z dziedziny kryptowirologii, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych (często poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego.

[9] DDoS (ang. *distributed denial of service*, rozproszona odmowa usługi) – atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów (np. zombie).

NOWE ROZWIĄZANIA W DZIEDZINIE ZASILACZY UPS

IMPAKT S.A. jest jedną z czołowych polskich firm zajmujących się dystrybucją w segmencie akcesoriów i podzespołów komputerowych, akcesoriów dla graczy, rozwiązań sieciowych oraz szeroko pojętej elektroniki użytkowej. Tę Grupę Kapitałową cechuje przede wszystkim dynamika rozwoju, dążenie do innowacyjnych i nieszablonowych rozwiązań oraz kreowanie wysokich standardów jakości usług, które oferuje. Hasło firmy „*Idziemy w tym samym kierunku*", które należy rozumieć – „uważamy naszych klientów za profesjonalistów potrafiących wybrać to, co dla nich najlepsze" oznacza, że Grupa oferuje produkty tylko uznanych producentów, którzy zasłużyli na miano leaderów w swojej branży. I tak właśnie jest z zasilaczami niemieckiej firmy BlueWalker Gmb założonej w 2004 w Neuss. Jako doświadczony i profesjonalny dostawca UPSów, regulatorów napięcia i inwerterów marki PowerWalker, firma oferuje dystrybucję tych produktów w całej Europie, a w Polsce korzysta z potencjału dystrybucyjnego Grupy Impakt. Portfolio produktów sięga 300 modeli, od urządzeń domowych, poprzez biurowe i serwerowe aż do rozwiązań przemysłowych. Szeroka gama akcesoriów, dodatków i modułów baterii pozwala na zastosowanie produktów w wielu sytuacjach. Urządzenia zasilające PowerWalker przechodzą dokładny, czterostopniowy proces kontroli jakości w fazie produkcji podzespołów, montażu, akceptacji produktu i przed wprowadzeniem na rynek. Dzięki temu oferuje na rynek produkty wysokiej jakości, z najlepszym współczynnikiem *cena/jakość*.

W ofercie tego producenta można znaleźć ekonomiczne UPSy offline z serii FVD, rozwiązania Line-Interactive z serii VI, VI LCD, VI RT LCD, a także zaawansowane UPSy On-Line VFI RM LCD, o mocy pozornej do 10000 VA. Ponadto PowerWalker oferuje rozwiązania w zakresie modułów bateryjnych do UPSów, kart SNMP, systemów redundantnego zasilania oraz innych akcesoriów. Wszystkie desktopowe UPSy Line Interactive, oprócz gniazd komputerowych IEC C13, posiadają standardowe gniazdka 230V obowiązujące w Polsce. W tej publikacji chcielibyśmy przedstawić państwu trzy ciekawe pod względem technologicznym najnowsze zasilacze awaryjne UPS, PowerWalker.

Fot. 1. Zasilanie kamery PoE za pomocą UPS PowerWalker Smart

Zasilacz UPS Smart PoE

Problemy z łącznością w dedykowanych systemach bezpieczeństwa i nadzoru, mogą być spowodowane nie tylko przypadkowymi zdarzeniami (takimi jak przerwy w dostawie prądu lub problemy z siecią), ale także celowymi i złośliwymi atakami. Zasilacz UPS PowerWalker Smart PoE, to kompaktowe urządzenie zaprojektowane specjalnie w celu zabezpieczenia kamer PoE przed utratą połączenia. Jest zasilany i ładowany z pojedynczej linii PoE (dane + zasilanie), umożliwiając jego instalację tuż obok kamery.

Dzięki zasilaczowi PowerWalker Smart PoE, w zasadzie każda kamera PoE o określonej pojemności pamięci przekształcana jest w sieć bezpieczeństwa z własnym systemem backup-u. Z nieoficjalnych informacji wynika, że zasilacze tej serii zostaną wykorzystane do zasilania kamer, na ciągle budowanym lotnisku w Berlinie, gdzie nie może zdarzyć się żadna przerwa

Zasilacz UPS PowerWalker Smart PoE	
Internet	10M/100M
Nap. wyj. przy pracy nominalnej	37-57 VDC (PoEStandard)
Nap. wyj. przy zasilaniu rezerwowym (backup)	48VDC +/–1%
Moc wyjściowa	15.4W max
Dopuszczalne napięcie wejściowe	37–57 VDC
Moc wejściowa	30W Max
Typ akumulatora	Li-ion36.47W h / 14.4V
Czas zasilania rezerwowego	90min @ 15.4W / 180min @ 8W
Czas ładowania akumulatora	7h to 90%
PoE Standard	802.3af / 802.3at
EMC	EN55032 Class B
LI akumulatora	IEC 62619
ME	ISTA 2A and EN60950
Temperatura pracy	0 do 40 stop. C
Temperatura przechowywania	– 20 do 45 stop. C
IP	P 30

w dostawie prądu, bezpieczeństwo jest kwestią priorytetową.

Zasilacz UPS Smart PoE wykonano w Standardzie PoE 802.3af / 802.3at – 48VDC z detekcją obciążenia, posiada wejście na pojedynczy kabel (dane + zasilanie) – odpowiednie do instalacji zdalnych i wysokowydajnych akumulatorów litowych. Posiada również dołączoną płytę ścienną.

Szczegółowe charakterystyki techniczne zasilacza UPS PowerWalker Smart PoE przedstawiono w tabeli poniżej.

Zasilacze UPS PowerWalker VFI 20k CPH	
Typ	Online
Moc	20000VA / 20000 W
Wsp. Mocy Wyjściowej	1.0
Zakres mocy wej.	190–520 VAC (3-phase) @ 50% load; 305–478 VAC (3-phase) @ 100% load
Max THDi	< 5% @ full linear load
PF wej.	>0.99 @ full load
Zakres częstotliwości	40 Hz–70 Hz
Częstotliwość (zakres synchronizowany)	46 Hz–54 Hz or 56 Hz–64 Hz
Nominalna moc wyjściowa	360VAC/380VAC/400VAC/415VAC (3Ph+N)
Czysta sinusoida	Tak
THDv	≤2% Full Linear Load; ≤4% Non-Linear Load
Regulacja napięcia (bat. rodzaj pracy)	±1%
Częstotliwość (bat. rodzaj pracy)	±0,1 Hz
Współczynnik szczytu ładowania	3 : 1
Czas przełączania (AC na akumulator)	0 ms
Czas przełączania (Inwerter na bypass)	0 ms
Wsparcie generatora	Tak
Zewnętrzna bateria akumulatorów	Tak
Ładowarka	4A
Sterowanie wentylatorem	Zawsze wł., aut. sterowanie prędkością
Wskaźniki LCD	Stan UPS, poziom ładowania, poziom akumulatora, napięcie wej./wyj., licznik rozładowania, stan błędów
Akumulatory	Zaprojektowane do pracy z zewn. baterią akumulatorów, akumulatory nie dołączone
Napięcie DC akumulatora	32–40 x 12V
Współczynnik hałasu	< 55dB
Temperatura	0°C – 40°C
Wilgotność	0%–95% RH (nie-skondensowana)

Zasilacz PowerWalker VFI 20k CPH 3/3 i 3/1

Jest to model zasilacza UPS o konstrukcji modułowej, w którym każdy moduł działa, jako autonomiczna jednostka i jednocześnie wspiera każdy podłączony moduł, stanowiąc ich bezpośrednie wsparcie w czasie rzeczywistym, bez żadnej przerwy. Zasilacze te wykorzystywane są wszędzie tam, gdzie niezbędny jest najwyższy poziom bezpieczeństwa energetycznego tj. w serwerowniach, urządzeniach medycznych, serwerach.

PowerWalker VFI CPH 3/3 to trójfazowy UPS online o szerokich możliwościach zastosowania. Dzięki współczynnikowi mocy 1.0 i wysokiej wydajności (> 94%) spełnia on najwyższe wymagania dotyczące zasilania. Został przystosowany do zainstalowania w szafie rack 19 cali (zajmując przestrzeń 3U), ale może również działać, jako samodzielna jednostka wieżowa. Równolegle można go połączyć do 10 jednostek (zasilaczy), czyniąc je w ten sposób prawdziwie modułowym rozwiązaniem. Taka całkowita instalacja (10 modułów) może pokryć zapotrzebowanie mocy do 100 kW.

Fot. 2. Zasilacz UBS model PowerWalker VFI CPH

Po zestawieniu w szafce rack VFI CPH, w postaci połączonych wzajemnie modułów, zasilacz może podjąć natychmiastowe zasilanie rezerwowe, dzięki zastosowaniu specjalnie zaprojektowanego złącza. Oprócz zobrazowania LCD istniejącego na każdym module UPS, może być on nadzorowany przez 10 calowy panel dotykowy, w celu zobrazowania sumarycznej informacji dotyczącej całego systemu. Rozwiązanie VFI CPH pozwala na dzielenie zestawu akumulatorów pomiędzy modułami, a ilość akumulatorów można regulować od 32 do 40 sztuk.

Pojedynczy zasilacz (samodzielna jednostka wieżowa) może być zainstalowany również w szafie rack z dopasowanym zestawem akumulatorów (3U).

Zasilacze UPS PowerWalker VFI 20k CPH mogą pracować samodzielnie lub jako część rozwiązania modułowego, ze względu na fazowość zasilania, są dostępne w wariantach wejście/wyjście – 3/1 lub 3/3, mogą być montowane w 19 calowych szafach rack, ale opcjonalnie mogą być montowane również w specjalnie zaprojektowanych szafach z 10 calowym ekranem dotykowym (do 40KW), skalowalne do 100KW.

Zasilacze serii VFI TGS

Jest to seria dedykowana do wymagających urządzeń gdzie niezbędny jest długi czas podtrzymania napięcia. Standardowy zasilacz UPS działa średnio 5–10 minut; tutaj przy odpowiednim doborze modułów bateryjnych czas pracy na baterii akumulatorów wydłuża się do godziny lub kilku w zależności od konfiguracji. Dużym atutem tego modelu jest 6A ładowarka dzięki czemu czas ładowania zewnętrznych modułów jest znacząco krótszy niż w przypadku standardowych modeli.

Fot. 3. Zasilacz serii VFI TG/TGB/TGS

Zasilacz PowerWalker VFI 1000–10000 TG/TGB/TGS jest profesjonalnym rozwiązaniem przeznaczonym dla biur i domów. Jest dostępny w kilku wersjach:

- TG: z wewnętrznym akumulatorem; zakres mocy 1000–3000 VA,
- TGB: z wewnętrznym akumulatorem i możliwością podłączenia zewnętrznego akumulatora; zakres mocy 1000–10000VA,
- TGS: bez wewnętrznego akumulatora, ale z silną ładowarką i złączem do podłączenia akumulatora; zakres mocy 1000–10000 VA.

Serie VFI TG/TGB/TGS, są wykrywane przez wewnętrzne sterowniki O/S, jako urządzenia HID (Human Interface Device) i mogą być zarządzane bez dodatkowego oprogramowania. Znajdują zastosowanie we wszystkich dedykowanych systemach do kiosków, bankomatów, a także w zastosowaniach wymagających wysokiego poziomu bezpieczeństwa, gdzie dodatkowe oprogramowanie nie jest dozwolone (np. w bankowości).

Zasilacze serii VFI TG/TGB/TGS posiadają 10 calowy zaawansowany ekran kontrolny, współczynnik mocy równy jeden (UPF, KVA = KW), (własna obudowa eliminuje problemy z instalacją), możliwość szybkiej naprawy przez wymianę całych paneli oraz regulowaną ilość akumulatorów dla zwiększenia efektywności – do 40 sztuk

Powyżej przedstawiono tabelę z podstawowymi danymi technicznymi jednego z zasilaczy z ww. serii.

Opracowanie: Impakt S.A.

Zasilacze UPS PowerWalker VFI 10000 TGS PF1	
Typ	Online
Moc	20000VA / 20000 W
Wsp. mocy wyjściowej	1.0
Zakres mocy wej.	160–276 VAC at 100% load 110–160VAC range linear between 50–100% load
PF wej.	≥ 0.995 przy pełnym naładowaniu
Zakres częstotliwości	45 Hz–55 Hz / 55 Hz–65 Hz 40 Hz–70 Hz at load ≤60%
Częstotliwość (zakres synchronizowany)	45 Hz–55 Hz at 50 Hz nominal 54 Hz–66 Hz at 60 Hz nominal and >60% rated load
Nominalna moc wyjściowa	208/220/230/240 VAC
Czysta sinusoida	Tak
THDv	≤1% w pełni liniowe obciążenie; ≤5% nieliniowe obciążenie
Regulacja napięcia (bat. rodzaj pracy)	±1%
Częstotliwość (bat. rodzaj pracy)	±0,1 Hz
Praca równoległa	Do 3, tego samego rozmiaru
Współczynnik szczytu ładowania	3 : 1
Czas przełączania (AC na akumulator)	0 ms
Czas przełączania (Inwerter na bypass)	0 ms
Czas przełączania (ECO na Inwerter)	10 ms
Wsparcie generatora	Tak
Możliwość przeciążenia	10min @105%–125%; 30s @125%–150%; 500ms @ >150%
Zewnętrzna bateria akumulatorów	Tak
Ładowarka	4A
Ochrona	Wyłącznik wejściowy
Sterowanie wentylatorem	Zawsze wł., aut. sterowanie prędkością
Dodatkowe informacje	Max. prąd rozruchowy 8xIrms
Wskaźniki LCD	Stan UPS, poziom ładowania, poziom akumulatora, napięcie wej./wyj., licznik rozładowania, stan błędów
Akumulatory	Zaprojektowane do pracy z zewn. baterią akumulatorów, akumulatory nie dołączone
Napięcie DC akumulatora	16 x 12V
Współczynnik hałasu	< 55dB
Temperatura	0°C–40°C (40°C–50°C @50% load)
Wilgotność	0%–95% RH (nie-skondensowana)

Impakt S.A. ul. Stanisława Lema 16, 62-050 Mosina
tel.: +48 61 898 32 23, +48 61 10 10 230 fax.: +48 61 898 32 23 wew. 215

DSO W ZASTOSOWANIACH SPECJALNYCH

Alarmowanie to, oprócz wykrywania pożaru w budynku, jedno z zadań systemu sygnalizacji pożarowej. Do tego celu wykorzystuje się dźwiękowe systemy ostrzegawcze (DSO), które umożliwiają rozgłaszanie sygnałów ostrzegawczych i komunikatów głosowych na potrzeby bezpieczeństwa osób przebywających w obiekcie. Obowiązek stosowania DSO powstał na początku 2004 roku, po wejściu w życie rozporządzenia, a obecnie w tej kwestii obowiązuje Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 roku w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów.

