CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 4(116)/2017

ZABEZPIECZENIA

WWW.ZABEZPIECZENIA.COM.PL • E-MAIL: ZABEZ@ZABEZPIECZENIA.COM.PL

TEMAT NUMERU – NOWOŚCI W SYSTEMACH PPOŻ. I OCHRONIE SERWEROWNI

- Systemy sygnalizacji pożarowej w serwerowniach
- Sterowanie systemami oddymiania w świetle wymagań rozporządzenia Ministra Infrastruktury
- Jak działa system mgły wodnej?
- Kompletne rozwiązanie problemu fałszywych alarmów

BE READY FOR AN EXTRA-ORDINARY NEW WORLD

- Extra-competitive
- Extra-light
- Extra-compact
- Extra-flexible

Nowe kamery MAXIMUS MMX pozwolą na realizację nawet najbardziej skomplikowanych zadań w portach, na nabrzeżach i pokładach okrętów oraz w instalacjach przemysłowych, w których panują bardzo trudne warunki eksploatacyjne.

MAXIMUS MMX CAMERA

ATEX

c UL us LISTED

TECEx

EAC Ex

VIDEO SECURITY PRODUCTS

www.videotec.com

Made in Italy

VIDEOTEC

axxnext

OTWARTA PLATFORMA

DO ZARZĄDZANIA I INTELIGENTNEJ ANALIZY WIDEO

AxxonSoft Polska Sp. z o.o.
ul. Olszańska 5H
31-513 Kraków

Tel.: +48 12 393 58 01
E-mail: poland@axxonsoft.com
www.axxonsoft.com/pl

SPIS TREŚCI 04 2017

TEMAT NUMERU
NOWOŚCI W SYSTEMACH PPOŻ. I OCHRONIE SERWEROWNI

6 Sprawdź, jak działa INERGEN – *DEKK Fire Solutions*

6 Gaśnica automatyczna – rewolucja w gaszeniu – *DEKK Fire Solutions*

7 Rewolucja w sterowaniu urządzeniami przeciwpożarowymi – *Ela-compil*

7 Nowość w ofercie firmy Polon-Alfa czujki DUO-6043 i DUO-6046 – *Polon-Alfa*

8 Proteng Firetrace stawia na innowacyjność rozwiązań – *Proteng Systems*

8 RST SAP 3A 24V S – przeznaczony do ochrony przed przepięciami obwodów sygnalizacyjnych SSP – *RST*

9 Dźwiękowy system ostrzegawczy APS-APROSYS w ofercie firmy Schrack Seconet Polska – *Schrack Seconet Polska*

9 Wewnętrzny pożarowy sygnalizator głosowy SG-Pgw2 – *W2*

10 Bezpieczeństwo pożarowe do wynajęcia – *P.U.I. ZETO-PROJEKT*

12 NOWOŚCI PRODUKTOWE

18 WYDARZENIA INFORMACJE

OCHRONA PRZECIWPOŻAROWA

24 Systemy sygnalizacji pożarowej w serwerowniach
– Jerzy Ciszewski, IBP NODEX

26 Jak działa system mgły wodnej? Przyjedź do Krakowa, aby się przekonać!
– Bettina McDowell, M.A., International Water Mist Association

30 Sterowanie systemami oddymiania w świetle wymagań rozporządzenia Ministra Infrastruktury
– Janusz Sawicki, IBP NODEX

34 AlarmCalm. Kompletne rozwiązanie problemu fałszywych alarmów
– Krzysztof Dembiński, P.U.I. Zeto-Projekt

CHMURA OBLICZENIOWA (CLOUD COMPUTING)

40 Bezpieczeństwo informacji w chmurze (część 2)
– Marek Blim

OCHRONA INFORMACJI

48 Prowadzenie audytu zarządzania bezpieczeństwem organizacyjno-technicznym obiektów (część 2)
– Andrzej Wójcik

TELEWIZJA DOZOROWA

54 Projektuj z firmą Hanwha Techwin
– Piotr Rogalewski, Hanwha Techwin Europe

60 Obraz o rozdzielczości 4 megapikseli w telewizji analogowej
– Patryk Gańko, AAT HOLDING

NOWE TECHNOLOGIE

64 Remote Services firmy Bosch – usługi zdalnego nadzoru i konserwacji
– Jakub Bednarz, Bosch Security Systems

SYSTEMY ZINTEGROWANE

66 Zasada działania zapalniczki, a sprawne systemy wykrywania włamań na terenie budynku
– Maciej Prelich, Firma ATLine sp.j. Sławomir Pruski

SSWiN

70 Ewolucja popularnych systemów alarmowych
– Michał Konarski

PREZENTACJA FIRMY

74 25 lat największych w Polsce spotkań projektantów, rzeczoznawców, instalatorów i konserwatorów systemów sygnalizacji pożarowej (część 1)
– Mariusz Radoszewski, Polon-Alfa

80 25 lat Polskiego Związku Pracodawców Ochrona
– Barbara Bujak-Kowerczuk, PZPO

WYWIAD

84 Rozmowa z Martinem Grenem, założycielem oraz dyrektorem generalnym firmy Axis Communications

88 KARTY KATALOGOWE

92 SPIS TELEADRESOWY

98 SPIS REKLAM

Sprawdź, jak działa INERGEN

Ta technika gaszenia oprócz mienia chroni ludzi i środowisko naturalne. **INERGEN** wyzwolony w gaszonym pomieszczeniu zmniejsza w nim zawartość tlenu, dzięki czemu ogień gaśnie, a ludzie znajdujący się w pomieszczeniu mogą cały czas oddychać. INERGEN został skomponowany wyłącznie z naturalnych gazów: azotu, argonu i dwutlenku węgla. Stosowanie INERGENU nie powoduje efektu zamglenia i zabrudzeń czy zagrożenia korozją.

INERGEN przynosi same korzyści. Jest bezpieczny dla ludzi, sprzętu i środowiska, opłacalny i prosty w utrzymaniu, skutecznie utrzymuje obojętną atmosferę i zapobiega ponownemu zapaleniu się ognia. System wykorzystujący INERGEN to najpewniejszy system gaśniczy. Jest też najczęściej wybierany. Stosuje się go do ochrony tego co bezcenne, wszędzie tam, gdzie inne rozwiązania (jak woda, piana czy proszek) mogą zagrozić chronionemu obiektowi.

Przekonaj się sam – skontaktuj się z nami, a wskażemy Ci najbliższy termin i miejsce przeprowadzenia próbnego wyzwolenia środka gaśniczego.

Najlepsza ochrona przeciwpożarowa to nie tylko zabezpieczenie mienia, ale również uzyskanie optymalnego rozwiązania w najlepszej cenie. Ważne jest nie tylko zabezpieczenie

cennych aktywów, ale również zapewnienie ciągłości biznesowej. Zaskocz pożar, zanim on zaskoczy Ciebie!

Szczegółowe informacje znajdują się na stronach internetowych *www.inergen.pl* oraz *www.dekk.pl.*

DEKK FireSolutions

Bezpośr. inf. DEKK Fire Solutions
email: info@dekk.pl

Gaśnica automatyczna – rewolucja w gaszeniu

FIRE NXT jest rewolucyjną gaśnicą w kształcie kuli, aktywującą się samoczynnie podczas kontaktu z ogniem. Jedno urzą-

dzenie gasi pożar pomieszczenia o kubaturze do trzech metrów sześciennych, zanim pożar zacznie się rozprzestrzeniać.

Brak ruchomych części mechanicznych, zawleczek, zaworów, dźwigni i innych elementów, które występują zwykle w standardowych gaśnicach, ułatwia obsługę, przyspiesza i ułatwia zastosowanie, a do tego eliminuje konieczność corocznych konserwacji i ewentualnych napraw.

Kula gasząca FIRE NXT działa szybko i niezawodnie. Jej dodatkową zaletą są małe wymiary (15 cm średnicy) oraz mała masa (do 1,1 kg). Kula nie wymaga obsługi. Dzięki zastosowaniu materiałów o najwyższej jakości i zachowaniu najlepszych standardów nie ma konieczności jej konserwowania i dokonywania przeglądów serwisowych. Udzielana jest na nią 5-letnia gwarancja.

FIRE NXT to nowoczesność i postęp w dziedzinie gaszenia pożarów. Wystarczy umieścić kulę gaszącą nad miejscem ewentualnego pożaru czy powstania płomienia albo wrzucić ją bezpośrednio do źródła ognia, aby samoczynnie się aktywowała i ugasiła pożar.

FIRE NXT może być umieszczona w szafach elektrycznych i sterowniczych, komorach silnika, bagażnikach, w kuchni czy przy kominku – wszędzie tam, gdzie występuje duże ryzyko pożaru.

Szczegółowe informacje znajdują się na stronie internetowej *www.kulagaszaca.pl.*

DEKK FireSolutions

Bezpośr. inf. DEKK Fire Solutions
email: info@dekk.pl

Rewolucja
w sterowaniu urządzeniami przeciwpożarowymi

Firma **Ela-compil** oferuje nowoczesne urządzenie do sterowania urządzeniami przeciwpożarowymi – centralę **FPM+**. Zadaniem centrali jest kompleksowe zarządzanie i nadzorowanie pracy znajdujących się w budynku urządzeń i systemów, które będą uruchomione na wypadek pożaru.

FPM+ (od ang. *Fire Protection Manager*) jest urządzeniem neutralnym i pozwala zarządzać dowolnymi systemami przeciwpożarowymi różnych producentów bez obawy o ich kompatybilność z urządzeniami innych producentów. Są nimi między innymi urządzenia do wentylacji pożarowej, elementy odcięć pożarowych, systemy wspomagające ewakuację oraz inne urządzenia i systemy – do kontroli dostępu, systemy sygnalizacji włamania i napadu, windy i schody ruchome, systemy kontroli mediów, pompy ciepła, systemy wentylacji i klimatyzacji. Dzięki takiemu rozwiązaniu poziom bezpieczeństwa przeciwpożarowego w budynku znacząco wzrasta.

Zaawansowana technika centrali FPM+ umożliwia najbardziej skomplikowane sterowanie odcięciami stref czy wentylacją pożarową. Projektant ma możliwość założenia nawet bardzo złożonego scenariusza dzięki jednej, wspólnej matrycy sterowań. Pozwala to uniknąć błędów już na etapie samego projektowania.

Centrala może stanowić niezależny system sterowania urządzeniami przeciwpożarowymi lub być zintegrowana z dowolnym systemem BMS.

elacompil

Bezpośr. inf. Karolina Brzuchalska
Ela-compil
www.ela.pl

Nowość w ofercie firmy Polon-Alfa
czujki DUO-6043 i DUO-6046

Dwusensorowe adresowalne czujki dymu są przeznaczone do skutecznego wykrywania pożaru w jego wczesnej fazie. Pracują na liniach dozorowych adresowalnych systemów sygnalizacji pożarowej **POLON 6000** i **POLON 4000** będących w ofercie firmy Polon-Alfa.

Nowe czujki powiększają asortyment oferowanych czujek szeregu 6000. Dostępne w dwóch wersjach różniących się oprogramowaniem.

Czujki zostały wyposażone w podwójny układ detekcji wykorzystujący sensory dymu pracujące w pasmach podczerwieni i ultrafioletu. Sensory czujek można aktywować niezależnie, można zadeklarować ich współpracę, pracę niezależną i koincydencję, można również ustawić jeden z czterech poziomów czułości. Odpowiedni dobór trybu pracy czujek pozwala na szybką detekcję możliwych zagrożeń pożarowych.

