20 lat
ZABEZPIECZENIA

CZASOPISMO BEZPŁATNE
ISSN: 1505-2419 DWUMIESIĘCZNIK NR 2(120)/2018

wydanie specjalne securex POLAND

HID Mobile Access®

Wygoda, inteligencja, bezpieczeństwo

ADVANTAGE HID Platinum Partner

ASSA ABLOY Poland Sp. z o.o.
ul. Jana Olbrachta 94
01-102 Warszawa
Polska

Kamery sieciowe AXIS Q3517-LV oraz AXIS Q3517-LVE

Gdy oczekujesz tylko najlepszych rozwiązań.

Szukasz dyskretnej i solidnej kamery sieciowej zapewniającej obraz w rozdzielczości 5MP przy pełnej poklatkowości, w zmiennym oświetleniu i trudnych warunkach pogodowych? Niezależnie od pory dnia i nocy oraz zastosowania, kamery sieciowe AXIS Q3517-LV oraz AXIS Q3517-LVE dostarczają bezkonkurencyjnej jakości obraz. Wyposażono je w zaawansowane funkcje, dzięki czemu mogą sprostać największym wyzwaniom w zakresie dozoru wizyjnego. Poznaj najlepsze możliwe rozwiązania na rynku.

Dowiedz się więcej na stronie www.axis.com/products/axis-q3517-lv lub na www.axis.com/products/axis-q3517-lve

AXIS COMMUNICATIONS

Najlepsze rozwiązanie do obserwacji tuneli

NXM36 HiPoE

PoE | IP66 | IP68 | IP69

Odporna na korozję obudowa NXM36 Hi-PoE ułatwia instalację kamer IP w trudnych warunkach środowiskowych. Zarówno kamera jak i grzałka systemu usuwającego wilgoć są zasilane metodą High Power PoE za pośrednictwem kabla Ethernet.

Wyposażenie dodatkowe stanowi wycieraczka przedniej szyby ze spryskiwaczem. Obudowa NXM36 może być zainstalowana na głowicy uchylno-obrotowej NXPTH, również wykonanej ze stali nierdzewnej.

VIDEOTEC

VIDEO SECURITY PRODUCTS

www.videotec.com

Made in Italy since 1986

SPIS TREŚCI

8 Nowości produktowe

18 Wydarzenia, informacje

Monitoring

22 **Procedury i instrukcje dotyczące centrum monitorowania**
– Daniel Kamiński

Kontrola dostępu

28 **Rozwój systemów kontroli dostępu na przykładzie zamków ryglujących drzwi**
– Maciej Prelich, Firma ATLine sp.j. Sławomir Pruski

32 **KaDe Premium Plus II. Integracja z rejestratorami IP marki NOVUS i systemem wind**
– Ryszard Sobierski, AAT HOLDING

curex® LAND

Telewizja dozorowa

36 RODO a telewizja dozorowa. Gotowe rozwiązania firmy Hanwha Techwin
– Piotr Rogalewski, Hanwha Techwin Europe

42 Sztuczna inteligencja w systemach bezpieczeństwa
– Maciej Pietrzak, Dahua Technology Poland

46 Dziesięć trendów w 2018 roku
– Johan Paulsson, Axis Communications

Ochrona przeciwpożarowa

52 WES+. Innowacyjny system ochrony przeciwpożarowej na budowie
– Geo-Kat

58 System detekcji gazów SDG 6000. Nowość w ofercie firmy POLON-ALFA
– Mariusz Michałek, POLON-ALFA

62 Ochrona przeciwpożarowa obiektów zabytkowych i muzealnych. Zastosowanie techniki bezprzewodowej
– Arkadiusz Milka, Insap

68 Bezpieczeństwo pożarowe dachów (część 2)
– Maria Dreger, Krzysztof Bagiński, Stowarzyszenie DAFA

74 Strategie ochrony przeciwpożarowej budynków (część 2)
– Dorota Brzezińska, Paul Bryant, Wydział Inżynierii Procesowej i Ochrony Środowiska, Politechnika Łódzka

80 Skuteczność instalacji gaśniczych a minimalizacja strat (część 2)
– Robert Kuczkowski, PZU Lab, Politechnika Łódzka

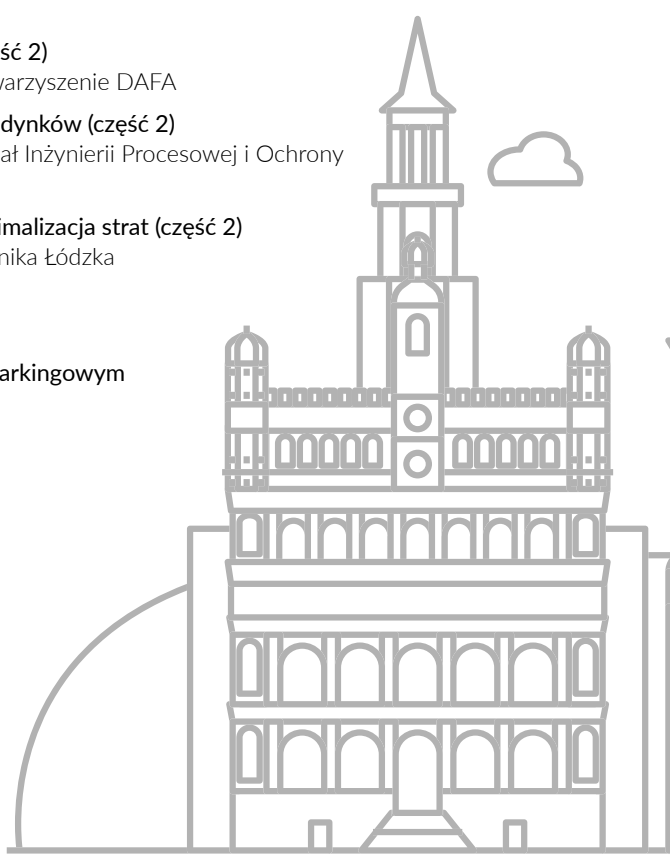
RFID

84 RFID w zautomatyzowanym systemie parkingowym
– Jacek Krywult

86 **Karty katalogowe**

90 **Spis teleadresowy**

94 **Spis reklam**



ZŁOTE MEDALE

SECUREX / POZNAŃ MEDIA EXPO

3x 2 Mpx Kamera multisensorowa 180° HDCVI, tulejowa
Dahua Technology Poland Sp. z o.o., Warszawa

APS-180-LOOP. Moduł linii pętlowych z izolatorami
G + M ELEKTRONIK AG, Szwajcaria
Zgłaszający: SCHRACK SECONET POLSKA Sp. z o.o., Warszawa

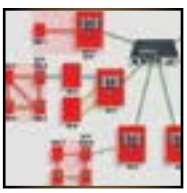
ARGUS 3D
TELBUD S.A., Poznań

Bezzałogowy Statek Powietrzny DC-01 Mucha wraz głowicą obserwacyjną oraz Lekką Mobilną Stacją Kierowania i Kontroli
UAVS Poland Sp. z o.o., Kraków

CENTRALA STERUJĄCA AUTOMATYKĄ POŻAROWĄ TYPU AFG-3
AFG ELEKTRONIKA PRZEMYSŁOWA
Maciej Garczarek, Poznań

Detektor zasysający VESDA-E, model VEA-040-A10
XTRAILS Pty Ltd., Australia
Zgłaszający: XTRALIS UK Ltd., Wielka Brytania

FFT AURA Ai-2 - światłowodowy system ochrony perymetrycznej
LINC Polska Sp. z o.o., Poznań



Integral WAN – sieć central sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi serii Intergal IP.
SCHRACK SECONET AG, Austria | Zgłaszający: SCHRACK SECONET POLSKA Sp. z o.o., Warszawa

INTEGRUM oprogramowanie dedykowane do zarzadzania rozproszonymi instalacjami systemów bezpieczeństwa
SATEL Spółka z o.o., Gdańsk

Kamera bispektralna TPC-BF2120
Dahua Technology Poland Sp. z o.o., Warszawa

Kamera DS-2DF6A236X – AEL
Hangzhou Hikvision Digital Technology Co., Ltd., Chiny
Zgłaszający: Hikvision Poland Sp. z o.o., Warszawa

Kamera DS-2TD2636-10/15
Hangzhou Hikvision DigitalTechnology Co., Ltd., Chiny
Zgłaszający: Hikvision Poland Sp. z o.o., Warszawa

Kamera DS-2TD8166-180ZE2F
Hangzhou Hikvision DigitalTechnology Co., Ltd., Chiny
Zgłaszający: Hikvision Poland Sp. z o.o., Warszawa

Kamera obrotowa 2DF8250I5X – AEL(W)
Hangzhou Hikvision DigitalTechnology Co., Ltd.,Chiny
Zgłaszający: Hikvision Poland Sp. z o.o., Warszawa

Kamera obrotowa DS– 2DF8225IH – AEL DarkFighter X
Hangzhou Hikvision DigitalTechnology Co., Ltd., Chiny
Zgłaszający: Hikvision Poland Sp. z o.o., Warszawa

Kamera panoramiczna DS-2CD6A64F – IHSNFC2
Hangzhou Hikvision DigitalTechnology Co., Ltd., Chiny
Zgłaszający: Hikvision Poland Sp. z o.o., Warszawa

MiniVES Zintegrowany kompaktowy system
AMBIENT SYSTEM Sp. z o.o., Gdańsk

NKB5000 Klawiatura sieciowa
Dahua Technology Poland Sp. z o.o., Warszawa

Rejestrator iDS – 96128NXI – I24
Hangzhou Hikvision DigitalTechnology Co., Ltd., Chiny
Zgłaszający: Hikvision Poland Sp. z o.o., Warszawa

Rejestrator pentabrydowy XVR5216AN-4KL-16P
Dahua Technology Poland Sp. z o.o., Warszawa

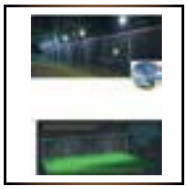
Rozwiązanie do rozpoznawania twarzy iDS-2CD8426G0/F-I + iDS-9632NXI – I8/4F
Hangzhou Hikvision DigitalTechnology Co., Ltd., Chiny
Zgłaszający: Hikvision Poland Sp. z o.o., Warszawa

SAFESTAR
DMSI Software Sp. z o.o., Warszawa

SAGITTARIUS® - PIERWSZY KOMPLETNY BEZPRZEWODOWY SYSTEM DETEKCJI POŻARU
ARGUS Security S.r.l., Włochy
Zgłaszający: CREATIO ARKADIUSZ WALIGÓRA, Milicz

SAIK TUBE
BT ELECTRONICS Sp. z o.o., Kraków

Senstar LM100
RABAN sp. z o.o., sp.k., Swarzędz



SOMFY ONE +
Somfy Sp. z o.o., Warszawa

SYGNALIZATOR GŁOSOWY POŻAROWY SG-Pgw2
W2 Włodzimierz Wyrzykowski, Białe Błota

System zasilania DSO 24V do systemu Paviro firmy Bosch
PULSAR Krzysztof Bogusz Sp. j., Łapczyca

VARYA PERIMETER
RONYO TECHNOLOGIES S.R.O., Czechy
Zgłaszający: RCS Engineering s.r.o., Czechy

ZESTAW DO MOBILNEGO PROGRAMOWANIA CENTRAL ALARMOWYCH Z APLIKACJĄ AVA INSTALL APP
EBS Sp. z o.o., Warszawa

Antena DVB-T dookólna GALA
DPMSolid Limited Sp.k., Oborniki Wielkopolskie

ODBIORNIK NAZIEMNEJ TELEWIZJI CYFROWEJ "COMSAT TE 1060 HD"
COMSAT Sp. z o.o. Sp.k., Poznań

Zestaw Internetu Domowego 300
InterPhone Service z Grupy Kapitałowej Cyfrowy Polsat, Mielec
Zgłaszający: CYFROWY POLSAT Sp. z o.o., Warszawa

Więcej informacji oraz opisy nagrodzonych poduktów na
www.zlotymedal.mtp.pl

Wszystkie przyznane Złote Medale MTP są równoważne.
Lista ułożona alfabetycznie wg produktów

Kontroler KT-1 firmy Kantech
w wersji autonomicznej

Aby spełnić oczekiwania klientów i instalatorów, firma **Kantech** udostępniła nowe oprogramowanie producenta (firmware) do kontrolera **KT-1**. Przesyłanie oprogramowania do kontrolera odbywa się za pośrednictwem programu **EntraPass** lub specjalnej strony na serwerze firmy Kantech (https://demo.kantech.com) – po zalogowaniu się na niej. Po przesłaniu nowego firmware'u można połączyć się z kontrolerem za pomocą przeglądarki (wpisuje się adres zgodnie ze schematem *http://kt-ab-cd-ef*, gdzie *ab-cd-ef* to końcówka adresu MAC kontrolera), natomiast dostęp do menu operacji i samego oprogramowania jest udzielany po zalogowaniu się. Przy pierwszym połączeniu poprzez przeglądarkę wymagana jest rejestracja kontrolera na serwerze firmy Kantech w celu późniejszej aktualizacji firmware'u.

Menu, dostępne poprzez przeglądarkę, umożliwia zarówno zaprogramowanie kontrolera, jak i wykonywanie określonych operacji na drzwiach obsługiwanych przez ten kontroler. W szczególności umożliwia dodawanie użytkowników kart wraz z uprawnieniami. Kontroler z nowym oprogramowaniem współpracuje również z programem EntraPass po zresetowaniu i ustawieniu parametrów adresowych do komunikacji z bramką i serwerem EntraPass.

Aktualna wersja nowego firmware'u to 2.00.14. Jest dostępna wraz z instrukcją na stronie www.kantech.com (po zalogowaniu się) – w plikach instalacyjnych programu EntraPass (w wersji 7.40 lub wyższej). W celu jej uzyskania można też skontaktować się z działem kontroli dostępu firmy AAT HOLDING.

Bezpośr. inf. Ryszard Sobierski
AAT HOLDING

Centrala sygnalizacji pożarowej i sterowania gaszeniem Ex-3001 w CNBOP

Centrala sygnalizacji pożarowej i sterowania gaszeniem **Ex-3001** jest podstawowym elementem systemu wykrywania i gaszenia pożaru **ExGo** produkowanego przez firmę **Advanced Electronics**. Firma **Zeto-Projekt**, jako partner Advanced Electronics na terenie Polski, złożyła wniosek do **CNBOP** o wydanie świadectwa dopuszczenia dla tej centrali. Obecnie udokumentowana została zgodność centrali Ex-3001 z normami EN12094-1 oraz EN54 (z częścią 2, 4 i 13).

System ExGo jest stosowany głównie tam, gdzie przechowywane są urządzenia i dane o znacznej wartości i strategicznym znaczeniu dla firm, czyli w serwerowniach, pomieszczeniach elektrycznych czy archiwach. Dzięki wysokiej niezawodności i łatwej obsłudze oraz bogatej ofercie akcesoriów umożliwiających dopasowaną do obiektu konfigurację sprzętową nadaje się do wszelkich typów pomieszczeń stanowiących jedną strefę gaszenia.

Zastosowanie trzech linii dozorowych zdecydowanie zwiększa niezawodność systemu w przypadku uszkodzenia urządzeń lub okablowania w jednej z linii. Podczas programowania działania systemu istnieje możliwość wyboru stref, które biorą udział w procesie uruchamiania stałego urządzenia gaśniczego.

Bardzo przydatną funkcją jest możliwość ustawienia czasu do uruchomienia stałego gazowego urządzenia gaśniczego (czasu opóźnienia) niezależnie dla sygnałów z czujek automatycznych i ręcznych przycisków uruchamiających gaszenie.

Obwód sterujący wyjściem do urządzenia gaśniczego podczas uruchamiania systemu automatycznie wykrywa typ przyłączonego wyzwalacza. Centrala może sterować wyzwalaczami, które potrzebują podania stałego impulsu o maksymalnym poborze prądu 1 A lub wyzwalaczami wzbudzanymi impulsami 15 ms o wartości prądu do 3 A.

W przypadku konieczności przekazania informacji o stanie systemu do odległych pomieszczeń mamy do dyspozycji zdalny panel obsługi, który jest dostępny w kilku wersjach.

Wbudowany port USB umożliwia pobranie do komputera zdarzeń zapisanych w pamięci centrali, odczyt zaprogramowanej konfiguracji oraz umieszczenie logotypu firmy instalatorskiej na wyświetlaczu LCD centrali Ex-3001.

Bezpośr. inf.
Krzysztof Dembiński
P.U.I. Zeto-Projekt

WiseNet Wave firmy Hanwha Techwin

wydajne i łatwe w obsłudze oprogramowanie do zarządzania systemami nadzoru wizyjnego i kontroli dostępu

Na początku 2018 r. firma **Hanwha Techwin** wprowadziła do swojej oferty zupełnie nowe oprogramowanie **WiseNet Wave** służące do zarządzania systemami nadzoru wizyjnego i kontroli dostępu. Łatwość i intuicyjność obsługi oraz niezwykła wydajność to najistotniejsze cechy nowego produktu. Innowacyjny, interaktywny interfejs, automatycznie adaptujący się do rozdzielczości ekranu monitora wykorzystywanego przez użytkownika, z pewnością zadowoli najbardziej wymagających klientów. Jako jeden z pierwszych na świecie producentów systemów zabezpieczeń Hanwha Techwin zapewnia obsługę swoich produktów nie tylko przez system operacyjny Windows, ale również przez systemy Apple/Mac oraz Linux. Zwiększa to elastyczność oprogramowania i umożliwia pełne dopasowanie go do potrzeb klienta bez konieczności zainwestowania w nowy sprzęt komputerowy. Możliwość swobodnego dostosowywania sposobu wyświetlania obrazów z kamer na podzielonym ekranie, zmiany wielkości każdego pola, obracania pól o dowolny kąt, wirtualnego, wektorowego sterowania funkcją PTZ i integracja z funkcjami analizy treści obrazu to kolejne użyteczne funkcje. Istotna jest także możliwość obsługi nowych kamer wielosensorowych, a także urządzeń produkowanych przez innych czołowych producentów kamer IP oraz systemów kontroli dostępu.

Rejestracja strumieni wizyjnych na serwerze i (lub) w rejestratorach sprzętowych, zastosowanie serwerów nadmiarowych, współpraca z urządzeniami mobilnymi, możliwość pracy w chmurze i wbudowany system autodiagnostyczny to nowe usprawnienia zwiększające funkcjonalność WiseNet Wave.

Więcej informacji znajduje się na stronie https://www.hanwha-security.eu/wisenet-wave/.

Bezpośr. inf. Piotr Rogalewski
Hanwha Techwin Europe

Wisenet eXtra LUX firmy Hanwha Techwin

kolorowy obraz w nocy i WDR o dynamice 150 dB

Firma **Hanwha Techwin Europe** wprowadziła do swojej oferty serię kamer **eXtra LUX** o bardzo wysokiej czułości, z przetwornikami obrazowymi o przekątnej ½ cala. eXtra LUX obejmuje pięć modeli: w obudowie standardowej (XNB-6005), kopułkowej (**XND-6005** z plastiku i **XND-6005V** z aluminium), wandaloodpornej kopułkowej (**XNV-6085**) oraz cylindrycznej (**XNO-6085R**). Wszystkie kamery, poza modelem w obudowie standardowej, są wyposażone w obiektyw o ogniskowej regulowanej zdalnie w zakresie od 4,1 mm do 16,4 mm. Wszystkie modele mają mechanicznie odsuwany filtr podczerwieni, jednak bardzo wysoka czułość przy pracy w trybie dziennym, na poziomie 0,004 lx przy F1,2 i 50 IRE, gwarantuje ostry, kolorowy obraz nawet nocy, w bardzo złych warunkach oświetleniowych, bez zmiany trybu na nocny i odsuwania filtra. Podobnie jak pozostałe kamery z serii X z procesorem Wisenet 5, wyżej wymienione modele oferują m.in. kompresję H.265 i H.264, dziesięć niezależnie transmitowanych strumieni danych, WDR o dynamice 150 dB, żyroskopową stabilizację obrazu, rewolucyjną metodę transmisji WiseStream II ograniczającą pasmo do 75% w stosunku do standardowej kompresji metodą H.264, a także bardzo bogaty zestaw funkcji do analizy treści obrazu. Całość jest uzupełniona przez trójsystemowe zasilanie (12 V_{DC}, 24 V_{AC} lub PoE), funkcję cyfrowego, automatycznego śledzenia obiektów, wykrywanie i korekcję zniekształceń obrazu na skutek mgły, dwa gniazda kart SD umożliwiające jednoczesne podłączenie kart o łącznej pojemności 512 GB oraz funkcje analizy dźwięku z klasyfikacją treści (wykrywanie strzałów z broni palnej, krzyku, eksplozji i stłuczenia szkła).

Więcej informacji znajduje się na stronie https://www.hanwha-security.eu.

Bezpośr. inf. Piotr Rogalewski
Hanwha Techwin Europe

Nowe funkcje kamer IP NOVUS
z serii 3000

Nowe modele kamer IP z **serii 3000** oraz wybrane modele z oprogramowaniem układowym w wersji 4.2.1 mają wiele funkcji.

W modelach z gniazdami **kart microSD** można stosować karty o maksymalnej pojemności 128 GB, co umożliwia ciągły zapis odpowiednio sformatowanego strumienia wizyjnego zgodnie z określonym harmonogramem. To z kolei umożliwia autonomiczny nadzór w miejscach oddalonych od centrum monitorowania, gdzie transmisja sygnału jest niemożliwa. Ponadto istnieje możliwość poklatkowego zapisu obrazów na karcie SD, ze zdefiniowaną prędkością od 1 kl./s do 1 kl./h. Pozwala to na obserwację procesów wolnozmiennych, a także tworzenie filmów reklamowych ukazujących proces budowy itp. Nagrania zapisane na karcie są dostępne z poziomu przeglądarki internetowej.

W przypadku obiektów, w których panują trudne lub zmienne warunki oświetleniowe, można określić różne tryby działania układu automatycznej regulacji ekspozycji. Mogą one być wyzwalane zgodnie z harmonogramem lub sterowane na podstawie pomiaru aktualnego poziomu oświetlenia. Dzięki temu można uzyskać wysoką jakość obrazu w różnych warunkach oświetleniowych. Ustawienie elektronicznej migawki, ręczne lub automatyczne, zgodne z ustalonymi progami oświetlenia, umożliwia wykorzystanie kamer w systemach odczytu danych z tablic rejestracyjnych.

W kamerach usprawniono procedury związane z bezpieczeństwem danych. Pięciokrotne nieudane logowanie blokuje dostęp do kamery na 30 minut, natomiast przy pierwszym logowaniu wymagana jest modyfikacja hasła dostępu. Kamera ma funkcję sprawdzania podczas zmian adresów IP, czy proponowany nowy adres nie jest już używany w sieci.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Kontroler RAID

w 32-kanałowym rejestratorze IP marki NOVUS

Rejestrator IP **NVR-7732-H8** może obsłużyć (zapis zarówno obrazu jak i dźwięku) równocześnie do 32 kamer o rozdzielczości 8 Mpx (popularnie określanej mianem 4K) z prędkością zapisu 30 kl./s dla każdego strumienia. Pojedyncze kamery w systemie mogą pracować nawet przy rozdzielczości 12 Mpx. Urządzenie ma pięć wyjść monitorowych podzielonych na dwie grupy: wyjścia monitora głównego HDMI/VGA (rozdzielczość 4K) i wyjścia monitora pomocniczego HDMI/VGA/BNC (rozdzielczość Full HD). Wyjście BNC pozwala na wyprowadzenie sygnału do monitora analogowego, na odległość nawet 200 m.

W rejestratorze można zamontować do **8 dysków twardych** o pojemności 8 TB każdy i utworzyć w ten sposób archiwum o sumarycznej pojemności **64 TB**. Ponadto rejestrator ma wbudowany kontroler **RAID**, który umożliwia zbudowanie dwóch macierzy RAID o pojemności 16 TB. Oprócz tego dyski mogą pracować w trybie *hot spare* – w przypadku awarii urządzenie *hot spare* automatycznie przejmuje rolę uszkodzonego dysku.

Rejestrator jest wyposażony w dwa interfejsy sieciowe 1 Gb/s, co umożliwia oddzielenie podsieci kamerowej od podsieci zapewniającej zdalny dostęp do urządzenia lub zdublowanie połączenia z podsiecią kamerową w celu zapewnienia dostępu w przypadku awarii okablowania. Do wszystkich stacji klienckich rejestrator może wysłać strumień danych o sumarycznej przepływności 320 Mb/s.

W celu zapewnienia dużej szybkości kopiowania danych rejestrator ma trzy porty USB, w tym jeden port USB 3.0. Rejestrator jest zgodny ze standardem ONVIF Profil S w wersji 2.2 lub wyższej.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Terminal dostępowy MCT86M-IO-CH
do systemu RACS5 firmy ROGER

MCT86M-IO-CH jest terminalem przeznaczonym do wykorzystania w systemie kontroli dostępu i automatyki budynkowej RACS 5 jako punkt identyfikacji użytkownika, sterowania systemem oraz prezentacji jego stanów. Terminal jest wyposażony w kieszeń na kartę zbliżeniową, której status jest w sposób ciągły raportowany – informacje o statusie są przesyłane do kontrolera. W reakcji na włożenie i wyjęcie karty kontroler podejmuje zaprogramowaną czynność, która może być dodatkowo uzależniona od uprawnień przypisanych do karty. Wbudowane linie wej./wyj., przyciski funkcyjne oraz wskaźniki LED terminalu mogą być skonfigurowane w dowolny sposób, aby ułatwiać realizację funkcji systemu RACS 5. Terminal rozróżnia krótkie i długie naciśnięcia przycisków funkcyjnych, co umożliwia zaprogramowanie dwóch niezależnych funkcji każdego z przycisków. Wskaźniki funkcyjne LED są wykorzystywane do sygnalizacji wybranych stanów systemu (np. włączenia oświetlenia, ogrzewania, systemu sygnalizacji włamania i napadu itp.). Zwykle wskaźnik funkcyjny jest wykorzystywany do sygnalizacji stanu systemu sterowanego za pomocą znajdującego się w jego sąsiedztwie przycisku. Terminal obsługuje szyfrowane sektory kart MIFARE, co zabezpiecza system przed użyciem obcych kart oraz duplikowaniem kart oryginalnych. Terminal wymaga podłączenia do kontrolera w systemie kontroli dostępu, który steruje funkcjami logicznymi systemu. Połączenie z kontrolerem jest realizowane za pośrednictwem adresowalnej magistrali RS485.

Bezpośr. inf. ROGER

Trendy w wykorzystaniu analizy treści obrazu w handlu detalicznym

Jak minimalizować straty i maksymalizować zyski sklepu? Odpowiedzią są inteligentne rozwiązania Axis z dziedziny wizyjnych systemów dozorowych, systemów kontroli dostępu oraz systemów akustycznych.

Wykrywanie ruchu w niewłaściwą stronę

Liczenie klientów to obecnie powszechnie stosowane rozwiązanie w handlu detalicznym, jednak nie jest ono stosowane w sklepach spożywczych, ponieważ klienci rzadko wchodzą do sklepu bez zamiaru kupna czegokolwiek, a współczynnik konwersji sięga prawie 100%. Wielu właścicieli sklepów spożywczych traktuje liczbę paragonów jako wskaźnik liczby klientów. Trzeba jednak zadbać o odpowiednie zabezpieczenie przed kradzieżą. Jednym ze sposobów jest wykorzystanie systemów Axis do wykrywania ruchu w niewłaściwą stronę. Oprogramowanie wykrywa osoby poruszające się w taki sposób i informuje je o tym od razu za pomocą komunikatu głosowego bądź alarmu dźwiękowego czy wizualnego. Program można również skonfigurować tak, aby reagował automatycznie, zamykając drzwi wejściowe lub bramę, powiadamiając pracowników ochrony pocztą elektroniczną lub SMS-em albo rozpoczynając rejestrację strumienia wizyjnego. Oprogramowanie pomaga wyeliminować dodatkowe bariery fizyczne, a także uwalnia od konieczności umieszczania pracowników przy wejściach.

Losowe kontrolowanie pracowników

Luksusowych sklepów specjalistycznych często dotyczy problem dużych strat finansowych na skutek kradzieży. Z tym samym problemem borykają się duże centra handlowe oferujące atrakcyjne produkty dla klientów detalicznych. W nich kradzieże wewnętrzne – dokonywane przez pracowników – zdarzają się dużo częściej niż kradzieże dokonywane przez klientów. Jedną z najlepszych strategii, jakie mogą zastosować właściciele sklepów detalicznych w celu zmniejszenia skali kradzieży wewnętrznych, jest kontrola lokalna. Niemniej wiąże się z nią pewne ryzyko. Jeśli kontrola nie zostanie przeprowadzona dyskretnie, może poważnie obniżyć morale pracowników. Dzięki pomocy narzędzia analitycznego liczącego osoby takie kontrole mogą być przeprowadzane skutecznie i systematycznie, bez ryzyka podejrzeń ze strony członków zespołu. Systemy analityczne można indywidualnie dostosować do potrzeb klienta, ustalając procentową częstotliwość kontroli oraz sposób powiadomienia o niej pracowników ochrony. Technika losowej kontroli ma zastosowanie zarówno w przypadku kontrolowania wychodzących klientów, jak i personelu.

Szybki zwrot inwestycji

Wykorzystanie wizyjnych systemów dozorowych w handlu detalicznym jest powszechne. Warto skorzystać dodatkowo z możliwości, jakie daje analiza treści obrazu. Może to przełożyć się na wymierne korzyści, a więc inwestycja może szybko się zwrócić.

Bezpośr. inf.
Axis Communications

XVR
jeden rejestrator, pięć standardów

Ekspansja analogowych systemów telewizyjnych o wysokiej rozdzielczości nikogo już dziś nie dziwi. Stare instalacje zyskały nowe zastosowania, a z wykorzystaniem istniejącego okablowania przesyłane są obrazy o rozdzielczościach 1080p, 4 Mpx czy 4K. Dystans pomiędzy techniką IP i techniką analogową zmniejszył się drastycznie. Na rynku występuje kilka różnych „standardów" transmisji sygnałów analogowych. Cudzysłów jest zamierzony. Jaki bowiem to standard, gdy urządzenia nie są ze sobą kompatybilne i użycie jednego z nich ogranicza wybór pozostałych?

Aby ograniczyć problemy z kompatybilnością, firma **Dahua** stworzyła uniwersalny rejestrator **XVR5216AN-4KL-16P**. To szesnastokanałowe urządzenie obsługuje wszystkie dostępne na rynku formaty (HDCVI, TVI, AHD, CVBS oraz IP) oraz rozdzielczości 720p, 1080p, 3 Mpx, 4 Mpx, 5 Mpx i 4K. Transmisję multisygnału wizyjnego uzupełnia transmisja dźwięku, sygnałów alarmowych czy też sygnałów do sterowania kamer PTZ, oczywiście tym samym przewodem. Kolejną innowacją jest szesnaście wejść BNC z funkcją zasilania podłączonych do nich kamer. Oczywiście nadal tym samym przewodem.

Popularyzacja urządzeń o coraz wyższych rozdzielczościach przekłada się na znacznie większe użycie przestrzeni dyskowej w rejestratorach, jednakże opisywany rejestrator **XVR** radzi sobie z tym problemem dzięki zastosowaniu kodeka H.264+. Kolejną zaletą omawianych urządzeń jest możliwość inteligentnej analizy treści obrazu. Rejestrator ma wyjście HDMI o rozdzielczości 3840x2160, a także wejścia umożliwiające podłączenie czujek ruchu czy wilgotności. Dynamiczny dobór prędkości obracania się wiatraka wentylatora pozwala na ograniczenie poziomu hałasu w miejscu instalacji rejestratora.