Dźwiękowe systemy ostrzegawcze DSO są jednym z niezbędnych elementów całego systemu ochrony przeciwpożarowej budynków, obiektów budowlanych oraz terenów. Służą przeprowadzeniu sprawnej ewakuacji budynku poprzez rozgłaszanie komunikatów w sposób automatyczny (po wysterowaniu przez systemy sygnalizacji pożaru SSP) lub poprzez tzw. „mikrofon strażaka". Nadawanie komunikatów głosowych pozwala na dużo sprawniejsze przeprowadzenie ewakuacji, gdyż precyzyjnie podaje informację słowną o konieczności ewakuacji w strefach gdzie istnieje taka konieczność. Stosowanie systemów DSO wymaga jednak od ich projektantów i instalatorów bardzo często indywidualnego podejścia, uwzględniającego specyfikę danego obiektu lub terenu. Niżej przedstawiono kilka rozwiązań, które właśnie takiego szczególnego podejścia wymagają.

Fot. 1. Głośniki DSO
Źródło: Blog Akustyczny – Propersound

DSO na promach i statkach żeglugi morskiej

Podstawy prawne do instalowania na statkach morskich systemów DSO w ramach systemów sygnalizacji pożarowej i systemów gaszenia pożaru reguluje Rozdział V – *Ochrona przeciwpożarowa – 2014,* „Przepisów Klasyfikacji i Budowy Statków Morskich", opracowanych i wydanych przez Polski Rejestr Statków S.A. (PRS). Rozdział ten został zatwierdzony przez Zarząd PRS w dniu 29 lipca 2014 r. i wszedł w życie z dniem 1 sierpnia 2014 r.[1] Rozdział ten reguluje m.in. kwestie stosowania na statkach i promach systemów sygnalizacji pożaru, systemów ostrzegawczych i instalacji przeciwpożarowych, montowanych na statkach morskich, a w tym takie kwestie szczegółowe, jak: instalacja sygnalizacji alarmowej pożaru, system oświetlenia dolnego dróg ewakuacji, system ostrzegania przed gazami wybuchowymi i tlenkiem węgla.

Nowoczesne systemy mają opcję trafnego wskazania miejsca powstania alarmu, przesłania informacji do systemu zarządzania bezpieczeństwem statku, jak też wysterowania innych urządzeń przeciwpożarowych takich jak: system oddymiania, system zamknięć ogniowych, dźwiękowy system ostrzegawczy **DSO**, odłączenie kontroli dostępu, itd. Jest podstawowym systemem zabezpieczającym statek przed rozprzestrzenianiem się ognia. Pełni on również często rolę nadrzędną sterując innymi instalacjami bezpieczeństwa, takimi jak wentylacja, oddymianie, kontrola dostępu. System sygnalizacji pożaru umożliwia monitorowanie stanu aktywacji wszystkich czujników pożarowych zainstalowanych na statku, do których należą czujki dymne, cieplne, ogniowe oraz urządzenia ostrzegające o pożarze tzw. ROP – ręczne ostrzegacze pożarowe. **System alarmowania (DSO),** w celu powiadomienia załogi i pasażerów o sytuacji panującej na statku, wykorzystuje system dzwonków alarmowych i rozgłośnię statkową (Public Adress System – PA). Wg „Przepisów" w strefach przeznaczonych dla osób z ograniczoną możliwością przemieszczania należy zastosować przyciski alarmowe na wysokości umożliwiającej użycie ich przez osoby znajdujące się na wózkach. Strefy przeznaczone dla osób z ograniczoną możliwością przemieszczania się powinny być wyposażone w odpowiednią sygnalizację alarmową świetlną i dźwiękową, umożliwiającą odbiór sygnałów alarmowych przez osoby z niepełnosprawnością wzrokową lub słuchową.

Fot. 2. Przykład głośnika okrętowego odpornego na wybuchy
Źródło: Public Address System

DSO w metrze

W obiektach takich jak metro, zwykle znajdują się osoby przypadkowe, w różnym wieku – również dzieci i starcy – także o różnych przypadłościach. Wszystkie te osoby muszą otrzymać zwięzłe i przede wszystkim, zrozumiałe instrukcje dotyczące zachowania i sposobu wydostania się z zagrożonego rejonu. W związku z tym systemy DSO instalowane w metrze muszą

[1] Z dniem wejścia w życie *Części V,* jej wymagania mają zastosowanie w pełnym zakresie do statków nowych.

spełniać na odpowiednim poziomie dwa bardzo ważne parametry, którymi są: głośność dźwięku, jaką wytwarzają głośniki systemu ostrzegawczego, oraz tzw. wskaźnik zrozumiałości mowy (ang. Speech Transmission Index – STI). Wskaźnik ten musi mieć wartość, co najmniej 0,7.

DSO w metrze przedstawimy szerzej na przykładzie jedynego polskiego metra – warszawskiego. Metro w Warszawie obejmuje obecnie 21 stacji, plus STP, czyli Stację Techniczno-Postojową na Kabatach. **DSO** na każdej stacji pasażerskiej stanowi system na wpół autonomiczny. Co to znaczy? W zakresie alarmowania i uruchamiania procedur ewakuacyjnych działa niezależnie, w sposób całkowicie automatyczny. Jednak dyspozytor, którego miejsce pracy znajduje się na STP Kabaty, może wysłać komunikat słowny do nagłośnienia wybranej stacji lub ich grupy. W centrali tej znajduje się też „czarna skrzynka", która rejestruje w sposób ciągły wszystkie zdarzenia, jakie miały miejsce w obrębie całego systemu – gdzie, kiedy i jaki naciśnięto przycisk, jaki komunikat został wyemitowany, wykrycie awarii itd.

Sprzęt na stacjach kontroluje się sam – taka zdolność jest zresztą także wymagana przepisami. Odpowiedni moduł kontroluje wszystkie żywotne parametry pracy systemu – m.in. funkcjonowanie linii głośnikowych i samych głośników, a także działanie zasilania sieciowego oraz rezerwowego. Każdy system stacyjny obejmuje dwie strefy: publiczną i techniczną. Te zaś dzielą się na łącznie trzy do pięciu – podstref. Publiczna obejmuje peron oraz antresolę – czyli zwykle pasaż handlowy w obrębie stacji. Z kolei strefa techniczna dzieli się na część techniczną, strefę tzw. torów odstawczych i podperony, to znaczy pomieszczenia techniczne znajdujące się, pod peronami. Na STP znajduje się „centrum zarządzania kryzysowego", uaktywniane w chwilach poważniejszych zagrożeń. Z pomieszczenia tego można przejąć kontrolę nad całym systemem ostrzegawczym, odpowiednio kierując akcją ratowniczą.

Fot. 3. Metro
Źródło: wikipedia.org

Reklama

Działanie DSO jest w zasadzie bardzo proste. Dźwiękowy system ostrzegania jest niejako organizmem podrzędnym względem systemu wykrywania zagrożeń. W przypadku pożaru, powiadomione zostają odpowiednie służby ratownicze. Ewakuowana jest tylko strefa zagrożona bezpośrednio. Jeśli więc ogień wybuchł w części technicznej, alarmy i odpowiednie komunikaty ewakuacyjne – zapisane w dedykowanym module, pod postacią plików mp3 – są transmitowane jedynie do strefy technicznej, zaś publiczna nie jest o tym informowana. Podobnie jest w odwrotnym przypadku. W razie rozprzestrzenienia się ognia system uruchamia procedury ewakuacji z kolejnych obszarów. Jeżeli ewakuowana jest strefa publiczna, wówczas system wykrywania zagrożenia otwiera bramki, uwalniając ich kołowroty. Dzięki temu ewakuowani pasażerowie mogą przechodzić przez nie bez zakłóceń. **System DSO** musi działać w warunkach nie tylko np. pożaru, ale i odbywającej się akcji gaśniczej. Oznacza to, że wymaga się od niego pełnej sprawności, gdy wokół temperatura znacząco rośnie, szaleje ogień, a za chwilę zaczyna lać się woda, czy to ze spryskiwaczy, czy węży strażackich. DSO musi zachować pełną funkcjonalność, co najmniej przez czas potrzebny na ewakuację obiektu, z pewnym rzecz jasna, naddatkiem. W instalacji DSO w metrze używa się niepalnego okablowania, a poszczególne stacje połączone są z centralą światłowodową linią redundantną. Ponieważ w razie pożaru objęty nim obiekt zazwyczaj zostaje odcięty od dopływu energii elektrycznej, to system ewakuacyjny musi dysponować własnym, autonomicznym zasilaniem awaryjnym – akumulatorowym

Specyfika systemów DSO w wybranych obiektach:

Porty lotnicze. W DSO montowanych w portach lotniczych ważnym jest uwzględnienie specyfiki tych obiektów tak, aby:

1. mikrofony strefowe, zainstalowane w punktach informacyjnych i strefach odpraw (GATE-ach), umożliwiały nadawanie komunikatów przez obsługę lotniska i przekazywanie informacji pasażerom czekającym na odprawę. Systemy DSO wiodących producentów zapewniają wystarczającą liczbę mikrofonów w systemie do aplikacji przewidzianych dla największych portów lotniczych. Komunikacja odbywa się zwykle po protokole TCP/IP, dlatego przy wykorzystaniu switchy ethernetowych przyłączenie dużej ilości mikrofonów jest bardzo proste.
2. wbudowany procesor DSP umożliwiał korekcję sygnałów audio na każdym wejściu i wyjściu systemu, jak również zastosowanie kolumn głośnikowych wyrównanych liniowo, zapewniających znacznie dalszy zasięg przy jednoczesnym zachowaniu wysokiej równomierności poziomu dźwięku w nagłaśnianym obszarze, gwarantują uzyskanie najlepszej zrozumiałości nadawanych komunikatów w pomieszczeniach o niekorzystnej akustyce, takich jak rozległe hale przylotów i odlotów.

Fot. 4. Tunel drogowy
Źródło: www.picswe.com

Dworce kolejowe i autobusowe. DSO na dworcach kolejowych i autobusowych instaluje się celem przekazywania komunikatów słownych przez obsługę dworca, nadawanych do wybranych lub wszystkich peronów i innych obszarów dworca, celem powiadomienia pasażerów czekających na pociąg/autobus o zmianie w organizacji ruchu lub o wystąpieniu zagrożenia w obiekcie. W DSO stosowanych w tych obiektach istotne jest:

- wbudowane wejścia audio w każdej centrali i mikrofonie powinny umożliwiać podłączenie sygnałów systemów zewnętrznych i przekazywanych komunikatów pochodzących od nadrzędnych, zewnętrznych systemów informacyjnych;
- wskazane jest wbudowanie funkcji buforowania komunikatów, umożliwiające nagrywanie informacji o niższym priorytecie, nadawanych do zajętych przez źródła nadrzędne stref głośnikowych i automatyczne ich odtwarzanie po zwolnieniu stref.

Tunele. Propagacja dźwięku w tak specyficznym obiekcie, jak tunel wymaga stosowania systemów DSO wyposażonych w specjalne funkcje. Przede wszystkim w tunelach wymagane jest stosowanie:

- funkcji definiowania opóźnienia sygnałów akustycznych emitowanych przez głośniki systemu nagłośnienia. Funkcja ta wbudowana jest najczęściej w system Dźwiękowego Systemu Ostrzegawczego i nie ma potrzeby stosowania dodatkowych, niecertyfikowanych urządzeń. Powyższa funkcja zapewnia zsynchronizowanie fal akustycznych emitowanych przez głośniki;
- dedykowanych kierunkowych głośników tunelowych dużej mocy, które powinny charakteryzować się wysokim poziomem emitowanego ciśnienia akustycznego i być zainstalowane w tunelu, co kilkadziesiąt metrów, zapewniając precyzyjną propagację dźwięku, eliminując niepożądane odbicia i zapewniając odpowiedni poziom głośności oraz szerszy zakres częstotliwości, gwarantujący najwyższy możliwy do uzyskania poziom zrozumiałości komunikatów;
- wbudowanej karty komunikacyjnej w każdym mikrofonie strażaka, umożliwiającej podłączenie mikrofonu, za pośrednictwem okablowania światłowodowego, bez konieczności stosowania dodatkowych konwerterów i wynoszenia mikrofonów na wymagane w tego typu obiektach bardzo duże odległości, sięgające nawet do kilkunastu kilometrów.