Zaawansowane algorytmy oprogramowania procesorów czujek przeprowadzają na bieżąco diagnostykę poprawności działania układów detekcji i wewnętrznych układów elektronicznych oraz poprawności komunikacji z centralą w celu zapewnienia jak najlepszego zabezpieczenia i poprawnej pracy całego systemu, jednocześnie zgłaszając do centrali wszelkie nieprawidłowości.

W celu zapewnienia bezawaryjnej pracy adresowalnej pętli dozorowej central systemu Polon czujki zostały wyposażone w dwustronne izolatory zwarć, które są aktywowane w przypadku przekroczenia parametrów prądowych pracy pętli. Umożliwiają zachowanie ciągłości pracy i prawidłową komunikację w pętli dozorowej.

POLON-ALFA

Bezpośr. inf. Polon-Alfa

Proteng Firetrace
stawia na innowacyjność rozwiązań

Firma **Proteng Systems**, obecna na polskim rynku od niespełna dwóch lat, stale się rozwija, pozyskując coraz więcej nowych klientów, a także realizując projekty dla dużych, działających globalnie koncernów. Kolejnym krokiem na drodze rozwoju firmy jest pojawienie się w jej ofercie systemów amerykańskiego producenta – firmy Firetrace. Jest to firma znana na całym świecie, obecna w branży ochrony przeciwpożarowej od ponad 30 lat, a jej systemy zabezpieczają wiele znaczących obiektów oraz urządzeń na całym świecie.

Firma Proteng Systems koncentruje się na zabezpieczeniu serwerowni oraz szaf sterowniczych, a także takich urządzeń jak np. maszyny CNC. Dzięki prostej zasadzie działania systemy są niezawodne oraz skuteczne. Funkcjonują bez zasilania elektrycznego, zatem w przypadku awarii zasilania możemy być spokojni, że zainstalowany system na pewno zadziała i ugasi powstałe zarzewie pożaru. Systemy Firetrace mają szeroki zakres zastosowań.

Systemy Firetrace są zatwierdzone przez FM Global. Nasza pełna oferta jest przedstawiona na naszej stronie internetowej (*www.ugasimy.pl*), za pośrednictwem której można również dokonać wyceny systemu online.

PROTENG

Bezpośr. inf. Michał Słomian
Proteng Systems
www.ugasimy.pl

RST SAP 3A 24V S przeznaczony do ochrony przed przepięciami obwodów sygnalizacyjnych SSP

RST z Białegostoku – producent i dystrybutor wielu produktów do ochrony przed przepięciami – wprowadza do sprzedaży nowy ogranicznik przepięć.

Zgodnie z normami PN-EN 62305 dotyczącymi ochrony odgromowej automatyczne systemy sygnalizacji pożarowej (SSP) stanowią skuteczny środek redukcji zagrożenia pożarem jedynie wtedy, gdy są objęte skoordynowaną ochroną przed przepięciami. W przypadku bezpośredniego wyładowania atmosferycznego w budynek elektromagnetyczne oddziaływanie prądu pioruna może doprowadzić do awarii niezabezpieczonego systemu sygnalizacji pożarowej, przez co nie będzie on w stanie ostrzec przed ewentualnym pożarem.

Ogranicznik przepięć **RST SAP 3A 24V S** (nr. kat 207 024) to najnowszy produkt firmy RST przeznaczony do ochrony obwodów sygnalizacyjnych SSP. W odróżnieniu od jego starszej wersji (RST SAP 3A 24V, nr. kat 201 030) ogranicznik wyposażono w dodatkowy zacisk do przyłączenia ekranu kabla, który w warunkach normalnej pracy zapewnia galwaniczną izolację względem uziemienia. Przy niskim napięciowym poziomie ochrony ($U_p \leq 40$ V względem ekranu) produkt charakteryzuje się jednocześnie bardzo dużą odpornością udarową zarówno na prądy indukowane ($I_{max} = 20$ kA 8/20 μs), jak i częściowe prądy pioruna ($I_{imp} = 3{,}5$ kA 10/350 μs), dzięki czemu może być stosowany także do zabezpieczania zewnętrznych elementów systemów sygnalizacji pożarowej. Bardzo mała rezystancja szeregowa ($R_{DC} = 0{,}07\ \Omega$), duży prąd znamionowy ($I_N = 3$ A) i izolacja względem uziemienia powodują, że element jest praktycznie niewidoczny dla systemu alarmowego i nie wpływa na jego pracę.

RST

Bezpośr. inf. RST
e-mail: rst@rst.pl
www.rst.pl

Dźwiękowy system ostrzegawczy APS-APROSYS w ofercie firmy Schrack Seconet Polska

W dobie budowania coraz większych obiektów wyposażanych w różnego rodzaju systemy bezpieczeństwa (np. SSP, DSO czy KD) firma **Schrack Seconet Polska** rozszerzyła swoją ofertę handlową o kolejną grupę produktów z tej branży – dźwiękowe systemy ostrzegawcze (DSO).

Mając na uwadze obszar działania naszych partnerów i wychodząc naprzeciw ich oczekiwaniom, uznaliśmy za niezbędne uzupełnienie naszej oferty, dzięki czemu inwestor otrzyma kompletny system sygnalizacji pożarowej wraz z dźwiękowym systemem ostrzegawczym, wykonany z produktów najwyższej jakości.

Oferowany dźwiękowy system ostrzegawczy jest produkowany w szwajcarskiej firmie G+M Elektronik AG, która, podobnie jak Schrack Seconet, należy do grupy SECURITAS AG. System posiada certyfikat zgodności (CPR) z normą PN-EN 54-16 oraz wymagane prawnie świadectwo dopuszczenia CNBOP-PIB.

System APS-APROSYS ma budowę modułową. Może pracować w układzie skupionym lub rozproszonym. Komunikacja pomiędzy poszczególnymi centralami odbywa się za pomocą konwerterów światłowodowych.

Dzięki modułowej budowie oraz innowacyjnemu układowi monitorowania linii głośnikowych z selektorami stref uzyskujemy możliwość dołączenia wielu linii głośnikowych do jednego wzmacniacza mocy. Maksymalna moc głośników przyłączonych do pojedynczej linii głośnikowej nie może przekroczyć 500 W.

Uzupełnieniem oferty są certyfikowane głośniki niemieckiej firmy IC Audio, do których należą głośniki sufitowe, naścienne i tubowe, projektory dźwięku oraz kolumny głośnikowe.

Wszystkich zainteresowanych możliwościami systemu APS-APROSYS zapraszamy do kontaktu z firmą Schrack Seconet Polska.

SCHRACK SECONET

Bezpośr. inf. Rafał Kowal
Schrack Seconet Polska
www.schrack-seconet.pl

Wewnętrzny pożarowy sygnalizator głosowy SG-Pgw2

Wewnętrzny pożarowy sygnalizator głosowy **SG-Pgw2** to nowy produkt w ofercie firmy W2. Sygnalizator ma certyfikat i świadectwo dopuszczenia wydane przez CNBOP-PIB. SG-Pgw2 to nowoczesny sygnalizator głosowy, który ułatwia wyraźne przekazanie informacji o zaistniałym zagrożeniu, dzięki czemu można szybciej podjąć odpowiednie działania.

Sygnalizator SG-Pgw2 ma możliwość pracy w dwóch trybach – do trzech lub do dziesięciu komunikatów. Fabrycznie wgrano trzy przykładowe komunikaty (każdy w trzech językach) oraz 18 wzorów sygnału alarmowego. Zastosowanie głośnika jako źródła dźwięku umożliwia generowanie wyraźnego komunikatu o natężeniu ponad 90dB@1m, które opcjonalnie może być regulowane za pomocą wbudowanego potencjometru. Komunikaty w formacie MP3 można w prosty sposób programować dzięki zastosowaniu złącza micro USB. Dodatkowe funkcje, takie jak autoadresowanie, automatyczne kopiowanie komunikatów do wszystkich sygnalizatorów w sieci, autodiagnostyka czy blokada podnapięciowa, są ułatwieniem pracy instalatora, gdyż pozwalają zaoszczędzić cenny czas.

Wraz z SG-Pgw2 można zastosować wyłącznik sygnału dźwiękowego WSD-1. Sygnalizator można zabezpieczyć przed uszkodzeniami mechanicznymi, stosując osłonę OZ-40-2, a jeśli ważna jest estetyka, można „ukryć" go w osłonie mocującej OM-1. Specjalistyczną puszką instalacyjną jest PIP-3AN.

Bezpośr. inf. Paulina Wyrzykowska
W2
http://www.w2.com.pl/sygnalizatory/pl

Bezpieczeństwo pożarowe do wynajęcia

Obiekty w fazie budowy są bardziej narażone na niebezpieczeństwo wybuchu pożaru niż obiekty oddane do użytku. Aby pomóc chronić obiekty w fazie budowy, oferujemy wynajem bezprzewodowych systemów sygnalizacji pożarowej.

Do dyspozycji jest pełen asortyment urządzeń – czujki punktowe (optyczne, temperatury oraz multisensorowe), ręczne ostrzegacze pożarowe, moduły wejścia/wyjścia, moduły linii bocznej oraz sygnalizatory. Brak okablowania umożliwia łatwą zmianę konfiguracji w zależności od postępu budowy.

Wykonujemy projekt SSP dostosowanego do budowanego obiektu, a wypożyczone od nas urządzenia dostarczamy na budowę, montujemy i uruchamiamy. Proponowane urządzenia są produkowane przez firmę **Advanced Electronics** pod nazwą **Axis EN**, a przedstawicielem tej firmy w Polsce jest **ZETO-PROJEKT**.

ZETO-PROJEKT

Bezpośr. inf. P.U.I. ZETO-PROJEKT
tel.: 71 311 05 91
e-mail: biuro@zeto-projekt.com.pl
www.zeto-projekt.com.pl

DSC

with PowerG Technology

WYKORZYSTAJ DWUKIERUNKOWĄ KOMUNIKACJĘ BEZPRZEWODOWĄ OPARTĄ NA TECHNOLOGII **PowerG**

NOWA KOMPAKTOWA CENTRALA ALARMOWA WP8010

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

Hybrydowa kamera szybkoobrotowa marki NOVUS

Kamera szybkoobrotowa **NVIP-3DN3520SD/IRH-2-II** może pracować jednocześnie w trybie IP oraz analogowym o wysokiej rozdzielczości. Urządzenie generuje sieciowy strumień wizyjny transmitujący obrazy o rozdzielczości 3 Mpx, a dodatkowo, poprzez wyjście BNC, dostarcza sygnał analogowy AHD lub TVI. W trybie analogowym generowany jest zawsze obraz o maksymalnej rozdzielczości 2 Mpx, niezależnie od zdefiniowanych parametrów sieciowego strumienia wizyjnego. Kamera może być sterowana z użyciem protokołu TCP/IP jak standardowe kamery IP, ale również przez interfejs RS485, z wykorzystaniem standardowych klawiatur (ta metoda jest preferowana przez osoby obsługujące systemy telewizji dozorowej ze względu na intuicyjność obsługi i dużą dynamikę sterowania). Dodatkowo z poziomu rejestratorów AHD marki **NOVUS** kamera może być sterowana za pośrednictwem kabla koncentrycznego na odległość do 300 m, z użyciem protokołu COAX.

Urządzenie ma moduł optyczny z obiektywem o ogniskowej regulowanej w zakresie od 5,5 do 110 mm i kącie widzenia od 3,2° do 58,7°, z wbudowanym promiennikiem podczerwieni o zasięgu do 100 m. W zależności od aktualnej ogniskowej obiektywu modułu kamerowego promiennik włącza odpowiednie sekcje diod o wysokiej mocy. Również w przypadku zmieniającej się odległości od oświetlanego obiektu kamera dostosowuje intensywność świecenia promiennika.