Nowy rejestrator XVR jest faktycznie pierwszym uniwersalnym rejestratorem hybrydowym.

Bezpośr. inf. Marian Maroszek
Dahua Technology Poland

Konwertery EoC

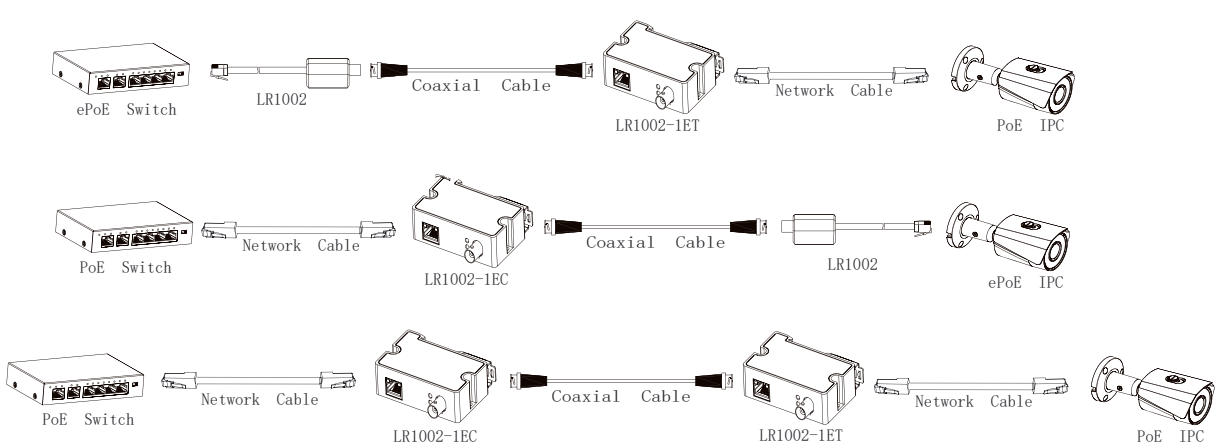
Elastyczne rozwiązania do transmisji danych

Firma **Dahua Technology**, czołowy producent na rynku CCTV, wprowadziła do swojej oferty **konwertery EoC** (Ethernet over Coax) pozwalające przesyłać strumień wizyjny z urządzeń IP poprzez kabel koncentryczny stosowany w starych instalacjach analogowych. Takie rozwiązanie ułatwia migrację z systemów analogowych do nowoczesnych systemów IP z wykorzystaniem istniejącego okablowania. Idąc z duchem czasu, kamery IP oferujące doskonałą jakość obrazu i funkcje analizy treści obrazu możemy klientowi zaproponować zawsze, bez względu na medium wykorzystywane do transmisji danych.

Pierwszymi urządzeniami z rodziny konwerterów EoC są nadajnik LR1002-1ET i odbiornik LR1002-1EC. Urządzenia te mają złącza Ethernet RJ-45 do podłączania kabla sieciowego oraz BNC do podłączenia kabla koncentrycznego. Oprócz przesyłania danych urządzenia te umożliwiają zasilanie urządzeń końcowych metodą PoE. Wykorzystując popularne w instalacjach analogowych kable RG59, możemy uzyskać przepustowość 100 Mbps na trasie o długości 400 m i przepustowość 10 Mbps na dystansie 1000 m. Urządzenia są zgodne ze standardem PoE oraz PoE+, to jest IEEE802.3af i IEEE802.3at. Kolejnym konwerterem dostępnym w bogatej ofercie firmy Dahua jest LR1002. Ten niewielkich rozmiarów produkt również ma złącza RJ-45 oraz BNC. Może współpracować z drugim konwerterem tego samego typu (jeden przy kamerze, drugi po stronie odbiorczej). Jest kompatybilny również z urządzeniami omawianymi wcześniej i pozwala na przesył energii zasilającej kamery na duże odległości. Zastosowanie to obrazuje grafika (rys. 1).

Zastosowanie tych urządzeń w infrastrukturze pozostałej po istniejących instalacjach analogowych pozwala na bezinwazyjne przesyłanie obrazu z kamer IP.

Bezpośr. inf. Łukasz Biskupski
Dahua Technology Poland



Rys.1. Sposoby łączenia konwerterów

Firma Axis Communications
otworzyła biuro w Warszawie

W związku z dynamicznym rozwojem swojej działalności w Polsce firma **Axis Communications** otworzyła biuro w Warszawie. Wydarzenie uświetnili swą obecnością **Ray Mauritsson** – dyrektor generalny – oraz **Anna Forsberg** – dyrektor regionalny na Europę Wschodnią.

Oprócz komfortowej przestrzeni biurowej jest w nim także nowoczesna i przestronna sala szkoleniowa, sala demonstracyjna, sala konferencyjna, a także kafeteria i zaplecze techniczne. Mieści się przy ul. Domaniewskiej 44, na 1. piętrze budynku Platinium Business Park IV. Jego powierzchnia to ok. 300 m^2. Pracuje w nim ośmiu pracowników.

W uroczystości otwarcia nowego biura wziął udział Ray Mauritsson, który odwiedził Polskę po raz pierwszy. – *Jesteśmy pod ogromnym wrażeniem dynamiki rozwoju rynku sieciowych systemów wizyjnych w Polsce i w tej części Europy. Miniony rok był dla nas bardzo udany. Zanotowaliśmy rekordowe wyniki sprzedaży netto, które przełożyły się na 15-procentowy wzrost (8603 mln SEK, czyli ok. 1091 mln USD). Zwiększyliśmy liczbę pracowników, najsilniejszy nacisk kładąc na inwestycje w dział badań i rozwoju oraz sprzedaży. Przed nami rok pełen wyzwań i kontynuacja stabilnego wzrostu. Mam nadzieję, że dzięki doskonałej partnerskiej współpracy zakończymy go kolejnym sukcesem* – powiedział Ray Mauritsson.

– *Widzimy w polskim rynku ogromny potencjał i z tego właśnie powodu głównie tutaj koncentrujemy działania, a także rozszerzamy kanały sprzedaży. W minionym roku wprowadziliśmy na rynek kilka innowacyjnych produktów (m.in. modułowe kamery przeznaczone do bardzo dyskretnej obserwacji, radar, a także urządzenia z zakresu sieciowej kontroli dostępu i sieciowe urządzenia dźwiękowe). Przełomem są kamery termowizyjne, dzięki którym możemy dotrzeć do nowej grupy klientów, zainteresowanych korzyściami płynącymi z obserwacji w widmie termicznym* – dodała Anna Forsberg.

– *W modelu biznesowym Axis kluczową rolę odgrywa współpraca z partnerami, którzy są współautorami naszego sukcesu. Chcemy zyskać ich lojalność i poszerzać ich wiedzę na temat produktów Axis, projektowania, instalowania i konfigurowania wyrafinowanych rozwiązań z dziedziny systemów bezpieczeństwa. Teraz, mając do dyspozycji nowoczesne centrum szkoleniowe, będziemy mogli zaplanować obszerny i różnorodny system dzielenia się tym, w czym jesteśmy najlepsi, czyli wiedzą i innowacjami* – podkreślił **Jakub Kozak**, dyrektor sprzedaży w Polsce i krajach bałtyckich.

Ceremonia otwarcia odbyła się 30 stycznia. Uroczystego przecięcia wstęgi dokonali Anna Forsberg, Ray Mauritsson i Jakub Kozak. Honory gospodarza pełnił Jakub Kozak, który oprowadził gości po nowym biurze, dzieląc się interesującymi informacjami na temat specyfiki pracy całego zespołu Axis.

Bezpośr. inf.
Axis Communications

Więcej informacji o firmie Axis Communications można znaleźć na stronie internetowej pod adresem https://www.axis.com/pl-pl

Czasopismo *Zabezpieczenia* zaprasza do obejrzenia fotorelacji na stronie http://zabezpieczenia.com.pl


AXIS


Wygrywaj
AXIS


AXIS
AXIS

III seminarium firm z branży elektronicznych systemów bezpieczeństwa

podsumowanie

20 lutego 2018 roku w **Instytucie Systemów Elektronicznych Wydziału Elektroniki Wojskowej Akademii Technicznej (WAT)** odbyło się kolejne, III seminarium firm z branży elektronicznych systemów bezpieczeństwa poprzedzone konkursem dla studentów o tytuł mistrza elektronicznych systemów bezpieczeństwa. Zwyciężył inż. Adrian Błażejczyk. Tytuł pierwszego wicemistrza wywalczył inż. Karol Michał Włosek, a drugiego Kamil Krzykawski. Wręczono również osiem wyróżnień. W trzeciej edycji konkursu wzięło udział 36 studentów Wydziału Elektroniki WAT.

Seminarium, zorganizowane dla kadry naukowo-dydaktycznej instytutu oraz studentów specjalności Inżynieria Systemów Bezpieczeństwa profilowanej przez instytut, było okazją do zaprezentowania przez czołowe firmy z branży swoich produktów oraz najnowszych rozwiązań z dziedziny zabezpieczeń. Wzięły w nim udział firmy AAT HOLDING, Bosch Security Systems, Janex International, POLON-ALFA, Pulsar, Satel oraz Schrack Seconet. W czasie wystąpień przedstawiły swoją strukturę, produkty, nowości rynkowe oraz przykładowe realizacje elektronicznych systemów bezpieczeństwa.

Po skończonych prezentacjach odbyło się uroczyste otwarcie czterech nowoczesnych pracowni dydaktycznych w Instytucie

Systemów Elektronicznych WEL WAT wyposażonych przez firmy, z którymi Wydział Elektroniki WAT podpisał porozumienia. Uroczystego otwarcia zespołu pracowni pod wspólną nazwą *Elektroniczne Systemy Bezpieczeństwa* dokonali prorektor ds. kształcenia WAT dr hab. inż. Zdzisław Bogdanowicz, prof. WAT, oraz wiceprezes AAT HOLDING Jarosław Kubacki, dyrektor handlowy firmy Bosch Krzysztof Góra, prezes firmy Janex International Justyna Kawacz-Matysiak, kierownik projektu Edu Satel Maciej Domagalski, prezes firmy Schrack Seconet Grzegorz Ćwiek i dyrektor sprzedaży krajowej firmy Pulsar Zbigniew Jarosz w obecności dziekana Wydziału Elektroniki WAT prof. dr. hab. inż. Andrzeja Dobrowolskiego, dyrektora Instytutu Systemów Elektronicznych WEL dr. hab. inż. Zbigniewa Watrala oraz koordynatora całego przedsięwzięcia dr. hab. inż. Jacka Pasia.

Oprócz studiów stacjonarnych i niestacjonarnych I i II stopnia (inżynierskich i magisterskich), profilujących specjalność inżynieria systemów bezpieczeństwa, w Instytucie Systemów Elektronicznych WEL WAT organizowane są także cyklicznie dwusemestralne studia podyplomowe pod nazwą *Techniczna Ochrona Osób i Mienia*, których XVI edycja rozpocznie się w październiku br.

Bezpośr. inf.
dr hab. inż. Jacek Paś
Wojskowa Akademia Techniczna
Wydział Elektroniki
Instytut Systemów Elektronicznych
Zakład Eksploatacji Systemów Elektronicznych

Czasopismo *Zabezpieczenia* dziękuje władzom uczelni za zaproszenie. Gratulujemy wiedzy i umiejętności studentom, zwycięzcom konkursu, i życzymy im kolejnych sukcesów na dalszych etapach kształcenia. Mamy nadzieję, że bardzo dobrze wyposażone sale dydaktyczne przyczynią się do wzrostu liczby studentów zainteresowanych podjęciem pracy w branży zabezpieczeń po ukończeniu studiów. Jesteśmy pewni, że wyposażenie pracowni to dobra inwestycja, która szybko się zwróci w postaci wysoce wykwalifikowanej kadry pracowniczej.

Procedury i instrukcje
dotyczące centrum monitorowania

Daniel Kamiński

Usługi monitorowania znów zyskują dużą popularność. Niestety wiele miejsc, w których przetwarzane są sygnały alarmowe, nie spełnia wymagań dotyczących centrum monitorowania. W związku z tym możliwe są awarie, przestoje oraz pomyłki. Najczęstszym powodem jest brak analizy zagrożeń oraz planu ciągłości działania. W większości centrów monitorowania utworzonych po 2000 roku nie ma procedur testowania, procedur awaryjnych czy procedur ochrony centrum

Zapotrzebowanie na usługi monitorowania alarmów pojawiło się po raz pierwszy w latach 90. ubiegłego wieku, jednakże wtedy koszty uruchomienia usługi były ogromne. Każdy, kto uruchamiał centrum, wiedział, że będzie musiał inwestować przez okres minimum dziesięciu lat, zanim zwrócą się koszty wyposażenia oraz budowy infrastruktury służącej do transmisji alarmów.

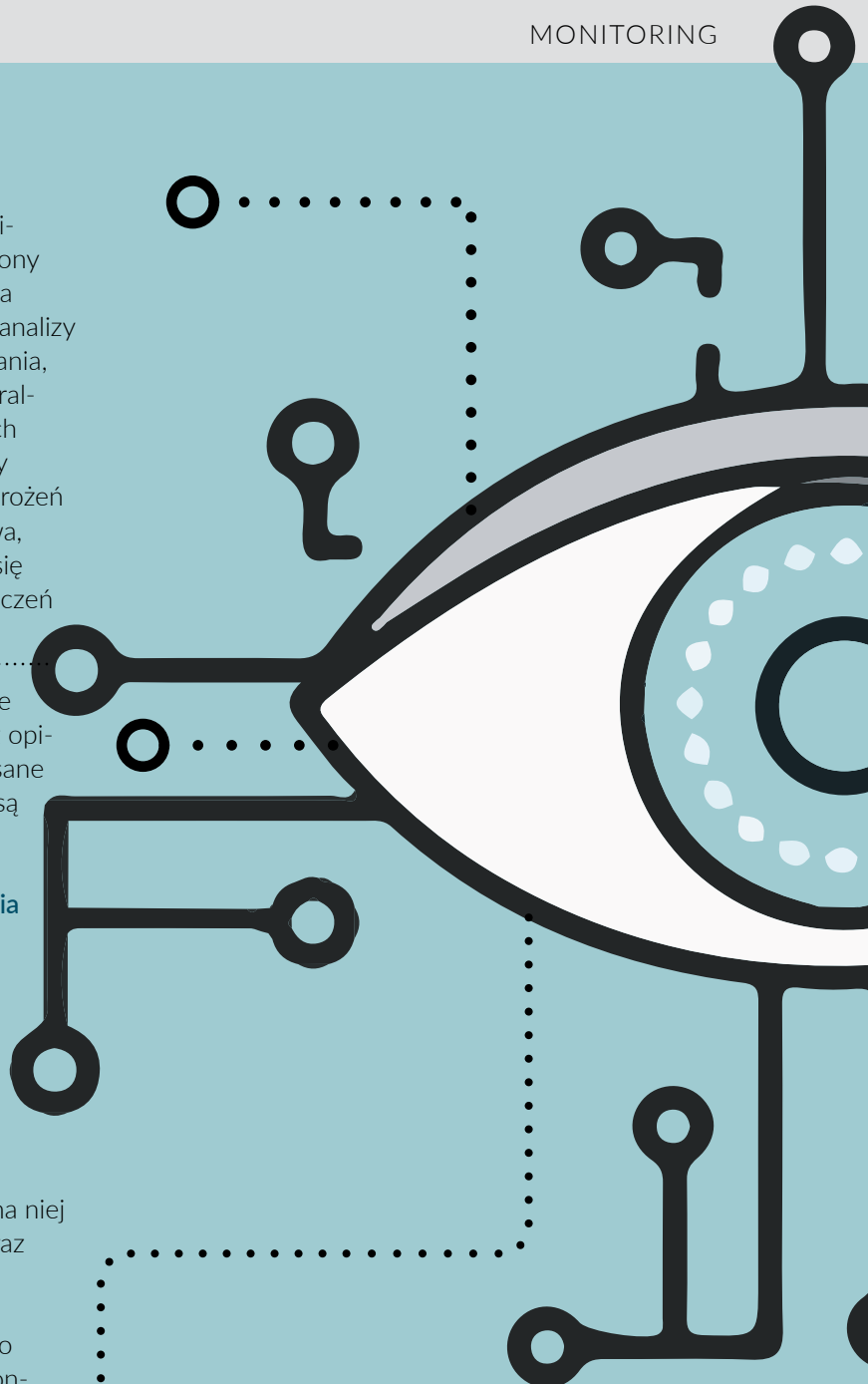
Świadczenie usług monitorowania alarmów jeszcze nie było uregulowane w przepisach i normach, więc każdy, kto inwestował w uruchomienie monitorowania, zakładał najgorsze: przerwy w dostawie prądu, awarie centrali telefonicznej, napady na obsługę centrum, sabotaże infrastruktury służącej do transmisji alarmów, alarmy bombowe i wiele innych zagrożeń, które obecnie są często pomijane. Z tego względu standardem było dublowanie łączności, zasilania, odbiorników alarmowych, serwerów, a nawet lokalizacji, w których obsługiwane były zdarzenia alarmowe.

Pod koniec lat 90. optymalizacje kosztów pracy w ochronie doprowadziły do sytuacji, w której za cenę zbliżoną do ceny usługi monitorowania można było zatrudnić pracownika ochrony. Koszty infrastruktury były wówczas jeszcze wysokie, więc w firmach ochrony zaczęły dynamicznie rozwijać się usługi ochrony fizycznej.

Nowe warunki uruchamiania centrum monitorowania

Ostatnie zmiany ustawowe dotyczące sposobu zatrudniania pracowników ochrony spowodowały, że usługi ochrony zaczęły się znacząco zmieniać. Wzrost kosztów pracy spowodował, że jest mniej pracowników ochrony. Rozpoczęły się poszukiwania usług, w których wykorzystuje się zdalny nadzór chronionych obiektów.

Koszty uruchomienia centrum monitorowania zmalały drastycznie. Znaczna część kosztów budowania infrastruktury została wyeliminowana. Infrastruktura sieci komórkowych stała się dostępna na terenie całego kraju, a koszty transmisji sygnałów alarmowych spadły. Pojawiły się wirtualne serwery pracujące w chmurze oraz programy do obsługi alarmów pracujące w środowisku rozproszonym. W efekcie dostępność nowych zdobyczy techniki doprowadziła do sytuacji, w której uruchomienie centrum monitorowania jest praktycznie darmowe, a koszt jego utrzymania może być pokrywany z abonamentów.



Niestety często ignoruje się potrzebę prawidłowej (zgodnej ze sztuką zawodową) ochrony miejsca, w którym obsługiwane są zdarzenia alarmowe. Bardzo często nie wykonuje się analizy zagrożeń dotyczących centrum monitorowania, czyli miejsca, w którym jest dostęp do newralgicznych informacji o chronionych obiektach i w którym pracują ludzie, od których zależy jakość świadczonych usług. Bez analizy zagrożeń trudno zaplanować systemy bezpieczeństwa, więc często centrum monitorowania staje się najsłabszym ogniwem w systemie zabezpieczeń chronionych obiektów.

Ze względu na to, że wymagania techniczne dotyczące centrum monitorowania były już opisywane, w niniejszym artykule zostaną opisane procedury, których najczęściej brakuje lub są błędnie interpretowane.

Procedury ochrony centrum monitorowania

W przypadku ochrony pomieszczeń centrum ważna jest **instrukcja wejścia.** Ma ona ograniczyć do minimum liczbę osób mających dostęp do sali obsługi alarmów. Z tego względu określa, kto i w jakim czasie ma prawo przebywać w centrum. Załącznikiem do instrukcji wejścia jest lista upoważnionych osób. Są na niej operatorzy centrum, obsługa techniczna oraz kierownictwo firmy.

Instrukcja wejścia opisuje sposób wejścia do centrum, które jest chronione systemem kontroli dostępu i którego personel otwiera drzwi wewnętrzne tylko po potwierdzeniu tożsamości wchodzącej osoby. Procedura ma być realizowana niezależnie od tego, czy wejście jest wyposażone w śluzę czy drzwi pojedyncze. Chodzi o to, aby w przypadku zagrożenia, np. wówczas, gdy podejrzewa się, że osoba uprawniona do wejścia została sterroryzowana przez intruza, obsługa centrum mogła pozostawić zaryglowane drzwi i uniemożliwić wejście.

Kolejnym dobrym rozwiązaniem jest **instrukcja wprowadzania gości** wraz z imiennym wykazem osób uprawnionych do ich wprowadzania. Goście mogą mieć niezamierzony dostęp do danych obiektów, których obrazy są wyświetlane w trakcie obsługi zdarzeń. Dlatego załącznikiem do instrukcji wprowadzania gości powinien być formularz rejestracji danych gości, którzy będą odwiedzać centrum. Ważne jest podanie godzin pobytu oraz celu wizyty. Dzięki temu w przypadku wycieku informacji będzie łatwiej ustalić, kto za niego odpowiada.

Niestety tego typu instrukcje są w centrach monitorowania rzadkością. Z reguły każda osoba funkcyjna ma dostęp do wszystkich pomieszczeń i może tam wprowadzać kogo chce na swoją odpowiedzialność. Takie zwyczaje są niewłaściwe i stwarzają zagrożenie dla wprowadzającego, operatorów centrum monitorowania oraz chronionego obiektu.

Procedury obsługi zdarzeń alarmowych

Z reguły dobrze opisanymi procedurami w centrach monitorowania są te, które dotyczą obsługi

zdarzeń alarmowych, takich jak napad, włamanie, sabotaż. Ewentualne problemy mogą być spowodowane przez odstępstwa od harmonogramu, takie jak za wczesne otwarcie czy niewłączenie w dozór. Dużą swobodę działania pozostawiono natomiast procedurom obsługiwania usterek technicznych, takich jak brak prądu, niskie napięcie akumulatora czy brak łączności.

Procedury **obsługi zdarzeń** powinny uwzględniać przyjęcie zgłoszenia przez operatora centrum, reakcję grup interwencyjnych lub służb technicznych, powiadomienie uprawnionych osób lub instytucji oraz dokumentację poszczególnych etapów działań. Dodatkowo powinny umożliwiać wprowadzenie podziału zdarzeń na uzasadnione oraz nieuzasadnione. W przypadku nieuzasadnionych istotne jest określenie powodu przypadkowej aktywacji systemu (wina użytkownika lub awaria).

Procedury obsługi zdarzeń powinny uwzględniać także informacje, jakie można przekazywać osobom upoważnionym, a także sposób weryfikacji i autoryzacji osoby dzwoniącej. Dodatkowo powinny uwzględniać sposób przekazywania informacji (w tym głosowy oraz automatyczny, np. poprzez SMS), a także możliwą sytuację, w której nie można przekazać powiadomienia (np. dlatego, że telefon osoby upoważnionej znajduje się poza zasięgiem operatora sieci telefonii komórkowej albo numer jest nieaktualny).

Na szczęście tego typu procedury często są zaimplementowane w programach do obsługi alarmów, więc ich obsługa może być ujednolicona. Kłopot pojawia się wtedy, gdy firma ma różne procedury w zależności od rodzaju obiektu – wtedy muszą być one odpowiednio wprowadzone w trakcie wprowadzania obiektów do bazy. Niestety firmom ochrony brakuje opisów wspomnianych procedur w wersji podręcznej, przydatnej podczas okresowych szkoleń lub wprowadzania nowego pracownika. Brak szkoleń dotyczących obsługi zdarzeń zgodnie z procedurą powoduje, że operatorzy z czasem wprowadzają własne modyfikacje, a w związku z tym identyczne zdarzenia są różnie obsługiwane przez różnych operatorów. To może spowodować reklamacje, a nawet szkody.

Procedury obsługi zdarzeń wizyjnych

Najnowsza tendencja dotycząca dozoru wizyjnego spowodowała wysyp usług, w których wykorzystuje się obraz z kamer, i które różnią się sposobem obsługi przez operatora centrum. Obecnie promuje się głównie zdalny nadzór wizyjny, wideopatrol oraz wideoweryfikację alarmów. Niestety usługi te nie mają ujednoliconych procedur, co często wykorzystują przedstawiciele handlowi oferujący rzekomo te same usługi.

Usługi wideo różnią się od siebie zarówno zaangażowaniem czasu operatora centrum, jak i wykorzystaniem zasobów infrastruktury, w szczególności pasma łącza internetowego, wydajności serwerów oraz pojemności dysków twardych. Dostępność tych zasobów powinna być okresowo testowana.

W przypadku obsługi zdarzeń wykrytych przez system dozoru wizyjnego kluczem do sukcesu jest określenie kryteriów reakcji operatora centrum na niechciane zachowania osób będących w kadrze. Należy pamiętać, że analiza obrazu ułatwia wykrywanie zagrożenia, ale to nie jej jedyne zastosowanie. Dziś dozór wizyjny stosuje się również w celu wykrywania naruszenia zasad bezpieczeństwa pracy. Operator centrum coraz częściej dostaje zadanie wykrywania zachowań niezgodnych z regulaminem danego obiektu, np. nienoszenia kasków na budowie albo ubrań ochronnych w magazynach sklepów, pozostawiania otwartych drzwi pomiędzy sklepem a magazynem.

Procedury dotyczące dozoru wizyjnego powinny być dostosowane do każdego obiektu indywidualnie, co utrudnia obsłudze centrum wprowadzanie ich do programu służącego do obsługi zdarzeń oraz szkolenie operatorów. Może dlatego większość firm niestety nie stosuje procedur indywidualnych.

Procedury testowania

Każde centrum monitorowania jest wyposażone w wiele kosztownych urządzeń odpowiedzialnych za jego ciągłą pracę. Do najważniejszych należą agregaty prądotwórcze, UPS-y, serwery, centrale telefoniczne oraz systemy klimatyzacji oraz wentylacji. Część urządzeń ma w wytycznych eksploatacyjnych wpisane terminy testów, np. wymagane jest uruchamianie agregatów prądotwórczych raz w tygodniu i ich działanie przynajmniej przez godzinę. W przypadku braku rozruchów testowych mogą one nie zadziałać wtedy, gdy będą potrzebne, a dodatkowo producent może cofnąć gwarancję. W przypadku UPS-ów zastosowane akumulatory wymagają wymiany co dwa–trzy lata, gdyż tracą one swoją pojemność, co skraca czas podtrzymania zasilania. Podobne ograniczenia mają dyski i zasilacze serwerów. W klimatyzatorach po każdym sezonie musi być uzupełniony czynnik chłodzący.

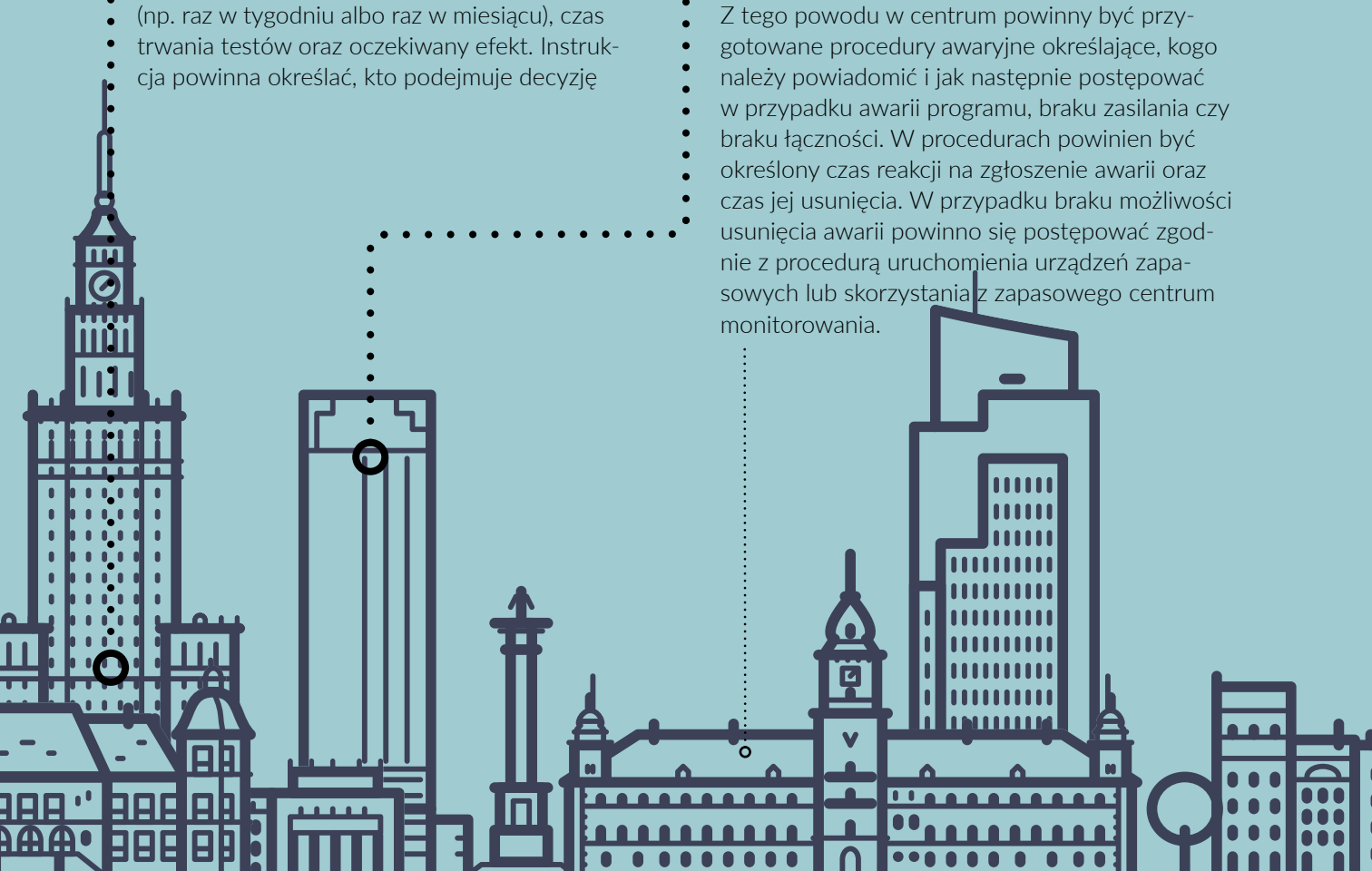
Centrum monitorowania powinno mieć przygotowane procedury testowania opisane w instrukcji określającej sposób przeprowadzenia testu (np. zmiana źródła zasilania), częstotliwość testowania (np. raz w tygodniu albo raz w miesiącu), czas trwania testów oraz oczekiwany efekt. Instrukcja powinna określać, kto podejmuje decyzję o rozpoczęciu testu, a także zawierać wskazówki dotyczące sytuacji awaryjnych.

Centrum monitorowania to również miejsce, w którym wykonywane są archiwizacje baz danych dotyczących historii obsługi zdarzeń oraz klientów. Procedury testowe powinny uwzględniać weryfikowanie jakości i poprawności wykonywanych archiwizacji – trzeba mieć pewność, że w przypadku awarii będzie można odtworzyć bazę danych z kopii.

Niestety tego typu procedury są przez firmy ochrony rzadko stosowane. Dlatego należy stworzyć **instrukcję testowania** wraz z dziennikiem testów, w którym będą podawane terminy oraz zakres testów.