Wykorzystano m.in.:
1. M. Korbecki, DSO w warszawskim metrze – Roboty „od metra", https://livesound.pl/prezentacje/realizacje/3770-dso-w-warszawskim-metrze-roboty-od-metra
2. Monitoring i systemy bezpieczeństwa na promach i statkach żeglugi morskiej, OMiI nr 6/2018
3. http://www.afsystems.pl/dzwiekowe-systemy-ostrzegawcze-dso/
4. https://ambientsystem.eu/pl/dzwiekowe-systemy-ostrzegawcze-trako-15spin/

Redakcja

KONTROLA DOSTĘPU, RUCHU OSOBOWEGO I TOWAROWEGO ORAZ OCHRONA NA PRZEJŚCIACH GRANICZNYCH

Systemy kontroli dostępu odgrywają istotną rolę w bezpieczeństwie przejść granicznych. Oferta rynkowa w tym zakresie jest bardzo bogata. Obejmuje ona, bowiem bramki, zamki elektromagnetyczne, czytniki biometryczne, a także kompleksowe systemy elektronicznej obsługi obiektów budowlanych. Ponadto zastosowanie znajduje szereg innych rozwiązań technicznych.

Zacznijmy może od czytników kart zbliżeniowych. Nowoczesne urządzenia tego typu cechują się niewielkimi rozmiarami, dzięki czemu jest możliwy montaż w miejscach o ograniczonej przestrzeni. Istotna pozostaje również praca w skrajnych warunkach atmosferycznych. Niektóre modele są montowane bezpośrednio na powierzchniach metalowych. Z pewnością przydadzą się obszerne możliwości komunikacyjne, które pozwalają na współpracę z wieloma typami kontrolerów.

Coraz większym uznaniem cieszy się biometria, która ma bardzo szerokie możliwości i zastosowanie. W czytnikach biometrycznych identyfikacja osób bazuje na wykrywaniu niepowtarzalnych cech. Są nimi na przykład wielkość i kształt dłoni, odciski palców, a także głos czy też budowa oka. Identyfikowanie wielkości kształtu i dłoni niejednokrotnie odbywa się w obrazie trójwymiarowym. W zależności od modelu komunikacja z urządzeniem zewnętrznym uwzględnia port RS-232, RS-485 lub Ethernet. W pamięci urządzenia mogą być przechowywane informacje o użytkownikach a każdemu z nich przypisuje się numer identyfikacyjny. Warto podkreślić, że proces odczytu przebiega bardzo szybko. Trwa on, bowiem mniej niż jedną sekundę.

Interesujące rozwiązanie stanowią również czytniki linii papilarnych. Urządzenia tego typu wykorzystują termiczny skaner liniowy. Nowoczesnych urządzeń nie da się oszukać silikonowymi sztucznymi palcami, a także odciskami naniesionymi na folie. Jeżeli proces czytania linii palca przebiegnie pozytywnie to są definiowane współrzędne punktów charakterystycznych, które zapisuje się w postaci binarnej. W oferowanych na rynku urządzeniach uwzględnia się wbudowaną pamięć i oprogramowanie, które pozwala zarówno na gromadzenie jak i przetwarzanie pozyskanych informacji. Wymiana danych bazuje na sieci Ethernet. Bardziej rozbudowane urządzenia łączą w sobie dodatkowo identyfikację PIN lub kart zbliżeniowych. Modele tego typu są wyposażone w oprogramowanie administracyjne, które pozwala na zdalne zarządzanie czytnikiem poprzez stronę www.

W nowoczesnych systemach kontroli dostępu uwzględnia się również kamery, pozwalające na identyfikację tęczówki oka.

Zabezpieczenie drzwi

Rygiel elektromagnetyczny, nazywany także elektrozaczepem, składa się z elementu mechanicznego, który jest blokowany układem elektromagnetycznym. Po otwarciu drzwi, kształt uchylnego języka spustowego umożliwia ponowne ich zatrzaśnięcie przy domykaniu.

Trzymacze drzwiowe są przeznaczone do blokowania drzwi w pozycji otwartej. Znajdują one zastosowanie przede wszystkim w systemach przeciwpożarowych. Przez czas podawania napięcia do elektromagnesu drzwi są utrzymywane w pozycji otwartej, umożliwiając ich samoczynne zamknięcie. W momencie odcięcia zasilania (ręcznego lub przez sterownik) zamek zwalnia blokadę a drzwi mogą zostać zamknięte.

Zwory elektromagnetyczne stanowią zamki, które znajdują zastosowanie w systemach kontroli dostępu, a także

Fot. 1. Przejście graniczne
Źródło: Dziennik Zachodni

w drzwiach przeciwpożarowych, ewakuacyjnych oraz wszędzie tam, gdzie jest wymagany system odblokowania po zaniku napięcia. Elektromagnesy montuje się na wszystkich rodzajach drzwi, niezależnie od materiału ich wykonania. Dostępne na rynku elektromagnesy cechują się zarówno estetycznym wyglądem jak i prostą obsługą. Można je montować powierzchniowo i w zabudowie wewnętrznej.

Zamki typu solenoid są wykonane w postaci cewki, która wytwarza pole elektromagnetyczne, powodujące wysunięcie się metalowego trzpienia. Ten z kolei wysuwa stalową płytkę montowaną w skrzydle drzwiowym. Urządzenie to pozwala na wyeliminowanie pośrednich układów mechaniczno-elektrycznych.

Samozamykacze drzwiowe stanowią urządzenia, które zamykają drzwi niedomknięte przez osobę przechodzącą. Samozamykacze są urządzeniami mechanicznymi. Ich głównym elementem jest sprężyna a czynnik tłumiący najczęściej stanowi płyn hydrauliczny.

Bramki obrotowe

Obrotowe bramki wysokie sprawdzają się w miejscach, gdzie jest wymagana kontrola ruchu osobowego w miejscach strzeżonych. Urządzenia tego typu współpracują m.in. z systemami rejestracji czasu pracy czy kontroli dostępu. W nowoczesnych wysokich bramkach obrotowych uwzględnia się sterowanie mikroprocesorowe, wspomaganie ruchu grzebienia, mechanizm dwukierunkowy, piktogramy diodowe lub lampki oraz odblokowywanie awaryjne. W niektórych modelach stelaż wykonuje się ze stali nierdzewnej lub malowanej proszkowo. Aby mechanizm odblokowujący mógł się uruchomić jest konieczne otrzymanie przez bramkę impulsu sterującego z urządzenia zewnętrznego. Wewnętrzny rygiel jest załączany elektrycznie na około 10 s. Stan otwarcia bramki jest sygnalizowany świecącą się strzałką w kolorze zielonym. Za pomocą czerwonego krzyżyka użytkownik jest z kolei informowany o stanie zamknięcia. Po odblokowaniu mechanizmu należy pchnąć ramię bramki, które jest usytuowane w pozycji poziomej w kierunku sygnalizowanego przejścia. Po pchnięciu następuje samoczynne załączenie mechanizmu dopychającego, który wspomaga przejście i zablokowanie obrotu do czasu otrzymania następnego sygnału sterującego. W razie potrzeby odblokowania mechanizmu należy odbezpieczyć blokadę ruchu ramion. Czynność taka może być konieczna na przykład przy ewakuacji osób lub braku zasilania.

Bramki z mechanizmem dwukierunkowym pozwalają na kontrolę ruchu osobowego w obu kierunkach lub w jednym z nich. W niektórych modelach przewidziano piktogramy diodowe, które określają stan odblokowania lub zablokowania bramki – czerwony krzyżyk-bramka zamknięta, zielona strzałka-bramka otwarta. Istotną rolę odgrywa elektromechaniczne wspomaganie ruchu ramion, które ma za zadanie zapewnienie płynnego przechodzenia oraz samoczynne blokowanie układu ramion.

Oprogramowanie wspomagające

Nowoczesne urządzenia systemów kontroli dostępu nie obejdą się bez specjalistycznego oprogramowania komputerowego. Należy podkreślić, że aplikacje tego typu współpracują z systemem alarmowym, przeciwpożarowym i telewizją przemysłową. W ramach zezwolenia dostępu istnieje możliwość definiowania grup pracowników. Każdemu z nich przypisuje się uprawnienia dostępu poprzez autoryzację, według stref czasowych i kalendarza. Zezwolenie dostępu może odbywać się także na podstawie klasyfikacji personelu, kontroli parzystości przejścia lub cech biometrycznych.

Komfort użytkowania poprawi moduł pozwalający na współpracę programu z siecią Intranet. Tym sposobem zyskuje się dostępność do systemu wszystkich zainteresowanych użytkowników. Należy podkreślić, że dostęp do danych jest przydzielany na różnych poziomach.

Fot. 2. Bramka obrotowa z modułowym mechanizmem (elektro)mechanicznym
Źródło: www.locinox.com

Zarządzanie zdarzeniami stwarza możliwość mapowania wielowarstwowego, czyli graficznej prezentacji rozmieszczenia urządzeń w pomieszczeniach. Wszystkie elementy kontroli mogą być określone na mapie pod względem pozycji. Zdarzenia są także sygnalizowane zarówno dźwiękami jak i wizualnie. Oprócz tego zdarzenia klasyfikuje się z uwzględnieniem np. kryterium wejścia autoryzowanego, włamania, pożaru, itp. Oprogramowanie wspomagające kontrolę dostępu jest w stanie nadzorować ruch osobowy.

Do przydatnych funkcji należy zaliczyć produkcję identyfikatorów. Fotografia pracownika jest zapisywana bezpośrednio w bazie danych. Program współpracuje z większością modeli drukarek również z tymi, które pozwalają na pracę z kartami plastikowymi. Do identyfikatora można dodać podpis pracownika. Istnieje możliwość wydrukowania na karcie kodu kreskowego. Z pewnością przydatną funkcję stanowi możliwość generowania raportów.

Ochrona perymetryczna

Ochrona perymetryczna, nazywana także obwodową, powinna zagwarantować wczesne wykrycie osób chcących wtargnąć na granicę chronionego obiektu. Informacja o zagrożeniu przekazana odpowiednio wcześnie pozwala na szybkie, a co najważniejsze, skuteczne podjęcie działań zapewniających bezpieczeństwo użytkowników obiektu. Podstawę ochrony stanowią bierne i aktywne systemy falowe. Chodzi przede wszystkim o radary naziemne oraz kamery zarówno termowizyjne jak i wizyjne.

Nie bez znaczenia pozostają także systemy odpowiedzialne za wykrywanie przekroczenia ogrodzenia. Aplikacje pracujące autonomicznie niejednokrotnie poddaje się procesowi integracji. Istotną cechą rozwiązań tego typu jest zasięg obejmujący nawet kilkadziesiąt kilometrów.

Przede wszystkim trzeba wspomnieć o technologii radarowej, którą uwzględnia się w procesie monitorowania dużych powierzchni. Radar zataczając pełne koła analizuje sygnały zwrotne, na których podstawie są wykrywane ruchy na określonym terenie. Zalet wynikających z ich stosowania jest wiele. Przede wszystkim należy zwrócić uwagę na pewność działania niezależnie od warunków atmosferycznych. Zatem opady deszczu czy też śniegu tylko nieznacznie zmniejszają pewność działania czujników radarowych. Skuteczności wykrywania nie zmniejsza

Fot. 3. Zestaw 2 kamer termowizyjnych dla ochrony granic
Źródło: Milmag

niższy poziom natężenia oświetlenia. Urządzenia bazujące na technologii radarowej są w stanie wykryć ludzi, a także pojazdy, łodzie i samoloty. Analizowany jest przy tym kierunek oraz prędkość poruszania. Tym sposobem użytkownik na bieżąco jest informowany o miejscu przebywania intruza.

Typowy system analizy radarowej obiektów militarnych bazuje na jednym lub wielu dowolnie rozmieszczonych aktywnych radarach, odpowiedzialnych za ciągłe skanowanie przestrzeni. Radary są łączone w sposób sieciowy zarówno za pomocą przewodów jak i w oparciu o bezprzewodowe technologie wymiany danych.

Systemy radarowe mogą współpracować z technologią GPS. Tym sposobem zyskuje się możliwość wgrania mapy do systemu nadzorującego. Oprogramowanie zarządzające systemem pozwala na nadanie wykrytemu obiektowi statusu. Jest przy tym możliwe wyłączenie spod ochrony określonego fragmentu terenu.

Mówiąc o ochronie perymetrycznej obiektów kolejowych warto wspomnieć o czujnikach doziemnych. Urządzenia tego typu wykrywają wszelkie zakłócenia pola elektromagnetycznego, pochodzącego od sensorycznego kabla nadawczego i odbieranego przez zainstalowany równolegle kabel odbiorczy. Kable tego typy najczęściej są umieszczane na głębokości mieszczącej się pomiędzy 15 a 25 cm pod ziemią na granicy chronionego terenu. Tym sposobem powstaje niewidzialna strefa detekcji. Typowy system wykrywania z czujnikami doziemnymi jest oparty na sterowniku mikroprocesorowym z układami generacyjnymi i odbiorczymi. Nie mniej istotną rolę odgrywają kable sensoryczne (aktywne i obojętne), terminatory oraz oprogramowanie systemowe. Czujniki doziemne zazwyczaj pracują w trybie autonomicznym i sieciowym. Czujniki autonomiczne chronią oddzielne strefy. Wymiana danych z systemem nadrzędnym może bazować na wyjściach przekaźnikowych lub standardach komunikacyjnych RS-485 lub RS-232. Interesujące rozwiązanie stanowi możliwość pracy w konfiguracji sieciowej, gdzie poszczególne czujniki są łączone w kaskady. Zasilanie do czujników oraz sygnały transmisji danych są przesyłane za pomocą kabli sensorycznych.