W kamerze można zainstalować kartę SD o pojemności do 64 GB w celu nagrywania zdjęć powiązanych ze zdefiniowanymi zdarzeniami. Model obsługuje algorytmy kompresji H.264 oraz H.265.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Aplikacje mobilne do systemu EntraPass firmy Kantech

Aby spełnić oczekiwania administratorów oprogramowania **EntraPass**, firma **Kantech** wprowadziła nowe aplikacje do obsługi i zdalnego komunikowania się z systemem. Są to **EntraPass WEB** i **EntraPass Go**.

EntraPass WEB to aplikacja dostępna w ramach pakietu EntraPass Corporate i Global. Podstawowa licencja udostępnia jeden kanał komunikacyjny. Aplikację można zainstalować na dowolnej liczbie komputerów w sieci, w której pracuje serwer systemu EntraPass. Liczba operatorów mogących jednocześnie zalogować się do systemu jest zależna od liczby wykupionych kanałów komunikacyjnych. Aktualna wersja daje operatorowi wiele funkcji, zbliżonych do tego, co oferuje stanowisko z podstawową licencją na stację operatorską (Workstation). Nowoczesny i funkcjonalny interfejs umożliwia przeprowadzanie operacji na kartach (dodawanie, usuwanie i modyfikacja), generowanie filtrowanych raportów, wyświetlanie map z ikonami elementów systemu i (lub) okien wizyjnych (jeżeli z aplikacją EntraPass zintegrowany jest system telewizji dozorowej firmy American Dynamics lub eqxacVision), jak również wysyłanie poleceń dotyczących kontroli nad drzwiami, liniami dozorowymi i wyjściami sterującymi. Każda ze stacji EntraPass WEB komunikuje się z serwerem EntraPass za pomocą aplikacji Smartlink (dostępnej w pakiecie programów podstawowych Corporate i Global).

Podobny zakres funkcji oferuje aplikacja EntraPass GO przeznaczona do pracy na urządzeniach mobilnych (tabletach i smartfonach) z systemem Android i iOS. W tym przypadku komunikacja z aplikacją pośredniczącą Smartlink odbywa się lokalnie poprzez sieć Wi-Fi lub poprzez sieć telefonii komórkowej i Internet (jeżeli komputer z aplikacją Smartlink jest udostępniony pod adresem publicznym). Interfejs dla operatora jest w tym przypadku inny niż w aplikacji EntraPass WEB, tzn. dostosowany do innego rozmiaru i kształtu ekranu. Aby korzystać z tego kanału komunikacyjnego, na urządzeniu mobilnym należy zainstalować bezpłatną aplikację o tej samej nazwie, dostępną w App Store i Google Play Store.

Obie wspomniane aplikacje korzystają z tych samych licencji i dostępnych kanałów komunikacyjnych. W praktyce oznacza to, że jeżeli mamy wykupione trzy kanały komunikacyjne, to np. może z nich korzystać trzech operatorów – jeden za pomocą tabletu, drugi za pomocą smartfonu, a trzeci może zalogować się na stanowisku komputerowym za pomocą EntraPass WEB.

Nowe możliwości obsługi i dostępu do systemu EntraPass cieszą się dużym zainteresowaniem użytkowników i są wciąż rozwijane.

Bezpośr. inf. Ryszard Sobierski
AAT HOLDING

Nowa funkcja wizualnej weryfikacji w systemach alarmowych DSC

Wizualna weryfikacja w systemach alarmowych to funkcja umożliwiająca określenie przyczyn alarmu na podstawie materiałów wizyjnych przesłanych z systemu alarmowego. Funkcja ta jest dostępna w centralach alarmowych serii **Power Neo** oraz w bezprzewodowej centrali **WP8010** dzięki wykorzystaniu czujek PIR z wbudowanymi kamerami – **PG8934** i **PG8944**. Czujki te powinno się instalować w newralgicznych miejscach chronionego obiektu. Funkcja wizualnej weryfikacji jest dostępna dla użytkownika systemu alarmowego lub operatora stacji monitorowania obsługującego dany system. Użytkownik systemu ma możliwość bezpłatnej weryfikacji wizualnej na urządzeniu mobilnym, na którym zainstalowana jest aplikacja Neo Go lub DSC WP. Stacja monitorowania musi być wyposażona w odbiornik Sur-Gard 5, dzięki czemu operator – na podstawie przesłanych zdjęć – może podjąć odpowiednie decyzje.

Kamery w czujkach są aktywowane jedynie w momencie wystąpienia alarmu. Podczas zdarzenia alarmowego czujka wykonuje serię 10 zdjęć (jedno zdjęcie co pół sekundy) i łączy je w poklatkowy film. Nagranie jest wysyłane w czasie rzeczywistym do urządzenia mobilnego użytkownika z odpowiednią aplikacją. Funkcja umożliwia właścicielowi chronionego obiektu podjęcie odpowiednich działań w zależności od rodzaju zaistniałego zdarzenia. Niezależnie od miejsca pobytu użytkownik może np. podjąć decyzję o odwołaniu przyjazdu grupy interwencyjnej, przez co zmniejszy koszty związane z obsługą przypadkowych alarmów.

Bezpośr. inf. Bartłomiej Kwiatkowski
AAT HOLDING

Kamery PTZ AUTODOME IP

Zmiennopozycyjne kamery sieciowe **AUTODOME IP 4000i** do zastosowań wewnętrznych oraz **IP 5000i** do zastosowań zewnętrznych umożliwiają użytkownikom ręczne sterowanie w celu śledzenia poruszających się osób – także w miejscach znajdujących się poza polem widzenia kamer stałopozycyjnych. Dzięki rozdzielczości 1080p oraz pracy z prędkością 60 klatek na sekundę kamery wytwarzają obrazy z bardzo dobrze odwzorowanymi szczegółami. W warunkach nocnych model IR pomaga identyfikować obiekty z odległości nawet 150 metrów.

Kamery te mają także funkcję Essential Video Analytics, dzięki której powiadamiają użytkownika o potencjalnych zagrożeniach już w momencie ich zaistnienia. Oznacza to także, że funkcjonalność kamer wykracza poza standardowy dozór wizyjny. Dostarczają one danych statystycznych, które można wykorzystać do analizy zachowań, zliczania osób, egzekwowania obowiązujących przepisów ruchu. Tak więc użytkownicy mogą chronić obiekty, a przy okazji wykorzystywać dane wizyjne w całkowicie odmienny sposób.

Bezpośr. inf. Bosch Security Systems

Siqura i Grundig pod jedną marką TKH Security Solutions

TKH Security Solutions – grupa firm należąca do holdingu **TKH Group** i zajmująca się systemami zabezpieczeń – odnotowała w 2015 roku blisko 60-procentowy wzrost sprzedaży i zajęła trzecią pozycję w opublikowanym przez miesięcznik *a&s International* rankingu Top 50, w którym zostały wskazane najszybciej rozwijające się firmy branży zabezpieczeń. Rozwój powodujący zmianę pozycji firmy na rynku spowodował, że TKH Group podjęła strategiczną decyzję o zebraniu produktów składających się na jej system nadzoru wizyjnego, dotychczas oferowanych jako produkty marek **Siqura i Grundig**, i oferowaniu ich jako produktów marki TKH Security Solutions. Proces ten ma na celu zapewnienie kompleksowych rozwiązań, jak najlepiej dopasowanych do potrzeb klientów końcowych oraz partnerów w kluczowych, zaawansowanych technologicznie projektach. Zapewnienie kontroli nad rozwojem poszczególnych produktów składających się na pełen system przez jeden zespół skutkuje tym, że tworzone systemy są zintegrowane na najwyższym poziomie, maksymalnie dopasowane do potrzeb klientów i mają unikatowe funkcje. Umożliwia to proponowanie pełnego pakietu integratorom, którzy mogą zaoszczędzić już na etapie zakupu i zarazem uzyskają wsparcie podczas wdrażania rozwiązań, a także w późniejszej fazie funkcjonowania systemu. Skorzystają też klienci zajmujący się dystrybucją, w której ważny jest odpowiedni stosunek jakości do ceny. Wszelkie istniejące oraz nowo powstające produkty będą projektowane i promowane przez jeden zespół specjalistów z działu o nazwie *TKH Security Solutions*.

Holding TKH jest grupą wyspecjalizowanych firm działających m.in. w branży zabezpieczeń. Połączenie ich indywidualnego know-how oraz wysokich kompetencji skutkuje rozwiązaniami znajdującymi szeroki zakres zastosowań. Znanym oraz udanym przykładem kompetencji TKH Security Solutions jest projekt Międzynarodowego Trybunału Karnego w Hadze – spółka dostarczyła okablowanie, kamery telewizji dozorowej, system interkomowy oraz system sygnalizacji włamania i napadu.

TKH Security Solutions jest grupą firm należących do holdingu TKH Group, wspólnie tworzących zintegrowane, kompletne systemy kontroli dostępu, nadzoru wizyjnego, zarządzania bezpieczeństwem oraz sygnalizacji włamania. Każda z firm ma ponad 35-letnie doświadczenie na rynku systemów zabezpieczeń.

Firma **C&C Partners**, jako członek TKH, jest generalnym przedstawicielem marki TKH Security Solutions na polskim rynku.

Więcej informacji na *www.tkhgroup.com*.

Bezpośr. inf. C&C Partners

Klawiatura NKB3000 firmy Dahua

Systemy dozoru wizyjnego stanowią nieodłączną część naszej rzeczywistości. Stykamy się z nimi niemal na każdym kroku. Kamery przyglądają się nam w centrach handlowych, na ulicach czy klatkach schodowych. Nierzadko instalacje składają się z dziesiątek czy setek kamer. W kontekście użyteczności kluczowym aspektem jest bezdyskusyjnie jakość rejestrowanego obrazu, jednakże czym byłby doskonałej jakości system telewizji dozorowej, który nie umożliwiałby wygodnego korzystania z dostępnych funkcji?

Elementem ułatwiającym życie operatorowi i poprawiającym wydajność jego pracy jest klawiatura sterująca. Przykładem bardzo zaawansowanego urządzenia z tej kategorii jest klawiatura **Dahua NKB3000**.

Klawiatura ta umożliwia sterowanie wszystkimi urządzeniami z oferty firmy Dahua, czyli rejestratorami, kamerami obrotowymi (sieciowymi i analogowymi), sieciowymi serwerami wizyjnymi czy platformą CMS.

Czteroosiowy joystick zapewnia doskonałą precyzję i wysoki komfort sterowania kamerami obrotowymi, a wbudowany dotykowy ekran LCD o rozdzielczości 800x480 pikseli umożliwia podgląd obrazu na żywo oraz wygodne sterowanie urządzeniami. Elektromechaniczna klawiatura wielofunkcyjna pozwala na szybki dostęp do najważniejszych funkcji czy ustawień.

Urządzenie tego typu znajduje wiele zastosowań dzięki mnogości dostępnych w nim interfejsów. W klawiaturze NKB3000 jest dostępny interfejs sieciowy 1 Gb/s, są dwa porty USB 2.0, port RS232 i dwa porty RS485. Dodano również wyjście akustyczne umożliwiające dwustronną komunikację głosową. Nic nie stoi na przeszkodzie, aby klawiaturę wyposażyć w kartę Wi-Fi.