Procedury awaryjne

Centrum monitorowania musi pracować sprawnie całodobowo, przez cały rok. Co więcej, ze względu na charakter świadczonych usług awaria musi być naprawiona w jak najkrótszym czasie. Do tego operatorzy centrum muszą być przygotowani do obsługi zdarzeń w trybie awaryjnym. Z tego powodu w centrum powinny być przygotowane procedury awaryjne określające, kogo należy powiadomić i jak następnie postępować w przypadku awarii programu, braku zasilania czy braku łączności. W procedurach powinien być określony czas reakcji na zgłoszenie awarii oraz czas jej usunięcia. W przypadku braku możliwości usunięcia awarii powinno się postępować zgodnie z procedurą uruchomienia urządzeń zapasowych lub skorzystania z zapasowego centrum monitorowania.



Warto rozróżnić rodzaje awarii, np. awarie krytyczne (uniemożliwiające pracę) i awarie niekrytyczne (utrudniające pracę). Należy pamiętać, że w przypadku awarii niekrytycznej praca operatorów będzie utrudniona, ale klienci mogą jej nawet nie zauważyć. Personel centrum powinien odbywać szkolenia dotyczące procedur awaryjnych. Przynajmniej raz w roku, w celach szkoleniowych, powinny być symulowane awarie poszczególnych systemów. Awarie powinny być odnotowywane w dzienniku awarii. Sumaryczny czas awarii w roku będzie podstawą wyliczenia dostępności centrum.

Plan ciągłości działania

Testowanie urządzeń oraz procedury na wypadek awarii świadczą o tym, że centrum monitorowania poważnie podchodzi do realizacji usług, za które pobiera opłaty. Szczególnie wysoko cenionym przez wymagających klientów dokumentem jest **plan ciągłości działania** określający, w jakim czasie zostanie odtworzona infrastruktura centrum w przypadku jej zniszczenia (np. na skutek pożaru).

W takim dokumencie opisuje się strategię odtworzenia infrastruktury. Uwzględnia się przy tym sprzęt potrzebny do odtworzenia centrum, rezerwowe magazyny danych, z których będą odtwarzane informacje biznesowe, mechanizmy przekierowywania połączeń telefonicznych oraz internetowych.

W przypadku firm, które mają urządzenia zapasowe, cała procedura uruchomienia serwerów, odtworzenia oprogramowania, przeniesienia operatorów i dokonania przekierowań może trwać nawet od czterech do sześciu godzin. W przypadku posiadania zapasowego centrum monitorowania replikującego dane takie działania mogą zająć 30–40 minut. Oba te czasy – tzn. minimalny i maksymalny – są akceptowalne pod warunkiem, że są podane w planie ciągłości działania i przećwiczono wykonanie wspomnianych czynności w odpowiednim czasie. Dobór czasu jest kompromisem pomiędzy niższymi kosztami w przypadku dłuższego czasu odtworzenia a ryzykiem biznesowym wynikającym z umów.

W firmach, które nie mają planu ciągłości działania, zakup komputerów, odbiorników, modemów, serwerów itp. oraz odtworzenie bazy danych zajmie ponad tydzień. Takiego czasu bez ochrony nie wytrzyma żaden klient. Nie da się też utrzymać w tajemnicy, że firma nie świadczy usług. Jej przyszłość stanie pod znakiem zapytania.

W przypadku planu ciągłości działania bardzo ważne jest opisanie, kto i w jakim przypadku może podjąć decyzję o skorzystaniu z centrum zapasowego. Ważne jest również opisanie, w jaki sposób należy powiadomić o sytuacji partnerów oraz kluczowych klientów. Od tego powiadomienia może zależeć przyszłość firmy, dlatego powinno być wcześniej uzgodnione.

Podsumowanie

Część firm, która zajmuje się monitorowaniem od początku lat 90., potraktuje ten artykuł jako niekompletny, ponieważ opisuję kilka kluczowych zagadnień dość pobieżnie. Zgodzę się z taką opinią, gdyż trudno opisać wszystkie zalecenia w jednym artykule. Dla niektórych podane zalecenia mogą wydać się zbyt ostrożne, bo przecież policja i MSWiA nie wymagają takich zabezpieczeń. Faktycznie jednak wynikają one z wymagań normy EN-PN 50518 oraz zasad sztuki zawodowej. Stosowanie się do tych zasad pomogło mnie oraz moim znajomym przetrwać sytuacje kryzysowe, dlatego je opisuję i zalecam. Na zakończenie podpowiem, że część ryzyka dotyczącego infrastruktury można zminimalizować poprzez korzystanie z profesjonalnych centrów danych oraz programów pracujących w chmurze, jednak procedury wejścia do centrum monitorowania, procedury testowania, procedury awaryjne (*disaster recovery plan*) oraz plan ciągłości działania (*business continuity plan*) i tak trzeba stworzyć.

Daniel Kamiński

Alert Control
ALARMY POD KONTROLĄ

ALERTCONTROL Daniel Kamiński
ul. Przyrodnicza 7E
05-126 Michałów-Grabina
alertcontrol@alertcontrol.pl
tel.: (+48) 784 646 386

RACS 5

System kontroli dostępu

- Wieloprzejściowe kontrolery dostępu serii MC
- Skalowalne oprogramowanie zarządzające VISO w architekturze klient – serwer
- Plikowa lub serwerowa baza danych w technologii MSSQL
- Bezpieczna komunikacja szyfrowana AES 128 CBC
- Funkcje automatyki budynkowej
- Integracja sprzętowa z systemem alarmowym
- Monitorowanie w trybie tekstowym i graficznym
- Integracje CCTV: Hikvision, Dahua
- Możliwość podziału systemu na zarządzane indywidualnie części

MCT86M-IO-CH

Terminal dostępu do systemu RACS 5

Wysoka niezawodność i funkcjonalność potwierdzona w tysiącach wdrożonych z sukcesem instalacji w Polsce i za granicą.

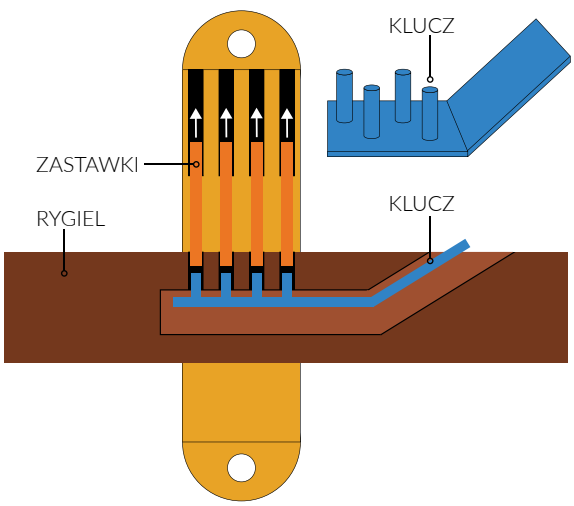
roger®

Rozwój systemów kontroli dostępu
na przykładzie zamków ryglujących drzwi

Maciej Prelich

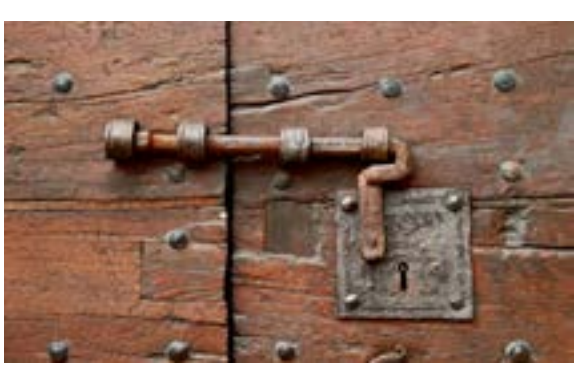
Ludzie od zawsze próbują chronić swoją własność przed dostępem oraz ingerencją osób trzecich lub zwierząt. Już w czasach prehistorycznych ludzie zabezpieczali miejsca swojego pobytu ścianami i drzwiami. Pierwsze wzmianki o drzwiach pochodzą ze starożytnego Egiptu, jednak różniły się one od drzwi, które stosuje się dzisiaj. Nie były elementem wyposażenia zwykłych domów. Można było zobaczyć je w takich miejscach jak świątynie – stanowiły symbol luksusu, były bogato zdobione oraz wykonane z drogich, szlachetnych materiałów, takich jak drewno cedrowe, oliwne czy cyprysowe. Najstarsze spośród zachowanych drzwi pochodzą z Mezopotamii, sprzed około 2000 lat przed naszą erą. Forma drzwi, którą znamy dzisiaj, powstała dopiero na przełomie XIX i XX wieku

Obecnie nieodłącznym elementem drzwi zewnętrznych jest zamek. Chociaż same niezablokowane drzwi stanowiły dostateczną ochronę przed zimnem i zwierzętami, były bardzo łatwe do sforsowania dla innych ludzi. Wiedzieli o tym już nasi przodkowie. Najstarszy pierwowzór dzisiejszego zamka do drzwi został odkryty w Chorsabad i został wyprodukowany około czterech tysięcy lat przed naszą erą. Sam zamek, w całości wykonany z drewna, bardzo różni się od dzisiejszych mechanizmów. Jest przedstawiony na rysunku 1. Dzięki pracy archeologów wiadomo, że podobne rozwiązania były używane przez starożytnych Greków, którzy zabezpieczali swoje domy drewnianą zasuwą poruszaną za pomocą klucza wkładanego w niewielki otwór w drzwiach. Podobny mechanizm stosowali starożytni Egipcjanie, jednak



Rys. 1. Mechanizm działania pierwszego zamka znalezionego w Egipcie

klucz był znacznie mniejszy. Dopiero w latach 870–900 naszej ery angielscy rzemieślnicy zaczęli wykonywać zamki w całości z metalu. Zasada ich działania pozostała bez zmian przez resztę średniowiecza. Fotografia 1 przedstawia typowe



Fot. 1. Typowy zamek stosowany w średniowieczu

rozwiązanie z tej ery. Nie trudno domyślić się, że dla wykwalifikowanych złodziei to zabezpieczenie nie stanowiło przeszkody trudnej do pokonania. Ślusarze oraz ówcześni konstruktorzy dokładali wszelkich starań, aby ulepszyć zamki poprzez dodanie mechanizmów strzelających do napastników lub obcinających palce po niewłaściwym włożeniu klucza do zamka. W epoce renesansu nowym rozwiązaniem stały się zamki-zagadki importowane z Chin – drzwi były odblokowywane po naciśnięciu jednego przycisku, ukrytego np. w ścianie lub ornamentach. Początki znanych nam dzisiaj zamków sięgają XVIII wieku, kiedy we Francji opracowano pierwsze zamki z zastawkami sprężynującymi, które później były unowocześniane przez angielskich ślusarzy, takich jak Robert Barron. Dopiero w 1861 roku amerykański inżynier Linus Yale wynalazł zamek bębenkowy,

Liczne usprawnienia tego wynalazku przyczyniły się do założenia istniejącej do dnia dzisiejszego firmy Yale produkującej zamki.

W przypadku wielu zastosowań nawet dosyć złożone zamki bębenkowe nie wystarczają. Klucze łatwo jest zgubić albo podrobić. Z myślą o bardziej wymagających użytkownikach oraz newralgicznych infrastrukturach stworzono zamki szyfrowe przeznaczone do drzwi zewnętrznych, wewnętrznych oraz, w późniejszym czasie, do drzwi w szafkach i komodach. Początkowo były to zamki mechaniczne blokujące dostęp do drzwi do momentu podania kodu odblokowującego przez użytkownika. Wymagania dotyczące budowy takich zamków są znacznie bardziej rygorystyczne – mechanizm musi działać bezgłośnie, a obudowa musi być odporna na prześwietlanie oraz próby mechanicznego sabotażu, co ma utrudnić dostęp osobom nieuprawnionym. Z powodu rosnących wymagań powstało wiele nowych zamków o różnych zasadach działania. Wykorzystano na przykład wirujące pole magnetyczne w celu zapewnia bezszelestnego odryglowywania zamka. Wielu producentów nie chce jednak ujawniać szczegółów tych konstrukcji w celu zmniejszenia ryzyka pokonania zabezpieczeń.

Kolejnym etapem ewolucji było wprowadzenie zamków elektronicznych, które są obecnie powszechnie stosowane w hotelach, obiektach o podwyższonym stopniu zagrożenia włamaniem, a także w biurach oraz na posesjach prywatnych. Szybko zdobyły popularność dzięki wygodzie użytkowania oraz zastosowaniu najnowszych technik uwierzytelniania użytkownika – obecnie, oprócz klasycznego kodu, do uwierzytelniania mogą służyć inteligentne karty chipowe, dane biometryczne (skan siatkówki oka, odcisk palca) i kody generowane w czasie rzeczywistym. Zastosowanie znajdują także systemy bezprzewodowej transmisji danych NFC oraz RFID. Tak szeroki asortyment pozwala użytkownikom oraz administratorom systemów dobrać rozwiązanie

Fot. 2. Mnogość sposobów uwierzytelniania w przypadku zamka CL5510

dostosowane do ich potrzeb. Fotografia 2 przedstawia jedno z najbardziej zaawansowanych rozwiązań – zamek CL5510, który można otwierać za pomocą kodu, karty lub telefonu komórkowego. Jest to produkt firmy Codelocks, jednego z liderów na rynku zamków szyfrowych.

Fot. 3. KL1200 – elektroniczny zamek szyfrowy do zastosowania w szafkach

Następnym krokiem była miniaturyzacja zamków, która umożliwiła zabezpieczanie indywidualnych szafek lub komód. Odpowiednie algorytmy pozwalają dostosować zamek do wielokrotnego otwierania przez jednego użytkownika, co sprawdza się na przykład w przypadku szafek pracowniczych, lub do użycia jednorazowych kodów, co jest przydatne na przykład w obiektach sportowych. Fotografia 3 przedstawia kolejne rozwiązanie firmy Codelocks – KL1200 przeznaczone do zastosowania w szafkach.

Kompletny asortyment zamków szyfrowych, dostosowanych do różnych potrzeb i nawet najwyższych wymagań, oferuje firma ATLine sp.j. Sławomir Pruski. Zamki szyfrowe poprawiają bezpieczeństwo obiektu i eliminują potrzebę noszenia kluczy, co eliminuje ryzyko ich zgubienia lub podrobienia przez osoby trzecie. Jest to wygodne rozwiązanie w przypadku najmu lokalu, gdyż kod można łatwo i szybko zmienić. To znacznie prostsze niż wymiana tradycyjnego zamka.

Rozwój zamków na przestrzeni wieków pokazuje, jak niezwykle ważne jest bezpieczeństwo własne oraz ochrona rzeczy wartościowych. Zamki należą do podstawowych i najważniejszych zabezpieczeń. Są ciągle ulepszane i coraz trudniejsze do sforsowania. W przyszłości należy spodziewać się ich dalszego rozwijania oraz wprowadzania coraz nowszych technik uwierzytelniania osób.

Maciej Prelich
Firma ATLine sp.j. Sławomir Pruski
mprelich@atline.pl

KaDe Premium Plus II

Integracja z rejestratorami IP marki NOVUS i systemem wind

Ryszard Sobierski

Program KaDe Premium Plus II, przeznaczony do stosowania w małych i średnich systemach kontroli dostępu, jest nieustannie rozwijany i wzbogacany w nowe funkcje. W najbliższym czasie zostanie udostępniona kolejna jego wersja. Oprócz kilku drobnych, ale bardzo użytecznych funkcji oferuje ona integrację z rejestratorami IP serii 6000 marki NOVUS i z prostym systemem kontrolującym pracę wind

Integracja z systemem telewizji dozorowej

Poprzednie wersje tego programu (KaDe Premium i KaDe Premium Plus) również umożliwiały prostą integrację z systemem telewizji dozorowej, ale dotyczyła ona rejestratorów współpracujących z kamerami analogowymi. Ze względu na to, że generacja wspomnianych urządzeń nie jest już oferowana przez AAT HOLDING, konieczna stała się integracja z nowymi modelami rejestratorów (typu NVR), kompatybilnymi z kamerami IP.

W ramach integracji umożliwiono skonfigurowanie połączenia IP z rejestratorem, który obsługuje pewną liczbę kamer (zależną od modelu). Po nawiązaniu komunikacji z rejestratorem IP program KaDe Premium Plus II pobiera z jego pamięci dane dotyczące liczby kamer i wyświetla symbole kamer w postaci ikon w specjalnym oknie pojawiającym się na pulpicie operatora. Eliminuje to konieczność powtórnej konfiguracji kamer. Po pobraniu listy kamer można przetestować komunikację z nimi, klikając poszczególne ikony i obserwując obraz w specjalnym okienku.

Kolejnym krokiem jest umieszczenie ikon kamer na mapie obiektu w miejscach faktycznej lokalizacji kamer. W trybie monitorowania operator może klikać te ikony w celu wyświetlenia obrazów z poszczególnych kamer. Podwójne kliknięcie otwiera okienko wizyjne – oddzielne dla każdej z kamer. Integracja umożliwia również stworzenie powiązań pomiędzy obrazami z kamer a elementami systemu kontroli dostępu, takimi jak czytniki i monitorowane linie dozorowe. Powiązanie powoduje automatyczne wyświetlenie obrazu z kamery przypisanej do danego elementu. Ta funkcja jest bardzo pożyteczna, ponieważ umożliwia operatorowi szybką weryfikację przyczyn zdarzenia.

W ramach opisywanej integracji umożliwiono również wyświetlanie obrazów z wielu kamer równocześnie. Operator ma do wyboru kilka opcji podziału ekranu monitora na okienka o różnej wielkości i możliwość szybkiego powiększenia wybranego obrazu.

Kolejnym elementem osiągniętym dzięki integracji jest sekcja raportów dotyczących zdarzeń i alarmów w trybie monitorowania w czasie rzeczywistym. W tej sekcji, oprócz listy zdarzeń lub alarmów, wyświetlane jest okienko wizyjne. Po wskazaniu wybranego zdarzenia lub alarmu kliknięciem w okienku tym odtwarzany jest materiał archiwalny zapisany przez rejestrator, tzn. obraz z kamery przypisanej do elementu związanego

z tym zdarzeniem (np. odczyt karty przez czytnik w systemie kontroli dostępu powoduje wyświetlenie nagranego obrazu z kamery przypisanej do danego przejścia). Odtwarzanie nagrania rozpoczyna się w momencie wystąpienia zdarzenia.

Integracja z systemem sterowania pracą wind

System kontroli dostępu spełnia swoje zadanie tylko wówczas, gdy jest szczelny. W związku z tym należy pamiętać również o zabezpieczeniu wind, jeżeli znajdują się one w danym budynku.

Najczęściej spotykane rozwiązania to:
- czytnik zainstalowany przed wejściem do windy,
- czytnik zainstalowany na panelu sterującym w kabinie windowej,
- czytnik zainstalowany na specjalnym panelu w holu windowym.

Za pomocą nowej wersji programu KaDe Premium Plus II można zrealizować pierwsze lub drugie rozwiązanie.

Pierwsze rozwiązanie działa analogicznie jak w przypadku czytnika kontrolującego wejście do chronionego pomieszczenia. Różnica polega tylko na tym, że przekaźnik kontrolera nie steruje zamkiem lecz zamyka obwód przycisku przywołania windy.

Fot. 1. Interfejs programu KaDe Premium Plus II

Fot. 2. Panel sterujący w kabinie windowej

W przypadku drugiego rozwiązania potrzebny jest nowy kontroler windy KDH-KS2000-IP-ELV wraz z modułem czterech przekaźników. Kontroler ten jest podobny do standardowego modelu KDH-KS2024-IP, ale ma inne oprogramowanie producenta (firmware). Wyposażony jest w pięć przekaźników, a moduł KDH-MOD2000-ELV w dodatkowe cztery. W sumie umożliwia to kontrolę dostępu do dziewięciu pięter. Wyjścia przekaźnikowe należy podłączyć przewodami do układu sterowania windą. Po odczycie karty w czytniku umieszczonym na panelu w kabinie windy do sterownika przesyłana jest informacja o tym, do których pięter użytkownik ma przydzielony dostęp. Układ sterowania windą aktywuje odpowiednie przyciski i użytkownik może wybrać piętro, na które chce się udać. W ustawieniach konfiguracyjnych programu znajduje się nowa pozycja służąca do przydzielania użytkownikom uprawnień dotyczących dostępu do wybranych pięter.

Pozostałe funkcje

Jak już wspomniałem, oprócz opisanych powyżej dwóch nowych funkcji integrujących w programie pojawiło się kilka nowych opcji.

Pierwsza z nich to opcja automatycznego dodawania kontrolerów IP do bazy danych systemu. W poprzednich wersjach programu należało wykonać dwie czynności w celu ich dodania. Na początku należało wyszukać kontrolery w sieci i przypisać im docelowe adresy IP. Następnie trzeba było ręcznie dodać każdy kontroler do systemu, wpisując ponownie adresy IP kontrolerów. W nowej wersji programu, po wybraniu opisywanej opcji, wyświetlana jest tabela z wyszukanymi kontrolerami IP. Podany jest w niej model każdego kontrolera, adres MAC oraz status – dodany/niedodany. Poza tym możliwe jest wpisanie docelowego adresu IP w kontrolerach, które chcemy dodać, i zapisanie całego zestawu adresów w bazie danych systemu. To znacznie przyspiesza i ułatwia konfigurowanie systemu przez instalatora.

Kolejną nową opcją jest możliwość generowania raportów dotyczących informacji o tym, do których drzwi dany użytkownik ma dostęp oraz informacji o tym, kto ma uprawnienia do korzystania z danego przejścia.

Nowością, o której warto wspomnieć, są też domyślne nazwy kontrolerów i użytkowników przypisywane im w procesie ich dodawania. Nazwy te w każdej chwili można zmienić na inne.

Polecam nową wersję oprogramowania wszystkim instalatorom i klientom, gdyż nowe możliwości, jakie stwarza, są bardzo użyteczne.

Ryszard Sobierski
AAT HOLDING

NOVUS® 7000 SERIA IP

RAID 4K HDMI 8 HDD

ipGO H.265

KOŁO RATUNKOWE DLA TWOICH DANYCH

WBUDOWANY KONTROLER RAID Z FUNKCJĄ HOT SPARE

AAT HOLDING S.A.

PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA

www.aat.pl

RODO a telewizja dozorowa

Gotowe rozwiązania firmy Hanwha Techwin

Piotr Rogalewski

25 maja 2018 r. we wszystkich krajach Unii Europejskiej wchodzi w życie Rozporządzenie o Ochronie Danych Osobowych (RODO). Ramy niniejszego artykułu pozwalają jedynie na bardzo ograniczoną analizę zapisów tego rozporządzenia, dlatego odnosi się on głównie do konsekwencji RODO dotyczących codziennej eksploatacji systemów telewizji dozorowej

RODO – ochrona danych na nowo

Media społecznościowe, e-bankowość, płatności elektroniczne, zakupy w sieci, profilowane reklamy, geolokalizacja, big data, upowszechnienie nadzoru wizyjnego z wykorzystaniem sieci IP oraz wiele innych nowych rozwiązań IT całkowicie odmieniło nasze codzienne życie i stało się to w bardzo krótkim czasie. Nie sposób było przewidzieć wszystkie możliwe konsekwencje, także te negatywne, jakie niosły ze sobą tak dynamiczne zmiany. Wycieki wielkich ilości danych, stalking, uporczywy telemarketing czy internetowy spam to tylko kilka przykładów. Regulacje RODO mają pomóc w ograniczeniu tych negatywnych zjawisk, a nade wszystko wprowadzić nowy porządek w zarządzaniu danymi osobowymi. Według RODO systemy telewizji dozorowej mogą generować i przetwarzać bardzo dużo danych osobowych, głównie w postaci obrazów twarzy osób znajdujących się w zasięgu działania wizyjnego systemu dozorowego. Oznacza to, że taki system gromadzi dane osobowe i sposób jego funkcjonowania musi spełniać wymogi rozporządzenia.

Co się zmieni?

Nowe reguły wynikające z rozporządzenia muszą być stosowane przez wszystkie przedsiębiorstwa, w tym osoby prowadzące działalność gospodarczą samodzielnie. Wprowadzenie katalogu zasad przetwarzania danych osobowych, nowe obowiązki dla przetwarzających dane, prawo do „bycia zapomnianym", prawo do przenoszenia danych, obowiązek zgłaszania naruszeń i nieprawidłowości czy wzmocnione prawo do dostępu i wglądu w nasze dane to tylko kilka najistotniejszych zmian wprowadzanych przez nowe rozporządzenie. Poniżej zajmiemy się ich analizą w praktycznym kontekście codziennej eksploatacji wizyjnych systemów dozorowych.

Zasada poufności

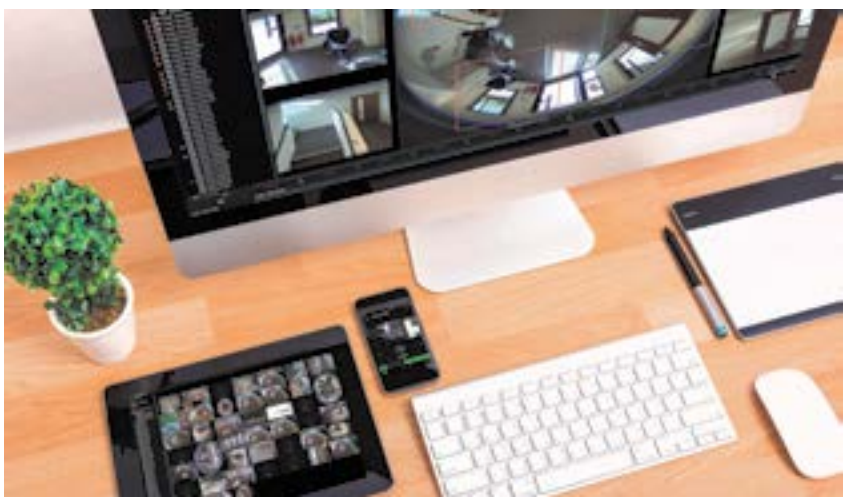
Zgodnie z tą zasadą należy wdrożyć środki zapobiegające ujawnieniu lub udostępnieniu gromadzonych danych nieuprawnionym podmiotom i (lub) ich przetwarzaniu. W przypadku wizyjnego systemu dozorowego oznacza to m.in. fizyczne zabezpieczenie samego urządzenia rejestrującego i dysków, ochronę dostępu na poziomie sieci czy właściwy stopień złożoności haseł, a także odpowiednie zabezpieczenie danych na wypadek ich nieuprawnionego pozyskania. Hanwha Techwin oferuje gotowe rozwiązania uwzględniające każdy z tych aspektów ochrony. Na przykład panel przedni rejestratora PRN-4011, zamykany na zamek, chroni fizycznie kieszenie z dyskami.

Fot. 1. Rejestrator PRN-4011 z fizycznym zabezpieczeniem dysków i logowaniem wieloma hasłami

Wymuszanie skomplikowanych i długich haseł używanych podczas logowania się znacznie utrudnia próby włamania metodą brutalnej siły (ang. *brute force*). Brak haseł domyślnych jest dodatkową ochroną na tym poziomie. Warto też wymienić filtrowanie adresów IP, które umożliwia zalogowanie się tylko konkretnym urządzeniom, oraz szyfrowanie plików konfiguracyjnych i oprogramowania układowego, które zapobiega próbie pozyskania loginu i hasła z wnętrza pliku. Szyfrowane są także pliki konfiguracyjne i tabele bazy danych oprogramowania zarządzającego (np. SSM i SmartViewer). Uwierzytelnianie użytkowników metodami SSL i TLS/EAP oraz możliwość współpracy z serwerami Radius stanowi bardzo ważne i skuteczne uzupełnienie systemu ochrony danych. Niezwykle istotna jest także możliwość zaszyfrowania kopii zapasowej, które gwarantuje ochronę materiału nawet w przypadku jego nieuprawnionego pozyskania. Na szczególną uwagę zasługuje funkcja automatycznego powiadamiania o podaniu nieprawidłowego hasła podczas logowania się, którą mają nowe modele urządzeń z serii Wisenet. Opisane wyżej metody zabezpieczenia oferuje znakomita większość rejestratorów, kamer IP oraz oprogramowania Hanwha Techwin, a niektóre z tych metod są umożliwione nawet przez klawiatury sterujące.

Zasada integralności

Zasada integralności narzucona w RODO oznacza obowiązek uniemożliwienia modyfikacji, usuwania i dodawania danych w sposób nieupoważniony, a także obowiązek zabezpieczenia ich przed zniszczeniem. W przypadku wizyjnych systemów dozorowych rozwiązania wynikające z konieczności przestrzegania tej zasady pokrywają się w dużej części z rozwiązaniami przedstawionymi wyżej, w opisie zasady poufności. Dodatkowo, w odniesieniu do zabezpieczenia danych przed zniszczeniem, warto wymienić zapis macierzowy RAID-5 i RAID-6, zapis awaryjny bezpośrednio na kartach SD umieszczonych wewnątrz kamer, automatyczne przywracanie kopii zapasowej ARB, redundancję Failover n+1



Fot. 2. Oprogramowanie Wisenet Wave z funkcją serwerów zapasowych

rejestratorów czy rozwiązania wysokiej dostępności na poziomie serwerów. To wszystko jest oferowane przez wybrane rejestratory IP serii Wisenet oraz oprogramowanie SSM i Wisenet Wave (to ostatnie działa w systemach operacyjnych Windows, Linux i Apple/Mac).

Zasada minimalizacji danych

Zgodnie z kolejną zasadą podaną w RODO zakres gromadzonych danych osobowych musi być ograniczony do niezbędnego minimum oraz adekwatny do celu ich gromadzenia. W przypadku rejestracji obrazu praktycznym sposobem przestrzegania tego wymogu jest zdefiniowanie

Fot. 3. Kamera serii Wisenet X z funkcją ARB, umożliwiająca lokalny zapis do 512 GB

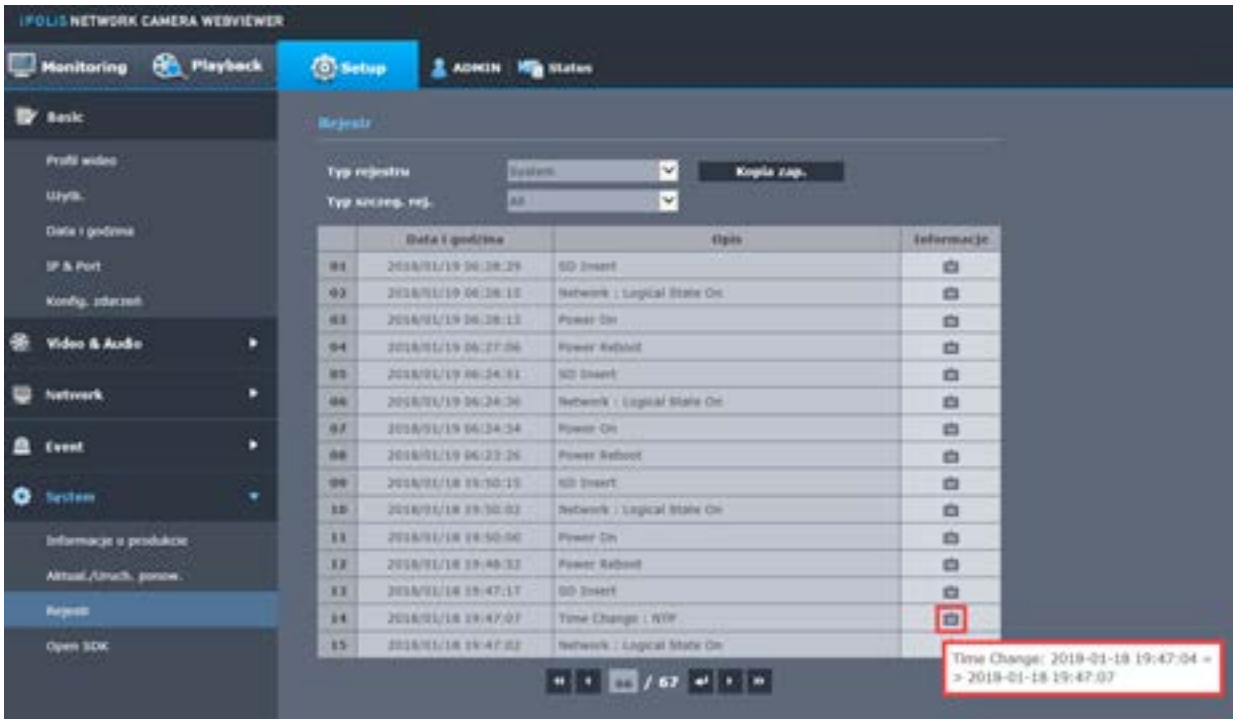
retencji danych. Proste wyliczenie szacowanego czasu zapisu jest niestety niewystarczające, gdyż z powodu zmienności czynników środowiskowych (takich jak poziom oświetlenia, szumy czy ilość ruchu w kadrze) zmienia się także zajętość miejsca na dyskach i nie można precyzyjnie określić docelowego czasu rejestracji materiału. Aby rozwiązać ten problem, Hanwha Techwin wprowadziła w swoich rejestratorach Wisenet funkcję kontroli retencji danych, która pozwala na precyzyjne określenie, po jakim czasie gromadzone dane mają zostać usunięte, nawet jeśli zastosowane dyski umożliwiają ich dalsze przechowywanie. Co istotne, funkcja ta jest dostępna także w kamerach IP serii Wisenet wyposażonych w gniazda dla kart SD, co jest kluczowe w przypadku wykorzystania zapisu awaryjnego wewnątrz kamer.