Bardzo często zastosowanie znajdują systemy bazujące na wykrywaniu zmian nacisku na grunt. Za działanie aplikacji odpowiadają specjalne rurki przebiegające w gruncie. Zmiana ciśnienia powoduje wygenerowanie sygnałów przesyłanych do sterownika, który przeprowadza analizę częstotliwościowo-czasową. Bardziej zaawansowane systemy są w stanie określić pozycję intruza. Standardowo miejsce wtargnięcia jest lokalizowane z dokładnością do 10 m. W systemach tego typu istotną rolę odgrywa stabilność pracy zapewniona dzięki odporności na szumy. Zastosowanie systemów wykrywających nacisk bardzo często obejmuje, zatem obiekty usytuowane w pobliżu torów kolejowych.

W systemach opartych na napłotowym kablu sensorycznym istotną rolę odgrywają moduły procesorów wysyłające impulsy wzdłuż kabli. Impulsy pod wpływem zakłócenia spowodowanego wibracją kabla są odbijane z powrotem do procesora. Za pomocą cyfrowego przetwarzania danych system precyzyjnie lokalizuje zakłócenia, określając ich charakter. Mikroprocesor rozpoznaje odkształcenia impulsów spowodowane przez intruza takie jak przejścia czy też przecięcia ogrodzenia, odróżniając zakłócenia pochodzące od wiatru lub intensywnych opadów deszczu.

Fot. 4. Radarowy system ochrony perymetrycznej sprzężony z kamerami PTZ
Źródło: ASDNews

Ochrona mobilna

W procesie obwodowej ochrony obiektów kolejowych niejednokrotnie uwzględnia się kamery termowizyjne. Urządzenia tego typu cechuje niezawodność, którą uzyskano dzięki chłodzonemu detektorowi. Nowoczesne kamery termowizyjne w kompletnej ciemności są w stanie wykryć cel z odległości 9 km. Zwraca się uwagę na precyzyjny mechanizm uchylno-obrotowy zapewniający dokładną kontrolę nad urządzeniem. Podczas ochrony obiektów mobilnych bardzo często są używane ręczne kamery termowizyjne. Obudowa wielu urządzeń tego typu bazuje na obserwacji obuocznej.

Istotną rolę odgrywają inteligentne czujki dopplerowskie o dalekim zasięgu. Bazują one na efekcie Dopplera z modulacją 2 częstotliwości (stereo Doppler) oraz kombinacji tego efektu z analizą metodą logiki rozmytej. Tym sposobem zyskuje się możliwość analizowania w strefie detekcji wszystkich nieistotnych ruchów na dystansie 100 m. Są przy tym pomijane wszelkie wywołania spowodowane przez ruch małych zwierząt lub innych zakłóceń, które pochodzą z otoczenia. Nowoczesne systemy tego typu są w stanie określić rozmiar intruza oraz kierunek jego poruszania. Rzecz jasna system poddaje analizie miejsce położenia z dokładnością wynoszącą 1 m. Zyskuje się, więc dostrzeżenie małych i niewyraźnych elementów.

Podsumowanie

Kontrola dostępu, kontrola ruchu osobowego i towarowego oraz ochrona przejść granicznych to bardzo szerokie zagadnienie. Oprócz wyżej wymieniowych rozwiązań warto również przynajmniej wymienić bramki do wykrywania metali pozwalające na precyzyjne wykrywanie zagrożeń. Skanowaniu poddaje się dużą liczbę osób w krótkim czasie przy zachowaniu wszystkich standardów bezpieczeństwa. Osobne systemy wykorzystywane są do monitorowania ruchu towarowego.

Damian Żabicki
Dziennikarz, analityk specjalizujący się w tematyce technicznej i przemysłowej

DRONY W SŁUŻBIE POLICJI

Drony wykorzystywane w Policji pozwalają przede wszystkim na dotarcie do miejsc, do których nie jest w stanie dotrzeć człowiek. Zapewniony jest przy tym najwyższy poziom bezpieczeństwa przeprowadzanych operacji.

Fot. 1. Drony w służbie policji
Źródło: Wiadomości – Gazeta

Wszystkie drony mają zbliżoną konstrukcję. W zależności od wersji wyposaża się je w nie mniej niż trzy śmigła, a także ramiona, które umożliwiają montaż śmigła i silnika. Ważna jest również podstawa przeznaczona do lądowania.

Spektrum zastosowania dronów w policji jest bardzo szerokie. Wykorzystuje się je chociażby podczas poszukiwania zaginionych. Można, bowiem szybko dotrzeć w miejsca, które są trudno dostępne. Bardzo często drony mają kamery termowizyjne.

Fot. 2. Mobilne centrum poszukiwań policji z dronem
Źródło: www.policja.pl

Za pomocą dronów obserwuje się i mierzy natężenie ruchu. Można także obserwować sytuacje na drogach oraz przechwytywać kierowców zagrażających bezpieczeństwu innych uczestników ruchu drogowego. Drony wiszące w powietrzu mogą nagrywać wykroczenia. Wykorzystywane są także drony wyposażone w fotoradary.

Drony uznaje się za urządzenia niezastąpione podczas ogłoszonego alarmu bombowego. Bez problemu są w stanie zbliżyć się do niebezpiecznego ładunku, co pozwala nie tylko na jego identyfikację, ale i zneutralizowanie. Za pomocą dronów bardzo często obserwuje się i śledzi podejrzanych. Stąd też drony wykorzystywane są w działaniach detektywistycznych.

Drony – cechy ogólne

Oferowane na rynku drony różnią się przede wszystkim wielkością, masą i siłą nośną, czyli masą załadunku, jaki mogą udźwignąć. Najmniejsze drony mieszczą się na dłoni i uniosą najwyżej pojedyncze gramy. Średnica dronów może przekraczać nawet jeden metr i są w stanie unieść masę większą niż kilkanaście kilogramów.

Nowoczesne drony bardzo często wyposaża się w gimbal[1], przez co obraz jest pozbawiony drgań i przechyłów. Drony bazują najczęściej na konstrukcjach wielowirnikowych, zatem lot ma zapewniony najwyższy poziom bezpieczeństwa. Istotną rolę odgrywa wbudowany system GPS, przez co dron utrzymuje stałą pozycję w powietrzu nawet przy silnym wietrze. Specjalne systemy pozwalają podejrzeć w czasie rzeczywistym obraz z dronu. Dodatkowo materiał wideo jest nagrywany i wykonywane są zdjęcia. Odpowiednie systemy sprawdzą się w momencie, kiedy dron utraci łączność z kontrolerem. Jeżeli dojdzie do zerwania transmisji dron samoczynnie powróci w miejsce startu zgodnie z określoną trasą. Ważny jest autonomiczny lot pozwalający zaplanować trasę, która ma być pokonana samodzielnie zgodnie określonymi parametrami.

Specjalna funkcja pozwala za podążanie dronu za obiektem. Na urządzeniu sterującym wyświetlają się funkcje takie jak ilość satelitów GPS, czy czas lotu. Do dyspozycji użytkownika jest również wskaźnik naładowania baterii, moc sygnału, ilość pamięci na karcie SD oraz wysokość, prędkość wznoszenia, prędkość opadania, odległość od operatora i przebieg trasy na mapie Google.

Inne funkcje zapewniają identyfikowanie obiektów i podążanie za nimi dzięki zasadzie kontrastu. Wraz ze wzrostem kontrastu koloru śledzonego obiektu do koloru tła poprawia się jakość śledzenia.

[1] Gimbal – lub inaczej stabilizator kamery – to niewielkie urządzenie elektroniczne, które wyposażone jest w żyroskop, zminiaturyzowane silniczki elektryczne oraz szereg dodatkowych czujników i mocowań.

Technologia stabilizacji kamery miała swój początek w produkcji dronów, ale szybko przeniosła się do innych dziedzin. Obecnie ręczne gimbale mogą być używane ze smartfonami, kamerami sportowymi, czy aparatami fotograficznymi. Obsługa takiego sprzętu jest prosta i po kilku minutach każdy pozna sposób jego działania.

Najważniejszą funkcją gimbala jest stabilizacja obrazu podczas filmowania. Obecnie najczęściej stosowana jest stabilizacja w trzech osiach. Mniej zaawansowane modele mogą działać ze stabilizacją w jednej lub dwóch osiach.

Jeżeli śledzony obiekt zniknie z pola widzenia np. wjedzie do tunelu lub przysłonią go drzewa dron zatrzyma się, zawiśnie w powietrzu i spróbuje re-lokalizować obiekt. Z kolei, gdy obiekt zniknie na stałe lub pojawi się w innym miejscu poza ramką aplikacji sterującej może dojść do utraty obiektu. Warto wtedy przejąć kontrolę nad dronem i samodzielnie odnaleźć obiekt lub wybrać inny. W przypadku utracenia łączności z dronem zostanie zainicjowana odpowiednia funkcja pozwalająca na powrót drona zgodnie ze swoją trajektorią lotu.

Drony z kamerą termowizyjną

W dronach najczęściej przewiduje się możliwość montażu pojedynczej kamery standardowo lub na jego szczycie. Ponadto jest możliwa instalacja dwóch kamer pod dronem jednocześnie. W typowym urządzeniu tego typu silniki o dużych mocach są połączone z 17-to calowymi śmigłami, co zapewnia bezpieczny lot z bardzo dobrą stabilizacją lotu również w trudnych warunkach. Specjalne aplikacje umożliwiają planowanie trasy, kontrolę ustawień oraz podgląd efektów pracy. Dzięki odpowiednim odbiornikom operator jest informowany o załogowych statkach powietrznych, jakie znajdują się pobliżu. Nowoczesne drony wyposaża się w szereg czujników i kamer po to, aby wykrywać i omijać wszelkie przeszkody. Chodzi tu m. in. o przednie czujniki wizyjne, dolne czujniki wizyjne i ultradźwiękowe oraz górne czujniki podczerwieni.

Drony z kamerami termowizyjnymi mogą pracować w kilku trybach. W jednym z nim dron jest w stanie śledzić poruszających się ludzi lub inne obiekty utrzymując je w kadrze, co sprawdzi się np. podczas akcji ratunkowych. Jest również możliwe okrążanie przez dron badanego obiektu. W efekcie operator może skupić się na zbieraniu interesujących go danych – np. podczas inspekcji. Nie mniej ważna jest również blokada kamery na wybranym celu przy zachowaniu swobody lotu.

Oprócz tego jedna z funkcji jest w stanie spowolnić prędkość lotu i obracać dron, co pozwala na dokładniejsze kadrowanie, a także bezpieczne poruszanie się np. w wąskich miejscach.

Spektrum zastosowania dronów wyposażonych w kamerę termowizyjną jest bardzo szerokie. Wykorzystuje się je chociażby podczas poszukiwań i akcji ratowniczych, w czasie akcji ratowniczo-gaśniczych, inspekcji dachów i linii wysokiego

Fot. 3. Dron z kamerą termowizyjną i gimbalem
Źródło: Drony dla Policji-Straży Pożarnej-SAR

napięcia, a także inspekcji substancji i instalacji fotowoltaicznych. Termowizja sprawdzi się również w ochronie, patrolowaniu wałów przeciwpowodziowych, przy wsparciu akcji ratowniczych na zbiornikach wodnych czy podczas koordynacji wypraw survivalowych.

Zarządzenie pracą dronów

Specjalne aplikacje służą do kontrolowania kamery termowizyjnej w kontekście wyboru palety barw, izoterm, powiększenia itd. Ponadto jest możliwe kontrolowanie ustawień nagrywania czy robienia zdjęć przy pomocy jednego palca, dzięki czemu bardzo szybko zapisywane są dane termalne. Proste zarządzanie jest gwarancją dostępu do ważnych funkcji takich jak system transmisji obrazu, automatyczne punkty zainteresowania, powrót do „domu" czy podążenie. Trzeba mieć również na uwadze możliwość rozdzielenia zadań operatora lotu drona i operatora kamery, dzięki zastosowaniu dwóch kontrolerów.

Drony dla Policji – specyfikacja techniczna

Pod koniec 2018 r. w Policji rozpisano przetarg na dostawę dronów pozwalających na obserwację i rejestrowanie obrazu w czasie, gdy prowadzone są działania operacyjno-rozpoznawcze. Warto podkreślić, że to już trzeci przetarg, jaki był ogłoszony przez Policję na dostawę dronów. Wcześniejszy przetarg został unieważniony, co argumentowano brakiem ofert niepodlegających odrzuceniu.

Drony wyspecyfikowane w ofercie to urządzenia wielowirnikowe, z co najmniej czterema ramionami z zespołami napędowymi. Przewidziano urządzenia pionowego startu i lądowania a maks. masa startowa (MTOP) miała wynosić do 7 kg. Drony wyspecyfikowane w poprzednim przetargu miały masę do 25 kg. Drony będą używane do lotów odbywających się poza zasięgiem wzroku. Promień pracy ma wynosić nie niej niż 3 km w terenie otwartym oraz 1 km w terenie zurbanizowanym. Maks. prędkość horyzontalna powinna wynosić nie mniej niż 20 m/s. Za bezpieczeństwo lotu odpowiadają systemy czujników, które wykrywają przeszkody z trzech stron – dół, przód, góra.

Przewidziano trzy rodzaje głowic optoelektronicznych – głowice z kamerą z zoomem optycznym minimum (30x) i zoomem cyfrowym minimum (6x) oraz głowice z kamerą dzienną i termowizyjną. Ten drugi typ głowic ma być zintegrowany z jednej obudowie. Ważna jest przy tym stabilizacja mechaniczna w trzech osiach. Trzeci typ to głowice z kamerą wysokiej rozdzielczości o ogniskowej obiektywu wynoszącej 45 mm.

Dostawa dronów powinna być uzupełniona szkoleniem dla dwóch operatorów z uprawnieniami VLOS na każdy zakupiony komplet. Zakończenie kursu powinno być potwierdzone wydaniem odpowiedniego certyfikatu.