Biorąc pod uwagę powyższe parametry, klawiatury z serii NKB można uznać za jedne z najwszechstronniejszych urządzeń sterujących dostępnych aktualnie na rynku.

Bezpośr. inf. Marian Maroszek
Dahua Technology Poland

Dahua NVR616DR-128-4KS2
rejestrator IP z serii Ultra

Rejestratory IP NVR616DR-128-4KS2 z serii Ultra firmy **Dahua** są urządzeniami najnowszej generacji. Zastosowano w nich czterordzeniowe procesory firmy Intel. Rejestrują obrazy o rozdzielczości 4K oraz 12 Mpx. Oferują prostotę obsługi oraz mnogość zaawansowanych funkcji. Dzięki dostępności funkcji analizy treści obrazu oraz wysokiemu poziomowi zabezpieczenia przechowywanych danych mogą być wykorzystane do budowania dużych systemów wizyjnych.

Rejestratory NVR616 w wersji 64- lub 128-kamerowej są dostarczane w obudowach przystosowanych do montażu w szafach Rack. Bezpieczeństwo danych zapewnia wbudowana 16-dyskowa macierz RAID. Warto dodać, że dyski są dostępne od frontu urządzenia, co upraszcza obsługę. NVR616 ma wbudowany monitor o przekątnej ekranu równej 7" i rozdzielczości 1080p, co ułatwia wprowadzanie zmian w konfiguracji bez użycia zewnętrznego wyświetlacza. Redundantne zasilanie przyczynia się do dodatkowego zabezpieczenia zapisywanych danych. Kolejną funkcją poprawiającą bezpieczeństwo systemu jest możliwość połączenia rejestratorów w trybie N+M. W przypadku awarii któregoś z rejestratorów urządzenie zapasowe bezzwłocznie przejmuje jego obowiązki, dzięki czemu utrzymana jest ciągłość zapisu danych.

Rejestrator NVR616 zapewnia zaawansowaną analizę treści obrazu, taką jak np. w serii kamer Ultra IP. Zliczanie osób, mapy ciepła, detekcja twarzy to tylko niektóre z obsługiwanych przez niego funkcji. Oczywiście NVR616 obsługuje również wszystkie funkcje analizy IVS (przekroczenie linii, wtargnięcie do strefy, pozostawienie/zniknięcie obiektu) dostępne w kamerach (już od serii EcoSavvy). Kolejnym atutem jest możliwość wykorzystania kamer do rozpoznawania tablic rejestracyjnych samochodów.

Rejestrator NVR616 to wszechstronne urządzenie umożliwiające wykorzystanie zaawansowanych metod analizy treści obrazu przy jednoczesnym zachowaniu najwyższego poziomu bezpieczeństwa zapisywanych danych.

Bezpośr. inf. Łukasz Biskupski
Dahua Technology Poland

Detektor wodoru H_2 EXpert G/E

Detektory wodoru **EXpert G/E** są przeznaczone do stosowania w stacjonarnych systemach pomiaru lub detekcji wysokich (wybuchowych) stężeń wodoru H_2 poza strefami zdefiniowanymi jako wybuchowe. Mogą współpracować z wieloma centralami i sterownikami.

Standardowe napięcie zasilania wynosi 12 V_{DC}. W zależności od wersji detektory mogą mieć wyjścia prądowe 4–20 mA, detekcyjne napięciowe NC lub NO oraz cyfrowe (wyjście RS485 z protokołem Modbus RTU).

W detektorze zastosowano selektywne, liniowe sensory elektrochemiczne. Dzięki temu może on pracować w systemach wykrywających przekroczenie stężeń wodoru przy ustaleniu dwóch lub trzech progów alarmowych oraz w systemach pomiarowych o ciągłej obserwacji wartości mierzonych. Sensory elektrochemiczne umożliwiają pomiar w zakresie od 0% do 4% V/V (100% DGW wodoru) lub w zakresie od 0% do 1% V/V.

Detektor ma optyczną sygnalizację zasilania, przekroczenia progów alarmowych i awarii.

Obudowa jest wykonana z tworzywa sztucznego PS. Do przyłączenia kabli służą wpusty kablowe (dławice) PG11 i PG9.

Obszary zastosowań detektorów – detekcja wodoru w przemyśle, laboratoriach, systemach ładowania akumulatorów itp.

Bezpośr. inf. Tadeusz Kapusta
Przedsiębiorstwo Wdrożeniowe PRO-SERVICE
www.alarmgas.com

Detektor wodoru H_2 EXpert IV/E

Detektory wodoru **EXpert IV/E** są przeznaczone do stosowania w stacjonarnych systemach pomiaru lub detekcji wysokich (zagrażających wybuchem) stężeń wodoru H_2, w strefach zagrożonych wybuchem typu 1 lub 2. Mogą współpracować z wieloma centralami i sterownikami. Standardowe napięcie zasilania wynosi 12 V_{DC}.

W zależności od wersji detektory mogą mieć wyjścia prądowe 4–20 mA, detekcyjne napięciowe NC lub NO oraz cyfrowe (wyjście RS485 z protokołem Modbus RTU).

W detektorze zastosowano selektywne, liniowe sensory elektrochemiczne. Dzięki temu może on pracować w systemach wykrywających przekroczenie stężeń wodoru przy ustaleniu dwóch lub trzech progów alarmowych oraz w systemach pomiarowych o ciągłej obserwacji wartości mierzonych. Sensory elektrochemiczne umożliwiają pomiar w zakresie od 0% do 4% V/V (100% DGW wodoru) lub w zakresie od 0% do 1% V/V.

Metalowa obudowa (z aluminium) zapewnia stopień ochrony IP-54. Okablowanie przyłącza się poprzez dławicę stalową. Kabel połączeniowy ma średnicę 5–11 mm.

Obudowa jest w wykonaniu przeciwwybuchowym, ognioszczelnym (typ „d").

Zgodność z wymaganiami dyrektywy ATEX została potwierdzona certyfikatem badania typu WE OBAC/10/ATEX/30. Umożliwia to stosowanie detektora w strefach zagrożenia wybuchem typu 1 lub 2, dla gazów grupy A, B, C.

Obszary zastosowań – detekcja wodoru w przemyśle, laboratoriach, systemach ładowania akumulatorów itp.

Bezpośr. inf. Tadeusz Kapusta
Przedsiębiorstwo Wdrożeniowe PRO-SERVICE
www.alarmgas.com

Czytnik z kieszenią w systemie RACS 5

Terminal **MCT82M-IOCH** jest czytnikiem zbliżeniowym kart standardu MIFARE (Ultralight, Classic, DESFire i Plus), przeznaczonym do pracy w systemie kontroli dostępu i automatyki **RACS 5**.

Czytnik jest wyposażony w kieszeń na kartę oraz zestaw linii wejściowych i wyjściowych. Oprogramowanie zarządzające systemem umożliwia określenie reakcji kontrolera zarówno na włożenie karty do kieszeni, jak i na jej wyjęcie z kieszeni. Ponadto reakcja kontrolera na włożenie lub wyjęcie karty może być uzależniona od uprawnień powiązanych z użytą kartą.

Czytnik posiada trzy linie dozorowe i trzy wyjścia sterujące, które mogą być wykorzystane do realizacji wybranych funkcji sterujących w systemie. W praktyce terminal najczęściej znajduje zastosowanie jako inteligentny wyłącznik zasilania elektrycznego pomieszczenia lub urządzenia elektrycznego.

Czytnik współpracuje z dowolnym kontrolerem serii MC16, do którego jest podłączany za pośrednictwem magistrali RS485. Obudowa czytnika jest zgodna z linią wzorniczą QUADRUS – ma wygląd neutralny, zbliżony do rozpowszechnionej stylistyki osprzętu elektrycznego. Dzięki temu pasuje zarówno do wnętrz tradycyjnych, jak i nowoczesnych.

Bezpoś. inf. ROGER

Publikacja oprogramowania systemu RACS w wersji 5.2

W nowej wersji systemu wprowadzono wiele nowych funkcji oraz ulepszeń. Do najważniejszych udogodnień należy zaliczyć możliwość pracy wielostanowiskowej bez limitu stanowisk w darmowej wersji oprogramowania VISO ST zarządzającej systemem oraz udostępnienie darmowej wersji programu do rejestracji czasu pracy RCP Master 3 w wersji obsługującej do 25 pracowników.

Z innych nowości na wzmiankę zasługuje możliwość definiowania tzw. stref obwodowych oraz komend globalnych. *Strefy obwodowe* umożliwiają blokowanie ruchu osób wewnątrz strefy w przypadku, gdy wcześniej nie zalogowały się one w punktach wejściowych strefy. *Komendy globalne* dają możliwość wydawania poleceń, które mogą wywoływać współbieżną, indywidualnie określaną reakcję na wielu kontrolerach systemowych. *Komendy globalne* mogą być wydawane zarówno z poziomu stacji roboczych systemu, jak i za pośrednictwem *Serwera integracji*, który umożliwia obcym aplikacjom zarządzanie systemem. Z innych udogodnień należy odnotować uproszczone procedury określania uprawnień w systemie oraz dostępność ulepszonego kreatora przejść. W programie RCP Master 3 dodano m.in. możliwość eksportu danych do popularnych programów OPTIMA, SYMFONIA, GRATYFIKANT, RCP ACCESS, TETA i WF-GANG.

Bezpoś. inf. ROGER

Dzień z Partnerem Technologicznym w IBP Nodex

Prezentacja systemu sygnalizacji pożarowej Axis EN firmy Advanced Electronics

Instytut Bezpieczeństwa Pożarowego
NODEX
www.IBPNODEX.pl

ZETO-PROJEKT

IBP Nodex oraz **ZETO-PROJEKT** zapraszają firmy zajmujące się bezpieczeństwem pożarowym na warsztaty promujące rozwiązania sprzętowo-programowe firmy **Advanced Electronics**. W trakcie spotkania zaprezentowane i omówione zostaną możliwości systemu sygnalizacji pożarowej **Axis EN**. Uwzględnione zostaną następujące innowacyjne rozwiązania producenta:

– AlarmCalm – kompletny system redukcji fałszywych alarmów,
– ipGateway – nadzór nad systemem sygnalizacji pożarowej z wykorzystaniem przeglądarki internetowej,
– TouchControl – dotykowy panel wyniesiony z obsługą aktywnych map,
– Dynamix Tools – pakiet oprogramowania do uruchomienia i prawidłowej eksploatacji SSP Axis EN.

Ponadto w trakcie warsztatów będzie można porozmawiać i skonsultować się z ekspertami z IBP Nodex. Spotkanie odbędzie się 10 października w siedzibie IBP Nodex w Warszawie przy ulicy Chrościckiego 93/105. Szczegółowe informacje dotyczące wydarzenia znajdują się na stronach ibpnodex.pl oraz www.zeto-projekt.com.pl.

Aby wziąć udział w warsztatach, należy wysłać zgłoszenie na adres e-mailowy ssp@zeto-projekt.com.pl do 5 października.

Bezpośr. inf. Krzysztof Dembiński
P.U.I. ZETO-PROJEKT
tel.: 71 311 05 91
www.zeto-projekt.com.pl

SICUREZZA 2017

Na pięć miesięcy przed rozpoczęciem wystawy **SICUREZZA**, która odbędzie się w dniach 15–17 listopada na terenie **Fiera Milano w Mediolanie**, swój udział zgłosiło ponad 250 firm zajmujących większość stoisk w pawilonach 5 i 7. Jeśli liczba uczestników wzrośnie, impreza obejmie też pawilon 3.