Zasada ograniczenia celu

Zgodnie z tą zasadą cel przetwarzania danych musi być wyraźnie określony, a proces przetwarzania nie może wykraczać poza realizację tego celu. Dotyczy to także ograniczenia dostępu do zbioru danych dla użytkowników, którzy przetwarzania dokonują, oraz możliwości okresowych przeglądów i modyfikacji ich uprawnień. W przypadku wizyjnych systemów dozorowych bardzo ważne jest skuteczne zarządzanie listą użytkowników ich uprawnieniami do dostępu do danych i do ich przetwarzania, np. do podglądu obrazu w czasie rzeczywistym, odtwarzania lub kopiowania materiału, łączności zdalnej. Uprawnienia do korzystania z poszczególnych funkcji można określać bardzo szczegółowo zarówno w rejestratorach IP, jak i w oprogramowaniu firmy Hanwha Techwin. Ograniczenie dostępu można określać niezależnie dla każdego z użytkowników, niezależnie dla każdej z kamer, niezależnie dla trybu podglądu, trybu odtwarzania i trybu kopii zapasowej. Możliwość wprowadzania wielu haseł, dostępna w przypadku wybranych modeli stanowi dodatkowe zabezpieczenie w procesie ograniczania celu przetwarzania.

Zasada rozliczalności

Zasada rozliczalności polega na nałożeniu na administratora systemu obowiązku wykazania, że wszystkie operacje wykonywane na zbiorze danych osobowych są zgodne z regulacjami RODO. Zasada ta nakłada również obowiązek zgłaszania organowi nadzorującemu wszelkich nieprawidłowości i naruszeń rozporządzenia. Na terenie RP takim organem jest GIODO. Na przykład atak hakerski na stronę internetową czy wyciek danych należy zgłosić najpóźniej w ciągu 72 godzin. W przypadku wizyjnych systemów dozorowych przestrzeganie zasady rozliczalności wiąże się bardzo ściśle z zastosowaniem środków technicznych mających na celu uwzględnienie opisanej wyżej zasady ograniczenia celu oraz innych zasad, np. umożliwiających bieżącą kontrolę aktywności użytkowników i osób nimi zarządzających. Doskonale sprawdzą się dzienniki systemowe i dzienniki zdarzeń, dostępne we wszystkich urządzeniach sieciowych i oprogramowaniu firmy Hanwha Techwin. Dzięki dużej szczegółowości



Fot. 4. Szczegółowy dziennik zdarzeń na przykładzie kamer Wisenet

wpisów w dziennikach można sprawdzić np. nie tylko, kto i kiedy utworzył, usunął czy zmodyfikował konto nowego użytkownika, wykonał kopię zapasową, zmienił czas systemowy itp., ale także ustalić, jakie nowe dane wprowadzono oraz z jakiego adresu IP dokonano zmian. Powiadamianie w czasie rzeczywistym o podejrzanych działaniach lub nietypowych zdarzeniach (np. o wielokrotnym wpisaniu błędnego hasła czy utracie połączenia sieciowego) również ułatwia przestrzeganie zasady rozliczalności.

Opisane wyżej funkcje produktów firmy Hanwha Techwin umożliwiają spełnienie wymagań RODO w przypadku wizyjnych systemów dozorowych. Oczywiście nie zostały tu omówione wszystkie zasady narzucone przez RODO i wszystkie rozwiązania firmy Hanwha Techwin, które ułatwiają dostosowanie się do nowych przepisów, dlatego gorąco zachęcamy do bezpośredniego kontaktu z przedstawicielami firmy w Polsce oraz do zapoznania się z informacjami dostępnymi na stronie www.hanwha-security.eu.

Piotr Rogalewski
p.rogalewski@hanwha.com
Hanwha Techwin Europe

CALLISTO 32
SECURITY SOLUTION

ZABEZPIECZ SWÓJ DOM

NOWA ODSŁONA CENTRALI **CALLISTO 32**

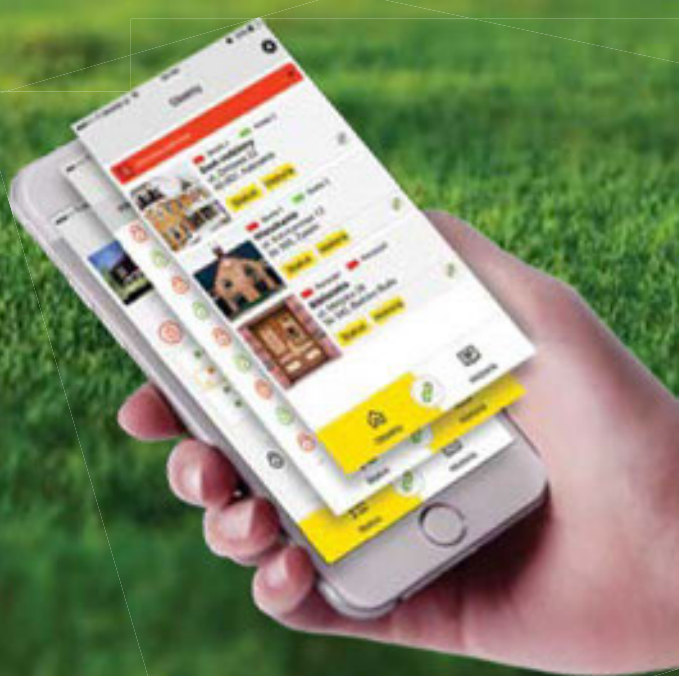
ELASTYCZNOŚĆ INSTALACJI
Obsługa 32 linii bezprzewodowych i do 14 przewodowych.

DOSTĘP MOBILNY
Bezpłatna, intuicyjna aplikacja AVA na smartfony. Komunikaty SMS o najważniejszych zdarzeniach.

ŁATWE PROGRAMOWANIE
Innowacyjne i banalnie proste konfigurowanie centrali za pomocą Twojego telefonu. Wystarczy 7 minut.

PEWNOŚĆ
Rozbudowana funkcjonalność zabezpieczenia centrali przed nieautoryzowaną rekonfiguracją i przywróceniem ustawień fabrycznych centrali.

NIEZAWODNOŚĆ
Pewne zasięgi, stabilny system, szyfrowane połączenia.



DO ZARZĄDZANIA SYSTEMEM ALARMOWYM

AVA Alert View App

DO ŁATWEGO PROGRAMOWANIA

AVA Install

WWW.CALLISTOALARM.PL
SALES@EBS.PL

EBS CREATING A SENSE OF SECURITY SINCE 1989

ZAPRASZAMY NA TARGI SECUREX 2018
W POZNANIU - PAWILON 7A, STOISKO 1

securex POLAND Międzynarodowe Targi Zabezpieczeń

Sztuczna inteligencja
w systemach bezpieczeństwa

Maciej Pietrzak

Sztuczna inteligencja jest rozwijana w wielu dziedzinach techniki, które mają bezpośredni wpływ na życie każdego z nas. Od jakiegoś czasu jest jednym z głównych przedmiotów zainteresowania branży zabezpieczeń

Fot. 1. Działanie algorytmu rozpoznawania twarzy

Aby zrozumieć pojęcie sztucznej inteligencji, należy cofnąć się do roku 1950, kiedy to Alan Mathison Turing zaproponował test, który miał na celu uzyskanie odpowiedzi na pytanie o to, czy maszyna może myśleć i czy robi to w sposób podobny do człowieka. Zadaniem maszyny było odpowiadanie na pytania człowieka w taki sposób, by rozmówca nie był w stanie rozstrzygnąć, czy rozmawia z człowiekiem czy z maszyną.

W kontekście sztucznej inteligencji zastosowanie mają specyficzne – inne niż tradycyjne – definicje uczenia się. Według Herberta Simona uczenie się w przypadku systemu polega na umiejętności adaptacji polegającej na ponownym wykonaniu takiego samego lub podobnego zadania bardziej efektywnie. Wynika z tego, że uczenie się to automatyczny proces mający na celu samodoskonalenie. Uczący się system gromadzi dane, szuka schematów, wyciąga wnioski i tworzy reguły. Samodzielnie opracowane schematy zachowania są nieustannie doskonalone. W takim procesie uczenia się niezbędny jest nadzór. Operator wprowadza przykłady i na bieżąco eliminuje błędy w działaniu systemu. Głębokie uczenie się (ang. *deep learning*) w odróżnieniu od samodzielnego uczenia się maszyn lub systemów (ang. *machine learning*) może przebiegać bez nadzoru.

Aktualnie jesteśmy świadkami ogromnego przyspieszenia rozwoju systemów bazujących na sieciach neuronowych. Internet rzeczy pozwala na pozyskiwanie ogromnych ilości danych z otoczenia, a przetwarzanie danych w chmurze i przetwarzanie z wykorzystaniem GPU (ang. *graphics processing unit*) umożliwia korzystanie z ogromnej mocy obliczeniowej, która jest koniecznie potrzebna w przypadku algorytmów uczenia się.

Jakie zadania stawiamy przed sztuczną inteligencją? Między innymi rozpoznawanie mowy i obrazu, przetwarzanie języka naturalnego. Takie zastosowania są codziennością. Mechanizmy sztucznej inteligencji otaczają nas zewsząd. Jadąc samochodem, większość z nas korzysta z nawigacji GPS, która wskazuje najkrótszą drogę dojazdu. Przy planowaniu trasy brana jest pod uwagę nie tylko odległość od celu, ale również takie zmienne jak utrudnienia na trasie. Innym przykładem sztucznej inteligencji jest medyczny system ekspercki wykorzystujący ogromną bazę danych, dzięki któremu w ułamku sekundy można uzyskać wstępną diagnozę po podaniu symptomów. Korzystając z przeglądarki Google, również mamy do czynienia z mechanizmami sztucznej inteligencji.

Branża zabezpieczeń może pochwalić się bardzo dużą intensywnością implementacji wszelkich nowinek technicznych. Producenci elementów systemów zabezpieczeń pokładają wielkie nadzieje w mechanizmach głębokiego uczenia się. Aktualnie możemy zacząć korzystać z pierwszych wdrożeń.

Dahua Technology, lider w dziedzinie systemów zabezpieczeń, jako jedna z pierwszych firm na świecie stworzyła (we współpracy z firmami Intel oraz nVidia) kamerę oraz rejestrator z zaimplementowanymi mechanizmami sztucznej inteligencji wykorzystującymi algorytmy głębokiego uczenia się. Kamera IP typu DH-HF8242F-FD/FR z serii Deep Sense to efekt wieloletnich doświadczeń firmy Dahua Technology w dziedzinie konstrukcji kamer. Wysokiej jakości obraz jest przetwarzany przez procesor Movidius wykorzystujący algorytmy głębokiego uczenia się. Wykorzystany w kamerze przetwornik obrazu 2 Mpx 1/1.9" CMOS to gwarancja doskonałego i bogatego w szczegóły obrazu wytwarzanego zarówno w dziennych, jak i nocnych warunkach oświetleniowych. Dodatkowo kamera ma wiele funkcji, takich jak WDR, HLC, BLC, AWB, AGC, 3DNR. Zadaniem algorytmu uczenia się jest detekcja i rozpoznawanie twarzy. Kamera analizuje obserwowaną scenę w poszukiwaniu twarzy. W momencie detekcji algorytm analizuje obraz. Operator otrzymuje informację o wykryciu twarzy wraz z opisanym zdjęciem. W opisie są informacje o wieku, płci, wyrazie twarzy oraz inne szczegóły. Zdjęcie jest porównywane z obrazami zebranymi w obszernej bazie danych. Baza mieści do 10 000 obrazów twarzy. Użytkownik jest informowany o podobieństwie wykrytej twarzy do wizerunku twarzy z bazy oraz o stopniu podobieństwa wyrażonym procentowo. Kryteria porównywania twarzy są

Fot. 2. Kamera Dahua Technology IPC-HF8242F-FR

konfigurowalne. Kamera DH-HF8242F-FD/FR jest w stanie wykryć do szesnastu twarzy w jednej scenie i porównać je z wizerunkami z bazy. Wszystkie te funkcje są dostępne z poziomu przeglądarki internetowej.

W kamerze Dahua służącej do rozpoznawania twarzy dostępny jest interfejs RESTful API, co umożliwia dostęp do platformy również w przypadku urządzeń lub oprogramowania firm trzecich. Wybór dostępnych rozwiązań jest duży, a doświadczony dział wsparcia firmy Dahua jest gotowy do pomocy w procesie integracji z zewnętrzną aplikacją API.

Na uwagę zasługuje to, że skuteczność algorytmu rozpoznawania twarzy została w 2016 r. przebadana, a rozwiązanie firmy Dahua Technology zajęło pierwsze miejsce w rankingu Labeled Faces in the Wild (LFW).

Kamera współpracuje z serwerem Dahua IVS-F7500. To urządzenie również zostało wzbogacone w algorytmy pozwalające na wykrywanie i rozpoznawanie twarzy. Serwer jest w stanie przeszukiwać nagrania archiwalne i wskazywać tylko te fragmenty nagrań, w których występuje rozpoznana osoba.

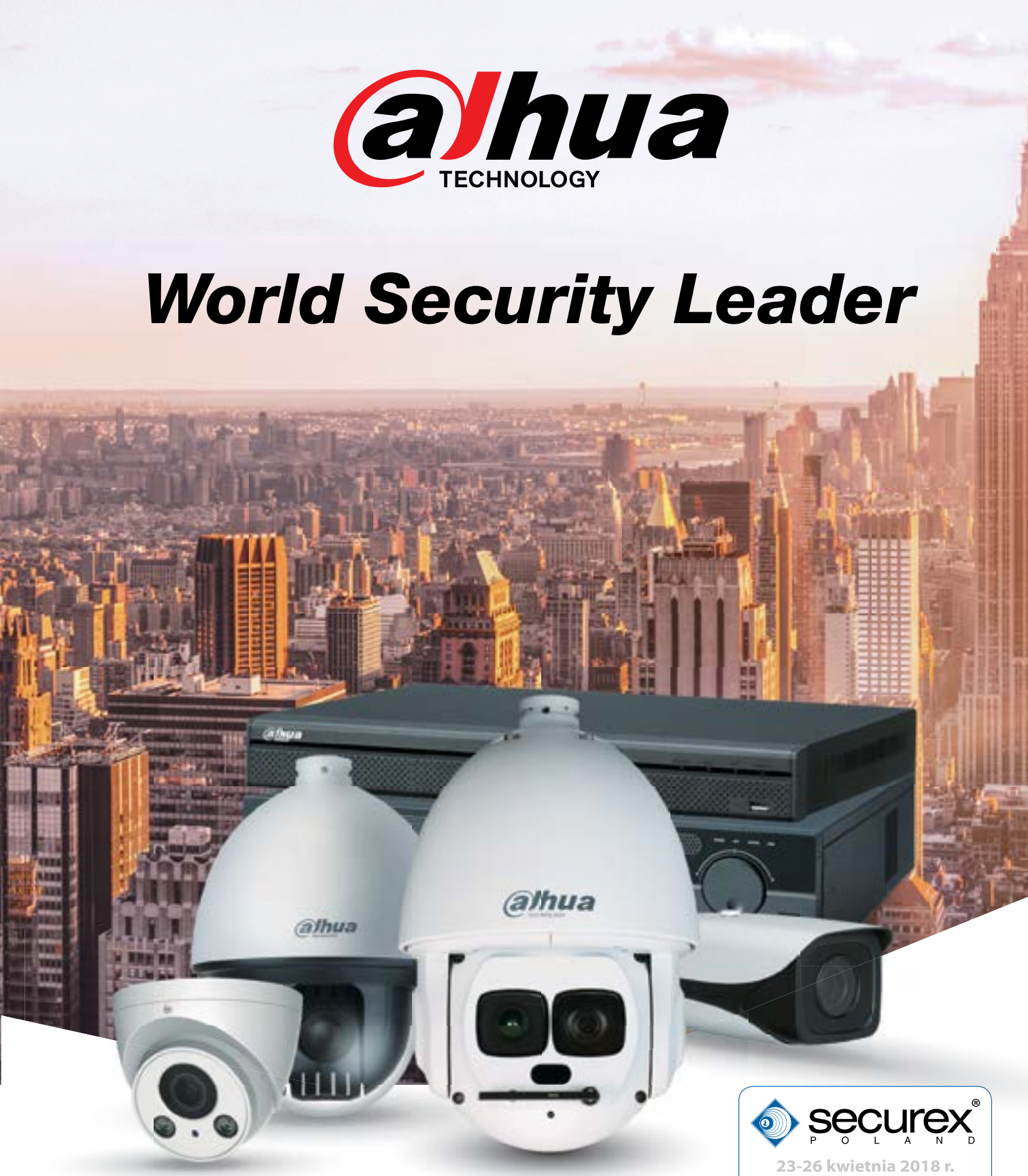
Jak widać, pojawiają się nowe możliwości dla projektantów, producentów, a przede wszystkim użytkowników systemów zabezpieczających. Otrzymują oni potężne narzędzie, dzięki któremu można uzyskać nieosiągalny do tej pory poziom bezpieczeństwa. System rozpoznawania twarzy opracowany przez firmę Dahua Technology z pewnością znajdzie zastosowanie w takich miejscach jak obiekty chronione systemami kontroli dostępu, miejsca publiczne, centra handlowe, dworce i lotniska oraz galerie handlowe. Służbom dbającym o bezpieczeństwo umożliwia wykrycie w tłumie osób poszukiwanych i śledzenie trasy, po której się poruszają.

Rozwiązania oferowane przez firmę Dahua Technology ponownie udowadniają, że głównym celem tego producenta jest rozwój. Dzięki temu samodzielnie uczące się systemy bezpieczeństwa to nie przyszłość, ale teraźniejszość.

Maciej Pietrzak
Dahua Technology Poland

alhua TECHNOLOGY

World Security Leader



securex® POLAND

23-26 kwietnia 2018 r.

PAWILON 8A
STOISKO 13

Serdecznie zapraszamy!

CE FC ISO 9001:2000

www.dahuasecurity.com/pl

Dahua Technology Poland Sp. z o.o.

ul. Salsy 2, 02-823 Warszawa
tel. +48 22 395 74 00, fax +48 22 395 74 10
e-mail: biuro.pl@global.dahuatech.com
www.dahuasecurity.com/pl

Dziesięć trendów w 2018 roku

Johan Paulsson

Jak mawiał grecki filozof Heraklit, życie jest ciągłą zmianą. Potwierdzi to każdy, kogo praca jest związana z techniką. Tempo wprowadzania innowacji jest tak duże, że nawet najdziwniejsze fantazje dotyczące przyszłości mogą szybko przerodzić się w rzeczywistość

Istniejące techniki i technologie w pewnym momencie osiągają kres swoich możliwości, co zmusza do poszukiwania nowych rozwiązań. Wraz ze współpracownikami wybraliśmy najbardziej istotne naszym zdaniem tegoroczne trendy rozwojowe w dziedzinie systemów dozoru wizyjnego.

1. Nacisk na wykorzystanie urządzeń peryferyjnych

Z dwóch niezaprzeczalnych dobrodziejstw technicznych ostatnich lat – chmury obliczeniowej i Internetu przedmiotów (ang. *Internet of Things – IoT*) – korzystają użytkownicy biznesowi i indywidualni. Efektem popularności obu tych rozwiązań jest jednak znaczne zwiększenie ilości danych przesyłanych do centrów danych w celu ich przechowywania lub przetwarzania, do czego z kolei wymagana jest określona przepustowość sieci. Odpowiedzą na to wyzwanie jest przetwarzanie danych w urządzeniach peryferyjnych (ang. *edge computing*), czyli blisko źródła danych. Pozwala to zredukować wymagania dotyczące łącz przesyłających dane z czujników i innych urządzeń peryferyjnych do centrum obróbki danych. Umożliwia też zachowanie anonimowości i szyfrowanie danych przed ich przesłaniem.

Stopień technicznego zaawansowania i jakość kamer sieciowych, urządzeń fonicznych i innych czujników (urządzeń peryferyjnych) stale rośnie, dlatego konieczne jest zrównoważenie intensywności przetwarzania w chmurze i w urządzeniach peryferyjnych, tak by dostarczane dane były precyzyjne, wiarygodne i użyteczne.

2. Chmura obliczeniowa

Powszechność przetwarzania danych w urządzeniach peryferyjnych nie oznacza wyparcia z infrastruktury informatycznej chmury obliczeniowej. Określenie *chmura obliczeniowa* sugeruje strukturę pojedynczą, jednak faktycznie odnosi się do wielu chmur wykorzystywanych na całym świecie. Wzrasta liczba firm oferujących usługi mające związek z przetwarzaniem danych w chmurze, dlatego systemy chmurowe są stosowane coraz częściej (zamiast tradycyjnych systemów lokalnych).

Jedną z korzyści wynikających z integracji różnych usług chmurowych jest ograniczenie zakresu niezbędnych usług informatycznych świadczonych w centrach obróbki danych. Dzięki interfejsom API możliwe jest tworzenie i wdrażanie zaawansowanych algorytmów analizujących treść obrazu, zarządzających pracą pamięci masowych etc. Zadaniem organizacji oferujących usługi bazujące na wykorzystaniu chmury pozostaje kontrolowanie ewentualnej integracji usług w celu usprawnienia obsługi klientów i partnerów.

3. *Machine learning, deep learning*

Osiągnęliśmy już poziom umożliwiający czerpanie korzyści z uczenia się maszyn lub systemów (ang. *machine learning*) oraz ich tzw. głębokiego uczenia się (ang. *deep learning*).

Posiadamy ogromne zbiory danych do analizy, wystarczającą moc obliczeniową do wykonania zadania w rozsądnym czasie, zaawansowane algorytmy oraz bogate doświadczenie. Potencjał analityczny wynikający z możliwości głębokiego uczenia się systemów jest imponujący, a w branży zabezpieczeń może być wykorzystany m.in. do interpretacji treści obrazu, rozpoznawania mowy i pomocy przy podejmowaniu decyzji.

Wykorzystanie głębokiego uczenia się przez programy pozwala usprawnić wizyjne funkcje detekcji ruchu, rozpoznawania twarzy oraz śledzenia obiektów, a także wyeliminować fałszywe alarmy. Aplikacje ułatwiają projektowanie, konfigurację, optymalizację oraz zarządzanie urządzeniami w systemie. Wraz z rozwojem aplikacji pojawia się możliwość dokonywania analiz predykcyjnych mających na celu zapobieganie bardzo różnym zdarzeniom (np. upadkom i poślizgnięciom, kradzieżom w sklepach, kolizjom drogowym, atakom terrorystycznym, samobójstwom na torach kolejowych).

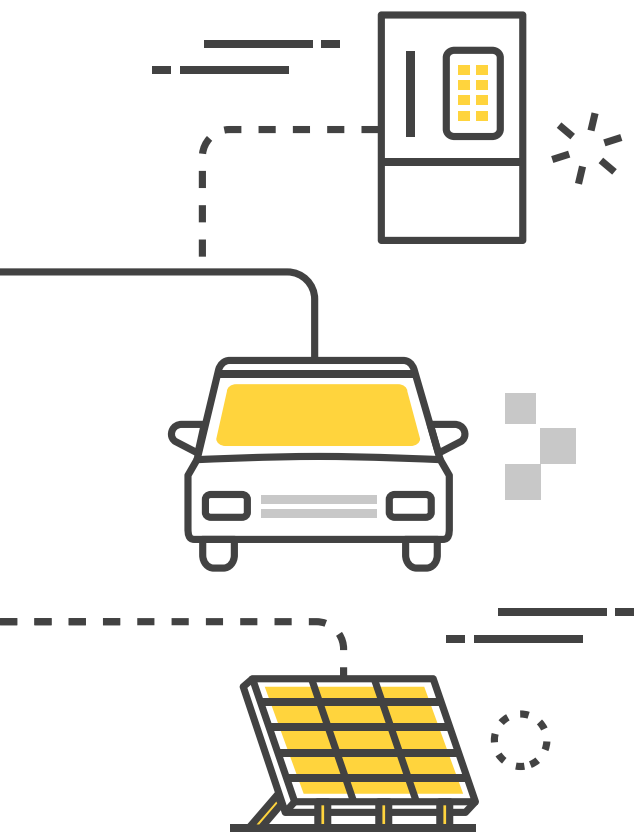
Jesteśmy w dalszym ciągu na wczesnym etapie rozwijania *machine learning* i *deep learning*, ale rozwój postępuje szybko i nieprzewidywalnie. Zapotrzebowanie na moc obliczeniową jest ogromne, a potencjał głębokiego uczenia się, które definitywnie prowadzi do autonomiczności systemów, jest olbrzymi.

4. Personalizacja usług a prywatność

Jednym z potencjalnych zastosowań głębokiego uczenia się jest dostarczanie spersonalizowanych usług. Wyobraźmy sobie galerię handlową, w której twarz klienta rozpoznawana jest tuż po wejściu do sklepu, i w której – na podstawie poprzednich zakupów, preferencji czy nawet ostatnio oglądanych towarów – na jego telefon komórkowy przesyłane są oferty dotyczące konkretnych towarów i usług. To, że taka sytuacja jest możliwa, nie oznacza, że powinna mieć miejsce. Paradoksalnie unaocznia ona raczej potrzebę zachowania prywatności w zderzeniu z niemal niekontrolowanym wykorzystaniem danych osobowych przez sektor komercyjny i rozmaite organizacje.

Obecnie tworzone są przepisy prawne regulujące te kwestie. Na obszarze Unii Europejskiej ogólne rozporządzenie o ochronie danych (General Data Protection Regulation) ma wejść w życie w maju 2018 roku, by zunifikować ochronę danych obywateli niezależnie od miejsca i sposobu ich przechowywania i wykorzystania.

Konieczność zrównoważenia coraz większej personalizacji usług oraz ochrony prywatności i danych osobowych będzie przedmiotem zainteresowania wszystkich organizacji w bieżącym roku bez względu na to, czy zrównoważenie to będzie wynikać z przepisów czy ze zwykłej przyzwoitości.



5. Cyberbezpieczeństwo

Tak jak wcześniej, cyberbezpieczeństwo musi pojawić się na liście trendów na rok bieżący i kolejne lata. Poprawa czy zmiana zabezpieczeń pozostanie ciągła, ponieważ dobrze przygotowani cyberprzestępcy nie zaniechają prób wykorzystania luk w zabezpieczeniach lub programach. W związku z tym, że liczba urządzeń pracujących w sieci rośnie wykładniczo, wzrasta ryzyko występowania błędów w oprogramowaniu, które należy nieustannie identyfikować i naprawiać. Brak reakcji może skutkować włamaniami przez sieć, zarażeniem szkodliwym oprogramowaniem typu ransomware czy wystąpieniem awarii, której naprawa może być kosztowna. Należy aktywnie i systematycznie wprowadzać uaktualnienia w programach – jak najszybciej po ich udostępnieniu (pomocą może być nasz dokument *Zalecenia dotyczące polepszenia funkcjonalności i bezpieczeństwa sieciowego*).

6. Platformy IoT

W dziedzinie Internetu przedmiotów osiągnięty został punkt, w którym efektywne skalowanie, zbieranie i analiza danych oraz skuteczne zarządzanie siecią urządzeń jest możliwe dzięki zastosowaniu skalowalnej architektury. Tzw. platformy IoT umożliwiają urządzeniom pochodzącym od różnych producentów współpracę i sprawną wymianę informacji celem utworzenia inteligentnych systemów przy użyciu istniejącej infrastruktury sieciowej. Obsługą urządzeń IoT zajmuje się już wiele firm. Są wśród nich dostawcy oprogramowania o ugruntowanej pozycji. Pojawia się też wiele nowych inicjatyw. Przewidywany jest dalszy rozwój tego rynku w bieżącym roku. W przyszłości istotne będzie opracowanie międzynarodowych standardów zapewniających współpracę różnych platform IoT obsługujących systemy kompleksowo, bez względu na ich producenta.

7. Łańcuch bloków – więcej niż bitmoneta

Dla wielu osób słowa *łańcuch bloków* (ang. *blockchain*) i *bitmoneta* (ang. *bitcoin*) oznaczają to samo. W rzeczywistości nie są one równoznaczne. Transakcja z wykorzystaniem bitmonet musi zostać potwierdzona w łańcuchu bloków, którego potencjał weryfikacyjny jest właściwie nieograniczony. W tym roku łańcuch bloków będzie testowany w licznych zastosowaniach w wielu sektorach.

Przy założeniu, że łańcuch bloków zapewnia uwierzytelnienie dowolnej treści, mógłby on być stosowany w naszej branży do weryfikacji treści obrazów pochodzących z wielu źródeł, np. z używanych przez służby porządkowe kamer nasobnych, z których materiał może być wykorzystany w postępowaniu sądowym. Co więcej, mógłby posłużyć do autoryzacji urządzeń dołączonych do sieci kamer.

8. Likwidowanie ograniczeń inteligentnego miasta

Od kilku lat w publicznej przestrzeni miejskiej umieszcza się różnego rodzaju urządzenia (np. kamery, czujniki) mające pozytywnie wpłynąć na jakość życia mieszkańców, np. sprawdzać stopień zanieczyszczenia powietrza, poprzez nadzór wizyjny umożliwiać zapobieganie lub przeciwdziałanie naruszaniu prawa. Liczba mieszkańców miast stale rośnie (do roku 2050 populacja miast wzrośnie o 25%), dlatego urządzeń wspomagających tworzenie przyjaznego, zrównoważonego i bezpiecznego środowiska miejskiego będzie coraz więcej.

Wizja inteligentnego miasta jest kojarzona z rozwojem bazującej na bezpiecznych technikach informatycznych, technikach przetwarzania danych, technikach komunikacji oraz IoT infrastruktury umożliwiającej zarządzanie. Zarządzanie to miałoby objąć systemy informacyjne jednostek samorządowych, szkoły, biblioteki, systemy transportu, szpitale, elektrownie, sieci wodociągowe, gospodarkę komunalną, służby interwencyjne i usługi miejskie.