Drony, jakie wyspecyfikowała Policja w dokumentacji przetargowej mają wznosić się na wysokość nie mniejszą niż 2500 m n.p.m. Ważne jest przy tym przystosowanie do prowadzenia lotów w oparciu o sterowanie ręczne przez operatora oraz lotów automatycznych wykonywanych w oparciu o wcześniej zaprogramowaną trasę. Czas lotu drona przy wykorzystaniu dwóch akumulatorów (składających się na zestaw) powinien wynosić nie mniej 25 min.

Podsumowanie

Drony, jakie znajdują zastosowanie w służbie Policji wykorzystuje się przede wszystkim przy poszukiwaniu zaginionych. Dzięki bezzałogowym statkom powietrznym można, bowiem dotrzeć w miejsca o utrudnionym dostępie. Szczególnie przydadzą się tutaj drony z kamerami termowizyjnymi.

Drony są niezastąpione przy pomiarze natężenia ruchu oraz podczas obserwowania sytuacji na drogach. Za pomocą dronów bardzo często obserwuje się i śledzi podejrzanych. Stąd też drony wykorzystywane są w działaniach detektywistycznych.

Damian Żabicki
Dziennikarz, analityk specjalizujący się w tematyce technicznej i przemysłowej

AXIS 200. KRÓTKA HISTORIA PIERWSZEJ NA ŚWIECIE KAMERY SIECIOWEJ

Nikt nie ma recepty na sukces, ale zgłębiając historie większości globalnych osiągnięć technologicznych można dojść do wniosku, że przełomowe wynalazki i innowacje mają kilka cech wspólnych. Mowa o entuzjastycznych i zaangażowanych ludziach z pomysłem, zapałem do pracy, wyczuciem czasu i przyszłych trendów. Te trzy czynniki okazały się kluczowe także w stworzeniu pierwszej na świecie kamery sieciowej. A wszystko zaczęło się od pewnej podróży do kraju kwitnącej wiśni...

Cofnijmy się w czasie

Powróćmy do początku lat 90., kiedy to Martin Gren, współzałożyciel Axis, odbywał podróż służbową do Tokio, na spotkanie z potencjalnymi klientami. Jeden z nich zaprosił go do współpracy przy dystrybucji kamer analogowych, ale według Grena produkt ten nie znalazłby odbiorców. Wówczas padła propozycja, by kamery te podłączyć do sieci internetowej – japoński kontrahent wiedział bowiem, że szwedzka firma pracuje nad innowacjami w zakresie rozwiązań sieciowych. Obie strony dostrzegły potencjał tego pomysłu, iskierka pod jego realizację zaczęła się tlić.

Co ciekawe, Gren nie wiedział wtedy, że jeden z inżynierów Axis, Carl-Axel Alm, był właśnie w trakcie opracowywania prototypu sieciowego systemu wideokonferencji. Kiedy Martin wrócił z Japonii z nowym pomysłem i zobaczył nad czym pracuje jego kolega, zdał sobie sprawę, że tak naprawdę firma jest już bliska jego urzeczywistnienia. Martin niezwłocznie zaproponował użycie nowego sprzętu do stworzenia kamery sieciowej.

Mamy to!

Warto pamiętać, że projektując sieciową kamerę wideo, czyli taką, która jednocześnie odbiera dane „sterujące" ze strony operatora, a z drugiej przesyła z powrotem nagrane obrazy przez Internet, cały proces rozwijania produktu następował w czasie, gdy sieć internetowa nie była powszechnie znana i używana. Internet wykorzystywały głównie wyspecjalizowane firmy i instytucje. Zespół inżynierski Axis musiał zatem zbudować produkt na bazie technologii, która była wówczas dostępna.

Pierwsza sprzedaż i narodziny ARTPEC

Założyciele i inżynierowie Axis po doświadczeniach na rozmaitych targach branżowych, takich jak IFSEC, zdali sobie sprawę, że czeka ich dużo pracy, ale z pewnością opłaci się ona w dłuższej perspektywie, ponieważ nie mieli konkurencji, a istniejąca technologia analogowa była przestarzała, podobnie jak sam model biznesowy branży dozoru wizyjnego.

Model ten polegał na sprzedaży produktów bezpośrednio integratorom i użytkownikom końcowym. Axis działał w ramach bardziej rygorystycznego schematu – szwedzka firma sprzedawała bowiem swoje produkty tylko dystrybutorom, którzy następnie sprzedawali je wybranym integratorom. Nie było wyjątków. Taki dwupoziomowy model biznesowy był znacznie bardziej skalowalny. Ponadto, w przeciwieństwie do wielu innych firm, Axis miał doświadczenie w operowaniu na rynku informatycznym i kompetencje w tworzeniu własnych komponentów. To znaczący atut, ponieważ kamery sieciowe wymagały opracowania całego ekosystemu IT, w tym oprogramowania, serwerów, przełączników i routerów.

Design – nowatorski, ale...

Firma Axis nie tylko zmieniała wnętrze kamer, ale też ich design, tak aby odejść od ciężkich wizualnie kształtów „cegły" i zarazem przystosować ich wygląd do większej funkcjonalności. Ten na owe czasy dość rewolucyjny projekt miał kilka skutków ubocznych – *Wzornictwo kamery sieciowej Axis trafiło wówczas na pierwsze strony wielu magazynów komputerowych, ponieważ było nietuzinkowe. Z drugiej strony, mieliśmy niemałe problemy z wyprodukowaniem obudowy, która w pełni pasowałaby do kamery* – wyjaśnia Carl-Axel.

Ograniczenia biznesowe i nowy rozdział w historii firmy

Dalszy rozwój produktu, wchodzenie na nowe rynki, inwestycje w kadry, planowanie rozwiązań komplementarnych – firma Axis musiała zmierzyć się z nowymi wyzwaniami. Zespół nigdy nie zniechęcał się trudnościami. Niewątpliwym wyzwaniem było przekonanie kierownictwa do produktu, który w latach dziewięćdziesiątych praktycznie nie istniał i początkowo nie był dobrze odbierany przez branżę. Ówczesne innowacje polegały głównie na rozszerzeniach lub ulepszeniach już istniejących produktów, co było łatwiejsze do promowania zarówno względem klientów, jak i zarządu.

Podczas spotkania z zarządem Axis próbowałem przekonać ich, że tworzymy coś wielkiego To był prawdziwy game-changer! Rozwiązanie to przekształciło się później w serwer web'owy z obrazowaniem na żywo. Ostatecznie umówiliśmy się z zarządem, że mamy sprzedać 10 000 sztuk w ciągu dwóch lat. Po tych dwóch latach osiągnęliśmy wynik 14 000 sztuk. Martin Gren dostał swój własny dział poświęcony kamerom. To był początek nowej ery dla Axis.

Mały krok Axis, to olbrzymi skok dla branży dozoru wideo

Na szczęście Martin i Carl-Axel nie pozwolili, aby przeszkody wyhamowały projekt AXIS 200. Urządzenie sieciowe, od którego to wszystko się zaczęło, dało technologiczne i biznesowe podwaliny pod inteligentny monitoring, ale też pod inne sieciowe systemy powiązane, tj. w zakresie analizy danych, kontroli dostępu i komunikacji audio.

1.	Dystrybutor
2.	Producent
3.	Fotografia urządzeń
4.	Nazwa systemu
5.	Numer certyfikatu CNBOP oraz data ważności
6.	Szczególne właściwości CDSO (centrali DSO)
7.	Zastosowane głośniki
8.	Linie głośnikowe
9.	Sposób kontroli linii głośnikowych
10.	Rodzaj interfejsu wywołań strefowych CSP – DSO
11.	Maksymalna liczba stref obsługiwanych przez system DSO
12.	Maksymalna liczba komunikatów alarmowych nadawanych jednocześnie do wybranych stref
13.	Liczba kanałów audio
14.	Mikrofon strażaka
15.	Liczba stref obsługiwanych przez mikrofon pożarowy
16.	Możliwość wyniesienia mikrofonów poza pokój centrum alarmowego
17.	Maksymalny czas łączny zapisywalnych komunikatów, w tym alarmowych i ewakuacyjnych
18.	Stan transmisji komunikatu alarmowego
19.	Sygnalizacja akustyczna stanu transmisji komunikatu alarmowego
20.	Opóźnienie transmisji komunikatu alarmowego
21	Zrozumiałość mowy (w skali CIS)
22.	Fazy ewakuacji – organizacja alarmowania
23.	Ręczne wyłączanie (wyciszanie) transmisji komunikatu alarmowego
24.	Ręczne kasowanie stanu transmisji komunikatu alarmowego
25.	Połączenie DSO z SSP
26.	Wyjście dla urządzeń przeciwpożarowych
27.	Wyjście stanu transmisji komunikatu alarmowego
28.	Uszkodzenia monitorowane przez CDSO
29.	Stan uszkodzenia
30.	Sygnały uszkodzeniowe toru transmisji do CSP
31.	Sygnały uszkodzeniowe ze stref transmisji komunikatu alarmowego
32.	Stan zablokowania
33.	Ręczne uruchamianie stanu transmisji komunikatu alarmowego
34.	Interfejs do zewnętrznych urządzeń sterujących
35.	Napięcie zasilania systemu
36.	Pojemności akumulatorów obsługiwanych przez pojedynczą jednostkę zasilania awaryjnego
37.	Maksymalna liczba jednostek zasilania awaryjnego
38.	Maksymalna liczba wzmacniaczy systemowych
39.	Rodzaje wzmacniaczy systemowych, np. klasa d
40.	Zakres temperatury pracy systemu DSO
41.	Klasa odporności IP
42.	Rodzaj szafy instalacyjnej / sposób instalowania
43.	Czy system posiada wejścia dodatkowe, np. wejście sygnału tła muzycznego
44.	Możliwości konfiguracji DSO: • autonomiczny, • skupiony, • rozproszony
45.	Maksymalna odległość wyniesienia szaf
46.	Wymagania dotyczące konstrukcji
47.	Rezerwowe wzmacniacze mocy

1.	**TOA Electronics Europe GmbH Sp. z o.o. Oddział w Polsce** ul. Migdałowa 4, 02-796 Warszawa tel. 022-645-11-98	
2.	TOA Corporation 7-2-1 Minatojima-Nakamachi, Chuo-ku, Kobe 650-0046, Japonia	
3.		
4.	VM-3000	VX-3000
5.	Certyfikat zgodności EN 54-16 nr 1438/CPR/0180 ważny do 25.02.2025. Świadectwo dopuszczenia nr 2318/2015 ważne do 04.03.2020 r.	Certyfikat zgodności EN 54-16 nr 1134/CPR/195 ważny bezterminowo. Świadectwo dopuszczenia nr 2905/2017 ważne do 20.04.2022 r.
6.	– uniwersalny, kompaktowy system do wszelkich aplikacji o nieskomplikowanej ewakuacji	Innowacyjny i przełomowy w technologii system do wszelkich aplikacji. Wyjątkowa oszczędność energii i niewielkie rozmiary systemu w stosunku do oferowanej mocy. Ponadnormatywna niezawodność i najwyższa jakość prosto z Japonii. Rozszerzenie funkcji muzycznych systemu o DSP, eliminator sprzężeń, pełen zakres ustawień parametrów dźwięku zaczerpniętych z profesjonalnych matryc audio czyni VX-3000 doskonałym narzędziem do dystrybucji audio wysokiej jakości do wielu stref.
7.	Głośniki certyfikowane do stosowania z dźwiękowym systemem ostrzegawczym każdego rodzaju (100V/70V/50V)	Głośniki certyfikowane do stosowania z dźwiękowym systemem ostrzegawczym każdego rodzaju (100V/70V/50V)
8.	Promieniowe z rozgałęzieniami lub pętlowe	Promieniowe z rozgałęzieniami lub pętlowe
9.	Pomiar impedancji lub kontrola za pomocą modułu końca linii (EOL) lub izolatory pętli zwarć	Pomiar impedancji lub kontrola za pomocą modułu końca linii (EOL) lub obie metody jednocześnie
10.	Hardware'owy (styk sterujący)	Hardware'owy (styk sterujący) lub software'owy; możliwość współpracy z dowolnym systemem BMS
11.	60	2560
12.	2	640
13.	2/1	640
14.	Tak	Tak
15.	60 pojedynczych stref lub grup stref	2560 stref lub grup stref
16.	Tak	Tak
17.	8 komunikatów	Ponad 1000 komunikatów wewnętrznych
18.	Tak	Tak
19.	Tak	Tak
20.	Nie	Nie
21	Najwyższa możliwa przy poprawnym projekcie i wykonaniu instalacji	
22.	Nie	Tak
23.	Tak	Tak
24.	Tak	Tak
25.	Hardware'owe (styki sterujące)	Hardware'owe (styki sterujące) lub software'owe; możliwość współpracy z dowolnym systemem BMS
26.	Tak	Tak
27.	Tak	Tak
28.	Uszkodzenie wszystkich obwodów, w tym: jednostek centralnych CPU, pamięci wewnętrznej, generatora komunikatów, bezpieczników, zasilania, akumulatorów, wzmacniaczy, linii głośnikowych, torów transmisji SAP-DSO, mikrofonu strażaka (test akustyczny) itp.	Uszkodzenie wszystkich obwodów, w tym: jednostek centralnych CPU, pamięci wewnętrznej, generatora komunikatów, bezpieczników, zasilania, akumulatorów, wzmacniaczy, linii głośnikowych, torów transmisji SAP-DSO, mikrofonu strażaka (test akustyczny), połączenia sieciowego itp.
29.	Tak	Tak
30.	Tak	Tak
31.	Tak	Tak
32.	Nie	Tak
33.	Tak	Tak
34.	Tak	Tak
35.	230 VAC	230 VAC
36.	całkowita pojemność akumulatorów obliczana jest na podstawie bilansu zapotrzebowania na moc dla całego systemu	całkowita pojemność akumulatorów obliczana jest na podstawie bilansu zapotrzebowania na moc dla całego systemu
37.	10 zależnie od konfiguracji	640 zależnie od konfiguracji
38.	10 + 1 rezerwowy	640
39.	Klasa wzmacniaczy AB: 1 x 240 W, 1x 360 W	Klasa wzmacniaczy D: 150 W, 300 W, 500 W
40.	-25 ÷ 45	-25 ÷ 45
41.	Minimum IP30 Dopuszczony montaż bez drzwi frontowych	Minimum IP30 Dopuszczony montaż bez drzwi frontowych
42.	Szafa Rack 19",wymiary podstawy oraz wysokość zależna od złożoności systemu	Szafa Rack 19",wymiary podstawy oraz wysokość zależna od złożoności systemu
43.	Tak	Tak
44.	Tak Tak Nie	Tak Tak Tak
45.	Nie dotyczy	30 km
46.	Nie dotyczy	Nie dotyczy
47.	Tak	Tak