Popularność wystawy SICUREZZA wynika z tego, że w jej trakcie można nie tylko zwiedzić stoiska poszczególnych dostawców, ale również uczestniczyć w szkoleniach prowadzonych na najwyższym profesjonalnym poziomie. Program szkoleń jest dynamicznie dostosowywany do zmieniającej się sytuacji rynkowej. Prezentowane są najnowsze trendy rozwojowe i osiągnięcia technologiczne.

W roku 2017 największy nacisk będzie położony na zabezpieczenia przeciwpożarowe – od metod wczesnego wykrywania pożaru do metod jego gaszenia. Współorganizatorem imprezy jest UMAN – włoskie stowarzyszenie firm działających w branży zabezpieczeń – oraz ANIMA/CONFINDUSTRIA – stowarzyszenie firm działających w branży pożarniczej.

Organizatorzy wystaw SICUREZZA zawsze zwracali uwagę na spójność tematyczną z innymi imprezami, dlatego w tym roku wystawa odbędzie się równolegle z targami SMART BUILDING EXPO – projektem powstałym w wyniku porozumienia między Pentastudio (agencją komunikacji i marketingu specjalizującą się w branży nowych technologii telekomunikacyjnych) a Fiera Milano. Celem jest przedstawienie koncepcji nowej cyfrowej ochrony budynku. Ewolucja takich systemów i wszystkich związanych z nimi usług zostanie omówiona w panelu tematycznym poświęconym integracji systemów elektronicznych wykorzystywanych w nowoczesnych budynkach.

Podczas wystawy omówione będą także zagadnienia prawne związane z zachowaniem prywatności i nietykalności osób przebywających w obiektach wyposażonych w elektroniczne systemy zabezpieczające. Będzie mowa m.in. o tym, jak zmodyfikować istniejący wizyjny system dozorowy, by nie naruszał zasad prywatności, o tym, że zapewnienie bezpieczeństwa w nowoczesnym mieście nie może wiązać się z ograniczeniem swobód obywatelskich, o zagrożeniu cyberatakami w związku z powszechnym wykorzystywaniem Internetu w życiu codziennym, a także o możliwych niebezpieczeństwach związanych z wykorzystaniem dronów w kontroli ruchu drogowego.

Więcej informacji dotyczących wystawy znajduje się w Internecie (*www.sicurezza.it/en, https://www.facebook.com/sicurezza.fieramilano - #SICUREZZA2017, https://www.linkedin.com/company/sicurezza-fiera-milano, @SICUREZZA2017 - #SICUREZZA2017*).

Biuro prasowe Fiera Milano
Rosy Mazzanti (rosy.mazzanti@fieramilano.it)
Mariagrazia Scoppio (mariagrazia.scoppio@fieramilano.it)
tel.: +39 024997.6214, faks: +39 024997.7174
Tłumaczenie: Redakcja

Studia podyplomowe współorganizowane przez AGH i NODEX

Uprzejmie informujemy, że dobiega końca I edycja studiów podyplomowych **Zarządzanie Systemami Bezpieczeństwa Pożarowego oraz Technicznego w Obiektach Budowlanych** organizowanych przez **Akademię Górniczo-Hutniczą w Krakowie** oraz **Instytut Bezpieczeństwa Pożarowego NODEX** w Warszawie.

Głównym celem studiów jest poszerzenie wiedzy i rozwinięcie interdyscyplinarnych umiejętności słuchaczy dotyczących systemów bezpieczeństwa technicznego obiektów budowlanych – ze szczególnym uwzględnieniem zaawansowanych systemów automatyki i bezpieczeństwa pożarowego. Program studiów nie tylko umożliwi uzyskanie lub podniesienie kwalifikacji zawodowych, ale również pozwoli na osiągnięcie sukcesu w nowej grupie zawodowej, jaką są niezbędni dzisiaj wysoko wykwalifikowani specjaliści do spraw zarządzania systemami bezpieczeństwa pożarowego i technicznego obiektów budowlanych.

Zajęcia zostały podzielone na dwie części – dydaktyczną i praktyczno-warsztatową. Część dydaktyczna – w pierwszym semestrze studiów – odbyła się w salach wykładowych Wydziału Zarządzania AGH, natomiast część praktyczno-warsztatowa – w semestrze drugim – jest prowadzona w salach laboratoryjnych i ćwiczeniowych Instytutu Bezpieczeństwa Pożarowego NODEX w Warszawie.

W ramach zajęć praktycznych studenci mają niepowtarzalną okazję do zapoznania się z najnowszymi technologiami dostępnymi w branży – ćwiczenia podczas zajęć warsztatowych są prowadzone z wykorzystaniem urządzeń i systemów kilkunastu czołowych producentów (tzw. partnerów technologicznych na co dzień współpracujących z Instytutem Bezpieczeństwa Pożarowego NODEX).

Pozyskanie wiedzy praktycznej i doświadczenia w zakresie zarządzania, obsługi, podstaw programowania i uruchamiania oraz serwisu elementów krytycznych dla infrastruktury budynków umożliwi słuchaczom osiągnięcie przewagi na rynku pracy.

Więcej informacji o studiach znajdziecie Państwo na stronie *http://www.zsbpo.zarz.agh.edu.pl/*.

Bezpośr. inf. Janusz Sawicki
IBP Nodex

Najbardziej rozwojowe targi branży zabezpieczeń

Międzynarodowe Targi Zabezpieczeń SECUREX to stabilna i silna marka. Targi zdobyły powszechne uznanie. Towarzyszą im najważniejsze konferencje i inne wydarzenia przeznaczone dla konkretnych grup odbiorców. Są organizowane w cyklu dwuletnim – zawsze w latach parzystych. To właśnie na zeszłorocznych targach SECUREX odbyło się pierwsze w historii Forum Bezpieczeństwa Społeczności Lokalnych, które organizator przygotował we współpracy z policją. Forum zyskało tak duże uznanie, że zorganizowano je również w tym roku (na terenie Międzynarodowych Targów Poznańskich), mimo iż w latach nieparzystych targi SECUREX nie są organizowane. Organizatorzy to Komenda Wojewódzka Policji Wielkopolskiej, Polska Platforma Bezpieczeństwa Wewnętrznego i Międzynarodowe Targi Poznańskie. Jak widać, SECUREX ewoluuje i przypomina o sobie również w latach nieparzystych. Z pewnością III Forum odbędzie się podczas targów w 2018 roku.

Poprzednia edycja w liczbach

W ubiegłym roku, podczas 21. Międzynarodowych Targów Zabezpieczeń SECUREX, dla zwiedzających udostępniona została ekspozycja z najlepszym asortymentem na rynku. W jednym miejscu i czasie, w pawilonach Międzynarodowych Targów Poznańskich, obecni byli reprezentanci niemal 300 firm, do których tłumnie dotarli zwiedzający związani z branżą. Udostępniono ponad 150 nowości z całego świata oraz przestrzenie specjalne. Równolegle z wystawą odbyły się seminaria, konferencje i debaty.

Warto zarezerwować czas na SECUREX 2018

Kolejna edycja Międzynarodowych Targów Zabezpieczeń SECUREX odbędzie się w dniach 23–26 kwietnia 2018 roku w Poznaniu. Już dziś warto zapisać to w kalendarzu. Organizatorzy serdecznie zapraszają wystawców. Już od kilku miesięcy zgłaszają się firmy, które wiedzą, że Międzynarodowe Targi Poznańskie zapewniają promocję marek i produktów na długo przed oficjalnym rozpoczęciem targów. Najniższe ceny za wynajem powierzchni obowiązują do 22 września 2017 roku. Zatem kolejna, 22. edycja Międzynarodowych Targów Zabezpieczeń Securex już rośnie w siłę! To w Poznaniu będzie bić serce całej branży zabezpieczeń. Zaprezentowana będzie największa ekspozycja produktów, a program wydarzeń będzie dotyczył rozmaitych rodzajów zabezpieczeń – od zabezpieczeń mechanicznych po rozwiązania informatyczne, systemowe, inteligentne zarządzanie itd.

Bezpośr. inf. Maria Kowalska
MTP

Infrastruktura budynków komercyjnych
podsumowanie warsztatów

18 maja w Hotelu MCC Mazurkas Conference Centre w Ożarowie Mazowieckim odbyły się warsztaty **Live Commercial Building Technology Workshops** zorganizowane przez firmę **Anixter**.

W spotkaniu wzięło udział prawie trzydziestu partnerów technologicznych firmy Anixter, która jest obecna w regionie Europy, Bliskiego Wschodu i Afryki od 27 lat. Firma ma globalny zasięg i duży potencjał finansowo-logistyczny, a jej roczny obrót wynosi 7 mld dolarów.

Anixter zajmuje się kompletacją i dystrybucją sprzętu do instalacji zabezpieczających duże obiekty budowlane, w tym budynki komercyjne. Kilkugodzinny program warsztatów wypełniły wystąpienia dotyczące współczesnych i przyszłych metod zabezpieczania takich obiektów.

Firma Anixter kooperuje z wieloma producentami i ma w swojej ofercie komponenty niezbędne do tworzenia profesjonalnych zabezpieczeń, w tym składniki systemów alarmowych, sygnalizacji pożarowej, kontroli dostępu, monitoringu wizyjnego, automatyki budynkowej. Sprzęt jest kompletowany na podstawie projektów i dostarczany wprost na miejsce instalacji, zgodnie ustalonym harmonogramem.

Prelegenci włożyli wiele wysiłku w wyjaśnienie tendencji rozwojowych w dziedzinie zabezpieczeń budynków komercyjnych z uwzględnieniem zmian, jakie zachodzą w sposobie prowadzenia działań biznesowych i w strukturze zatrudnienia. Celem działań, jakie podejmuje Anixter, jest zapewnienie bezpiecznego miejsca pracy, zredukowanie kradzieży, osiągnięcie zgodności z przepisami, zapobieganie skutkom cyberataków, ograniczenie fizycznego dostępu do budynku i sieci. Takim wyzwaniom nie jest w stanie sprostać pojedynczy producent – niezbędna jest integracja systemów pochodzących od różnych dostawców, o otwartej architekturze sprzętowej i programowej.

Prelegenci nie tylko omówili zagadnienia związane z bezpieczeństwem budynków komercyjnych, ale również położyli duży nacisk na zagadnienia dotyczące pracy zdalnej, gdy pracownicy stacjonują w odległych miejscach i komunikują się poprzez publiczną sieć internetową. Tego typu praca zdobywa coraz większą popularność, zaś zdalnym pracownikom także należy zapewnić odpowiedni poziom bezpieczeństwa. Podczas spotkania zostały omówione problemy związane z niezawodnością działania oraz bezpieczeństwem pracy w rozległych sieciach internetowych. Zwrócono także uwagę na tendencję wzrostową w korzystaniu z sieci bezprzewodowych, które wymaga zastosowania odpowiednich zabezpieczeń.

Omówiono także sposoby wykorzystania aplikacji i banków danych pracujących w chmurze internetowej. Wykazano wyraźny wzrost wykorzystania tego typu narzędzi, który skutkuje poważnymi wyzwaniami związanymi z koniecznością zapewnienia odpowiedniego poziomu bezpieczeństwa biznesowego.

Organizatorzy przewidzieli przerwy w prelekcjach, podczas których uczestnicy spotkania mogli przedyskutować zagadnienia techniczne i zapoznać się z ofertą sprzętową na stoiskach producentów. Spotkanie zakończyło się obiadem, po którym nastąpiło wręczenie wylosowanej nagrody.