Większość struktur miejskich działa indywidualnie, co stanowi barierę w wymianie informacji i tym samym utrudnia realizację koncepcji inteligentnego miasta. Miasto jest prawdziwie inteligentne, gdy wszystkie dane są dostępne i możliwe do wykorzystania przez każdą ze służb miejskich bądź jednostek administracyjnych. Skuteczne zarządzanie i radzenie sobie z takimi wyzwaniami jak zapewnienie bezpieczeństwa mieszkańcom, zapobieganie przeciążeniom w ruchu ulicznym, starzejąca się infrastruktura czy reakcje na zdarzenia w rodzaju katastrof naturalnych lub ataków terrorystycznych wymaga skoordynowanych analiz dostępnych danych celem dostarczenia odpowiednich i efektywnych rozwiązań.

9. Czujniki inne niż wizyjne wnoszą nową jakość

Do tej pory źródłem podstawowych, o ile nie jedynych danych dostępnych dla operatorów systemów dozorowych były dwuwymiarowe obrazy z kamer. Nowe, niewizyjne czujniki pozwolą na uzyskanie danych wielowymiarowych, umożliwiających szybszą i dokładną ocenę sytuacji, a co za tym idzie szybką reakcję, podjęcie odpowiednich działań oraz minimalizację liczby fałszywych alarmów.

Dobrym przykładem mogą być radarowe metody wykrywania ruchu wykorzystujące fale elektromagnetyczne. Radar nie reaguje na czynniki, które zwykle wywołują fałszywe alarmy, takie jak przemieszczające się cienie czy smugi światła, małe zwierzęta, krople deszczu, owady, wiatr czy inne czynniki atmosferyczne, i jest w stanie podać dokładną pozycję obiektu oraz kierunek jego ruchu. Z innych technik można by tu wymienić dobrze znane obrazowanie termowizyjne, a także detekcję dźwięku. Postęp w rozwoju tej drugiej dziedziny oznacza pozyskiwanie informacji, których nie uzyskuje się poprzez analizę obrazu.

10. Wykorzystanie wirtualnych asystentów i tzw. rozszerzonej rzeczywistości w biznesie

Ostatni rok przyniósł znaczący wzrost zainteresowania wirtualnymi asystentami. Amazon Alexa, Google Home, Apple Siri i Microsoft Cortana ugruntowały już swoje pozycje w dziedzinie zarządzania codzienną aktywnością użytkowników. W przyszłości wirtualni asystenci będą wykorzystywani przez inne serwisy, np. Facebook. Wirtualne wsparcie obejmujące kompletację, instalację, konfigurację urządzeń i zarządzanie systemami będzie nie tylko oczekiwane, ale wręcz wymagane od dostawców produktów i usług.

Te same oczekiwania dotyczą tzw. rozszerzonej rzeczywistości (ang. *augmented reality* – AR) jako techniki, która ujawniła swój ogromny potencjał biznesowy, a pierwotnie była wykorzystywana tylko w niektórych dziedzinach, takich jak wojskowość i lotnictwo. W naszej branży rozszerzona rzeczywistość może służyć na przykład do tego, by potrzebne dane były prezentowane w pełniejszej formie, np. wizualnej, co oczywiście może mieć zastosowanie np. w nadzorze wizyjnym oraz podczas instalacji i konserwacji systemów.

Oto 10 istotnych, jak sądzimy, trendów, które będą miały wpływ na rozwój systemów dozoru wizyjnego w roku 2018. Są to jednak tylko nasze przewidywania. Być może dostrzegają Państwo inne kierunki rozwoju naszej branży?

Johan Paulsson
Axis Communications
Opracowanie: Redakcja

Międzynarodowe Targi Poznańskie

prawdziwe spotkania

securex® POLAND

Międzynarodowe Targi Zabezpieczeń

23-26.04.2018

POZNAŃ

Securex to:

- **Największe wydarzenie biznesowe przemysłu zabezpieczeń w Środkowo-Wschodniej Europie**
- **Arena** dla prezentacji nowości produktowych i innowacyjnych rozwiązań
- **Możliwość** zaprezentowania oferty szerokiemu gronu odbiorców (instytucjonalnych i prywatnych), projektantom, dostawcom, integratorom oraz instalatorom
- **Szansa** na sprawdzenie swojej oferty pod kątem konkurencyjności i innowacyjności
- **Okazja** do spotkania twarzą w twarz z potencjalnymi partnerami biznesowymi z rynku polskiego oraz zagranicznego i zbudowanie nowych perspektywicznych relacji z klientami
- **Możliwość** uczestniczenia w programie wydarzeń: konferencje i szkolenia, debaty, pokazy

Zabezpiecz swój sukces!

Wiedza i doświadczenie na Securex

- VI Mistrzostwa Polski Instalatorów Systemów Alarmowych
- Inteligentny Budynek
- Securex BeIN – cyberbezpieczeństwo
- Drone Zone
- Forum Bezpieczeństwa Społeczności Lokalnych – przeciwdziałanie współczesnym zagrożeniom (w tym terrorystycznym)
- Pokazy specjalne

Targi z rekomendacją Polskiej Izby Przemysłu Targowego

www.securex.pl

WES+

Innowacyjny system ochrony przeciwpożarowej na budowie

Geo-Kat

Plac budowy jest narażony na zagrożenia. Jednym z największych jest zagrożenie pożarem. Na skutki pożaru ma wpływ szybkość rozprzestrzeniania się ognia, brak instalacji przeciwpożarowych czy trudności w komunikacji i sygnalizacji zagrożenia przy wykonywaniu prac budowlanych. To wszystko może spowodować narażenie zdrowia i życia pracowników przebywających na terenie budowy oraz straty materialne. Jak efektywnie zadbać o bezpieczeństwo ludzi i mienie firmy? Kluczem do sukcesu jest WES+ - mobilny i bezprzewodowy system sygnalizacji pożarowej, który jest zastosowany już w 80% nowych inwestycji w Wielkiej Brytanii

WES+ to innowacyjny produkt przeznaczony do ochrony ludzi, terenu i zaplecza budowy, infrastruktury przemysłowej oraz do innych tymczasowych zastosowań. Jego zaletą jest to, że pozwala zabezpieczyć inwestycje budowlane już w momencie pojawienia się pierwszych kontenerów na placu budowy. Mobilny, bezprzewodowy system sygnalizacji pożaru WES+ to jedyne w swoim rodzaju dostępne na rynku rozwiązanie, certyfikowane zgodnie z wymaganiami normy PN-EN 54, które spełnia wymogi i zalecenia ubezpieczycieli oraz umożliwia łatwe i niedrogie zabezpieczenie terenu budowy.

Zintegrowany system

System składa się z kilku kluczowych elementów. Głównym z nich jest stacja bazowa, która umożliwia centralne zarządzanie wszystkimi jednostkami pracującymi w systemie. Spełnia ona rolę huba. Zastosowano także moduł GSM umożliwiający transmisję danych oraz powiadamianie według różnych scenariuszy osób wprowadzonych do systemu. Stacja bazowa nie jest elementem niezbędnym, ale znacznie usprawnia obsługę całego systemu. System jest adresowalny, co oznacza, że – w przypadku zagrożenia – z poziomu stacji bazowej można szybko dowiedzieć się, gdzie doszło do zdarzenia, i dzięki temu zareagować w maksymalnie krótkim czasie. Stacja umożliwia także łatwą konfigurację całego systemu oraz raportowanie zdarzeń. Ma wbudowaną pamięć zdarzeń, dzięki której jest szczególnie przydatna dla specjalistów przeprowadzających audyt BHP. To tylko niektóre spośród jej wielu możliwości. Poza stacją w skład systemu wchodzą ręczne ostrzegacze pożarowe wraz sygnalizatorem optyczno-akustycznym, czujki dymu i ciepła oraz moduł wyjść/wejść umożliwiający komunikację z innymi systemami, co pozwala na realizację prostych scenariuszy. Żaden z elementów systemu nie wymaga okablowania, a ich rozmieszczenie można dowolnie konfigurować na całym obszarze budowy. Elementy systemu komunikują się z wykorzystaniem sieci radiowej *mesh*, dzięki

Rys. 1. Obszary zastosowań systemu WES+

czemu urządzenia „widzą się" nawet w promieniu 1000 m. Każda jednostka wzmacnia sygnał kolejnego wykrytego urządzenia, tym samym skutecznie zwiększając zasięg całego systemu. Warto podkreślić, że bezprzewodowość jest dużym ułatwieniem na budowie, gdyż eliminuje potrzebę czasochłonnego przenoszenia instalacji zabezpieczającej. Wszystkie elementy WES+ są zasilane bateryjnie. Każde urządzenie dysponuje akumulatorem, który zapewnia działanie przez minimum trzy lata. Ostatnim, ale nie mniej ważnym elementem systemu WES+ jest aplikacja na urządzenia mobilne z systemem operacyjnym Android albo iOS. Dzięki takiemu rozwiązaniu bez względu na miejsce przebywania możemy swobodnie konfigurować system oraz przeglądać raporty, które mogą również zostać przesłane w formie pliku w formacie PDF lub CSV pocztą e-mail. Dostęp do aplikacji można zapewnić klientowi, aby w każdej chwili mógł on przeglądać raporty dotyczące zdarzeń. Aplikacja ułatwia zarządzanie systemem.

Minimalizuj zagrożenie

Cechą wyróżniającą system WES+ jest to, że można go umieścić na placu budowy na dowolnym etapie prac budowlanych. Jego kluczowe zalety to łatwość obsługi i mobilność. Dane są transmitowane bezprzewodowo. Poszczególne elementy alarmowe mogą być zamontowane tam, gdzie są najbardziej potrzebne, i można zmieniać ich umiejscowienie. Oprócz sygnalizacji dźwiękowej system ma także sygnalizację optyczną. Na budowach często funkcjonuje system ostrzegania sygnałem dźwiękowym, którego źródło jest zainstalowane na zewnątrz. To dobry sposób na początkowym etapie, jednak później, gdy budowa ma się ku końcowi i budynek ma już pełną elewację, która często spełnia funkcję wygłuszającą, nie wszyscy pracownicy są w stanie usłyszeć sygnał alarmowy z zewnątrz, co znacznie wydłuża czas ewakuacji. W przypadku zastosowania WES+ nie ma problemu, gdyż ostrzegacze można zamontować w dowolnym miejscu (także wewnątrz budynku) i – co ważniejsze – zmieniać ich położenie dowolnie i w każdej chwili, więc sygnał będzie słyszalny tam, gdzie jest potrzebny, a nie tam, dokąd dochodzą przewody. Ostrzeganie musi być skuteczne, czyli zrozumiałe dla wszystkich i głośniejsze niż hałas z otoczenia, w którym się pracuje. Ciekawą funkcją jest także sygnalizowanie alarmu medycznego, który nie wymaga ewakuacji z budynku wszystkich pracowników. Ponadto służby medyczne będą mogły szybko dotrzeć na miejsce zdarzenia, gdyż system wskazuje dokładną lokalizację. Ewakuacja może być potrzebna nie tylko z powodu pożaru – może dojść do wycieku gazu, wycieku substancji chemicznych czy przypadkowego odkrycia niewypału.

Pewność i bezpieczeństwo

Dlaczego warto zaufać systemowi WES+? Jednym z najważniejszych powodów jest to, że jest jedynym certyfikowanym zgodnie z odpowiednimi

standardami systemem sygnalizacji pożarowej przeznaczonym do stosowania na budowach. Jest łatwy do zainstalowania (nie wymaga okablowania i ma wbudowane akumulatory) i utrzymania oraz intuicyjny w obsłudze. Dzięki komunikacji radiowej powiadamia natychmiast, i to nie tylko w przypadku zagrożenia pożarowego. WES+ może poinformować także o wypadku pracownika, który wymaga pomocy medycznej, lub o próbie kradzieży bądź niekontrolowanego usunięcia elementu systemu. Dzięki sieci czujek zagrożenie i jego lokalizacja są identyfikowane od razu, co bezpośrednio wpływa na efektywność ewakuacji i minimalizuje ewentualne straty materialne.

Prewencja obniża koszty

Dlaczego warto zabezpieczyć budowę systemem WES+? Przede wszystkim dla obniżenia różnego rodzaju kosztów. Nie chodzi tu tylko o fakt zabezpieczenia się przed ewentualnym pożarem i związanymi z nim stratami. Znaczenie ma również koszt ubezpieczenia. WES+ to bowiem jedyne tego rodzaju rozwiązanie na rynku, które posiada certyfikat zgodny z wymaganiami normy PN-EN 54. Dzięki temu WES+ spełnia wymogi i zalecenia branży ubezpieczeniowej, co z kolei może mieć wpływ na obniżenie kosztów ubezpieczenia inwestycji. W dodatku, w przypadku zdarzenia, miejsce jego wystąpienia jest szybko lokalizowane, co znacznie przyspiesza reakcje odpowiednich służb, a ich efektywnie przeprowadzona akcja minimalizuje skalę strat.

Fot. 1. Elementy systemu WES+

Kupno lub wypożyczenie – model biznesowy dla każdego

System WES+ służy do tymczasowego zabezpieczania inwestycji w czasie budowy, dlatego możliwe jest zarówno kupienie systemu, co jest dobrym rozwiązaniem dla generalnych wykonawców, jak i jego wypożyczenie, jeśli na przykład dana firma realizuje pojedyncze zlecenie. Okazuje się, że kupienie systemu może też być dla firmy źródłem zysku – firma może zakupić WES+ i wypożyczać go odpłatnie swoim spółkom obsługującym poszczególne inwestycje, zależnie od potrzeb. Na podstawie obserwacji

WES+ jest oceniany w branży wyłącznie pozytywnie jako sprzęt nowoczesny i wysokiej jakości, a jednocześnie łatwy w instalacji i obsłudze. Został wykorzystany m.in. podczas budowy galerii Wroclavia. – *Z czystym sumieniem polecamy system WES+ polskim inwestorom, bo to system sprawdzony i niezawodny. Ostatecznie chodzi przecież o to, co najważniejsze – o bezpieczeństwo ludzkiego życia* – powiedział Marcin Malinowski, Product Manager opiekujący się systemem.

Fot. 2. WES+ na budowie

firmy dystrybuującej można stwierdzić, że już po roku taka inwestycja może się zwrócić, a kolejne miesiące przyniosą rentowne funkcjonowanie całego systemu. Nie ma jednak problemu z wypożyczeniem systemu od dystrybutora na czas budowy. W takim przypadku okres użytkowania jest ustalany indywidualnie, zależnie od potrzeb i rozmiaru placu budowy.

Więcej informacji na temat systemu mogą Państwo znaleźć pod adresem http://www.wesfire.com.pl/.

Geo-Kat

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

PROJEKTUJEMY
zgodnie ze sztuką

SYSTEMY SYGNALIZACJI POŻAROWEJ

- innowacyjnie rozproszony **POLON 6000**
- interaktywny **POLON 4000**
- konwencjonalny **IGNIS 1000/2000**

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

SYSTEM DETEKCJI GAZÓW SDG 6000

POLON-ALFA S.A. (dawniej Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.)
85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.pl

System detekcji gazów SDG 6000

Nowość w ofercie firmy POLON-ALFA

Mariusz Michałek

Od dłuższego czasu można zaobserwować coraz większe zainteresowanie systemami detekcji gazów. Coraz więcej osób uświadamia sobie konieczność ich stosowania w związku z potencjalnymi zagrożeniami powodowanymi przez powszechnie stosowane paliwa wykorzystywane w przemyśle, transporcie czy budownictwie mieszkaniowym. Do największych zagrożeń należy przede wszystkim zagrożenie zdrowia i życia ludzkiego spowodowane wydzielaniem się tlenku węgla w procesie spalania (np. podczas spalania paliw w silnikach spalinowych). Wydostawanie się propanu-butanu (LPG) oraz gazu ziemnego z nieszczelnych lub uszkodzonych instalacji stwarza zagrożenie wybuchem

Ze względu na rosnące zapotrzebowanie firma POLON-ALFA pod koniec ubiegłego roku wprowadziła do sprzedaży system detekcji gazów SDG 6000, który wraz z systemami sygnalizacji pożarowej umożliwia kompleksowe zabezpieczenie całych obiektów. Takie rozwiązanie stosuje się na przykład na obecnie budowanych osiedlach z garażami podziemnymi. Zgodnie z *Rozporządzeniem Ministra Infrastruktury z dn. 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie* (Dz. U. z 2002 r., nr 75, poz. 690 z późniejszymi zmianami) w przeznaczonym dla samochodów osobowych garażu zamkniętym, w którym znajduje się więcej niż dziesięć stanowisk, musi być stosowana wentylacja mechaniczna sterowana detektorami tlenku węgla.

Produkowany przez firmę POLON-ALFA system detekcji gazów SDG 6000 umożliwia wykrywanie i sygnalizowanie wycieków gazów palnych (gazu ziemnego, propanu-butanu) oraz niebezpiecznych stężeń tlenku węgla. System składa się z centrali detekcji gazów CDG 6000 oraz kilku rodzajów adresowalnych detektorów gazów PSG-6000 pracujących na linii dozorowej centrali.

Po dobraniu właściwych detektorów system ten może być szczególnie przydatny w garażach dzięki umożliwieniu jednoczesnego sterowania wentylacją. Można go stosować również w kotłowniach gazowych i umożliwić w ten sposób sterowanie zaworem odcinającym dopływ gazu w przypadku rozszczelnienia instalacji. Uzupełnieniem SDG 6000 są autonomiczne detektory gazów ASG-2000, które mogą pracować samodzielnie lub tworzyć niewielkie instalacje kilku współpracujących ze sobą detektorów.

Centrala detekcji gazów CDG 6000

Adresowalna centrala detekcji gazów CDG 6000 jest przeznaczona do sygnalizowania wycieków gazów palnych (CNG, LPG) oraz niebezpiecznych stężeń tlenku węgla (CO) po odebraniu informacji

Fot. 1. Centrala CDG 6000

od współpracujących z nią detektorów gazów PSG-6000. Centrala uruchamia alarmową sygnalizację akustyczną i optyczną, umożliwia uruchomienie wentylacji w celu usunięcia nadmiaru szkodliwych gazów z pomieszczenia i może podać sygnał sterujący zaworem odcinającym dopływ gazu. Za pomocą wbudowanych linii kontrolnych można kontrolować stan sterowanych urządzeń sygnalizacyjnych i wykonawczych. Istnieje także możliwość przyjęcia informacji o zagrożeniu (alarmie) z innych systemów zabezpieczeń. Centrala ma możliwość przesłania informacji o alarmie do zainstalowanych w obiekcie systemów sygnalizacji pożarowej POLON 4000 lub POLON 6000 poprzez programowalne wyjścia przekaźnikowe. Ponadto urządzenie zostało przygotowane do pracy na pętli dozorowej central systemu POLON 6000, dzięki czemu wymiana informacji i poleceń odbywa się cyfrowo.

Detektory są połączone z centralą CDG 6000 specjalnie zaprojektowaną linią dozorową, a każdemu z nich zostaje przydzielony adres. Dzięki temu centrala ma informacje o stanie każdego z detektorów. Linia detektorów może pracować w dwóch trybach – jako promieniowa lub pętlowa. W rekomendowanym przez producenta trybie linii pętlowej koniec linii jest połączony z centralą. Dzięki temu system jest w stanie pracować poprawnie nawet wtedy, gdy linia zostanie w jednym miejscu przerwana. Detektory mają wbudowane izolatory zwarć, które, włączając się, izolują zwarcie w linii tak, aby maksymalna liczba detektorów nadal pracowała poprawnie.

Centrala CDG 6000 może sygnalizować trzy stopnie alarmowe odpowiadające trzem poziomom stężeń gazów, o których informują współpracujące detektory. Identyfikuje ona alarmujące detektory, podając stosowne informacje na wyświetlaczu. Ma również rozbudowany system do autodiagnostyki oraz diagnozowania dołączonych urządzeń zewnętrznych. Analogicznie do alarmów, pełna lista występujących uszkodzeń jest dostępna na wyświetlaczu urządzenia.

Adresowalne detektory gazów typu PSG-6000

Adresowalne detektory gazów PSG-6000 są przeznaczone do wykrywania oraz ciągłej kontroli obecności gazów palnych i toksycznych w pomieszczeniach zagrożonych ich emisją, szczególnie w garażach i kotłowniach. Każdy detektor ma ustawione trzy progi alarmowe odpowiadające ściśle określonym stężeniom gazu w powietrzu. Po ich przekroczeniu detektory przekazują informacje do współpracującej centrali CDG 6000. Do centrali przekazywane są także informacje o uszkodzeniu sensora lub konieczności przeprowadzenia jego kalibracji. Detektory mają wbudowane wymienne moduły sensorów gazów.

Detektor	Wykrywany gaz	Zasilanie dodatkowe
PSG-6001	CNG (gaz ziemny)	9 ÷ 30 V_{DC}
PSG-6002	LPG (propan-butan)	9 ÷ 30 V_{DC}
PSG-6003	CO (tlenek węgla)	9 ÷ 30 V_{DC}
PSG-6103	CO (tlenek węgla)	tylko z linii dozorowej

Fot. 2. Adresowalne detektory gazów

Detektory PSG-6000 pracują wyłącznie na liniach dozorowych adresowalnych central detekcji gazów CDG 6000. Wymagają dodatkowego zasilania ze źródła napięcia stałego 12 V lub 24 V (za wyjątkiem detektorów PSG-6103, które są zasilane z linii dozorowej centrali). Warto nadmienić, że centrala ma wyjście do zasilania urządzeń zewnętrznych lub detektorów gazów o obciążalności 0,5 A/12 V.

Wysoki stopień szczelności obudów detektorów zapewnia odporność na stosunkowo trudne warunki środowiskowe.

Autonomiczne detektory gazów typu ASG-2000

Autonomiczne detektory gazów ASG-2000 są przeznaczone do wykrywania obecności gazów palnych i toksycznych w pomieszczeniach zagrożonych ich emisją, szczególnie w garażach i kotłowniach. Każdy detektor ma ustawione trzy progi alarmowe, które odpowiadają ściśle określonym stężeniom gazu w powietrzu. Po ich przekroczeniu zostaje włączona sygnalizacja optyczna w detektorach oraz zostają uaktywnione odpowiednie wyjścia sterujące zewnętrzną sygnalizacją akustyczno-optyczną. Możliwe jest także uruchomienie wentylacji w celu przewietrzenia pomieszczenia i usunięcia z niego nadmiaru szkodliwych gazów. Detektory ASG-2000 są przeznaczone do pracy samodzielnej, jednak można je łączyć ze sobą i tworzyć w ten sposób niewielkie instalacje detekcji gazów. Detektory mają wbudowane wymienne moduły sensorów gazów, co pozwala na obniżenie kosztów ich eksploatacji. Sygnalizowana jest konieczność przeprowadzenia kalibracji sensorów. Obudowy detektorów charakteryzują się wysokim stopniem szczelności. Detektory są zasilane z zewnętrznego zasilacza 12 V lub 24 V, lub ze źródła napięcia przemiennego 230 V.

Detektor	Wykrywany gaz	Zasilanie dodatkowe
ASG-2001	CNG (gaz ziemny)	9 ÷ 30 V_{DC}
ASG-2001HV	CNG (gaz ziemny)	~230 V_{AC}
ASG-2002	LPG (propan-butan)	9 ÷ 30 V_{DC}
ASG-2002HV	LPG (propan-butan)	~230 V_{AC}
ASG-2003	CO (tlenek węgla)	9 ÷ 30 V_{DC}
ASG-2003HV	CO (tlenek węgla)	~230 V_{AC}

Fot. 3. Autonomiczny detektor gazów

Firma POLON-ALFA nieustająco rozwija asortyment oferowanych produktów, które wchodzą w skład systemu detekcji gazów. W kolejnym artykule przedstawimy optyczne tablice ostrzegawcze oraz inne detektory gazów.

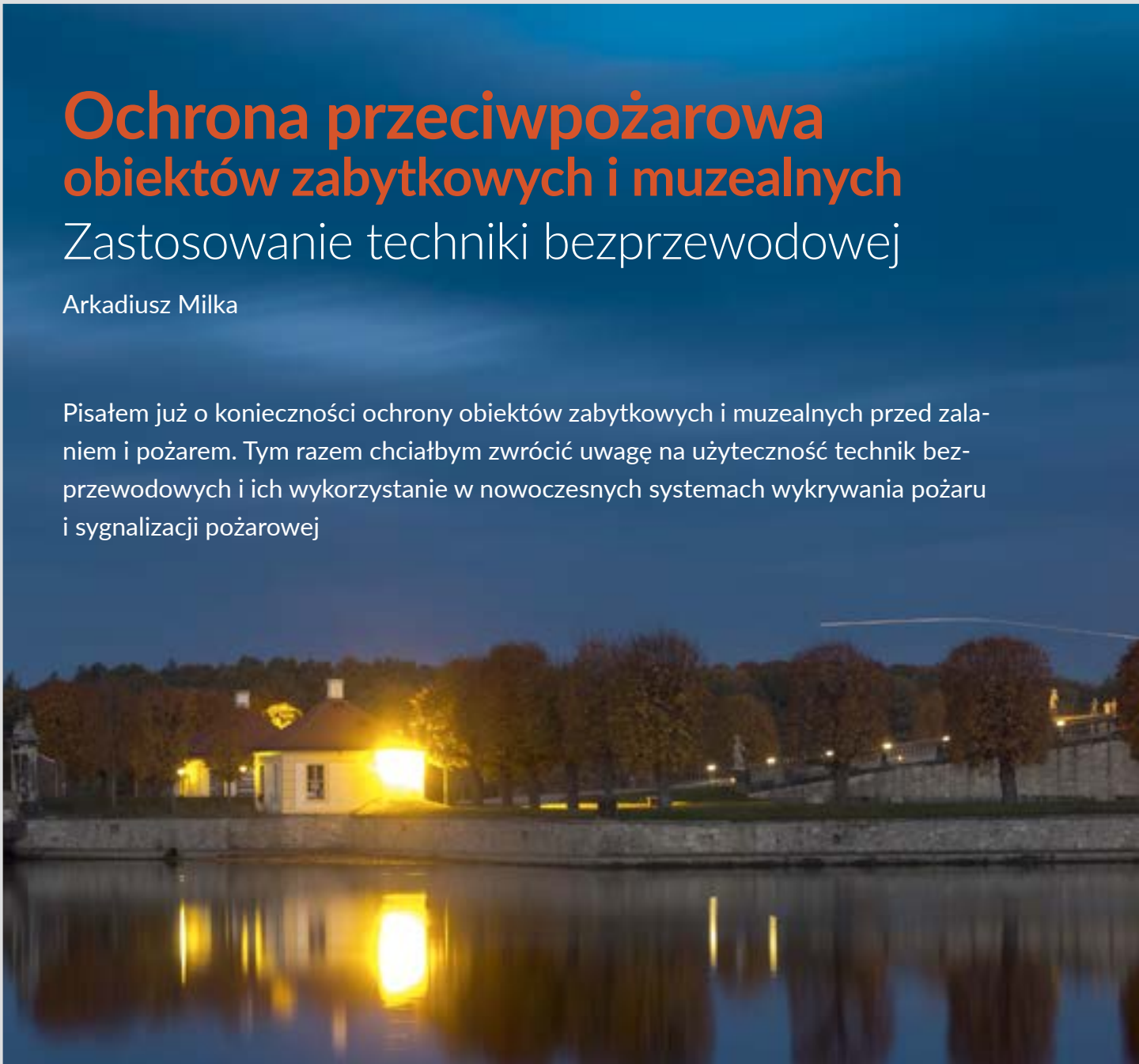
Mariusz Michałek
POLON-ALFA

Ochrona przeciwpożarowa obiektów zabytkowych i muzealnych

Zastosowanie techniki bezprzewodowej

Arkadiusz Milka

Pisałem już o konieczności ochrony obiektów zabytkowych i muzealnych przed zalaniem i pożarem. Tym razem chciałbym zwrócić uwagę na użyteczność technik bezprzewodowych i ich wykorzystanie w nowoczesnych systemach wykrywania pożaru i sygnalizacji pożarowej



Kiedy w 1986 roku rozpoczynałem swoją zawodową przygodę związaną z systemami sygnalizacji pożarowej, na rynku dostępne były tylko systemy konwencjonalne produkowane przez firmy ZUD Polon oraz Telfa z Bydgoszczy, które były wówczas jedynymi producentami tego typu systemów w Polsce. Ze względu na bardzo wysokie koszty, systemy produkowane przez renomowane firmy zachodnie były instalowane bardzo rzadko. Wadą instalowanych wtedy systemów było generowanie dużej liczby fałszywych alarmów (które bezpośrednio wynikało z tego, jakie rozwiązania techniczne były wówczas dostępne i stosowane). Były to nieadresowalne systemy konwencjonalne z otwartymi liniami dozorowymi. Systemy te nie mogły wskazywać obsłudze dokładnej lokalizacji zagrożenia. Ponadto częste alarmy skutkowały tym, że obsługa zazwyczaj nie reagowała na powtarzające się sygnały, sądząc, że to kolejny fałszywy alarm. Zdarzało się, że obsługa wyłączała cały system, gdyż emitowane zakłócenia przeszkadzały w słuchaniu radia na portierni. Gdy w takim przypadku faktycznie był pożar, interwencja zazwyczaj była spóźniona i nie mogła być skuteczna. Powodowało to szkody, mimo że system był zainstalowany i sprawny technicznie. Innym problemem była wówczas zapewnienie awaryjnego zasilania systemów sygnalizacji pożarowej. W praktyce tylko niektóre były wyposażone w dodatkowe akumulatory. Dostępne wówczas akumulatory kwasowe i zasadowe były

sporych rozmiarów, w związku z czym wymagały dodatkowego miejsca, a ponadto wymagania eksploatacyjne uwzględniające szkodliwy wpływ zastosowanego w nich elektrolitu na otoczenie nie były łatwe do spełnienia. Nieliczne obiekty były przyłączone do jednostek straży pożarnej. Co ciekawe, powszechna była wówczas opinia, że w przypadku systemów sygnalizacji pożarowej technika bezprzewodowa nigdy nie znajdzie zastosowania. Opinia ta wynikała ze słabości ówczesnych rozwiązań. Można jednak śmiało powiedzieć, że rozwiązania dzisiejsze i te sprzed trzydziestu lat dzieli przepaść. Wspomniane mankamenty właściwie już nie występują. Niestety, zanim nastąpiły zmiany, na skutek pożarów utraciliśmy bezpowrotnie wiele cennych i niepowtarzalnych obiektów, w tym również wiele obiektów zabytkowych. Można się o tym przekonać,

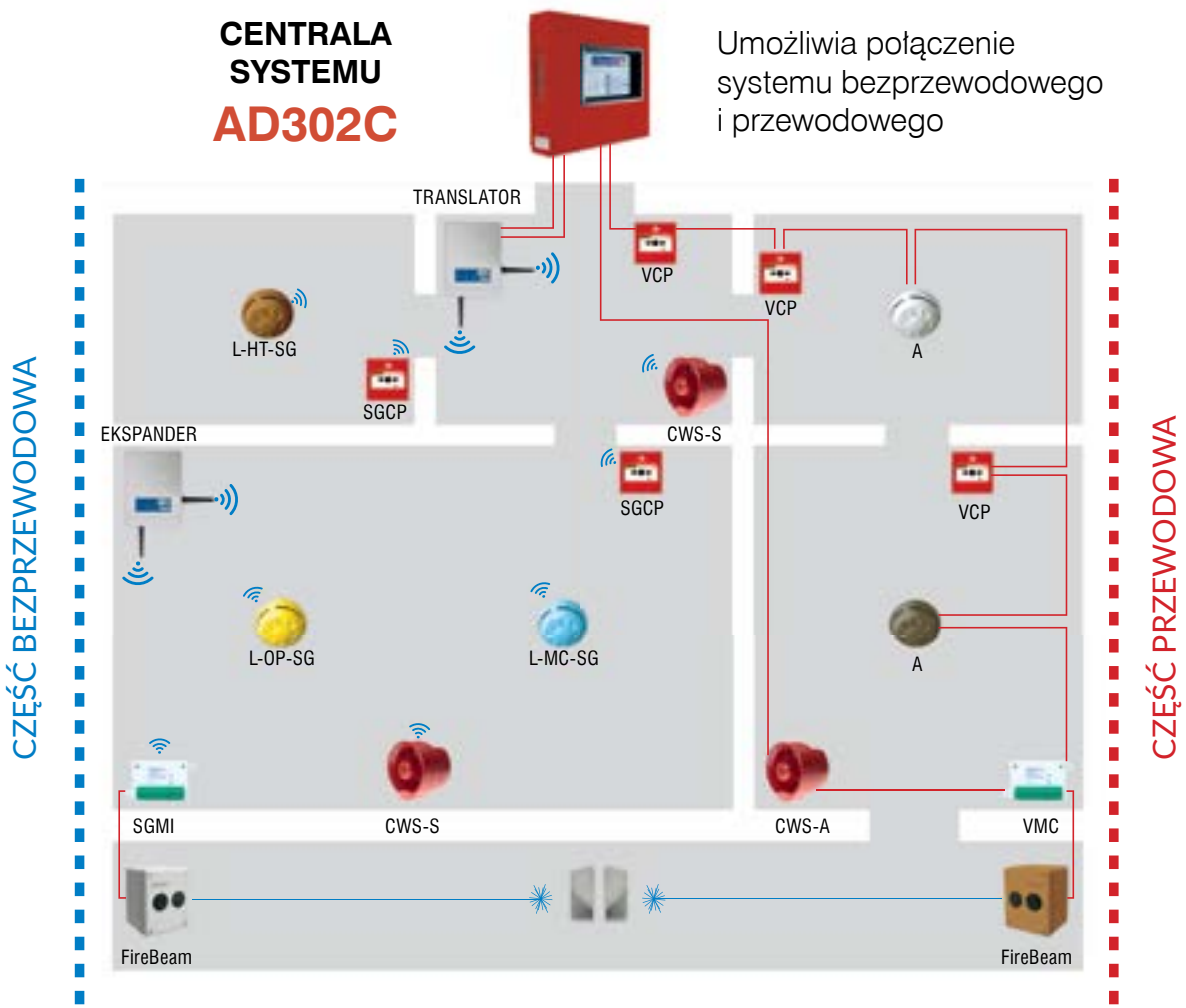
Fot. 1. Centrale AD301C/302C

studiując choćby materiały udostępniane przez Państwową Straż Pożarną czy Narodowy Instytut Muzealnictwa i Ochrony Zbiorów w Warszawie.