1.	Dystrybutor
2.	Producent
3.	Fotografia urządzeń
4.	Nazwa systemu
5.	Numer certyfikatu CNBOP oraz data ważności
6.	Szczególne właściwości CDSO (centrali DSO)
7.	Zastosowane głośniki
8.	Linie głośnikowe
9.	Sposób kontroli linii głośnikowych
10.	Rodzaj interfejsu wywołań strefowych CSP – DSO
11.	Maksymalna liczba stref obsługiwanych przez system DSO
12.	Maksymalna liczba komunikatów alarmowych nadawanych jednocześnie do wybranych stref
13.	Liczba kanałów audio
14.	Mikrofon strażaka
15.	Liczba stref obsługiwanych przez mikrofon pożarowy
16.	Możliwość wyniesienia mikrofonów poza pokój centrum alarmowego
17.	Maksymalny czas łączny zapisywalnych komunikatów, w tym alarmowych i ewakuacyjnych
18.	Stan transmisji komunikatu alarmowego
19.	Sygnalizacja akustyczna stanu transmisji komunikatu alarmowego
20.	Opóźnienie transmisji komunikatu alarmowego
21	Zrozumiałość mowy (w skali CIS)
22.	Fazy ewakuacji – organizacja alarmowania
23.	Ręczne wyłączanie (wyciszanie) transmisji komunikatu alarmowego
24.	Ręczne kasowanie stanu transmisji komunikatu alarmowego
25.	Połączenie DSO z SSP
26.	Wyjście dla urządzeń przeciwpożarowych
27.	Wyjście stanu transmisji komunikatu alarmowego
28.	Uszkodzenia monitorowane przez CDSO
29.	Stan uszkodzenia
30.	Sygnały uszkodzeniowe toru transmisji do CSP
31.	Sygnały uszkodzeniowe ze stref transmisji komunikatu alarmowego
32.	Stan zablokowania
33.	Ręczne uruchamianie stanu transmisji komunikatu alarmowego
34.	Interfejs do zewnętrznych urządzeń sterujących
35.	Napięcie zasilania systemu
36.	Pojemności akumulatorów obsługiwanych przez pojedynczą jednostkę zasilania awaryjnego
37.	Maksymalna liczba jednostek zasilania awaryjnego
38.	Maksymalna liczba wzmacniaczy systemowych
39.	Rodzaje wzmacniaczy systemowych, np. klasa d
40.	Zakres temperatury pracy systemu DSO
41.	Klasa odporności IP
42.	Rodzaj szafy instalacyjnej / sposób instalowania
43.	Czy system posiada wejścia dodatkowe, np. wejście sygnału tła muzycznego
44.	Możliwości konfiguracji DSO: • autonomiczny, • skupiony, • rozproszony
45.	Maksymalna odległość wyniesienia szaf
46.	Wymagania dotyczące konstrukcji
47.	Rezerwowe wzmacniacze mocy

1.	SCHRACK SECONET
2.	g+m
3.	
4.	APS®-APROSYS
5.	1438-CPR-0176, 01.11.2026
6.	• możliwość budowy systemu liniowego, pętlowego z izolatorami zwarć lub mieszanego; • możliwość rozgłaszania komunikatów słownych za pośrednictwem połączenia telefonicznego; • możliwość rozgłaszania komunikatów lub BGM zgodnie z przyjętym w obiekcie harmonogramem; • optymalizacja mocy w systemie – selektory stref; • wysoka sprawność wzmacniaczy – powyżej 82%; • wzmacniacz rezerwowy w osobnej obudowie z własną sekcją zasilania; • brak konieczności stosowania dodatkowego chłodzenia w szafie RACK; • integracja cyfrowa z systemem zarządzania bezpieczeństwem pożarowym SIS-FIRE
7.	ic audio, g+m, inne
8.	Linie promieniowe, Pętle głośnikowe z izolatorami zwarć
9.	Metoda impedancyjna lub system pętlowy z izolatorami zwarć
10.	Przekaźnikowy
11.	Autonomiczny / Skupiony – 128, Rozproszony B/O
12.	Autonomiczny/skupiony – 4 Rozproszony – 2044
13.	B/O
14.	Spełnia
15.	56 / APS-356.2-3AL-EV, 216/ APS-388.1-3AL-EV
16.	Tak
17.	Zależnie od liczby modułów APS-19.2 w systemie
18.	Spełnia
19.	Spełnia
20.	Spełnia
21	Spełnia
22.	Spełnia
23.	Spełnia
24.	Spełnia
25.	Analogowe, cyfrowe
26.	Spełnia
27.	Spełnia
28.	Spełnia
29.	Spełnia
30.	Spełnia
31.	Spełnia
32.	Spełnia
33.	Spełnia
34.	Spełnia
35.	230 V AC
36.	24 Ah
37.	Zależna od konfiguracji CDSO
38.	Autonomiczny / Skupiony – 128 Rozproszony B/O
39.	Klasa D
40.	Zgodnie z PN-EN 54-16
41.	Zgodnie z PN-EN 54-16
42.	RACK: ZPAS (600X600) ZPAS (600x800)
43.	Tak + regulatory głośności
44.	Tak Tak Tak
45.	B/O
46.	Spełnia
47.	Tak

1.	Producent, dystrybutor
2.	Nazwa i informacja o systemie oraz fotografia urządzeń
3.	Typ lub inne oznaczenie centrali
4.	Zgodność z wymaganiami
5.	Rodzaj centrali (adresowalna / nieadresowalna)
6.	Zasilanie rezerwowe (wewn./zewn.)
7.	Zasilacz znajduje się w obudowie centrali (tak / nie)
8.	Napięcie zasilania centrali
9.	Napięcie wyjściowe zasilacza (napięcie znamionowe pracy) [V DC]
10.	Zasilanie rezerwowe
11.	Maksymalne ciągłe obciążenie zasilacza [A]
12.	Maksymalna pojemność akumulatorów [Ah]
13.	Maksymalny prąd ładowania [A]
14.	Sygnalizacja obniżenia napięcia baterii (tak / nie)
15.	Napięcie odcięcia baterii akumulatorów [V DC]
16.	Rodzaj linii dozorowych (pętlowe / otwarte)
17.	Liczba linii dozorowych / oraz maksymalna liczba linii dozorowych (szt.)
18.	Maks. liczba elementów w linii dozorowej (bez linii bocznych / z uwzględnieniem linii bocznych)
19.	Dopuszczalna rezystancja linii (≤ Ω)
20.	Dopuszczalna pojemność skuteczna linii (≤ nF)
21.	Sposób izolacji zwarć w linii: • ograniczenie prądowe w obwodzie wyj. centrali, • autonomiczne izolatory instalowane w linii, • izolator w każdym elemencie liniowym
22.	Liczba programowanych wejść kontrolnych
23.	Maksymalna liczba nadzorowanych linii sygnałowych (do podłączenia sygnalizatorów akustycznych z możliwością ich wyciszenia) (szt.)
24.	Wyjścia przekaźnikowe bezpotencjałowe (podać dodatkowo obciążalność styków w [A] / [V]) (szt.)
25.	Wyjścia przekaźnikowe potencjałowe (szt.)
26.	Przekaźnik uszkodzenia
27.	Wyjścia potencjałowe typu OC (szt.)
28.	Programowalne wyjścia alarmowe
29.	Wejścia sterujące: • nadzorowane (szt.), • nienadzorowane (szt.)
30.	Opóźnienia sygnałów na wyjściach (tak / nie)
31.	Możliwość pracy sieciowej (tak / nie)
32.	Pojemność pamięci zdarzeń
33.	Pojemność licznika alarmowania
34.	Wyświetlacz
35.	Interfejs komunikacyjny (np. USB)
36.	Zakres temperatury
37.	Maksymalna wilgotność
38.	Wymiary
39.	Masa (bez akumulatorów)

1.	Panasonic Fire & Security Europe AB RAJ International Sp. z o.o.
2.	Centrala EBL512 G3 – mikroprocesorowa **z czujkami**: kompensującymi zabrudzenie, wykrywającymi pożary tlewne, kompensującymi chwilowe zadymienia. Odczyt zadymienia każdej czujki w [%/m]. **Sterowania**: warunki sterujące z użyciem algebry Bool'a, opóźnienie włączenie, wyłączenia, sterowanie impulsem, sterowanie z pierwszej czujki w alarmie. Bardzo prosta konstrukcja warunków sterujących z użyciem numeru prezentacyjnego alarmu (strefa-adres w strefie). **Wejścia programowane** jako: uszkodzenia, interlokingi, alarmy techniczne, ewakuacja, wejście pożarowe, kanały czasowe. **Sieć central** (do 30) – komunikacja po TLON-ie przewodowo lub po światłowodach.
3.	5000PRTPL / 5000PL / 5001PL
4.	EN54 / PN-EN 54
5.	Adresowalna
6.	Akumulatory 24 V DC wewnętrzne lub zewnętrzne
7.	Tak
8.	230 V AC / 24 VDC
9.	24 V DC
10.	24 V DC
11.	6,5 A
12.	65 Ah
13.	2,4 A
14.	Tak
15.	21,6 V DC
16.	Pętlowe (otwarte pakiet 4580 czujek konwencjonalnych)
17.	4 / 4
18.	254
19.	42,6 Ω
20.	140 nF / km
21.	• ograniczenie prądowe w obwodzie wyj. centrali, • autonomiczne izolatory instalowane w linii, • izolator w każdym elemencie liniowym
22.	512
23.	4
24.	2 + 8 x 6 / 2 A; 30 V
25.	Nie ma
26.	1 (ogólny do monitoringu)
27.	Nie ma
28.	2 (w samej centrali) / 512 (z urządzeniami pętlowymi)
29.	• 400 (interlokingi) • 512
30.	Tak
31.	Tak
32.	1000 / 10 000
33.	1000
34.	ciekłokrystaliczny
35.	Web serwer / EBLnet / EBLTalk / Tateco / OPCserwer / MODBUS / SIA / ESPA 4.4.4
36.	-5 ÷ +40°C
37.	< 95%
38.	5000: 438 x 628 x 187 mm / 5001: 418 x 625 x 177 mm
39.	5000: 23,1 kg / 5001: 19 kg

1.	Producent, dystrybutor
2.	Nazwa i informacja o systemie oraz fotografia urządzeń
3.	Typ lub inne oznaczenie centrali
4.	Zgodność z wymaganiami
5.	Rodzaj centrali (adresowalna / nieadresowalna)
6.	Zasilanie rezerwowe (wewn./zewn.)
7.	Zasilacz znajduje się w obudowie centrali (tak / nie)
8.	Napięcie zasilania centrali
9.	Napięcie wyjściowe zasilacza (napięcie znamionowe pracy) [V DC]
10.	Zasilanie rezerwowe
11.	Maksymalne ciągłe obciążenie zasilacza [A]
12.	Maksymalna pojemność akumulatorów [Ah]
13.	Maksymalny prąd ładowania [A]
14.	Sygnalizacja obniżenia napięcia baterii (tak / nie)
15.	Napięcie odcięcia baterii akumulatorów [V DC]
16.	Rodzaj linii dozorowych (pętlowe / otwarte)
17.	Liczba linii dozorowych / oraz maksymalna liczba linii dozorowych (szt.)
18.	Maks. liczba elementów w linii dozorowej (bez linii bocznych / z uwzględnieniem linii bocznych)
19.	Dopuszczalna rezystancja linii (≤ Ω)
20.	Dopuszczalna pojemność skuteczna linii (≤ nF)
21.	Sposób izolacji zwarć w linii: • ograniczenie prądowe w obwodzie wyj. centrali, • autonomiczne izolatory instalowane w linii, • izolator w każdym elemencie liniowym
22.	Liczba programowanych wejść kontrolnych
23.	Maksymalna liczba nadzorowanych linii sygnałowych (do podłączenia sygnalizatorów akustycznych z możliwością ich wyciszenia) (szt.)
24.	Wyjścia przekaźnikowe bezpotencjałowe (podać dodatkowo obciążalność styków w [A] / [V]) (szt.)
25.	Wyjścia przekaźnikowe potencjałowe (szt.)
26.	Przekaźnik uszkodzenia
27.	Wyjścia potencjałowe typu OC (szt.)
28.	Programowalne wyjścia alarmowe
29.	Wejścia sterujące: • nadzorowane (szt.), • nienadzorowane (szt.)
30.	Opóźnienia sygnałów na wyjściach (tak / nie)
31.	Możliwość pracy sieciowej (tak / nie)
32.	Pojemność pamięci zdarzeń
33.	Pojemność licznika alarmowania
34.	Wyświetlacz
35.	Interfejs komunikacyjny (np. USB)
36.	Zakres temperatury
37.	Maksymalna wilgotność
38.	Wymiary
39.	Masa (bez akumulatorów)