Zapraszamy do obejrzenia fotorelacji na stronie *http://www.zabezpieczenia.com.pl/fotogalerie.*

Bezpośr. inf. Andrzej Walczyk
Redakcja

Nedap Security Day
podsumowanie

7 czerwca 2017 roku w Warszawie odbyło się spotkanie **„Nedap Security Day”**, podczas którego polski zespół **Nedap Security Management** i **Nedap Identification Systems**, którego przedstawicielem był Ido Wentink, zaprezentowały rozwiązania i korzyści płynące ze współpracy obu działów.

Celem spotkania było przedstawienie sposobów zwiększenia poziomu bezpieczeństwa w organizacjach i miastach dzięki użyciu innowacyjnych systemów kontroli dostępu i systemów do identyfikacji osób i pojazdów.

W spotkaniu wzięli udział klienci oraz partnerzy biznesowi firmy, a miejscem spotkania było Studio 8 Smolna w Warszawie. Z tarasu widokowego uczestnicy spotkania mogli podziwiać panoramę miasta.

Nedap to holenderski producent zintegrowanych systemów bezpieczeństwa i dostawca zintegrowanej platformy bezpieczeństwa **AEOS**. Funkcja platformy AEOS jest zależna od oprogramowania, a nie od sprzętu. Bazując na oprogramowaniu można zmieniać funkcje systemu i poziomy bezpieczeństwa. Platforma AEOS to rozwiązanie bazujące na otwartym standardzie. Klient może używać produktów różnych dostawców jednocześnie, dzięki czemu wybiera zabezpieczenia najlepiej odpowiadające swoim potrzebom.

AEOS jest zintegrowany m.in. z systemami firm: Milestone, Axis Communications, Canon, Honeywell, Assa Abloy, Salto.

Firma Nedap oferuje również systemy identyfikacji pojazdów i osób. Wiodącym rozwiązaniem są czytniki dalekiego zasięgu TRANSIT wykorzystujące technologię RFID i zapewniające wygodny dostęp do miejsc parkingowych, np. na lotnisku Heathrow w Londynie i Helsinki-Vantaa. W ofercie firmy znajduje się również uPASS – platforma wykorzystująca technologię UHF oraz Nedap ANPR, platforma służąca do identyfikacji tablic rejestracyjnych.

Podczas spotkania użytkownicy mogli na żywo zapoznać się z możliwościami platformy AEOS.

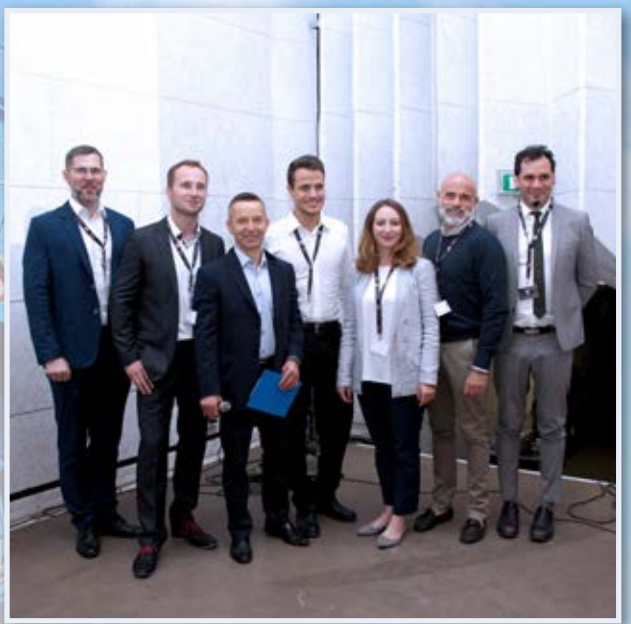
Serdecznie dziękujemy za zaproszenie, a polskiemu zespołowi Nedap Security Management życzymy powodzenia i sukcesów.

Zapraszamy do obejrzenia fotorelacji ze spotkania: *www.zabezpieczenia.com.pl.*

Bezpośr. inf. Ela Końka
Redakcja

http://www.zabezpieczenia.com.pl/fotogalerie/nedap-security-day

Kolejna edycja seminarium firm Videotec i CBC (Poland) już za nami



27 czerwca br. w kopalni **Guido** odbyła się kolejna edycja seminarium polskiego oddziału **CBC** (Poland), partnera firmy **Videotec** w Polsce. Tym razem na miejsce spotkania organizatorzy wybrali jedyną w Polsce i w Europie kopalnię węgla kamiennego, którą można zwiedzać. Kopalnia powstała w 1855 r., a nazwę zawdzięcza swojemu założycielowi. Obiekt jest jednym z siedmiu w Polsce punktów kotwicznych Europejskiego Szlaku Dziedzictwa Przemysłowego.

320 m pod powierzchnią ziemi firma Videotec, czołowy producent wysokiej klasy produktów do nadzoru wizyjnego, zaprezentowała rozwiązania dla infrastruktury krytycznej, transportu, branży paliwowej, gazowej i morskiej. Włoski producent istnieje na rynku od 1986 roku i ma dystrybutorów w ponad 100 krajach na całym świecie, w tym w Polsce od 1996 roku.

Kamery firmy Videotec znalazły zastosowanie na całym świecie m.in. w miastach, na autostradach, lotniskach, stadionach, w tym na Stadionie Narodowym w Warszawie oraz w tunelach, zakładach przemysłowych i chemicznych.

We współpracy z CBC (Poland) rozwiązania włoskiego producenta zastosowano w Polsce m. in. w elektrowni w Rybniku, PGE Elektrowni Opole, Grupie Azoty Zakłady Azotowe Kędzierzyn, na stacjach benzynowych SHELL, BP oraz Statoil.

Wśród zaprezentowanych produktów pojawiły się: zintegrowany punkt kamerowy MAXIMUS MPX, który może być instalowany w obszarach zagrożonych wybuchem, kamery MAXIMUS MVX, które spełniają najwyższe wymagania przemysłowe oraz kamery ULISSE PTZ i obudowy ze stali nierdzewnej, które można używać w środowisku morskim.

Przedstawiono również najnowszy produkt, którym jest punkt kamerowy MAXIMUS MMX, który jest przeznaczony do efektywnego nadzoru wizyjnego i kontrolowania procesów w trudnych warunkach, w których obecność gazów lub łatwopalnego pyłu może doprowadzić do wybuchu.

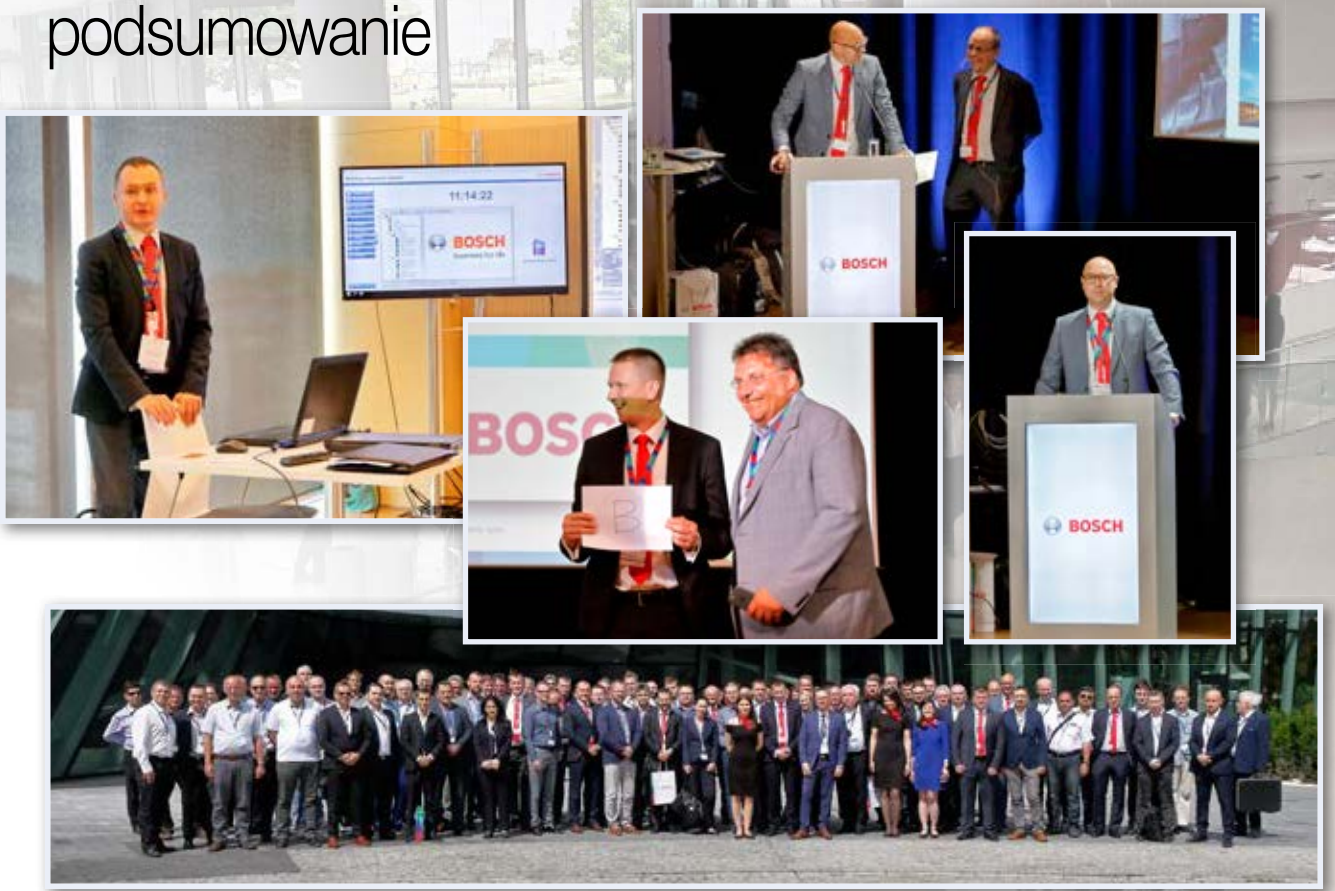
Produkty firmy Videotec przeznaczone do pracy w obszarach zagrożonych wybuchem mają certyfikat IECEX i spełniają dyrektywę ATEX.

Atrakcją spotkania była możliwość zwiedzenia kopalni Guido, poznania trudu pracy górników, zanim część ich pracy zastąpiły maszyny i przejazd podwieszaną kolejką elektryczną.

Zapraszamy do obejrzenia fotorelacji na *www.zabezpieczenia.com.pl.*

Bezpośr. inf. Ela Końka

International Consultant Event
podsumowanie



4 czerwca 2017 roku w krakowskim centrum konferencyjnym **ICE (International Conferences and Entertainment)** odbyła się międzynarodowa konferencja **International Consultant Event** zorganizowana przez firmę **Bosch**. W jej trakcie wygłoszonych zostało kilkanaście prelekcji oraz odbyły się prezentacje poprowadzone przez partnerów biznesowych firmy Bosch, głównie z Europy Środkowo-Wschodniej. Tematem przewodnim było zabezpieczanie dużych budynków biurowych i przemysłowych, a także obiektów, w których niezbędne jest zapewnienie bezpieczeństwa w warunkach krytycznych.

Trudno w kilku słowach opisać tak szeroki zakres tematyczny prelekcji i prezentacji, jednak należy podkreślić, że głównym celem konferencji było przedstawienie możliwości integracji najnowszych produktów Bosch z systemami zabezpieczeń pochodzącymi od innych dostawców. Tego typu integracja jest potrzebna zawsze, gdy w obiekcie już pracują różne systemy zabezpieczające, zaś Bosch stawia sobie za cel obsługę całego obiektu z użyciem jednej, wspólnej platformy programowej.