Fot. 2. Bezprzewodowa czujka multisensorowa, linia „Decoline" wykończenie – dąb

Niestety nadal wiele osób odpowiedzialnych za ochronę przeciwpożarową, tj. właścicieli i zarządców obiektów, nie uświadamia sobie powagi zagrożeń i nie dąży do poprawy bezpieczeństwa poprzez zastosowanie nowoczesnych rozwiązań i systemów, które są dostępne na rynku. Dotyczy to również obiektów, o które powinno się dbać ze szczególną starannością. Niestety niektóre obiekty nie muszą być chronione obligatoryjnie. Jest to zjawisko niepokojące, tym bardziej, że obecnie mamy do dyspozycji odpowiednie środki techniczne, a wykorzystywana w urządzeniach elektronika jest relatywnie tania i w związku z tym bardziej dostępna. Wcześniej takich możliwości nie było.

Często podstawowym kryterium, które przesądza o wyborze rozwiązania, nie jest skuteczność, lecz cena. Oczywiście cena jest ważna, ale system musi przede wszystkim być skuteczny. Niestety często zdarza się, że wprawdzie teoretycznie jest zgodny z wymaganiami, ale nie funkcjonuje właściwie. Może to wynikać ze zmian wprowadzonych na etapie realizacji projektu w celu ograniczenia kosztów (np. wskutek nacisków inwestora lub zaniżenia kosztów na etapie przetargu). Jeśli te zmiany doprowadzą do tego, że system nie zadziała prawidłowo w czasie pożaru, na refleksję i reakcję będzie już za późno. Ubezpieczyciel może wstrzymać wypłatę odszkodowania, uznając ją w takiej sytuacji za nienależną.



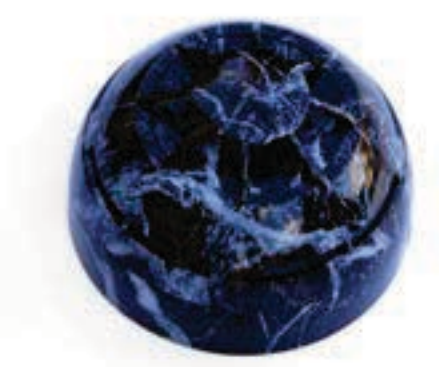
Rys. 1. Poglądowy schemat konfiguracji systemu hybrydowego

Fot. 3. Sygnalizator akustyczno-optyczny bezprzewodowy

Niestety nie działa w Polsce mechanizm ograniczania ryzyka, powszechny w większości krajów Europy i na świecie, polegający na stawianiu konkretnych wymagań przez instytucje ubezpieczeniowe. W przypadku obiektów prywatnych lub komercyjnych firmy ubezpieczeniowe coraz częściej zaczynają stawiać takie wymagania. Trzeba jednak stwierdzić z przykrością, że praktycznie nie dotyczy to obiektów stanowiących własność skarbu państwa. Nie wszystkie obiekty zabytkowe podlegają ochronie obligatoryjnej, co najczęściej oznacza, że nie są chronione wcale, bo nie wymagają tego wprost obowiązujące przepisy. W wielu obiektach odpowiednie zabezpieczenia przeciwpożarowe nigdy nie zostały wykonane wskutek braku zgody na ingerencję w zabytkową strukturę oraz ze względu na duże ryzyko naruszenia lub trwałego uszkodzenia takiego obiektu podczas wykonywania prac instalacyjnych związanych z okablowaniem.

Cieszy jednak to, że przedstawiane aktualne możliwości właściwej ochrony obiektów zabytkowych za pomocą systemów bezprzewodowych są chętnie brane pod uwagę przez konserwatorów.

Uważa się, że systemy bezprzewodowe są bardzo drogie, a przynajmniej sporo droższe od przewodowych. Wyższa cena urządzeń bezprzewodowych wynika z tego, że muszą być one dodatkowo wyposażone w układy radiowej transmisji sygnału, układy zasilania, a w systemie muszą być instalowane dodatkowe elementy, np. odbiorniki – translatory czy ekspandery, które w instalacji przewodowej nie są wymagane. Nie wspomina się jednak o tym, że nie trzeba wykonywać okablowania albo zakres takiego okablowania jest stosunkowo niewielki, w związku z czym nie ponosi się dużych kosztów z tym związanych. To jednak nie koszty samego okablowania są tutaj istotne. W przypadku obiektów zabytkowych chodzi głównie o prace budowlano-wykończeniowe, które będą niezbędne, jeśli utworzy się instalację przewodową. W niektórych obiektach wykonanie okablowania może być trudne albo nawet niemożliwe. Instalacje systemu sygnalizacji pożarowej są układane przede wszystkim na stropach, sufitach i ścianach Montaż rur instalacyjnych, koryt i przewodów wymaga ingerencji we wszelkiego rodzaju zabytkowe detale, takie jak freski, sztukaterie, stiuki, rozety, gzymsy itp. Obiekty zabytkowe są zazwyczaj użytkowane. Mogą znajdować się w nich cenne zbiory, dzieła sztuki lub bardzo wartościowe wyposażenie. W związku z tym wszelkie prace instalacyjne wymagają odpowiedniego zabezpieczenia istniejącej substancji, dzieł i wyposażenia, co nie należy do czynności prostych i tanich. Naruszone czy uszkodzone w efekcie tych prac fragmenty ścian, stropów lub inne elementy muszą być na koniec odpowiednio odbudowane i odrestaurowane. Wymaga to zatrudnienia profesjonalnych konserwatorów oraz zastosowania specjalistycznych materiałów i narzędzi. Prace powinny być objęte stałym nadzorem, a ich zakres powinien być uzgodniony ze służbą konserwacji zabytków.



Fot. 4. Bezprzewodowa czujka multisensorowa, linia „Decoline" wykończenie – czarny marmur

Przy założeniu, że zakres okablowania w przypadku systemu bezprzewodowego jest bardzo ograniczony, można zaoszczędzić czas potrzebny zarówno na wykonanie systemu, jak i na uzgodnienia. Niektórzy sądzą, że koszty jego eksploatacji i obsługi są wyższe. Taki pogląd nie jest prawdziwy. Konserwacja odbywa się praktycznie

Fot. 5. Translator/Ekspander systemu bezprzewodowego

tak samo, jak konserwacja urządzeń przewodowych. Częsta wymiana baterii służących do zasilania urządzeń bezprzewodowych też nie jest potrzebna. W obecnie dostępnych systemach bezprzewodowych nie trzeba wymieniać baterii nawet przez kilka lat.

Bezprzewodowy system sygnalizacji pożarowej OCTOPUS, oferowany od blisko czterech lat przez firmę Insap, jest idealnym rozwiązaniem do ochrony obiektów małych i średnich. W przypadku sieciowego połączenia central możliwe jest również zabezpieczenie obiektów większych lub kompleksów budynków.

Dlaczego warto na ten system zwrócić uwagę? Istnieje co najmniej kilka bardzo istotnych powodów. Oto niektóre z nich:

1. Wszystkie oferowane komponenty systemu (w tym ręczne ostrzegacze pożarowe, moduły i sygnalizatory) zostały formalnie dopuszczone do stosowania na terenie Rzeczypospolitej Polskiej.
2. System może pracować zarówno jako przewodowy, jak i bezprzewodowy, a także jako jeden i drugi łącznie – czyli hybrydowy. Pozwala to każdorazowo na dostosowanie go do warunków panujących w danym obiekcie. Optymalnie konfigurując system, można ograniczyć koszty instalacji oraz eksploatacji.
3. Urządzenia wchodzące w skład systemu są produkowane na terenie państw Unii Europejskiej, tj. Niemiec, Hiszpanii i Włoch. Gwarantuje to najwyższą jakość i niezawodność komponentów i urządzeń.
4. System korzysta z najnowocześniejszego, zaawansowanego technicznie protokołu komunikacji.
5. Oferujemy bardzo wiele elementów detekcyjnych, sterowniczych, sygnalizacyjnych i podzespołów. Praktycznie wszystkie elementy są oferowane zarówno w wersji przewodowej, jak i bezprzewodowej.
6. Urządzenia, szczególnie czujki, są bardzo estetyczne. Zaprojektowali je najwybitniejsi projektanci zajmujący się sztuką użytkową.
7. Istnieje możliwość wykonania czujek w dowolnym kolorze z palety RAL. Ponadto powierzchnia obudowy czujki w wersji DECOR-LINE może być imitacją drewna, kamienia, metalu (złota, srebra, aluminium) oraz włókna węglowego.
8. W urządzeniach bezprzewodowych można stosować ogólnie dostępne baterie (czas pracy wynosi od pięciu do siedmiu lat).

Wyżej wymienione zalety systemu OCTOPUS znakomicie predestynują go do zastosowania w małych i średnich obiektach zabytkowych, sakralnych, muzealnych i wystawowych, we wszelkiego rodzaju hotelach, pałacach, rezydencjach, dworkach, domach pomocy i w wielu innych obiektach.

Dawniej nie mogliśmy stosownie zabezpieczyć obiektów zabytkowych. Dziś odpowiednie rozwiązania są już dostępne, więc należy z nich skorzystać, by nie utracić kolejnych dóbr kultury.

Zapraszam wszystkich zainteresowanych tą tematyką do dyskusji i współpracy.

Arkadiusz Milka
Insap
a.milka@insap.pl

EVIX®

MADE IN EU

NOWY WYMIAR OCHRONY
CZUJKI DUALNE PIR + MW

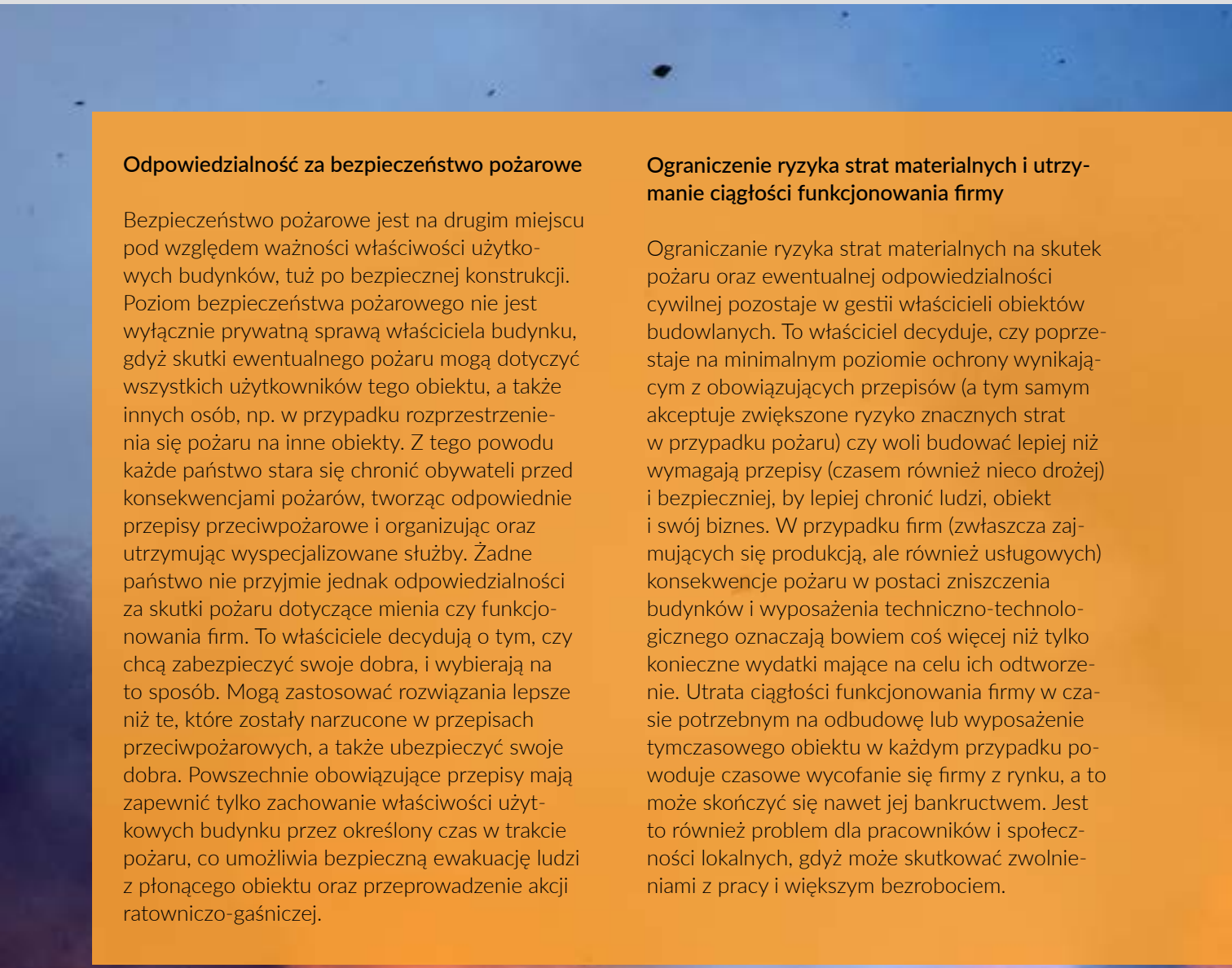
IDEALNE UZUPEŁNIENIE KAŻDEGO SYSTEMU ALARMOWEGO

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

Bezpieczeństwo pożarowe dachów
(część 2)

Krzysztof Bagiński | Maria Dreger
Stowarzyszenie DAFA

Wiedza wszystkich uczestników procesu inwestycyjnego, użytkowników i administratorów budynków na temat bezpieczeństwa pożarowego jest koniecznym warunkiem zapewnienia bezpieczeństwa. To właśnie działania człowieka są przyczyną prawie wszystkich pożarów, a wielkość i rodzaj strat na skutek pożaru jest bezpośrednio uzależniona od ludzkich decyzji i działań podejmowanych na wszystkich etapach – od decyzji inwestycyjnych i projektowania, przez budowę, aż po eksploatację obiektów budowlanych



Odpowiedzialność za bezpieczeństwo pożarowe

Bezpieczeństwo pożarowe jest na drugim miejscu pod względem ważności właściwości użytkowych budynków, tuż po bezpiecznej konstrukcji. Poziom bezpieczeństwa pożarowego nie jest wyłącznie prywatną sprawą właściciela budynku, gdyż skutki ewentualnego pożaru mogą dotyczyć wszystkich użytkowników tego obiektu, a także innych osób, np. w przypadku rozprzestrzenienia się pożaru na inne obiekty. Z tego powodu każde państwo stara się chronić obywateli przed konsekwencjami pożarów, tworząc odpowiednie przepisy przeciwpożarowe i organizując oraz utrzymując wyspecjalizowane służby. Żadne państwo nie przyjmie jednak odpowiedzialności za skutki pożaru dotyczące mienia czy funkcjonowania firm. To właściciele decydują o tym, czy chcą zabezpieczyć swoje dobra, i wybierają na to sposób. Mogą zastosować rozwiązania lepsze niż te, które zostały narzucone w przepisach przeciwpożarowych, a także ubezpieczyć swoje dobra. Powszechnie obowiązujące przepisy mają zapewnić tylko zachowanie właściwości użytkowych budynku przez określony czas w trakcie pożaru, co umożliwia bezpieczną ewakuację ludzi z płonącego obiektu oraz przeprowadzenie akcji ratowniczo-gaśniczej.

Ograniczenie ryzyka strat materialnych i utrzymanie ciągłości funkcjonowania firmy

Ograniczanie ryzyka strat materialnych na skutek pożaru oraz ewentualnej odpowiedzialności cywilnej pozostaje w gestii właścicieli obiektów budowlanych. To właściciel decyduje, czy poprzestaje na minimalnym poziomie ochrony wynikającym z obowiązujących przepisów (a tym samym akceptuje zwiększone ryzyko znacznych strat w przypadku pożaru) czy woli budować lepiej niż wymagają przepisy (czasem również nieco drożej) i bezpieczniej, by lepiej chronić ludzi, obiekt i swój biznes. W przypadku firm (zwłaszcza zajmujących się produkcją, ale również usługowych) konsekwencje pożaru w postaci zniszczenia budynków i wyposażenia techniczno-technologicznego oznaczają bowiem coś więcej niż tylko konieczne wydatki mające na celu ich odtworzenie. Utrata ciągłości funkcjonowania firmy w czasie potrzebnym na odbudowę lub wyposażenie tymczasowego obiektu w każdym przypadku powoduje czasowe wycofanie się firmy z rynku, a to może skończyć się nawet jej bankructwem. Jest to również problem dla pracowników i społeczności lokalnych, gdyż może skutkować zwolnieniami z pracy i większym bezrobociem.

W krajach bardziej rozwiniętych dużą rolę w zwiększaniu bezpieczeństwa pożarowego odgrywają firmy ubezpieczeniowe. Wysokość składki uzależniają one od zastosowanych rozwiązań konstrukcyjnych, instalacji, wyposażenia. Zdarza się, że odmawiają ubezpieczenia nawet wówczas, gdy spełnione są formalno-prawne wymagania zawarte w przepisach przeciwpożarowych, jeżeli uznają, że zastosowane rozwiązania nie zabezpieczają mienia w sposób wystarczający. W Polsce takie podejście ubezpieczycieli nie jest jeszcze powszechne, gdyż rynek ubezpieczeń wciąż się kształtuje, ale już można zaobserwować pojawianie się podobnych tendencji.

O bezpieczeństwie decyduje praktyka

Nie wystarczy poprawnie zaprojektować obiekt oraz użyć materiałów i wyrobów o zadeklarowanych właściwościach, odpowiedniej klasy i dobrej jakości. Jeżeli na etapie realizacji wystąpią nawet pozornie drobne odstępstwa od wymagań, efektem może być nieuzyskanie oczekiwanych właściwości ogniowych i niższy niż zakładany poziom ochrony i bezpieczeństwa pożarowego.

Podobnie jest na etapie użytkowania obiektu. Wykonanie dodatkowych, nawet niewielkich, otworów w ścianach może zupełnie zmienić właściwości i klasy ogniowe całych fragmentów budynku. Na przykład używanie otwartego ognia podczas prac remontowych w sąsiedztwie elementów zawierających palne materiały (lub w trakcie ich przebudowy) – mimo deklarowanego nierozprzestrzeniania przez nie ognia i ich odporności ogniowej – może skończyć się pożarem ze wszystkimi jego konsekwencjami.

Do bezpieczeństwa pożarowego budynków przyczyniają się na równi:
- zgodność projektu z przepisami i innymi wymaganiami (np. wymaganiami ubezpieczyciela),
- staranność na wszystkich etapach realizacji,
- użytkowanie budynku w sposób zapewniający utrzymanie obiektu i znajdujących się w nim instalacji, w tym wszystkich biernych i czynnych zabezpieczeń ppoż., w stanie pełnej sprawności i gotowości, zgodnie z instrukcjami.

Przydatne definicje i określenia związane z bezpieczeństwem pożarowym

Budynki ZL – budynki mieszkalne, do zamieszkania zbiorowego i użyteczności publicznej, czyli budynki zaliczane do różnych kategorii na podstawie zagrożenia dla ludzi

ZL I – budynki zawierające co najmniej jedno pomieszczenie przeznaczone do jednoczesnego przebywania ponad 50 osób, które nie są jego stałymi użytkownikami, np. duże pomieszczenia handlowo-usługowe, lokale gastronomiczno-rozrywkowe, poczekalnie dworcowe, a także niektóre sale konferencyjne i wykładowe

ZL II – budynki przeznaczone przede wszystkim dla ludzi o ograniczonej zdolności poruszania się, którzy nie mogą ewakuować się samodzielnie, takie jak szpitale, żłobki, przedszkola, domy dla osób starszych

ZL III – budynki użyteczności publicznej z wyjątkiem budynków przeznaczonych przede wszystkim dla ludzi o ograniczonej zdolności poruszania się oraz zawierających pomieszczenie dla ponad 50 osób, o przeznaczeniu biurowym lub socjalnym

ZL IV – pomieszczenia mieszkalne w dowolnych budynkach

ZL V – budynki przeznaczone do zamieszkania zbiorowego z wyjątkiem budynków przeznaczonych przede wszystkim dla ludzi o ograniczonej zdolności poruszania się oraz zawierających pomieszczenie dla ponad 50 osób, które nie są jego stałymi użytkownikami

Budynki PM – budynki produkcyjne i magazynowe

Budynki IN – budynki inwentarskie (służące do hodowli inwentarza)

Budynki niskie (N) – budynki o wysokości do 12 m (włącznie) nad poziomem terenu lub mieszkalne o wysokości do czterech kondygnacji nadziemnych (włącznie)

Budynki średniowysokie (SW) – budynki o wysokości od ponad 12 m do 25 m (włącznie) nad poziomem terenu lub mieszkalne o wysokości od ponad czterech do dziewięciu kondygnacji nadziemnych (włącznie)

Budynki wysokie (W) – budynki o wysokości od ponad 25 m do 55 m (włącznie) nad poziomem terenu lub mieszkalne o wysokości od ponad dziewięciu do 18 kondygnacji nadziemnych (włącznie)

Budynki wysokościowe (WW) – budynki o wysokości powyżej 55 m nad poziomem terenu

Gęstość obciążenia ogniowego – ilość energii cieplnej, która może powstać przy spaleniu materiałów palnych (składowanych, wytwarzanych, przerabianych lub transportowanych w sposób ciągły) znajdujących się w pomieszczeniu, strefie pożarowej lub składowisku, przypadająca na jednostkę powierzchni tego pomieszczenia, strefy pożarowej lub składowiska; jednostką miary tej wielkości fizycznej jest MJ/m^2; gęstość obciążenia ogniowego stanowi jeden z podstawowych parametrów przyjmowanych w przepisach techniczno-budowlanych przy określaniu wymagań dotyczących budynków produkcyjno-magazynowych

Klasy odporności pożarowej budynków lub ich części (od najwyższej do najniższej): A, B, C, D, E (od tych klas zależą wymagania przeciwpożarowe zawarte w warunkach technicznych; w przypadku budynków ZL klasa odporności pożarowej zależy od wysokości i kategorii ZL, a w przypadku budynków PM i IN – od gęstości obciążenia ogniowego i liczby kondygnacji)

Przykładowe klasy odporności ogniowej elementów budynku

R 15 – nośność elementu konstrukcyjnego

E 30, EI 30 – szczelność ogniowa i szczelność/izolacyjność elementu nienośnego

B_{300}30 – klapy dymowe odpowiednie przy temperaturach dymu nieprzekraczających 300°C

Budynek	ZL I	ZL II	ZL III	ZL IV	ZL V
1	2	3	4	5	6
niski (N)	B	B	C	D	C
średniowysoki (SW)	B	B	B	C	B
wysoki (W)	B	B	B	B	B
wysokościowy (WW)	A	A	A	B	A

Tab. 1. Klasy odporności pożarowej budynków ZL

Maksymalna gęstość obciążenia ogniowego strefy pożarowej w budynku Q [MJ/m^2]	Budynek o jednej kondygnacji nadziemnej (brak ograniczenia wysokości)	Budynek wielokondygnacyjny			
		niski (N)	średniowysoki (SW)	wysoki (W)	wysokościowy (WW)
1	2	3	4	5	6
Q 500	E	D	C	B	B
500 < Q 1000	D	D	C	B	B
1000 < Q 2000	C	C	C	B	B
2000 < Q 4000	B	B	B		
Q > 4000	A	A	A		

Tab. 2. Klasy odporności pożarowej budynków PM

Klasy reakcji na ogień wyrobów budowlanych i elementów budynków z wyjątkiem posadzek i wyrobów liniowych

A1		
A2-s1,d0	A2-s2,d0	A2-s3,d0
A2-s1,d1	A2-s2,d1	A2-s3,d1
A2-s1,d2	A2-s2,d2	A2-s3,d2
B-s1,d0	B-s2,d0	B-s3,d0
B-s1,d1	B-s2,d1	B-s3,d1
B-s1,d2	B-s2,d2	B-s3,d2
C-s1,d0	C-s2,d0	C-s3,d0
C-s1,d1	C-s2,d1	C-s3,d1
C-s1,d2	C-s2,d2	C-s3,d2
D-s1,d0	D-s2,d0	D-s3,d0
D-s1,d1	D-s2,d1	D-s3,d1
D-s1,d2	D-s2,d2	D-s3,d2
E		E-d2
F		

Odporność dachów na ogień zewnętrzny

B_{ROOF} (t1), F_{ROOF} (t1)

Określenia dotyczące rozprzestrzeniania ognia

NRO, SRO, silnie rozprzestrzeniające ogień

Wysokość budynku – w związku z warunkami technicznymi jest mierzona od poziomu terenu, od najniżej położonego wejścia znajdującego się na pierwszej kondygnacji nadziemnej budynku do górnej powierzchni najwyżej położonego stropu, łącznie z grubością izolacji cieplnej i warstwy ją osłaniającej

Kondygnacja nadziemna – kondygnacja, która nie jest kondygnacją podziemną

Kondygnacja podziemna – kondygnacja zagłębiona ze wszystkich stron budynku, co najmniej do połowy jej wysokości w świetle poniżej poziomu przylegającego do niego terenu, a także każda kondygnacja usytuowana pod nią

Konstrukcja dachu – konstrukcja nośna

Przekrycie dachu – przegroda (jedno- lub wielowarstwowa) osłaniająca dach od strony zewnętrznej i chroniąca go w ten sposób przed oddziaływaniem czynników atmosferycznych

Elementy wyposażenia dachu – klapy dymowe, klapy wentylacyjne, świetliki, wyłazy dachowe

Klapy dymowe – urządzenia przeznaczone do grawitacyjnego odprowadzania gazowych produktów spalania oraz ciepła powstającego podczas pożaru

Klapy wentylacyjne – urządzenia przeznaczone do naturalnej wentylacji oraz doświetlenia pomieszczenia

Krzysztof Bagiński
Maria Dreger
Stowarzyszenie DAFA

Autorzy są ekspertami ze Stowarzyszenia DAFA – organizacji, która aktywnie działa na rzecz ujednolicenia i poprawy standardów wykonawczych oraz rozwoju wiedzy o technologiach i funkcjonowaniu dachów płaskich i fasad. W artykule wykorzystano treść ich publikacji *Bezpieczeństwo pożarowe dachów*. Wytyczne Stowarzyszenia DAFA w postaci publikacji technicznych są dostępne na stronie www.dafa.com.pl.

SPRAWDŹ
JAK ZMIENIAMY
SIĘ DLA CIEBIE

NOWA STRONA INTERNETOWA

OPROGRAMOWANIA **NMS**

www.nms.aat.pl

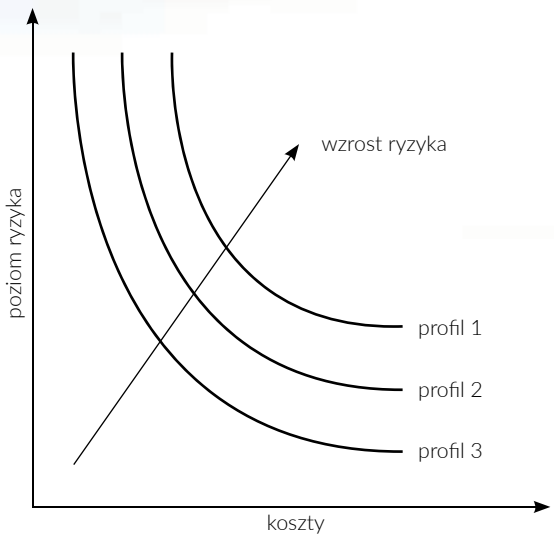
www.nms.aat.pl

Strategie
ochrony przeciwpożarowej budynków
(część 2)

Dorota Brzezińska | Paul Bryant

Profile ryzyka w strategii przeciwpożarowej

Różne rozwiązania, odpowiadające jednocześnie różnym profilom ryzyka, mogą wymagać odmiennych środków i nakładów mających na celu zmniejszenie ryzyka do poziomu akceptowalnego. Z kolei te same środki zastosowane w przypadku dwóch różnych profilów ryzyka dadzą w efekcie różne poziomy ryzyka wynikowego. W rzeczywistości profile ryzyka można zilustrować jako



Rys. 1. Profile ryzyka pożaru [1–3]

Podejście strategiczne do ochrony przeciwpożarowej oznacza uwzględnienie całokształtu uwarunkowań, jakie występują w analizowanym obiekcie, które mogą mieć istotny wpływ na warunki panujące w czasie pożaru. Wymaga ono holistycznego spojrzenia na ochronę przeciwpożarową i zastanowienia się, które z dostępnych rozwiązań może w danym przypadku zapewnić najlepsze rezultaty. W pierwszej części artykułu omówione zostały cele zastosowania poszczególnych systemów przeciwpożarowych oraz dwa różne podejścia do projektowania – podejście, które polega na skupieniu się wyłącznie na zgodności z przepisami, oraz podejście, w którym celem nadrzędnym jest określona funkcjonalność. Niniejsza część jest poświęcona metodom tworzenia strategii oraz sposobom dokonywania ich oceny

krzywe, które niczym nie różnią się od powszechnie stosowanych w ekonomii krzywych podaży i popytu. Jest to przedstawione na rysunku 1.