1.	SIEMENS Ingenuity for life **Siemens Switzerland Ltd** Building Technologies, Fire Systems Gubelstrasse 22, CH-6301 Zug Siemens Sp. z o.o. ul. Żupnicza 11, 03-821 Warszawa					
2.	System sygnalizacji pożaru FS720 jest nową ogólnoświatową generacją central pożarowych Cerberus®PRO firmy Siemens. Łączy wysokie standardy bezpieczeństwa z innowacyjnością oraz nowoczesną technologią. Zapewnia wysoką elastyczność umożliwiając tworzenie systemów o różnej skali złożoności zaczynając od systemów autonomicznych po rozległe rozwiązania sieciowe. Innowacyjne redundantne węzły sieciowe wyznaczają nie tylko nowy standard w zakresie odporności na uszkodzenia, ale również szybki przesył danych. Przy zastosowaniu światłowodowej sieci szkieletowej możemy połączyć ze sobą do 14 klastrów (maksymalnie do 16 stacji na klaster). Topologia ta umożliwia tworzenie sieci zgodnych z normą EN-54 zawierającą do 64 stacji. Kompaktowe i modułowe centrale mikroprocesorowe o pojemności od 126 (FC721) do 1 512 (FC726) adresów charakteryzują się: • Praca zarówno w wersji autonomicznej jak i sieciowej (nie dotyczy FC721) • Redundantna sieć, pracująca w trybie awaryjnym zgodnie z EN54 • Interfejs Ethernet • Szereg opcji takich jak: drukarka, klucz dostępowy, wskaźniki diodowe, tablice synoptyczne, konwertery światłowodowe, porty RS232 i RS485 • Wykrywanie i automatyczna konfiguracja wszystkich urządzeń • Panele informacyjne i kontrolne oraz sygnalizatory instalowane bezpośrednio na magistrali (C-NET) • Elastyczne oprogramowanie centrali i sterowań systemowych • Podłączenie do systemu zarządzania bezpieczeństwem za pomocą BACnet-u • Możliwość migracji systemów poprzednich generacji					
3.	FC361	FC721	FC722	FC723 (modułowa)	FC724	FC726 (modułowa)
4.	0832-CPR-F1346 CNBOP 3111/2018 LPCB 531q/03	0786-CPR-20767 CNBOP 2410/2015 FM 3051081 LPCB 126bn/05	0786-CPR-20721 CNBOP 2410/2015 VdS G209076 FM 3051081 DNV GL (marine) MEDV00003US LPCB 126bn/06	0786-CPR-21328 CNBOP 2410/2015 VdS G214021 LPCB 126bn/09	0786-CPR-20722 CNBOP 2410/2015 VdS G209077 FM 3051081 DNV GL (marine) MEDV00003US LPCB 126bn/07	0786-CPR-20983 CNBOP 2410/2015 VdS G210084 FM 3051081 LPCB 126bn/08
5.	adresowalna					
6.	wewnętrzne					
7.	tak					
8.	85…265 VAC 50/60 Hz					
9.	20.5...28.6	20.5...28.6	20.5...28.6 /21…28,4	21…28,4		
10.						
11.	2,5	2,5	2,5 / 5,0		5,0	
12.	12 / 25	7	12 / 26	26	26	45
13.	1,6	1,6	1,6 / 5		5	
14.	Tak					
15.	20,5	20,5	20,5 / 21		21	
16.	pętlowe / otwarte					
17.	1	1	2 / 4	2 / 12	4 / 8	4 / 28
18.	126	126	252			
19.	240					
20.	500					
21.	izolator w każdym elemencie liniowym					
22.	4	4	8	8/32	12	12/72
23.	2 / 6	1 / 4	1/4	2/24	2/8	2/48
24.	3 (2A@60V DC)	2 (0,4A @ 60 V DC)	2 (0,4A @ 60 V DC)	2 (0,4A @ 60 V DC) / 4 (0,4A @ 36V DC)	2 (0,4A @ 60 V DC)	2 (0,4A @ 60 V DC) / 10 (0,4A @ 36V DC)
25.	0 / 4	2		2 / 18	2	2 / 42
26.	tak					
27.	4	4	8	8 / 32	12	12 / 72
28.						
29.	– 4	– 4	– 8	– 8/32	– 12	– 12/72
30.	Nie	Tak				
31.	Nie	Tak				
32.	2000	10000				
33.	999	10000				
34.	LCD					
35.	RJ45 (Ethernet), RS232, RS485					
36.	-5…+40	-8…+42				
37.	95% wzgl.					
38.	402 x 372 x 132 402 x 372 x 211	430 x 398 x 103	430 x 398 x 183 430 x 796 x 183	430 x 796 x 183	430 x 796 x 183	430 x 796 x 283
39.	5.24 kg 6.44 kg	6.784 kg 6.904 kg	8.576 kg / 8.696 kg 14.658 kg / 15.207 kg	16.495 kg	15.061 kg 15.313 kg	21.143 kg

1.

SCHRACK SECONET AG
Eibesbrunnergasse 18, A-1120 Wiedeń, Austria
Schrack Seconet Polska Sp. z o.o., ul. Adama Branickiego 15, 02-972 Warszawa
tel. +48 22 33 00 620-623, faks. +48 22 33 00 624

2.

System sygnalizacji pożarowej Integral IP posiada następujące parametry/funkcje:

1. Niezawodność działania i elastyczna architektura systemu
   - 100% redundancja wszystkich komponentów architektury sprzętowej i programowej CSP/CSG;
   - modułowa i zdecentralizowana budowa systemu;
   - elastyczne oprogramowanie umożliwiające zdefiniowanie dowolnych algorytmów sterowań;
   - element składowy zintegrowanego systemu zarządzania bezpieczeństwem pożarowym SIS-FIRE – centrala sterująca urządzeniami przeciwpożarowymi;
   - rozszerzona pamięć zdarzeń – 65 000 zdarzeń;
   - kompatybilność „wstecz" i „w przód";
   - możliwość wyboru jednej z 4 wersji językowych „online"
   - wyjścia sterujące z funkcją „fail-safe",
   - możliwość filtrowania informacji dla paneli obsługi i drukarki,
   - nadzorowanie instalacji tryskaczowych zgodnie z VdS CEA 4001.
2. Praca w sieci – techniki Integral LAN (do 16 central) i Integral WAN (do 4048 central)
   - możliwość pracy w różnych konfiguracjach
     a) sieć w układzie otwartym (redundantna linia),
     b) sieć w układzie zamkniętym (redundantna pętla),
     c) sieć kratowa (4 połączenia redundantne na każdą centralę)
   - komunikacja w sieci za pomocą protokołu TCP/IP,
   - możliwość pracy w sieci równorzędnej i hierarchicznej,
   - zastosowanie zdublowanych torów miedzianych i światłowodowych.
3. Możliwość sterowania Stałymi Urządzeniami Gaśniczymi
   - możliwość pracy w trybie dualnym (CSP + CSG),
   - sterowanie do 8(10) stref gaszenia z jednej centrali Integral IP MX,
   - możliwość sieciowania CSP i CSG.
4. Zdalny Dostęp do systemu i opcje powiadamiania – Remote Integral
   - dostęp do systemu z dowolnego miejsca na świecie (połączenie TCP/IP);
   - możliwość zdalnej obsługi, konfiguracji i uruchamiania,
   - narzędzia/aplikacje do obsługi mobilnej i stacjonarnej,
   - możliwość wysyłania e-maili o alarmach, uszkodzeniach i innych stanach systemowych.
5. Współpraca z systemami automatyki budynków (BMS)
   - pełna integracja (protokoły BACnet, OPC, MODBUS, inne);
   - integracja zcentralizowana lub zdecentralizowana

   Urządzenia współpracujące: m.in. interaktywne czujki wielokryteryjne (dymu, ciepła, CO) nowej generacji serii CUBUS (TF1-TF9), ręczne ostrzegacze pożarowe MCP 545X / MCP 535X, moduły we/wy serii X-LINE, czujki zasysające dymu AirSCREEN ASD 53x, liniowe czujki dymu typu SPC-E, FIRERAY, OSID, liniowa czujka ciepła LISTEC, czujki płomienia SPECTREX, TALENTUM, DET-TRONICS, zewnętrzny panel obsługi z/bez drukarki Integral MAP, panel wskazań PIP, panel wskazań B5-EPI-PIC, zewnętrzny panel wskazań dal 64 grup dozorowych B3-MMI-EAT64, zewnętrzny panel wskazań dla 8 stref gaszenia B3-MMI-IPEL, panele obsługi dla PSP.
6. Zgodność z wymaganiami PN-EN 54, PN-EN 12094, CNBOP, VdS

3.	Integral IP MXF	Integral IP CXF	Integral IP BXF
4.	PN-EN 54, VdS, CNBOP	PN-EN 54, VdS, CNBOP	PN-EN 54, VdS, CNBOP
5.	adresowalna	adresowalna	adresowalna
6.	wewn.	wewn.	wewn.
7.	tak	tak	tak
8.	110 VAC -15% – 230 VAC +10%	110 VAC -15% – 230 VAC +10%	110 VAC -15% – 230 VAC +10%
9.	U(0°C) = 28,3 V ± 1 % U(50°C) = 26,3 V ± 1 %	U(0°C) = 28,3 V ± 1 % U(50°C) = 26,3 V ± 1 %	U(0°C) = 28,3 V ± 1 % U(50°C) = 26,3 V ± 1 %
10.	akumulatory kwasowo-ołowiowe SLA, szczelne	akumulatory kwasowo-ołowiowe SLA, szczelne	akumulatory kwasowo-ołowiowe SLA, szczelne
11.	7,5 ± 2%	4 ± 1%	2,5 ± 1%
12.	88 Ah (4 aku. 44 Ah)	34 Ah (4 aku. 17 Ah)	7 Ah (2 aku. 7Ah)
13.	5,28 ± 7%	3,19A ± 7%	1,3 ± 7%
14.	tak	tak	tak
15.	18, 3 ± 3%	18, 3 ± 3%	18, 3 ± 3%
16.	pętlowe/otwarte	pętlowe/otwarte	pętlowe/otwarte
17.	maks. 16	maks. 4	1
18.	250	250	250
19.	≤ 255	≤ 255	≤ 255
20.	≤ 240	≤ 240	≤ 240
21.	obustronny izolator zwarć w każdym elemencie liniowym oraz na wyj/wej z CSP	obustronny izolator zwarć w każdym elemencie liniowym oraz na wyj/wej z CSP	obustronny izolator zwarć w każdym elemencie liniowym oraz na wyj/wej z CSP
22.	maks. 64	maks. 12	2
23.	maks. 64	maks. 10	2
24.	maks. 176 (30 V / 3A); maks. 30 (230 V / 3A) – tylko centrala; dodatkowe wyjścia na modułach pętlowych	maks. 5 (230 V / 3A) – tylko centrala; dodatkowe wyjścia na modułach pętlowych	wyjścia na modułach pętlowych
25.	–	–	–
26.	TAK (dowolnie programowalny)	TAK (dowolnie programowalny)	wyjście na module pętlowym (dowolnie programowalny)
27.	Na karcie we/wy B3-MMI-UIO poprzez magistralę MMI-BUS	Na karcie we/wy B3-MMI-UIO poprzez magistralę MMI-BUS	-
28.	TAK	TAK	TAK
29.	maks. 64	maks. 12	2
30.	tak (dowolnie programowalne)	tak (dowolnie programowalne)	tak (dowolnie programowalne)
31.	tak (4096 CSP w sieci)	tak (4096 CSP w sieci)	Tak (dla celów wizualizacji)
32.	65000	65000	10000
33.	99999	99999	99999
34.	LCD	LCD	LCD
35.	USB, ETHERNET	USB, ETHERNET	USB, ETHERNET
36.	od -5° do +50°C	od -5° do +50°C	od -5° do +50°C
37.	od 5 do 95%, bez kondensacji	od 5 do 95%, bez kondensacji	od 5 do 95%, bez kondensacji
38.	600 × 445 × 225 mm (WxSZxG)	400 x 445 x 140 (W x Sz x G)	300 x 360 x 85 (W x Sz x G)
39.	15 kg	7,6 kg	2,2 kg

1.	Producent, dystrybutor
2.	Nazwa i informacja o systemie oraz fotografia urządzeń
3.	Typ lub inne oznaczenie centrali
4.	Zgodność z wymaganiami
5.	Rodzaj centrali (adresowalna / nieadresowalna)
6.	Zasilanie rezerwowe (wewn./zewn.)
7.	Zasilacz znajduje się w obudowie centrali (tak / nie)
8.	Napięcie zasilania centrali
9.	Napięcie wyjściowe zasilacza (napięcie znamionowe pracy) [V DC]
10.	Zasilanie rezerwowe
11.	Maksymalne ciągłe obciążenie zasilacza [A]
12.	Maksymalna pojemność akumulatorów [Ah]
13.	Maksymalny prąd ładowania [A]
14.	Sygnalizacja obniżenia napięcia baterii (tak / nie)
15.	Napięcie odcięcia baterii akumulatorów [V DC]
16.	Rodzaj linii dozorowych (pętlowe / otwarte)
17.	Liczba linii dozorowych / oraz maksymalna liczba linii dozorowych (szt.)
18.	Maks. liczba elementów w linii dozorowej (bez linii bocznych / z uwzględnieniem linii bocznych)
19.	Dopuszczalna rezystancja linii (≤ Ω)
20.	Dopuszczalna pojemność skuteczna linii (≤ nF)
21.	Sposób izolacji zwarć w linii: • ograniczenie prądowe w obwodzie wyj. centrali, • autonomiczne izolatory instalowane w linii, • izolator w każdym elemencie liniowym
22.	Liczba programowanych wejść kontrolnych
23.	Maksymalna liczba nadzorowanych linii sygnałowych (do podłączenia sygnalizatorów akustycznych z możliwością ich wyciszenia) (szt.)
24.	Wyjścia przekaźnikowe bezpotencjałowe (podać dodatkowo obciążalność styków w [A] / [V]) (szt.)
25.	Wyjścia przekaźnikowe potencjałowe (szt.)
26.	Przekaźnik uszkodzenia
27.	Wyjścia potencjałowe typu OC (szt.)
28.	Programowalne wyjścia alarmowe
29.	Wejścia sterujące: • nadzorowane (szt.), • nienadzorowane (szt.)
30.	Opóźnienia sygnałów na wyjściach (tak / nie)
31.	Możliwość pracy sieciowej (tak / nie)
32.	Pojemność pamięci zdarzeń
33.	Pojemność licznika alarmowania
34.	Wyświetlacz
35.	Interfejs komunikacyjny (np. USB)
36.	Zakres temperatury
37.	Maksymalna wilgotność
38.	Wymiary
39.	Masa (bez akumulatorów)