Tego typu rozwiązania bazują niemal wyłącznie na oprogramowaniu, dlatego nie zabrakło akcentów dotyczących bezpieczeństwa w sieci IP. Ciekawą prelekcję wygłosił zawodowy haker, który jest zatrudniany do podejmowania prób włamania się do systemu komputerowego zleceniodawcy. Wymaga to oczywiście odpowiednich gwarancji prawnych, zwalniających hakera od odpowiedzialności w przypadku pokonania zabezpieczeń. Obecnie uznaje się, że tego typu metoda wykrywania luk w systemie zabezpieczeń jest najskuteczniejsza.

Futurystyczną wizję projektowania wielkich obiektów budowlanych zaprezentowała firma dostarczająca oprogramowanie i sprzęt do systemów wirtualnej rzeczywistości. Uczestnicy spotkania mogli sami przekonać się, jak wygląda olbrzymi stadion, po którym można było chodzić w wirtualnej rzeczywistości. Obserwując z boku zwiedzającego wirtualnie, ma się nieodparte wrażenie, że ten człowiek ma halucynacje, gdyż wykonuje jakieś dziwne ruchy rękami, chwyta i ogląda jakieś nieistniejące przedmioty, tymczasem w wirtualnej rzeczywistości widzi on realistyczne, trójwymiarowe obrazy.

Konferencja odbyła się w centrum konferencyjnym ICE nie tylko ze względu na to, że ten obiekt doskonale nadaje się do organizowania tego typu imprez, lecz także dlatego, że cały system zabezpieczeń tego budynku jest wykonany z użyciem oprogramowania i sprzętu firmy Bosch. Zintegrowane są także wszystkie systemy niezbędne do funkcjonowania budynku, takie jak klimatyzacja, ogrzewanie, oświetlenie etc. Ostatnią z prelekcji wygłosił dyrektor ICE, który stwierdził, że do obsługi wszystkich systemów zabezpieczających oraz systemów automatyki budynkowej w tym gigantycznym obiekcie wystarczyło zatrudnić zaledwie 40 osób.

Na zakończenie spotkania wszyscy jego uczestnicy zostali oprowadzeni po obiekcie i mogli naocznie przekonać się, na czym polegają rozwiązania techniczne wykorzystane w systemach zainstalowanych przez firmę Bosch.

Andrzej Walczyk
Redakcja

Systemy sygnalizacji pożarowej w serwerowniach

mgr inż. Jerzy Ciszewski

Serwerownie są wydzielonymi obiektami, w których zapewnia się odpowiednie warunki fizyczne i środowiskowe oraz właściwe warunki elektromagnetyczne umożliwiające odpowiednie zasilanie komputerów pełniących rolę serwerów. Główną rolą serwerów jest usługa polegająca na udostępnianiu zasobów innym komputerom, a także pośredniczenie w wymianie informacji między nimi

Pomieszczenia i zainstalowane w nich urządzenia, systemy elektroniczne i elektryczne wymagają specyficznych środków nadzoru za pomocą automatycznych systemów wykrywania pożaru (ASWP), a także specjalnych rozwiązań służących do gaszenia wykrytych pożarów czy nawet środków uniemożliwiających powstanie pożaru płomieniowego. Typowe wytyczne i zasady dotyczące projektowania nie są w stanie zagwarantować odpowiedniej czułości oraz szybkości reakcji systemu. Ma to szczególne znaczenie w przypadku pomieszczeń z urządzeniami komputerowymi, centralami telefonicznymi itp.

Zbyt późne wykrycie pożaru w systemie mającym zapewnić bezprzerwowe zasilanie może doprowadzić do uszkodzenia albo nieprawidłowego działania urządzeń, co oczywiście może mieć poważne następstwa.

Zabezpieczenie serwerowni

Pożar w pomieszczeniu serwerowni musi być stłumiony w jak najkrótszym czasie. Systemy sygnalizacji pożarowej umożliwiają wykrycie pożaru w bardzo wczesnym stadium. Ewentualne uszkodzenia czy zniszczenia mogą być znacznie ograniczone, jeżeli:

I) Zostanie ustalone miejsce uszkodzenia skutkującego pożarem.

II) Zostaną wykonane następujące czynności uniemożliwiające powiększenie się uszkodzenia i pożaru:

1) Wyłączenie dopływu energii elektrycznej do uszkodzonego urządzenia. W większości przypadków materiały stosowane w układach elektronicznych są samogasnące, dlatego bez dopływu energii rozwój pożaru zostanie zahamowany. Uruchomienie urządzenia gaśniczego całkowicie uniemożliwi ponowny wybuch pożaru. Personel w obiekcie może wykryć i usunąć źródło zagrożenia oraz przystąpić do czynności naprawczych.

2) Uruchomienie urządzenia gaśniczego bez wyłączenia dopływu energii elektrycznej. Obecnie dominuje właśnie taka procedura ochrony serwerowni. W takim przypadku źródło pożaru (praktycznie bez względu na jego stopień rozwoju) może być nadal aktywne (ze względu na niemożność zidentyfikowania miejsca uszkodzenia będącego źródłem pożaru i nieusunięcie tego uszkodzenia poprzez wykonanie odpowiednich czynności naprawczych). Tak więc po wyładowaniu środka gaśniczego, ewentualnym uruchomieniu systemu rezerwowego w celu podtrzymania jego stężenia (tzw. dogaszanie) i spadku koncentracji środka gaśniczego pożar może zostać ponownie wzniecony.

Z powyższego wynika, że w przypadku pożarów, w których do uszkodzonego urządzenia elektrycznego lub elektronicznego nadal dostarczana jest energia elektryczna, nawet zastosowanie systemu gaśniczego nie rozwiązuje całkowicie problemu. Jeżeli natomiast przyczyny pożaru i jego charakter są inne niż opisane wyżej (np. mamy do czynienia z pożarem samopodtrzymywalnym – tleniem, pożarem płomieniowym), wówczas gaszenie będzie skuteczne. W takim przypadku zastosowanie stałego urządzenia gaśniczego jest w pełni uzasadnione.

Koncepcje ochrony serwerowni przedstawię w artykule w numerze 5/2017 *Zabezpieczeń*.

mgr inż. Jerzy Ciszewski
IBP NODEX

Jak działa system mgły wodnej?

Przyjedź do Krakowa, aby się przekonać!

Bettina McDowell

Pomysł, aby wykorzystać drobne krople do opanowania oraz ugaszenia pożaru, nie jest nowy. Już ponad 130 lat temu amerykańska firma F.E. Myers stworzyła pierwszy gadżet – system plecakowy do zwalczania małych pożarów lasu. Pomysł ten nie był jednak dalej rozwijany przez branżę ochrony przeciwpożarowej, być może ze względu na niegdysiejszy niedostatek wiedzy i wyobraźni, do czasu, kiedy około 30 lat temu, w drugiej połowie lat 80., w konsekwencji postanowień Protokołu Montrealskiego, zaczęto szukać alternatywnych systemów gaszenia. Inną przyczyną zmian był wybuch pożaru na promie pasażerskim Scandinavian Star 7 kwietnia 1990 roku. Od tego czasu wiele się zmieniło i dziś systemy mgły wodnej są w powszechnym użytku

Nadal jednak istnieje pewien niedostatek wiedzy, a także sceptycyzm dotyczący tego rodzaju ochrony przeciwpożarowej. Niemniej nawet nieprzekonani muszą przyznać, że są sytuacje, w których lepiej użyć mniejszej ilości wody. Ochrona centrów danych czy cennych obrazów jest dobrym przykładem, gdyż zniszczenia dokonane przez wodę mogłyby być gorsze w konsekwencjach niż pożar. Innym przykładem może być gaszenie pożarów wieżowców. Każdy rozumie, że pompowanie mniejszej ilości w wody w górę (na ostatnie piętro) jest łatwiejsze i kosztuje mniej. Ponadto nie ma czynnika strachu, który występuje np. w przypadku używania systemów gazowych. Mgła wodna może zostać użyta bez konieczności ewakuacji ludzi z pokoju czy budynku.

Fot. 1. Prezes IWMA, Ragnar Wighus, otwiera konferencję (fot. Jasmina Rahmanovic, IWMA)

Przez ostanie 30 lat powstało wiele firm kierujących się przekonaniem, że systemy mgły wodnej to autonomiczne systemy ochrony przeciwpożarowej. Do swojej oferty dodało je wiele firm zajmujących się produkcją systemów tryskaczowych.

Jak działa mgła wodna? Pożar może powstać pod warunkiem współobecności materiału palnego, ciepła i tlenu. W odróżnieniu od tradycyjnych zraszaczy mgła wodna usuwa dwa spośród tych elementów – ciepło i tlen (tradycyjne systemy zraszające usuwają tylko ciepło). Uzyskuje się to przez natryskiwanie wody pod niskim, średnim lub wysokim ciśnieniem przez specjalnie zaprojektowane do tego celu dysze. Gdy ciśnienie w systemie wzrasta, zmniejsza się wielkość kropelek, zajmują one większą przestrzeń i tworzy się mgła. W konsekwencji system ten jest w stanie szybko obniżyć temperaturę i ograniczyć dostęp tlenu do płomieni. W ten sposób pożar traci energię. Schładzające działanie mgły wodnej zapobiega ponownemu wzniecaniu się ognia.

Niskociśnieniowe systemy wytwarzające mgłę wodną wytwarzają ciśnienie 12,5 bara, średniociśnieniowe – między 12,5 a 35 barów, a wysokociśnieniowy – dochodzące do 120 barów. Każdy z tych systemów ma swoje zastosowanie – niskociśnieniowy jest wykorzystywany do innych celów niż średnioczy wysokociśnieniowy i na odwrót.

Ze względu na to, że do opanowania i ugaszenia pożaru potrzebna jest mniejsza ilość wody niż w przypadku tradycyjnego systemu zraszającego, zastosowanie systemu wytwarzającego mgłę wodną może być korzystnym pod względem kosztów sposobem ochrony przeciwpożarowej. Ponadto jest to system przyjazny dla środowiska, nie powiększa dziury ozonowej, nie przyczynia się do globalnego ocieplenia, nie prowadzi do zanieczyszczenia wody i jest niezawodny.

Fot. 2. Słuchacze 16. International Water Mist Conference (fot. Jasmina Rahmanovic, IWMA)

Obecnie system wytwarzający mgłę wodną jest też dobrze unormowany. Pierwszym organem, który stworzył dotyczącą go normę, było National Fire Protection Association, które

w 1996 r. opublikowało *NFPA 750 Standard for Water Mist Fire Protection Systems*. Później pojawiły się inne normy i wytyczne dotyczące wykorzystania mgły wodnej, opracowane przez FM (FM 5560), VdS (wytyczna 3188) oraz Europejski Komitet Normalizacyjny (CEN TS 14972).

ny narzucanych przez Międzynarodową Organizację Morską (ang. *International Maritime Organisation* – IMO) wymogów dotyczących bezpieczeństwa pożarowego i wytycznych dotyczących instalacji. Ponadto ulepszono procedury przeprowadzania testów pożarowych dla alternatywnych systemów zraszających.