Oś pozioma na wykresie odpowiada wielkości wymaganych nakładów finansowych, natomiast oś pionowa określa uzyskany poziom ryzyka w przypadku danego profilu. Biorąc jeden profil ryzyka jako przykład, zakładamy, że przy minimalnych kosztach związanych z zastosowaniem środków ochrony przeciwpożarowej uzyskamy pewien poziom ryzyka. Środki ochrony przeciwpożarowej są ujęte w strategii pożarowej, dlatego poziom ryzyka będzie stopniowo obniżał się, aż do osiągnięcia optymalnego poziomu ryzyka i kosztów. Jeżeli w dalszym ciągu ponoszone będą wydatki na kolejne zabezpieczenia, w pewnym momencie ryzyko przestanie już się zmniejszać.

Należy pamiętać, że budynki mają różne profile ryzyka (w zależności od ich rodzaju i przeznaczenia), a ich charakterystyki znajdują się na różnych poziomach – im ryzyko jest większe, tym bardziej krzywa przesuwa się w prawo. W metodzie oceny strategii przeciwpożarowych opisanej w książce *Strategie ochrony przeciwpożarowej budynków* [1] zalecam uwzględnianie profilów ryzyka, jakie proponuje brytyjska norma BS 9999 [4], przedstawionych w tabeli 1.

W celu dokonania wstępnej oceny ryzyka pożaru w różnych częściach budynku można skorzystać z prostej macierzy „dwa na dwa". Używając jej tak, jak pokazano na rysunku 2, można łatwo i szybko ocenić każdą część budynku.

Charakterystyka użytkowników	Szybkość rozwoju pożaru	Profil ryzyka
A (osoby, które nie śpią i znają budynek)	1 – wolny	A1
	2 – średni	A2
	3 – szybki	A3
	4 – bardzo szybki	A4 (A)
B (osoby, które nie śpią i nie znają budynku)	1 – wolny	B1
	2 – średni	B2
	3 – szybki	B3
	4 – bardzo szybki	B4 (A)
C (użytkownicy, którzy mogą spać)	1 – wolny	C1 (B)
	2 – średni	C2 (B)
	3 – szybki	C3 (B, C)
	4 – bardzo szybki	C4 (A, B)

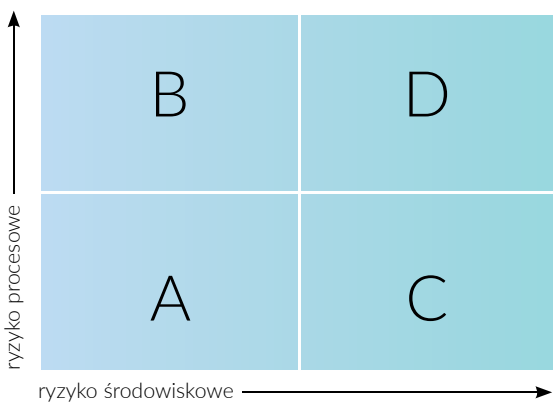
Tab. 1. Profile ryzyka pożaru według BS 9999 [4]

A – profil (kategoria) ryzyka, który nie jest akceptowalny (według BS 9999); dodanie samoczynnego systemu gaśniczego pozwala na zmianę kategorii na niższą poprzez zmniejszenie zakładanej szybkości rozwoju pożaru o jedną pozycję

B – profil (kategoria) ryzyka, który ma podkategorie

C – profil ryzyka, który nie jest akceptowalny, chyba że zostaną podjęte specjalne środki ostrożności

Poszczególne ćwiartki macierzy ryzyka pożaru odpowiadają różnym poziomom ryzyka i ich charakterystykom przedstawionym w tabeli 2.



Rys. 2. Macierz ryzyka pożaru [1–3]

Dzięki zastosowaniu macierzy można precyzyjnie określić profil ryzyka pożaru odpowiadający danemu budynkowi. Opracowując strategię przeciwpożarową, można zatem skupić się na najważniejszych miejscach i poszukać odpowiednich rozwiązań. Gdy przypiszemy każde miejsce w budynku do części macierzy, uzyskamy możliwość oceny ryzyka dotyczącego tego miejsca. Jest to narzędzie porównawcze. Strategia pożarowa jest niekompletna bez dokonania odpowiedniej oceny ryzyka.

Siatka strategii przeciwpożarowej

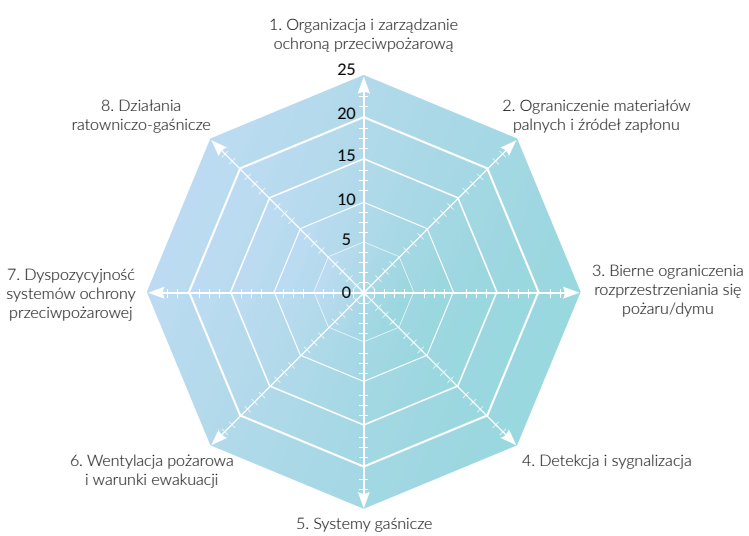
Strategia przeciwpożarowa może być zobrazowana w formie diagramu (siatki). Taka forma jest zasugerowana w normie BS PAS 911. Można ukazać w ten sposób elementy składowe

Ćwiartka	Poziom ryzyka pożaru	Charakterystyka
A	Małe ryzyko środowiskowe/małe ryzyko procesowe	Idealna sytuacja – niewielkie ryzyko pożaru w budynku
B	Małe ryzyko środowiskowe/duże ryzyko procesowe	Sytuacja, w której ryzyko procesowe jest nieuniknione, a małe ryzyko środowiskowe jest jak najbardziej odpowiednie (np. w budynkach produkcyjnych)
C	Duże ryzyko środowiskowe/małe ryzyko procesowe	Dobrym przykładem jest budynek zabytkowy lub budynek, w którym znajdują się zasłony, regały z książkami i inne rzeczy zwiększające ryzyko środowiskowe, a jednocześnie ryzyko procesowe jest w tym miejscu kontrolowane i prawdopodobnie zarządzanie bezpieczeństwem pożarowym jest odpowiednie
D	Duże ryzyko środowiskowe/duże ryzyko procesowe	Można powiedzieć, że ryzyko pożaru jest w tym przypadku nieuniknione, a nie tylko prawdopodobne

Tab. 2. Poziomy ryzyka pożaru przypisane do poszczególnych fragmentów macierzy i ich charakterystyki

strategii oraz ważność każdego z nich w danym przypadku. Ma to ułatwić ustalenie wpływu poszczególnych elementów na całość. W idealnej sytuacji obraz powinien zajmować jedną stronę w formacie A4.

Strategię przeciwpożarową opracowuje się zespołowo, w gronie osób uczestniczących w realizacji projektu. Najczęściej w skład zespołu wchodzi reprezentant inwestora, architekci, rzeczoznawca (inżynier zabezpieczeń pożarowych) oraz projektanci branżowi.



Rys. 3. Siatka strategii przeciwpożarowej [1]

Jest osiem elementów strategii przeciwpożarowej. Ważność każdego z nich w danym przypadku określa się w skali od 0 do 25 i zaznacza na siatce. Takie przypisanie wartości liczbowych daje wyobrażenie o proporcjach związanych z nimi kosztów. Jeżeli na przykład każdemu elementowi zostanie przypisana maksymalna wartość 25, to obraz graficzny na diagramie będzie obejmował maksymalną możliwą powierzchnię. Rozwiązania mające zapewnić bezpieczeństwo i ochronę przeciwpożarową mogą być w takim przypadku bardzo kosztowne. Jeżeli zajęty obszar na diagramie będzie mniejszy, realizacja strategii przeciwpożarowej (np. zastosowanie odpowiednich systemów) będzie tańsza. Należy pamiętać o tym, że strategia ma być skuteczna, nawet jeśli koszty muszą być niższe.

W Polsce, poza ogólną charakterystyką strategii przeciwpożarowej przedstawioną w formie siatki, niezbędna jest metodologia umożliwiająca dokonywanie porównania jakościowo-ilościowego różnych rozwiązań stosowanych jako rozwiązania zamienne bądź zastępcze, czy też jako elementy umożliwiające odstąpienie od zastosowania zabezpieczeń wymaganych wprost przez przepisy techniczno-budowlane. W związku z tym na bazie siatki strategii przeciwpożarowej opracowywany jest model obiektywnej i holistycznej oceny poziomów zabezpieczenia budynków uzyskiwanych poprzez zastosowanie poszczególnych rozwiązań. Model ten umożliwia sprawdzenie, czy uzyskany w danym przypadku poziom bezpieczeństwa jest co najmniej równy poziomowi wymaganemu przez polskie przepisy. Jest on ściśle dostosowywany do rodzaju analizowanego obiektu.

Podsumowanie

Przedstawione w niniejszym artykule strategie ochrony przeciwpożarowej budynków są w Polsce nowością. Wydaje się, że niewielka zmiana podejścia inżynierów pożarowych, w tym rzeczoznawców do spraw zabezpieczeń przeciwpożarowych, i stosowanie przedstawionych powyżej metod może znacząco wpłynąć na jakość przygotowywanych przez nich opracowań i podnieść poziom bezpieczeństwa budynków przy jednoczesnej optymalizacji nakładów finansowych. Opisana w książce *Strategie ochrony przeciwpożarowej budynków* pełna metodyka oceny strategii przeciwpożarowych pozwala na dokonywanie porównań różnych rozwiązań i określanie, czy uzyskany poziom bezpieczeństwa jest co najmniej równy poziomowi zgodnemu z przepisami, wymaganemu w przypadku danego profilu ryzyka pożaru.

dr inż. Dorota Brzezińska
mgr inż. Paul Bryant
Wydział Inżynierii Procesowej
i Ochrony Środowiska
Politechnika Łódzka

Literatura:

1. D. Brzezińska, P. Bryant, *Strategie ochrony przeciwpożarowej budynków*, Łódź 2018.
2. BS PAS 911:2007 – *Fire Strategies – Guidance and Framework for Their Formulation*.
3. P. Bryant, *Fire Strategies – Strategic Thinking*, London 2013.
4. *BS 9999:2017. Fire safety in the design, management and use of buildings. Code of practice.*

STRATEGIE OCHRONY PRZECIWPOŻAROWEJ BUDYNKÓW

nowa metoda oceny poziomu bezpieczeństwa pożarowego budynków projektowanych i istniejących

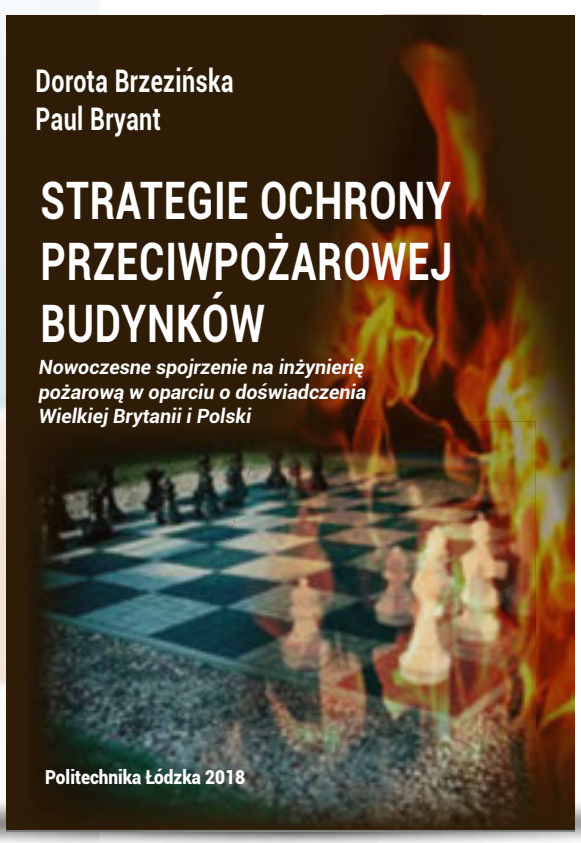
W lutym 2018 r. ukazała się publikacja z zakresu ochrony przeciwpożarowej, autorstwa Doroty Brzezińskiej i Paula Bryanta, dająca nowe spojrzenie na inżynierię pożarową, oparte o doświadczenia wywodzące się zarówno z Polski jak i z Wielkiej Brytanii. Książka nosi tytuł „Strategie ochrony przeciwpożarowej budynków". Powstała ona na podstawie brytyjskiej książki Fire Strategies - Strategic Thinking, autorstwa Paula Bryanta z myślą o czytelnikach z różnych krajów świata. Jej treść bazowała na doświadczeniach jakie zdobył Paul Bryant w Wielkiej Brytanii oraz innych krajach, w których pracował. Wydanie polskie opracowane przez Dorotę Brzezińską zostało częściowo zmodyfikowane i uzupełnione, tak aby dostosować je do polskich uwarunkowań i aby książka ta była inspirująca dla polskiego czytelnika, któremu jest dedykowana. **Szczególnie cennym elementem książki jest opracowana przez autorów, specjalnie do wydania polskiego, metodyka ilościowej oceny ogólnego poziomu bezpieczeństwa pożarowego budynków, przy zastosowaniu różnych środków zabezpieczeń przeciwpożarowych.** Może ona być wykorzystywana między innymi do przygotowania ekspertyz pożarowych służących do uzyskania odstępstw od wymagań obowiązujących przepisów, gdzie niezbędne jest rekompensowanie niedoboru jednego środka zabezpieczeń innymi środkami. Opisana w dwunastu rozdziałach teoria na temat tworzenia oraz dokonywania oceny strategii przeciwpożarowych, została dodatkowo zobrazowana trzema przykładowymi strategiami dla różnych rodzajów budynków, które znajdują się w załącznikach A1-A3.

Książka jest przeznaczona zarówno dla profesjonalistów z zakresu ochrony przeciwpożarowej, jak i dla tych wszystkich, którzy są z ochroną przeciwpożarową budynków związani, w tym architektów, inżynierów budownictwa i konstruktorów, służb kontrolujących obiekty, osób prowadzących ich odbiory dopuszczające do użytkowania, ubezpieczycieli, zarządców i osób odpowiedzialnych za bezpieczeństwo pożarowe w trakcie eksploatacji. Może ona być również pomocna studentom kierunków i specjalności związanych z ochroną przeciwpożarową, które coraz bardziej rozpowszechniają się w naszym kraju.

Opracowana przez autorów metodyka wyznaczania Indeksu Ryzyka Pożaru jest propozycją praktycznego narzędzie do dokonywania oceny, czy zastosowane w budynku rozwiązania zamienne, przyjęte w rzeczywistej strategii przeciwpożarowej, stanowią równoważny poziom jego zabezpieczenia w stosunku do rozwiązań strategii oczekiwanej, opartej na profilu ryzyka danego budynku lub na wymaganiach przepisów.

Książka uzyskała pozytywną opinię wybitnych polskich recenzentów, jak:

1. prof. dr hab. Kazimierz Lebecki, Wyższa Szkoła Zarządzania Ochroną Pracy, Katowice
2. dr hab. inż. Adam Markowski prof. ndzw. Politechnika Łódzka, WIPOS
3. dr inż. Paweł Janik, Stowarzyszenie Inżynierów i Techników Pożarnictwa SITP
4. dr inż. Dariusz Gołębiewski, Wiceprezes Zarządu Spółki PZU Lab.



Książkę można zakupić:

Izba Rzeczoznawców SITP, ul. Świętokrzyska 14, I piętro, tel.: (22) 620 32 25, 850 37 56, e-mail: sitp@wa.home.pl

Skuteczność instalacji gaśniczych a minimalizacja strat (część 2)

Robert Kuczkowski

Zakres stosowania i zasady działania gazowego systemu gaśniczego

Gazowe systemy gaśnicze bardzo dobrze sprawdzają się tam, gdzie instalacje gaśnicze z innym medium roboczym (np. np. z wodą albo proszkiem) nie są w stanie zapewnić osiągnięcia należytej ochrony. Zastosowania gazowych systemów gaśniczych:

- gaszenie obiektów użyteczności publicznej, np. archiwów, bibliotek, centrów przetwarzania danych, miejsc, w których przechowywane są dzieła sztuki,
- gaszenie pomieszczeń produkcyjnych, magazynowych lub elektrycznych, np. rozdzielni elektrycznych, kabin lakierniczych, serwerowni w firmach, pomieszczeń, w których przechowywane są materiały niebezpieczne, pomieszczeń z UPS-ami, szaf sterowniczych/elektrycznych usytuowanych na poziomach technicznych,
- gaszenie obiektów wojskowych o szczególnym przeznaczeniu,
- gaszenie bezobsługowych obiektów w systemach rozproszonych (elektrowni wiatrowych, kontenerów technicznych w biogazowniach),
- gaszenie poszczególnych elementów dużej linii technologicznej, np. tuneli utwardzania druku w drukarniach offsetowych, gaszenie całych maszyn i urządzeń, np. w zespołach turbokompresorów, itp.

Jak widać, systemy gaszenia gazem są przydatne w bardzo wielu różnych obiektach. Za ich pomocą można gasić całe obiekty, wybrane pomieszczenia, newralgiczne węzły w zakładach przemysłowych i pojedyncze urządzenia. Wybrane pomieszczenia to np. własne serwerownie firm. W dzisiejszym coraz bardziej zinformatyzowanym świecie bardzo trudno sobie wyobrazić możliwość funkcjonowania firmy bez własnej serwerowni, którą oczywiście należy zabezpieczyć przed pożarem. Podczas produkcji w zakładzie przemysłowym mogą zachodzić procesy, które stwarzają zagrożenie pożarem. Zagrożenie może mieć związek z własnościami fizykochemicznymi materiałów lub warunkami, w jakich przebiegają poszczególne procesy, np. z wysoką temperaturą – dobrym przykładem jest kabina lakiernicza.

Należy chronić newralgiczne węzły, w szczególności te, które są usytuowane w miejscach, gdzie nie ma stałej obsługi. Duże pożary, które miały miejsce w zakładach tego typu, w większości przypadków były spowodowane zwarciami instalacji elektrycznej w szafach elektrycznych. Ochrona indywidualnych maszyn, takich jak chociażby przykładowy zespół turbokompresorów w tłoczniach gazu, znacznie ogranicza ryzyko pożaru w tego typu obiektach.

Gaszenie gazem polega głównie na obniżeniu zawartości tlenu w powietrzu do wartości, przy której proces spalania nie może być dłużej podtrzymywany.

Schłodzenie płomieni dodatkowo ułatwia gaszenie. Gwarancją skuteczności gazowej instalacji gaśniczej jest spełnienie następujących warunków:

- dobór odpowiedniego środka gaśniczego,
- dobór rodzaju i rozmieszczenia elementów instalacji oraz lokalizacji zapasu środka gaśniczego,
- dobór stężenia środka gaśniczego i obliczenie wymaganej ilości środka,
- zaprojektowanie i wykonanie armatury systemu transportu i dystrybucji gazu.

Aby gaszenie było skuteczne, ważny jest sposób aktywacji systemu. Systemy sterowania umożliwiają kilka sposobów: ręczne uruchamianie elektryczne lub mechaniczne, uruchamianie automatyczne po weryfikacji przez obsługę, bezzwłoczne uruchamianie automatyczne. Najczęściej stosowana jest bezpośrednia aktywacja systemu po uzyskaniu informacji z systemu detekcji pożaru. Dlatego ważne jest prawidłowe wykonanie tego systemu, dobranie i rozmieszczenie czujek pożarowych, a także wykonanie linii dozorowych, sygnałowych, sterujących i zasilających. System detekcji pożaru musi być przystosowany i przeznaczony do sterowania systemem gaszenia gazem. W projekcie powinno się uwzględnić takie elementy infrastruktury technicznej i budowlanej, jak podłoga techniczna, sufit podwieszany, występujące instalacje (wentylacyjna/klimatyzacyjna). Mając na względzie nadrzędną wartość, jaką jest ludzkie życie, należy zwrócić uwagę na cały szereg czynników, takich jak czas opóźnienia potrzebny na ewakuację ludzi, sygnalizacja informacyjna i alarmowa (akustyczna i optyczna), uruchomienie i wstrzymywanie procedury gaszenia wewnątrz i na zewnątrz strefy gaszenia, warunki ewakuacji, w tym kierunki otwarcia drzwi na zewnątrz strefy gaszenia. Stężenie gazu

po wyładowaniu powinno być utrzymane przez dłuższy czas w celu uzyskania pełnego gaszenia, dlatego należy pamiętać, że chronione pomieszczenie powinno być odpowiednio szczelne oraz odpowiednio zabezpieczone przed dostępem osób nieuprawnionych.

Nieprawidłowości i błędy w systemach bezpieczeństwa

W trakcie audytów można stwierdzić wiele nieprawidłowości w systemach gaszenia gazem i ich funkcjonowaniu. Chodzi o ich złe zaprojektowanie, błędy montażowe, nieprawidłowe serwisowanie i konserwacje, niewłaściwą obsługę i zmiany funkcji pomieszczeń, w których zainstalowano elementy tych systemów. Źle dobrane i rozmieszczone podzespoły instalacji, niewłaściwe umiejscowienie zapasu środka gaśniczego, źle dobrane stężenia gazów gaśniczych, nieuwzględnienie elementów infrastruktury technicznej i budowlanej, takich jak podłoga techniczna, sufit podwieszany, występujące instalacje wentylacyjne/klimatyzacyjne, to najczęściej spotykane błędy popełniane na etapie projektowania, które są najtrudniejsze do późniejszego naprawienia. Najczęściej spotykanymi błędami na etapie wykonawstwa są niewłaściwe sposoby mocowania poszczególnych elementów systemu. Bardzo często spotykane nieprawidłowości mają związek z niewłaściwą konserwacją i nierzetelnymi przeglądami instalacji. Brak uregulowań prawnych dotyczących kompetencji osób zajmujących się serwisem i konserwacją nie jest tu bez znaczenia. Główne i niejednokrotnie jedyne kryterium, jakim jest cena za wykonaną usługę, skutkuje tym, że serwisowanie instalacji często bywa ograniczone do wykonania podstawowych czynności i nie wykonuje się wymaganych czynności konserwacyjno-remontowych. Oczywiście ma to wpływ na ogólną ocenę firm oferujących usługi serwisowe, która jest krzywdząca w przypadku tych przedsiębiorstw, które wykonują pracę fachowo i sumiennie.

Podsumowanie

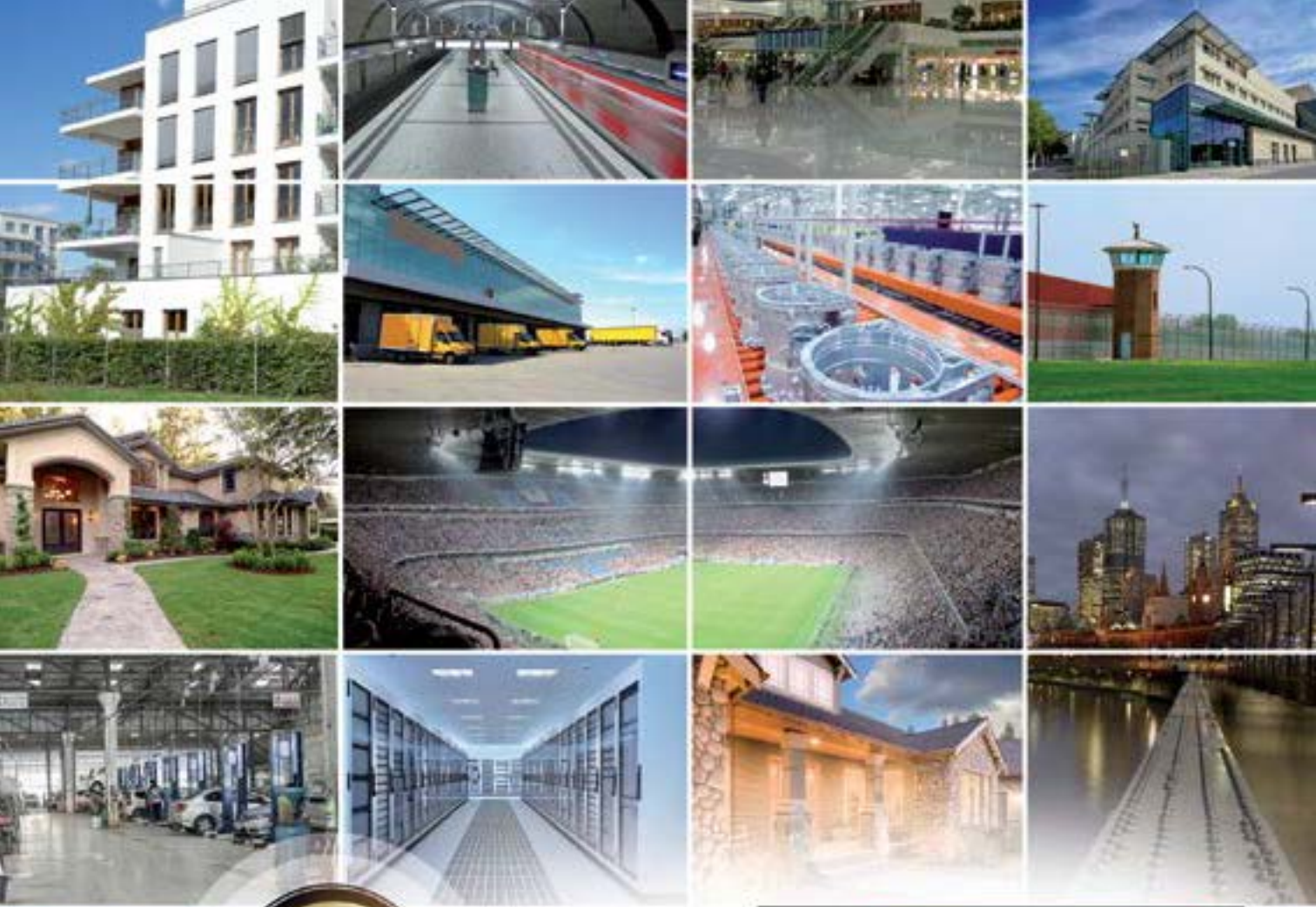
Efektywne rozwiązywanie wielu problemów technicznych wymaga odpowiedniego zasobu wiedzy, umiejętności krytycznej oceny danego zagadnienia, rzetelnej analizy, powiązywania faktów, zdroworozsądkowych zasad podejmowania decyzji. Niestety bardzo często systemy są wykonane źle i funkcjonują nieprawidłowo. Aby uniknąć podstawowych błędów, należy zadbać o:

1. Dobranie koncepcji ochrony przeciwpożarowej do konkretnego zakładu z uwzględnieniem jego specyfiki, dotyczących go zagrożeń i rekomendacji ubezpieczyciela już na etapie projektu (analiza danych historycznych).
2. Opracowanie projektów instalacji przeciwpożarowych z uwzględnieniem zasad ich współdziałania ze sobą w ramach całościowego systemu bezpieczeństwa – holistyczne spojrzenie na funkcjonowanie systemów bezpieczeństwa. W celu zapewnienia pełnej funkcjonalności i dyspozycyjności poszczególnych systemów niezbędne jest współdziałanie projektantów tychże systemów ze sobą.
3. Zlecenie budowy systemów firmom doświadczonym, posiadającym odpowiednie kwalifikacje, najlepiej potwierdzone certyfikatami. Wybierając wykonawcę, nie należy kierować się kryterium najniższej ceny za usługę. Projektanci, wykonawcy i serwisanci powinni być przeszkoleni, posiadać certyfikaty CNBOP-PIB, wykształcenie techniczne i szczegółową wiedzę.
4. Zagwarantowanie właściwego nadzoru nad stanem technicznym urządzeń przeciwpożarowych.

mgr inż. Robert Kuczkowski
PZU Lab, Politechnika Łódzka

Literatura

1. *200 lat ubezpieczania*, PZU S.A., Ośrodek Karta, Warszawa 2003.
2. A. Brandowski, *Nauka o bezpieczeństwie*, Warszawa 1993.
3. D. Gołębiewski, *Audyt ubezpieczeniowy*, Poltext, Warszawa 2010.
4. D. Gołębiewski, *Risk Assessment For Insurance Purposes of High Risk Plants*, Fundacja Rozwoju Uniwersytetu Gdańskiego, Gdańsk 2007.
5. P. Guzewski, D. Wróblewski, D. Małozięć, *Czerwona księga pożarów* (publikacja opracowana w ramach projektu nr DOBR-BIO4/050/13009/2013 finansowanego przez NCBR), Józefów 2014.



IS VENO

INTEGRACJA SYSTEMÓW BEZPIECZEŃSTWA

JEDNO OPROGRAMOWANIE – WIELE SYSTEMÓW
JEDEN CEL: EFEKTYWNE ZARZĄDZANIE OBIEKTEM

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

RFID
w zautomatyzowanym systemie parkingowym

Jacek Krywult

Potrzeba zabezpieczenia terenów firm przed nieuprawnionym dostępem powoduje, że coraz częściej stosuje się systemy kontroli dostępu oraz ewidencji ruchu osób i pojazdów

Ręczne wypisywanie przepustek to czynność czasochłonna, często zakłócająca płynność ruchu na danym terenie. Denerwuje się każdy, kto musi czekać na wjazd, a także pracownicy ochrony, którzy tracą cenne minuty na papierową ewidencję. Powoduje to wrażenie chaosu organizacyjnego, a więc może nawet zniechęcić potencjalnych klientów czy partnerów biznesowych.

Automatyczny system parkingowy wykorzystujący technikę RFID może wyeliminować wady tradycyjnej metody ewidencji ruchu. Przepustki papierowe zostają zastąpione znacznikami RFID UHF. System daje możliwość wydawania różnych przepustek. Typ przepustki zależy od przyznanych uprawnień. Mogą to być przepustki stałe, tymczasowe, VIP – całość jest w pełni konfigurowalna. Kontrola ruchu na parkingu za pomocą systemu RFID umożliwia łatwe ustalanie czasu parkowania i ewentualne egzekwowanie opłat za wjazd – system automatycznie uniemożliwi uzyskanie dostępu za pomocą karty lub etykiety, która utraciła ważność.