1.	**SATEL** Lista dystrybutorów dostępna na www.satel.pl			
2.	System sygnalizacji pożarowej CSP	System sygnalizacji pożarowej CSP	System sygnalizacji pożarowej CSP	System sygnalizacji pożarowej CSP
3.	CSP-208	CSP-108	CSP-204	CSP-104
4.	CPR (zgodność z EN 54-2, EN 54-4) Świadectwo Dopuszczenia	CPR (zgodność z EN 54-2, EN 54-4) Świadectwo Dopuszczenia	CPR (zgodność z EN 54-2, EN 54-4) Świadectwo Dopuszczenia	CPR (zgodność z EN 54-2, EN 54-4) Świadectwo Dopuszczenia
5.	nieadresowalna	nieadresowalna	nieadresowalna	nieadresowalna
6.	Pojedynczy akumulator 12V umieszczony w obudowie centrali.	Pojedynczy akumulator 12V umieszczony w obudowie centrali.	Pojedynczy akumulator 12V umieszczony w obudowie centrali.	Pojedynczy akumulator 12V umieszczony w obudowie centrali.
7.	tak	tak	tak	tak
8.	230 V AC/12 V DC	230 V AC/12 V DC	230 V AC/12 V DC	230 V AC/12 V DC
9.	nie specyfikujemy	nie specyfikujemy	nie specyfikujemy	nie specyfikujemy
10.	Pojedynczy akumulator 12 V	Pojedynczy akumulator 12 V	Pojedynczy akumulator 12 V	Pojedynczy akumulator 12 V
11.	2,5 A	2,5 A	2,5 A	2,5 A
12.	w obudowie centrali 17 Ah/18 Ah/22 Ah, w dodatkowym pojemniku akumulatorów 24 Ah	w obudowie centrali 17 Ah/18 Ah/22 Ah, w dodatkowym pojemniku akumulatorów 24 Ah	w obudowie centrali 17 Ah/18 Ah/22 Ah,	w obudowie centrali 17 Ah/18 Ah/22 Ah,
13.	1,4 A	1,4 A	1,4 A	1,4 A
14.	tak	tak	tak	tak
15.	11,5 V awaria akumulatora, Około 10,5 V odcięcie	11,5 V awaria akumulatora, Około 10,5 V odcięcie	11,5 V awaria akumulatora, Około 10,5 V odcięcie	11,5 V awaria akumulatora, Około 10,5 V odcięcie
16.	konwencjonalna	konwencjonalna	konwencjonalna	konwencjonalna
17.	8	8	4	4
18.	32 czujniki na linii lub 10 ROP	32 czujniki na linii lub 10 ROP	32 czujniki na linii lub 10 ROP	32 czujniki na linii lub 10 ROP
19.	100 Ω (2 x 50 Ω)	100 Ω (2 x 50 Ω)	100 Ω (2 x 50 Ω)	100 Ω (2 x 50 Ω)
20.	brak wymagań	brak wymagań	brak wymagań	brak wymagań
21.	brak izolatorów zwarć	brak izolatorów zwarć	brak izolatorów zwarć	brak izolatorów zwarć
22.	4	4	4	4
23.	2 wyjścia kontrolowane	2 wyjścia kontrolowane	2 wyjścia kontrolowane	2 wyjścia kontrolowane
24.	8 sztuk 2 A 30 V DC	8 sztuk 2 A 30 V DC	4 sztuk 2 A 30 V DC	4 sztuk 2 A 30 V DC
25.	brak	brak	brak	brak
26.	Tak, programowalny	Tak, programowalny	Tak, programowalny	Tak, programowalny
27.	brak	brak	brak	brak
28.	Tak	Tak	Tak	Tak
29.	4 wejścia kontrolowane	4 wejścia kontrolowane	4 wejścia kontrolowane	4 wejścia kontrolowane
30.	tak	tak	tak	tak
31.	nie, (możliwość podłączenia panelu wyniesionego PSP oraz CSP-ETH (virtual panel)	nie, (możliwość podłączenia panelu wyniesionego PSP oraz CSP-ETH (virtual panel)	nie, (możliwość podłączenia panelu wyniesionego PSP oraz CSP-ETH (virtual panel)	nie, (możliwość podłączenia panelu wyniesionego PSP oraz CSP-ETH (virtual panel)
32.	8999	8999	8999	8999
33.	9999	9999	9999	9999
34.	Tak	Nie	Tak	Nie
35.	RS-232	RS-232	RS-232	RS-232
36.	-5…+40 °C	-5…+40 °C	-5…+40 °C	-5…+40 °C
37.	93±3%	93±3%	93±3%	93±3%
38.	324 x 382 x 108 mm	324 x 382 x 108 mm	324 x 382 x 108 mm	324 x 382 x 108 mm
39.	< 3 kg	< 3 kg	< 3 kg	< 3 kg

1.	**Producent:** NSC Sicherheistechnik GmbH **Dystrybutor:** MIWI URMET Sp. z o.o. 91-341 Łódź, ul. Pojezierska 90a	
2.	Solution F2 	Solution F1
3.	Solution F2	Solution F1
4.	EN54 VdS	
5.	Adresowalna	
6.	Wewnętrzne	
7.	Tak	
8.	–	
9.	24Vdc	
10.	2 x akumulator 12V	
11.	3.5 A	6.7 A
12.	26 Ah	65 Ah
13.	1,3 A	3,6 A
14.	Tak	
15.	21,3 V	
16.	Pętlowe i otwarte	
17.	1 pętla, max 2 pętle lub 2 linie otwarte, max 4	2 pętle, max 18 pętli lub 8 linii otwartych, max 72
18.	127 czujników/rop/modułów + 127 sygnalizatorów w gniazdach – protokół HOCHIKI 126 czujników/rop/modułów – protokół APOLLO	
19.	224	
20.	350	
21.	ograniczenie prądowe w obwodzie wyj. centrali, autonomiczne izolatory instalowane w linii, izolator w każdym elemencie liniowym	
22.	12 + 2 wejścia do monitorowania zewnętrznego systemu gaszenia + 4 wejścia monitorowane na dodatkowej karcie sterowania gaszeniem	8 na płycie centrali + 2 do monitorowania zewnętrznego systemu gaszenia + 8 x 4 wejścia monitorowane na dodatkowej karcie sterowania gaszeniem
23.	4 + 2 na karcie sterowania gaszeniem	3 + 8 x 2 na opcjonalnych kartach sterowania gaszeniem
24.	6 x 1 A/30 Vdc + 8 x 5 A/250 V + 2 x 1 A/30Vdc na karcie sterowania gaszeniem	4 x 1 A/30 V + 9 x 8 x 5 A/250 V (opcjonalnie na kartach pętlowych)
25.	4 wyjścia 1.5 A/24 V każde do kontroli zaworów systemu gaszenia na opcjonalnej karcie	8 x 4 wyjścia 1.5 A/24 V każde do kontroli zaworów systemu gaszenia na opcjonalnych kartach
26.	Każde wyjście może być zaprogramowane dla tej funkcji	
27.	17	16 + 9 x 8 na kartach pętlowych, razem 98
28.	–	
29.	Nienadzorowane 8 Nadzorowane 4 + 4 na karcie sterowanie gaszeniem	Nienadzorowane 8 Nadzorowane 1 + 8 x 4 nadzorowane na kartach sterowania gaszeniem
30.	Tak, wyjścia mogą być również impulsowe a także migające	
31.	nie	tak
32.	3000	10 000
33.	3000	10 000
34.	LCD 240 x 60 punktów	
35.	USB ISDN Webserwer RS232 x 2 RS485 x 2	USB ISDN Webserwer RS232 x 2 RS485 x 3 ARCNET redundantny
36.	-5°C – +40°C	
37.	95%	
38.	370 x 320 x 128 mm (obudowa A) 500 x 440 x 175 mm (obudowa B1 i B2)	540 x 492 x 162 mm (obudowy A1 i A2) 540 x 540 x 245 mm ((obudowy B1 i B2)
39.	6,5 kg (obudowa A) 8,5 kg (obudowa B1 i B2)	14 kg (obudowy A1 i A2) 18.5 kg (obudowy B1 i B2)

Prenumerata

Dział prenumeraty

Tel. + 48 22 53 53 229
prenumerata@mediafachowe.pl

Zamówienie prenumeraty przyjmujemy

- Telefonicznie **+ 48 22 53 53 229**
- e-mailem **prenumerata@mediafachowe.pl**
- przez internet **www.czasopisma.net**

Prenumerata

→ **Roczna**	drukowana: **86 zł**	elektroniczna: **bezpłatna**
→ **Dwuletnia**	drukowana: **147 zł**	elektroniczna: **bezpłatna**
→ **Studencka**	drukowana: **66 zł**	elektroniczna: **bezpłatna**

Prenumerata dostępna także przez

- **RUCH S.A.**
- **Kolporter Sp. z o.o. S.K.A.**
- **Garmond Press S.A.**
- **G.L.M. Sp. z o.o.**
- **AS Press Andrzej Szlachciuk**

SKLEP INTERNETOWY
www.czasopisma.net

BEZPŁATNA PRENUMERATA ELEKTRONICZNA DO POBRANIA NA STRONIE
www.ochrona-mienia.pl

Lubię to!

Wejdź na nasz profil i polub nas!

www.facebook.com/ **ochronamieniaiinformacji**

Dwumiesięcznik powstaje we współpracy z:

Kontakt

Ochrona Mienia i Informacji

ISSN 1732-5951 **Rok XXI nr 3/2019 (144)**

www.ochrona-mienia.pl

Czasopismo branży security, pełniące rolę informacyjną, publicystyczną, doradczą oraz promocyjną w zakresie bezpieczeństwa osób, mienia i informacji.

Wydawca:

Mediafachowe, ul. Rosoła 10a
02-786 Warszawa , tel. +48 22 53 53 227

Prezes zarządu: **Katarzyna Polesińska**

Dyrektor wydawnicza

Joanna Jaworska
j.jaworska@euro-media.pl
tel. 606 911 070

Redakcja:

ul. Rosoła 10a, 02-786 Warszawa
redakcja@ochrona-mienia.pl
www.ochrona-mienia.pl

Krzysztof Surdyk
Redaktor Naczelny

tel. 606 911 071
k.surdyk@ochrona-mienia.pl

Lidia Tuchowska
Redaktor/Marketing i PR

tel. 604 995 466
l.tuchowska@ochrona-mienia.pl

Katarzyna Kalata-Kieblesz
Kierownik Działu Reklamy

tel. 604 588 851
k.kalata@ochrona-mienia.pl

Stała współpraca: Edmund Basałyga, Jerzy Ciszewski, Andrzej Dubrawski, Robert Gabrysiak, Sebastian Hładun, Waldemar Kubik, Krzysztof Łangowski, Dobrosław Mąka, Cezary Mecwaldowski, Jarosław Stelmach, Ewa Sobór, Krzysztof Młudzik, Robert Poklek, Jerzy Taczalski, Damian Żabicki.

Zdjęcia: zespół redakcyjny, materiały promocyjne, www.fotolia.com

Łamanie i opracowanie graficzne: Ważka Łukasz Piotrowski

Druk: Drukarnia GREG – Otwock

Prawa autorskie zastrzeżone. Przedruk i wykorzystywanie materiałów możliwe tylko po uzyskaniu pisemnej zgody Wydawcy. Redakcja nie ponosi odpowiedzialności za treść reklam, ogłoszeń oraz artykułów firmowych, ani za opinie wyrażone w artykułach, które pozostają prywatnymi opiniami Autorów.

SpyShop

BEZPIECZNE BIURO

Kompleksowe podejście do zabezpieczenia biur i sal konferencyjnych przed inwigilacją

- Indywidualne projekty systemów zabezpieczających przed wyciekiem widma akustycznego
- Wykrywanie i lokalizacja podsłuchów radiowych
- Sprawdzanie sieci energetycznej, telefonicznej, alarmowej i innych instalacji przewodowych
- Wykrywanie urządzeń rejestrujących
- Zagłuszanie dyktafonów i mikrofonów w telefonach
- Kontrola dostępu

71 341 14 00 www.spyshop.pl

BYDGOSZCZ GDYNIA KATOWICE KRAKÓW POZNAŃ RZESZÓW SZCZECIN WROCŁAW

securex®
POLAND
Międzynarodowe Targi Zabezpieczeń

ZAPRASZA
mtp
GRUPA

21-23.04.2020
POZNAŃ

www.securex.pl

Międzynarodowe
Targi Poznańskie

ZABEZPIECZ SWÓJ SUKCES!