System parkingowy, w którym wykorzystuje się znaczniki RFID, zabezpiecza przed nieuprawnionym wjazdem oraz umożliwia raportowanie liczby osób przebywających na terenie objętym działaniem tego systemu. Rejestruje także zużycie dróg wewnętrznych przez pojazdy o dużym tonażu. Co ważne, system kontroli ruchu wykorzystujący znaczniki RFID wspomaga lub zastępuje personel zajmujący się ochroną danego terenu.

Wszystkie wymienione wyżej funkcje kontroli ruchu są realizowane dzięki wykorzystaniu szlabanów, bram, kołowrotów oraz odpowiednich czytników dalekiego zasięgu. Wjazd oraz wyjazd przez szlaban jest kontrolowany dzięki zdalnej identyfikacji osób oraz pojazdów. Umożliwia ona pełną ewidencję wejść i wyjść osób, a także kontrolę wjazdów i wyjazdów samochodów. Gdy stosowane są znaczniki RFID UHF, nie ma konieczności wychodzenia z samochodu czy otwierania szyby przez kierowcę w celu identyfikacji – wystarczy posiadać kartę lub etykietę naklejoną na szybie.

Fot. 1. System parkingowy na jednym z katowickich osiedli

Fot. 2. Czytnik RFID dalekiego zasięgu

Fot. 3. Brama parkingowa z czytnikiem RFID

Fot. 4. System parkingowy RFID

System parkingowy, w którym wykorzystuje się znaczniki RFID, umożliwia pełne raportowanie dzięki rejestrowaniu wszystkich zdarzeń. Informuje o tym, kto w danej chwili znajduje się na chronionym terenie, co staje się bardzo ważne w przypadku konieczności ewakuacji. Ponadto skalowalność systemu jest możliwa na każdym etapie wdrażania i eksploatacji.

Dzięki znacznikom RFID możliwa jest nawet pełna automatyzacja systemu kontroli dostępu. W efekcie pracownicy oszczędzają czas, a ruch odbywa się płynnie i może być w pełni ewidencjonowany.

Jacek Krywult

Kontroler KT-1

Kontroler KT-1 firmy Kantech za sprawą nowego oprogramowania producenta może pracować w **trybie autonomicznym**. Konfiguracja i zarządzanie urządzeniem odbywają się przy użyciu intuicyjnego oprogramowania za pośrednictwem przeglądarki internetowej. Kontroler wyposażony jest w 2 porty czytników pozwalające na kontrolę jednych drzwi jednostronnie lub dwustronnie. Menu dostępne przez przeglądarkę umożliwia zarówno zaprogramowanie, jak i wykonywanie określonych operacji na drzwiach obsługiwanych przez ten kontroler. W szczególności zapewnia dodawanie użytkowników kart wraz z uprawnieniami.

Charakterystyka	
Pamięć kart	100 000
Pamięć zdarzeń	20 000
Porty czytników	Wiegand, ABA Track II
Porty komunikacyjne	1xEthernet 10/100 (RJ-45), 2xRS-485, 1xRS-232 (RJ-12)
Typy czytników	zbliżeniowe, magnetyczne, biometryczne
Zasilanie kontrolera	12 V_{DC} / 2 A
Wilgotność względna	93% maksimum, bez kondensacji
Temperatura pracy	10° do 55° C, do instalacji wewnątrz pomieszczeń
Przekaźniki	2 szt., typu NO/NC, obciążalność styków: 30 V_{DC}/3 A
Wejścia linii dozorowych	4 wejścia linii dozorowych (Z1 do Z4), bez rezystora EOL, z pojedynczym rezystorem EOL lub podwójnym oraz czujnik sabotażowy
Wyjścia sterujące do sygnalizatorów w czytnikach	4 do diod LED (LED, OUT1, OUT2) oraz do brzęczyka - o obciążalności 25 mA, tranzystorowe, typu „otwarty kolektor”
Możliwość pracy autonomicznej	tak (wersja oprogramowania 2.00.14 lub wyższa)
Możliwość pracy pod programem EntraPass	tak
Restart	automatyczny restart po całkowitej utracie zasilania oraz nieograniczony czas przechowywania danych i zdarzeń
Obsługiwane przeglądarki	Safari, Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa

tel. 22 546 05 46, faks 22 546 05 01
e-mail: kontakt@aat.pl
www.aat.pl

NVR-7732-H8

Rejestrator IP marki NOVUS z funkcją RAID

Rejestrator może obsłużyć równocześnie **32 kamery** o rozdzielczości 4K, zapisuje on obrazy z prędkością zapisu 30 kl./s dla każdego strumienia wizyjnego, oraz dźwięk z kamer. Ma pięć wyjść monitorowych podzielonych na dwie grupy: monitor główny i monitor pomocniczy.
W urządzeniu można zamontować maksymalnie osiem dysków twardych o pojemności 8 TB każdy oraz dodatkowo zbudować dwie macierze **RAID** o pojemności 16 TB każda.

Wizja	
Kamery IP	32 kanały o rozdzielczości 3840 x 2160 (obraz i dźwięk)
Maks. rozdzielczość	3840 x 2160
Kompresja	H.264, H.264+, H.265
Wyjścia monitorowe	główne (podział, pełny ekran, sekwencja): 1 x VGA, 1 x BNC, 1 x HDMI (4K UltraHD) (dla trzech monitorów jednocześnie) pomocnicze: 1 x HDMI (FullHD), 1 x VGA
Zapis obrazów	
Prędkość zapisu	960 kl./s (32 x 30 kl./s dla 3840 x 2160)
Sumaryczna przepływność strumienia wizyjnego	320 Mb/s łącznie ze wszystkich kamer
Odtwarzanie	
Prędkość odtwarzania	480 kl./s (16 x 30 kl./s dla 3840 x 2160) **
Dyski	
Dyski montowane wewnątrz urządzenia	możliwość montażu: 8 x HDD 3.5" 8 TB SATA ***
Maks. łączna pojemność dysków	64 TB
Alarmy	
Wejścia/wyjścia alarmowe lokalne	16/4 typu przekaźnikowego
Detekcja ruchu	obsługa funkcji detekcji ruchu dostępnej w kamerach*
Reakcja na zdarzenia alarmowe	sygnał dźwiękowy, aktywacja wyjścia alarmowego, aktywacja zapisu, zmiana ustawień PTZ, wysłanie e-mail z załącznikiem
Sieć	
Interfejs sieciowy	2 x Ethernet - złącze RJ-45, 10/100/1000 Mb/s
Zgodność z ONVIF	Profil S (ONVIF 2.2 lub wyższy)
Programy na PC/MAC	NMS, Internet Explorer, Firefox, Chrome, Opera/Safari
Programy na Smartphone	NVR 7000 Viewer (iPhone, Android)
Maks. liczba połączeń z rejestratorem	2
Dodatkowe interfejsy	
Porty USB	3 x USB 2.0, 1 x USB 3.0
Parametry instalacyjne	
Mocowanie w szafie RACK 19"	wysokość 2U

* Obsługa tej funkcji jest uzależniona od zastosowanego protokołu komunikacji, szczegółowe dane znajdują się w tabeli kompatybilności dostępnej w zakładce PLIKI DO POBRANIA na stronie produktu na www.aat.pl.
** W przypadku odtwarzania dwóch strumieni wizyjnych jednocześnie.
*** Informacje o kompatybilnych modelach twardych dysków oraz maksymalnych ich pojemnościach znajdują się w pliku dostępnym w zakładce PLIKI DO POBRANIA na stronie produktu na www.aat.pl.

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa

tel. 22 546 05 46, faks 22 546 05 01
e-mail: kontakt@aat.pl
www.aat.pl

MCT86M-IO-CH

Terminal dostępu do systemu RACS 5

MCT86M-IO-CH jest terminalem przeznaczonym do wykorzystania w systemie kontroli dostępu i automatyki budynkowej RACS 5, jako punkt identyfikacji użytkownika, sterowania systemem oraz prezentacji jego stanów. Terminal wyposażony jest w kieszeń na kartę zbliżeniową, której status jest w sposób ciągły raportowany do kontrolera. W reakcji na włożenie i wyjęcie karty z kieszeni kontroler podejmuje indywidualnie zaprogramowaną akcję, która może być dodatkowo uzależniona od uprawnień przypisanych do karty. Wbudowane linie we/wy, przyciski funkcyjne oraz wskaźniki LED terminala mogą być skonfigurowane do dowolnych funkcji dostępnych w systemie RACS 5. Terminal rozróżnia krótkie i długie naciśnięcie przycisków funkcyjnych, co umożliwia zaprogramowanie 2 niezależnych funkcji dla każdego z przycisków. Wskaźniki funkcyjne LED są wykorzystywane do sygnalizacji wybranych stanów systemu (np. oświetlenie, ogrzewanie, uzbrojenie, alarm itp.). Zwykle, wskaźnik funkcyjny jest wykorzystywany do sygnalizacji stanu systemu sterowanego przez znajdujący się w jego sąsiedztwie przycisk funkcyjny. Terminal obsługuje szyfrowane sektory kart MIFARE co zabezpiecza system przed użyciem obcych kart oraz duplikowaniem kart oryginalnych. Terminal wymaga podłączenia do kontrolera dostępu, który steruje logiką działania systemu. Połączenie z kontrolerem jest realizowane za pośrednictwem adresowalnej magistrali RS485.

Charakterystyka

- Kieszeń na kartę MIFARE Ultralight/Classic/DESFire/Plus
- 4 dotykowe przyciski funkcyjne
- 4 funkcyjne wskaźniki LED
- 3 linie wejściowe EOL
- 2 wyjścia tranzystorowe 150 mA
- Wyjście przekaźnikowe 1,5 A
- Głośnik o regulowanym poziomie dźwięku
- Ściemnianie wskaźników LED w stanie oczekiwania
- Komunikacja z kontrolerem przez interfejs RS485
- Zasilanie 12 V_{DC}
- Czujnik antysabotażowy
- Praca w warunkach wewnętrznych
- Wymiary: 155,5 x 85,0 x 21,5 mm (szer. x wys. x grub.)
- Linia wzornicza QUADRUS
- Znak CE

ROGER Sp. z o.o. Sp. k.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

tel. 55 272 0132, faks 55 272 0133
e-mail: roger@roger.pl
http://www.roger.pl

MCT88M-IO

Terminal dostępu do systemu RACS 5

MCT88M-IO jest terminalem dostępu przeznaczonym do wykorzystania w systemie RACS 5. Urządzenie ma kolorowy wyświetlacz matrycowy, klawiaturę dotykową z 4 przyciskami funkcyjnymi oraz czytnik MIFARE Ultralight/Classic/DESFire/Plus/Bluetooth. MCT88M-IO może być podłączony do magistrali RS485 kontrolera dostępu MC16 bezpośrednio lub poprzez ekspander MCX16-RS z wykorzystaniem sieci Ethernet (LAN). Alternatywnie MCT88M-IO może być podłączony do wirtualnego kontrolera dostępu poprzez sieć Ethernet (LAN). W przypadku podłączenia do kontrolera MC16 urządzenie może funkcjonować jako terminal kontroli dostępu i (lub) rejestracji czasu pracy, jak też do sterowania systemem kontroli dostępu z uwzględnieniem oferowanej przez system RACS 5 automatyki budynkowej. W przypadku podłączenia do kontrolera wirtualnego urządzenia może funkcjonować jako terminal POS (ang. *Point of Sale*). Logowanie użytkowników na terminalu może odbywać się za pomocą kart zbliżeniowych, kodów PIN lub z poziomu urządzeń mobilnych wyposażonych w Bluetooth.

Charakterystyka

- Terminal dostępu do systemu RACS 5
- Kolorowy wyświetlacz matrycowy
- Czytnik MIFARE Ultralight/Classic/DESFire/Plus
- Identyfikacja mobilna Bluetooth
- Klawiatura dotykowa
- 4 przyciski funkcyjne
- 3 wejścia parametryczne
- 2 wyjścia tranzystorowe
- 1 wyjście przekaźnikowe
- RS485
- Ethernet (LAN)
- Wymiary: 155,5 x 85,0 x 21,5 mm (szer. x wys. x grub.)
- Linia wzornicza QUADRUS
- Znak CE

roger®

ROGER Sp. z o.o. Sp. k.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

tel. 55 272 0132, faks 55 272 0133
e-mail: roger@roger.pl
http://www.roger.pl

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa
tel. 22 546 05 46; faks 22 546 05 01
e-mail: kontakt@aat.pl
www.aat.pl

D PROD S

Oddziały:
ul. Koniczynowa 2A, 03-612 Warszawa II
tel./faks 22 743 10 11, 811 13 50
e-mail: aat.warszawa-praga@aat.pl

ul. Antoniuk Fabryczny 22, 15-741 Białystok
tel. 85 688 32 33
tel./faks 85 688 32 34
e-mail: aat.bialystok@aat.pl

ul. Łęczycka 37, 85-737 Bydgoszcz
tel./faks 52 342 91 24, 342 98 82
e-mail: aat.bydgoszcz@aat.pl

ul. Ks. W. Siwka 17, 40-318 Katowice
tel./faks 32 351 48 30, 256 60 34
e-mail: aat.katowice@aat.pl

ul. Prosta 25, 25-371 Kielce
tel./faks 41 361 16 32, 361 16 33
e-mail: aat.kielce@aat.pl

ul. Biskupińska 14, 30-732 Kraków
tel./faks 12 266 87 95, 266 87 97
e-mail: aat.krakow@aat.pl

ul. Energetyków 13a, 20-468 Lublin
tel. 81 744 93 65/66; faks 81 744 91 77
e-mail: aat.lublin@aat.pl

ul. Dowborczyków 25, 90-019 Łódź
tel./faks 42 674 25 33, 674 25 48
e-mail: aat.lodz@aat.pl

ul. Racławicka 82, 60-302 Poznań
tel./faks 61 662 06 60, 662 06 61
e-mail: aat.poznan@aat.pl

Al. Niepodległości 606/610, 81-855 Sopot
tel./faks 58 551 22 63, 551 67 52
e-mail: aat.sopot@aat.pl

ul. Zielona 42, 71-013 Szczecin
tel./faks 91 483 38 59, 489 47 24
e-mail: aat.szczecin@aat.pl

ul. Na Niskich Łąkach 26, 50-422 Wrocław
tel./faks 71 348 20 61, 348 42 36
e-mail: aat.wroclaw@aat.pl

ACSS ID Systems Sp. z o.o.
ul. Karola Miarki 20C
01-496 Warszawa
tel. 22 832 47 44; faks 22 832 46 44
e-mail: biuro@acss.com.pl
www.acss.com.pl

D I

ALARMNET BORKIEWICZ Sp. J.
ul. Karola Miarki 20c
01-496 Warszawa
tel. 22 663 40 85; faks 22 833 87 95
e-mail: biuro@alarmnet.com.pl
www.alarmnet.com.pl

I D PROD PROJ S

ALARMTECH POLSKA Sp. z o.o.
Oddział w Gdańsku
ul. Kielnieńska 115
80-299 Gdańsk
tel. 58 340 24 40; faks 58 340 24 49
e-mail: info@alarmtech.pl
www.alarmtech.pl

D PROD PROJ S

ALARM-TECH Systemy Zabezpieczeń s.c.
ul. Graniczna 4
32-086 Boleń
tel. kom. 775 453 453
e-mail: sklep@napad.pl
www.napad.pl

Oddział:
os. Jagiellońskie 19, 31-834 Kraków
tel. kom. 609 197 800

D PROD S

ASSA ABLOY POLAND Sp. z o.o.
ul. Jana Olbrachta 94
01-102 Warszawa
tel. 22 751 53 54; faks 22 751 53 56
e-mail: biuro@assaabloy.com
www.assaabloy.com.pl

D I PROJ S

BOSCH SECURITY SYSTEMS
ul. Jutrzenki 105
02-231 Warszawa
tel. 22 715 40 00
e-mail: securitysystems@pl.bosch.pl
www.boschsecurity.pl

D S

P.W.H. BRABORK LABORATORIUM Sp. z o.o.
ul. Ratuszowa 11
03-450 Warszawa
tel. 22 619 29 49; faks 22 619 25 14
e-mail: brabork@braborklab.pl
www.braborklab.pl

I PROJ

bt electronics Sp. z o.o.
ul. Dukatów 10
31-431 Kraków
tel. 12 429 36 16; faks 12 410 85 11
e-mail: bte@bte.pl
www.bte.pl

I PROD PROJ S

CBC (Poland) Sp. z o.o.
ul. Anny German 15
01-794 Warszawa
tel. 22 633 90 90; faks 22 633 90 60
e-mail: info@cbcpoland.pl
www.cbcpoland.pl

D PROD PROJ S

CMA Monitoring Group Sp. z o.o.
ul. Puławska 359
02-801 Warszawa
tel. 22 546 0 888; faks 22 546 0 619
e-mail: info@cma.com.pl
www.cma.com.pl

D I PROD PROJ

Oddziały:
ul. Składowa 2, 41-902 Bytom
tel. 32 388 09 50; faks 32 388 09 60

ul. Zatorska 36, 51-215 Wrocław
tel. kom. 697 972 558
faks 71 341 16 26

Biura handlowe:
ul. Nowy rynek 2, 62-002 Suchy Las k/Poznania
tel. kom. 601 203 664, 601 410 979
faks 61 861 40 51

ul. Hallera 140, lok. 124, 80-416 Gdańsk
tel kom. 693 694 339

CONTROL SYSTEM FMN
Al. KEN 96 lok. U-15
02-777 Warszawa
tel. 22 855 00 17/18; faks 22 855 00 19
e-mail: cs@cs.pl
www.cs.pl

DAHUA TECHNOLOGY POLAND Sp. z o.o.
ul. Salsy 2
02-823 Warszawa
tel. 22 395 74 00
e-mail: biuro.pl@global.dahuatech.com
www.dahuasecurity.com/pl

DG ELPRO Sp. J.
ul. Bonarka 21
30-415 Kraków
tel. 12 263 93 85; faks 12 263 93 86
email: biuro@dgelpro.pl
www.dgelpro.pl

DYSKRET POLSKA
Spółka z ograniczoną odpowiedzialnością Sp. K.
ul. Mazowiecka 131
30-023 Kraków
tel. 12 423 31 00; faks 12 423 44 61
e-mail: office@dyskret.com.pl
www.dyskret.com.pl

EBS Sp. z o.o.
ul. B. Czecha 59
04-555 Warszawa
tel. 22 518 84 00; faks 22 518 84 99
e-mail: sales@ebs.pl
www.ebs.pl

PHU ELPROMA Sp. z o.o.
ul. Syta 177
02-987 Warszawa
tel. kom. 606 270 756
tel. 22 398 96 53
e-mail: elproma@elproma.pl
www.elproma.pl

ELSTECH
os. Złota Podkowa 38/P1
31-352 Kraków
tel. kom. 570 400 537, 570 400 538;
faks 12 350 45 03
e-mail: info@elstech.pl
www.elstech.pl

Eltrox
ul. Główna 23
42-280 Częstochowa
tel. 34 333 57 04
e-mail: sklep@eltrox.pl
www.eltrox.pl

Oddziały:
ul. Św. Rocha 87, 42-202 Częstochowa
tel. 34 333 57 13
e-mail: czestochowa@eltrox.pl

ul. Hynka 6/2, 80-465 Gdańsk
tel. kom. 517 015 441
e-mail: gdansk@eltrox.pl

ul. Myśliborska 2-6, 66-400 Gorzów Wlkp
tel. 95 766 65 16
e-mail: gorzow@eltrox.pl

ul. Wybickiego 42a, 31-302 Kraków
tel. 12 210 06 25
e-mail: krakow@eltrox.pl

ul. 6 sierpnia 14, 90-416 Łódź
tel. 42 233 49 96
e-mail: lodz@eltrox.pl

ul. Orla 7/I, 41-205 Sosnowiec
tel. kom. 501 945 219
e-mail: sosnowiec@eltrox.pl

ul. ks. kard. S. Wyszyńskiego 22
70-203 Szczecin
tel. 91 443 56 36
e-mail: szczecin@eltrox.pl

ul. Joachima Lelewela 33, 87-100 Toruń
tel. 56 645 94 24
e-mail: torun@eltrox.pl

ul. Radzymińska 308, 03-694 Warszawa
tel. 22 676 78 40
e-mail: warszawa@eltrox.pl

ul. Komandorska 53R, 50-258 Wrocław
tel. kom. 504 904 689
e-mail: wroclaw@eltrox.pl

EUROPEAN SECURITY TRADING POLSKA Sp. z o.o.
ul. Wilcza 54a lok. 1
00-679 Warszawa
tel. 22 629 53 49
e-mail: kontakt@estpolska.pl
www.estpolska.pl

EWIMAR Sp. z o.o.
ul. Konarskiego 84
01-355 Warszawa
tel. 22 691 90 65
e-mail: handel@ewimar.pl
www.ewimar.pl

FES TRADING Sp. z o.o.
ul. Schuberta 100
80-171 Gdańsk
tel. 58 340 00 41 ÷ 44; faks 58 340 00 45
e-mail: fes@fes.pl
www.fes.pl

GDE POLSKA
Włosań, ul. Świątnicka 88
32-031 Mogilany
tel. 12 256 50 35; faks 12 270 56 96
e-mail: biuro@gde.pl
www.gde.pl

HANWHA TECHWIN EUROPE LTD.
Biuro w Polsce
ul. Posag 7 Panien 1
02-495 Warszawa
e-mail: hte.poland@hanwha.com
www.hanwha-security.eu

ICS POLSKA
ul. Poleczki 82
02-822 Warszawa
tel. 22 646 11 38; faks 22 849 94 83
e-mail: biuro@ics.pl
www.ics.pl

INSAP Sp. z o.o.
ul. Ładna 4-6
31-444 Kraków
tel. 12 411 49 79, 411 57 47; faks 12 411 94 74
e-mail: insap@insap.pl
www.insap.pl

JANEX INTERNATIONAL Sp. z o.o.
ul. Płomyka 2
02-490 Warszawa
tel. 22 863 63 53; faks 22 863 74 23
e-mail: janex@janexint.com.pl
www.janexint.com.pl

KATON Sp. z o.o.
ul. Bajana 31E
01-904 Warszawa
tel. 22 869 43 92; faks 22 869 43 93
e-mail: biuro@katon.eu
www.katon.eu

KOLEKTOR
K. MIKICIUK I R. RUTKOWSKI Sp. J.
ul. Obrońców Westerplatte 31
80-317 Gdańsk
tel. 58 553 67 59; faks 58 553 48 67
e-mail: info@kolektor.pl
www.kolektor.pl

LEGRAND POLSKA Sp. z o.o.
ul. Domaniewska 50
02-672 Warszawa
tel. 22 549 23 30
e-mail: info@legrand.com.pl
www.legrand.pl

MICROMADE
Gałka i Drożdż Sp. J.
ul. Wieniawskiego 16
64-920 Piła
tel./faks 67 213 24 14
e-mail: mm@micromade.pl
www.micromade.pl

MICRONIX Sp. z o.o.
ul. Spółdzielcza 10
58-500 Jelenia Góra
tel. 75 755 78 78
e-mail: info@micronix.pl
www.micronix.pl

POLON-ALFA S.A.
ul. Glinki 155
85-861 Bydgoszcz
tel. 52 363 92 61; faks 52 363 92 64
e-mail: polonalfa@polon-alfa.pl
www.polon-alfa.pl

PROFICCTV Sp. z o.o.
ul. Strzeszyńska 66
60-479 Poznań
tel./faks 61 842 29 62
e-mail: biuro@proficctv.pl
www.profisystems.pl

RAMAR s.c.
ul. Modlińska 237
03-120 Warszawa
Tel. 22 676 77 37, 676 82 87
e-mail: ramar@ramar.com.pl
www.ramar.com.pl

RETT-POL

RETT-POL
Bogusław Godlewski
ul. Podmiejska 21
01-498 Warszawa
tel. 22 632 72 22; faks 22 833 09 07
e-mail: biuro@rettpol.pl
www.rettpol.pl

Oddział:
ul. Sportowa 3, 35-111 Rzeszów
tel. 17 785 18 16; faks 22 833 09 07
e-mail: rzeszow@rettpol.pl

ROPAM elektronik

ROPAM Elektronik s.c.
Polanka 301
32-400 Myślenice
tel. 12 272 39 71, 341 04 07; faks 12 379 34 10
www.ropam.com.pl

SCHRACK SECONET

SCHRACK SECONET POLSKA Sp. z o.o.
ul. Domaniewska 44A
02-672 Warszawa
tel. 22 33 00 620; faks 22 33 00 624
e-mail: jolanta.paska@schrack-seconet.pl
www.schrack-seconet.pl

Oddziały:
ul. M. Gomółki 2, 80-279 Gdańsk
tel. 58 526 35 70
e-mail: gdansk@schrack-seconet.pl

ul. Jasnogórska 23 lok. 17
(wejście od ul. Stawowej)
31-358 Kraków
tel. 12 637 11 74
e-mail: krakow@schrack-seconet.pl

ul. Wierzbięcice 1, 61-569 Poznań
tel./faks 61 833 31 53, 833 50 37
e-mail: poznan@schrack-seconet.pl

ul. Mydlana 1, 51-502 Wrocław
tel./faks 71 345 00 95
e-mail: wroclaw@schrack-seconet.pl

TAP

TAP- Systemy Alarmowe Sp. z o.o.
ul. Tatrzańska 8
60-413 Poznań
tel./faks 61 677 48 00
e-mail: tap@tap.com.pl
www.tap.com.pl

TECHOM

Zakład Rozwoju Technicznej Ochrony Mienia
TECHOM Sp. z o.o.
Al. Wyzwolenia 12
00-570 Warszawa
tel. 22 625 34 00
e-mail: techom@techom.com
www.techom.com

W2

W2 Włodzimierz Wyrzykowski
ul. Czajcza 6
86-005 Białe Błota
tel. 52 345 45 00
faks 52 584 01 92
e-mail: biuro@w2.com.pl
www.w2.com.pl

WINKHAUS

WINKHAUS POLSKA BETEILIGUNGS
Spółka z ograniczoną odpowiedzialnością Sp.K.
ul. Przemysłowa 1
64-130 Rydzyna
tel. 65 525 57 00
faks 65 525 58 00
e-mail: winkhaus@winkhaus.pl
www.winkhaus.pl

Legenda

Kategorie*

- bezpieczeństwo IT
- biometria
- DSO
- monitoring
- ochrona fizyczna
- RFID
- systemy domofonowe i wideodomofonowe
- systemy komunikacyjne
- systemy kontroli dostępu
- systemy nagłośnieniowe
- systemy ochrony peryferyjnej
- systemy ochrony zewnętrznej
- systemy przeciwkradzieżowe
- systemy przywoławcze
- systemy sygnalizacji pożarowej
- systemy sygnalizacji włamania i napadu
- systemy telewizji dozorowej
- systemy zintegrowane
- zabezpieczenia mechaniczne
- zasilanie

Działalność*

- B badania
- C certyfikacja
- D dystrybucja
- I instalacja
- PROJ projektowanie
- PROD produkcja
- S szkolenia

* Szybkie wyszukiwanie przez filtrowanie na naszej stronie www.zabezpieczenia.com.pl

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Paweł Karczmarzyk
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

Redaguje zespół
Marek Blim
Patryk Gańko
Norbert Góra
Daniel Kamiński
Paweł Karczmarzyk
Arkadiusz Milka
Adam Rosiński
Ryszard Sobierski
Waldemar Szulc
Andrzej Wójcik

Współpraca
Marcin Buczaj
Piotr Czernoch
Marcin Pyclik

Projekt graficzny, skład i łamanie
Piotr Przybylski

Adres redakcji
ul. Przy Bażantarni 13
02-793 Warszawa
tel. 22 670 09 19
faks 22 649 97 19
www.zabezpieczenia.com.pl

Wydawca
AAT HOLDING S.A.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

Druk
Regis Sp. z o.o.
ul. Napoleona 4, 05-230 Kobyłka

Dostępne formy reklamy

Reklama wewnątrz czasopisma
cała strona, pełny kolor
cała strona, czarno-biała
1/2 strony, pełny kolor
1/2 strony, czarno-biała
1/3 strony, pełny kolor
1/3 strony, czarno-biała
1/4 strony, pełny kolor
1/4 strony, czarno-biała
karta katalogowa, 1 strona

Reklama na okładkach
pierwsza strona
druga strona
przedostatnia strona
ostatnia strona

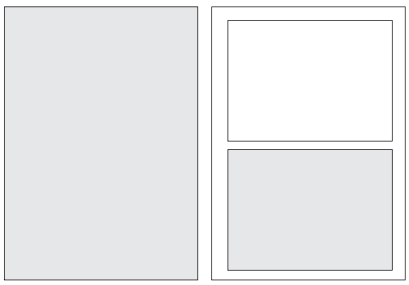
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie

Spis teleadresowy
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Ceny negocjujemy indywidualnie

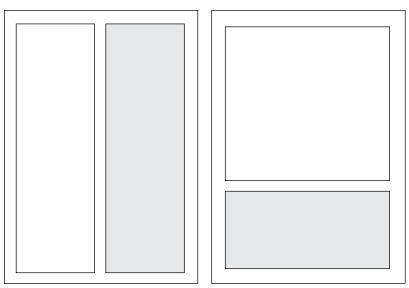
Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej http://www.zabezpieczenia.com.pl w dziale Reklama

Udostępniamy również powierzchnię reklamową na naszej stronie internetowej http://www.zabezpieczenia.com.pl



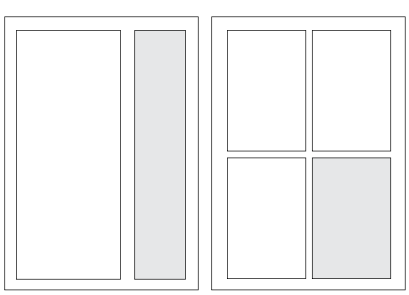
cała strona
(200 x 282 mm + 3mm spad)

1/2 strony
(170 x 125 mm)



1/2 strony
(83 x 260 mm)

1/3 strony
(170 x 80 mm)



1/3 strony
(54 x 260 mm)

1/4 strony
(83 x 125 mm)

Spis reklam

AAT HOLDING	35, 67, 73, 83, 86, 87	Fujinon (Europe)	95
ASSA ABLOY Poland	1	Hanwha Techwin Europe	96
Axis Communications Poland	2	Polon-Alfa	57
Brzezińska Dorota, Bryant Paul	79	ROGER	27, 88, 89
Dahua Technology	16, 17, 45	SECUREX	6, 7, 51
EBS	41	Videotec	3
Firma ATline	21		

FUJIFILM
Value from Innovation

Bezpieczeństwo w nowym wymiarze:

4K

Pierwszy 4K obiektyw Fujinon typu Vari Focal

Day Night

Nowy DV2.2x4.1SR4A-SA2L firmy Fujifilm
Doskonała rozróżnialność szczegółów dzięki rozdzielczości obrazu 4K.
Nadający się do użytku 24 godziny na dobę dzięki technologii dzień/noc.
Więcej informacji na stronie www.fujifilm.eu/fujinon lub per scan.
Fujinon. Widzisz więcej. Wiesz więcej.

kremer agency

FUJINON

Samsung Security to teraz

WISENET

ROZWIJAMY SIĘ

dzięki zaufaniu

ROZWIJAMY SIĘ dzięki zaufaniu naszych partnerów

ROZWIJAMY SIĘ dzięki najwyższej koreańskiej jakości

ROZWIJAMY SIĘ dzięki bezpieczeństwu cybernetycznemu

ROZWIJAMY SIĘ dzięki najlepszemu serwisowi w branży

ROZWIJAMY SIĘ dzięki 5-letniej gwarancji

Hanwha-security.eu/wemove

Hanwha Techwin