Fot. 3. Dyskusja panelowa na IWMC 2016 w Wiedniu (fot. Jasmina Rahmanovic, IWMA)

Jak już wcześniej wspomniano, do upowszechnienia wykorzystania mgły wodnej w gaszeniu pożarów przyczyniły się dwa wydarzenia. Pierwszym z nich było wprowadzenie w życie Protokołu Montrealskiego w sprawie „substancji zmniejszających warstwę ozonową" pod koniec lat 80. XX wieku. Drugie to pożar na promie pasażerskim Scandinavian Star, który wydarzył się o poranku 7 kwietnia 1990 r. W tym pożarze zginęło

W Szwecji już w latach 1975–1990 pracowano nad rozwojem wysokociśnieniowego systemu wykorzystującego mgłę wodną. Głównym celem była ochrona hoteli i kabin pasażerskich. Prowadzono również badania nad łatwopalnymi cieczami. Pożar Scandinavian Star przyczynił się do umożliwienia przedstawienia wyników tych prac 20 czerwca 1990 r. – zaledwie dwa miesiące po katastrofie.

Fot. 2. Słuchacze 16. International Water Mist Conference (fot. Jasmina Rahmanovic, IWMA)

158 osób – prawie połowa wszystkich pasażerów.

Do czasu podpisania Protokołu Montrealskiego do gaszenia pożarów wykorzystywano halony – chemiczne środki na bazie bromu. Halony były skuteczne, wydajne, a systemy łatwe w instalacji. Ich stopniowe wycofywanie utorowało drogę dla systemów wykorzystujących mgłę wodną, które stały się ważnym przedmiotem badań i zaczęły być rozwijane.

W takich dziedzinach jak ochrona przeciwpożarowa często dopiero poważne incydenty doprowadzają do zmian. Katastrofa w dniu 7 kwietnia 1990 r. doprowadziła ostatecznie do zmia-

Był to punkt wyjścia dla nowo powstałej szwedzkiej firmy UltraFog. Tylko sześć miesięcy później inna firma – Marioff z Finlandii – także zaczęła opracowywać wysokociśnieniowe systemy gaszenia mgłą wodną. Od tego czasu wielu poszło za ich przykładem, m.in. Fogtec w Niemczech, VID Fire-Kill w Danii oraz Telesto i SUPO Cerber w Polsce.

W 1998 roku powstała organizacja International Water Mist Association (IWMA). Jej celem było i nadal jest bycie platformą kontaktu dla przedsiębiorstw, organów badawczych, instytutów, firm ubezpieczeniowych, organów prawodaw-

Fot. 4. Prezes IWMA Ragnar Wighus i zwycięzca nagrody IWMA Daniel Martin (fot. Jasmina Rahmanovic, IWMA)

czych i innych stron zainteresowanych techniką gaszenia mgłą wodną. Organizacja promuje tę technikę. W jej imieniu przeprowadzono prace badawcze. Każdego roku odbywa się międzynarodowa konferencja (w 2017 r. odbędzie się w Rzymie – 25 i 26 października). IWMA organizuje również lokalne seminaria.

Następne spotkanie organizowane przez IWMA odbędzie się 15 listopada w Krakowie, w hotelu Galaxy. Program obejmie następujące zagadnienia: sposób działania systemu wykorzystującego mgłę wodną do gaszenia, normalizacja na poziomie europejskim i międzynarodowym, certyfikacja, instalacja i konserwacja. Prelegenci z Polski i innych krajów będą rozmawiać o wykorzystywaniu systemu mgły wodnej w praktyce. Seminarium będzie towarzyszyć wystawa, na której swoje produkty zaprezentują firmy z Polski i zagranicy. Wstęp będzie wolny dla delegatów. Zainteresowani mogą zarejestrować się od 30 czerwca 2017 r. za pośrednictwem strony internetowej IWMA.

Bettina McDowell, M.A.

International Water Mist Association
e-mail: McDowell@iwma.net
www.iwma.net

Tłumaczenie: Paweł Karczmarzyk

Sterowanie systemami oddymiania w świetle wymagań rozporządzenia Ministra Infrastruktury

Janusz Sawicki

W poprzednich artykułach omawiane były zagadnienia związane z systemami oddymiania stosowanymi w obiektach budowlanych w celu umożliwienia wydłużenia przejść i dojść ewakuacyjnych, zwiększenia powierzchni strefy pożarowej lub podwyższenia klasy odporności pożarowej jednokondygnacyjnych budynków kategorii PM, dzięki czemu mogą zostać spełnione wymagania zawarte w rozporządzeniu Ministra Infrastruktury (§227 pkt 4, §229, §237 pkt 6, §256 pkt 4 i §215)

Dla przypomnienia wymieniam wyodrębnione instalacje i urządzenia, z których zbudowane są systemy oddymiania i których działanie powinno być niezawodne:

1) Źródła zasilania, zarówno podstawowe, jak i rezerwowe, dla instalacji elektrycznych i pneumatycznych.
2) Zespoły kablowe służące do zasilania, przesyłania sygnałów sterujących, a także orurowania napędów pneumatycznych.
3) Instalacje służące do wczesnej detekcji dymu, autonomiczne lub wykorzystujące odrębny system sygnalizacji pożarowej.
4) Urządzenia wykonawcze, takie jak wentylatory, klapy oddymiające zawierające napędy elektromechaniczne i pneumatyczne, urządzenia otwierające otwory dolotowe powietrza z napędami elektromechanicznymi i pneumatycznymi.
5) Urządzenia wydzielające strefę pożarową, takie jak klapy odcinające, drzwi i bramy przeciwpożarowe.
6) Urządzenia wydzielające strefy dymowe stanowiące część strefy pożarowej – kurtyny dymowe aktywowane w czasie alarmu.

7) Centrale i sterowniki sterujące poszczególnymi składowymi systemu oddymiania, w tym centrale zgodne z projektem normy EN12101-9.

W niniejszym artykule postaram się przedstawić główne wymagania dotyczące central i sterowników oddymiania.

Wymagania dotyczące sterowników oddymiania

Określenie funkcji i wymagań dotyczących sterowników i central realizujących oddymianie i odprowadzanie ciepła jest bardzo ważne.

O złożoności zagadnienia świadczy przebieg uzgadniania normy EN 12101-9 *Control Panels*. Ta część normy do dzisiaj jest projektem. Zgodnie z rozporządzaniem Rady Europy nr 301/2011 certyfikaty dotyczące właściwości użytkowych powinny być przyznawane na podstawie europejskich lub krajowych dokumentów zawierających ocenę techniczną.

Centrale i sterowniki stosowane w systemach oddymiania pożarowego powinny być przede wszystkim niezawodne. Dotyczy to szczególnie układów podstawowego i rezerwowego zasilania zarówno central, jak i urządzeń peryferyjnych i wykonawczych. Niezawodność działania jest ściśle związana z odpornością samej centrali na warunki środowiskowe i oddziaływanie pożaru (oczywiście w ograniczonym zakresie). W związku z tym centrala musi być zainstalowana w odpowiednim pomieszczeniu lub miejscu.

Centrale sterujące urządzeniami służącymi do oddymiania grawitacyjnego, mechanicznego, powinny być umieszczone w pobliżu urządzeń wykonawczych, którymi sterują i które zasilają oraz kontrolują. Dotyczy to przede wszystkim siłowników elektromechanicznych na niskie napięcie 24 V_{DC} – ze względu na występowanie spadków napięć i związane z nimi dobieranie przekrojów przewodów zasilających.

Gdy nie można umieścić centrali sterowania oddymianiem grawitacyjnym w pobliżu własnych urządzeń wykonawczych, należy rozważyć zastosowanie siłowników elektromechanicznych na napięcie 230 V_{AC}. Oczywiście takie rozwiązanie będzie wymagało zastosowania centrali lub tablicy sterującej z możliwością komutacji napięcia 230 V_{AC}. Tablice sterujące i zasilające wentylatory oddymiające 3x400 V_{AC} powinny być instalowane w pobliżu tych wentylatorów, gdyż także zasilanie awaryjne powinno być doprowadzone jak najbliżej silnika napędowego wentylatora. Podczas planowania instalacji oddymiających koniecznie trzeba pamiętać o zespołach kablowych, które są częścią systemu i powinny gwarantować odpowiedni, narzucony przez scenariusz pożarowy, czas działania urządzeń, a same kable zasilające i sterujące powinny być dobierane z uwzględnieniem warunków środowiskowych.

Wymagania funkcjonalne

Oprócz wymaganej sygnalizacji optycznej stanów pracy urządzenia (dozór, uszkodzenie, blokada) centrale i sterowniki oddymiania powinny mieć możliwość odbioru sygnałów wyzwalających z innych central i sterowników, w szczególności z centrali sygnalizacji pożarowej (CSP). Centrale autonomiczne, czyli mające własne linie dozorowe, na których instalowane są czujki dymowe, powinny spełniać wymagania dotyczące CSP. Ze względu na warunki środowiska, w którym centrala pracuje, konieczny jest wyższy stopień ochrony obudowy centrali (IP).

Wymagania funkcjonalne dotyczące central i sterowników służących do sterowania oddymianiem grawitacyjnym są zawarte w projekcie normy EN 12101–9, natomiast w normie PN-EN 12101–6 zawarte są wytyczne dotyczące systemów różnicowania ciśnień. Centrale i sterowniki systemów oddymiania mechanicznego i mieszanego, grawitacyjno-mechanicznego, zostały opracowane przez ITB i CNBOP-PIB jako dokumenty oceny technicznej, stanowiące podstawę do wydania krajowej oceny technicznej zgodnie z rozporządzeniem RE nr 305/2011 (poprzednio jako ZUAT do opracowania aprobat technicznych).

Od systemów oddymiania grawitacyjnego i mieszanego wymaga się umożliwienia prawidłowego sterowania systemem w przestrzeniach podzielonych na więcej niż jedną strefę dymową – przy założeniu, że system oddymiania jest jednocześnie wykorzystywany do przewietrzania budynku. Jest to jedno z ważniejszych wymagań funkcjonalnych.

Należy pamiętać o tym, że oddymianie powinno zadziałać tylko w tej strefie oddymiania, w której czujki dymowe (przyporządkowane do niej) wykryły pożar, lub po użyciu ręcznego przycisku oddymiania (RPO) przyporządkowanego tej strefie oddymiania.

Jeżeli centrale lub sterowniki obsługujące kilka stref oddymiania są wykorzystywane do przewietrzania budynku (otwarte są wszystkie klapy oddymiające), to po wykryciu pożaru w którejkolwiek strefie powinny natychmiast zamknąć wszystkie klapy oddymiające oprócz tych znajdujących się w strefie, w której wykryto pożar. W przypadku przewietrzania otwory dolotowe powietrza kompensacyjnego nie muszą być otwierane.

Jeżeli w obiekcie zastosowano kilka central sterujących, z których każda obsługuje swoją strefę oddymiania, należy je wyposażyć w interfejsy umożliwiające spełnianie wyżej opisanej funkcji. Dzięki temu dym i ogień nie przedostaną się do innych stref oddymiania przez otwarte klapy oddymiające wskutek zassania dymu i strumienia cieplnego.

Podsumowanie

Niniejszy artykuł podsumowuje cykl dotyczący realizacji procesów sterowania oddymianiem umożliwiających spełnienie wymagań dopuszczających zwiększenie strefy pożarowej, wydłużenie dróg ewakuacyjnych czy wreszcie podwyższenie klasy odporności pożarowej budynku. Należy pamiętać, że zastosowane instalacje oddymiania powinny niejako „zastępować" stałe elementy konstrukcyjne obiektów budowlanych, a więc powinny funkcjonować niezawodnie, być uruchamiane natychmiast po wykryciu pożaru, a czasami funkcjonować w warunkach pożarowych dłużej niż obliczany czas ewakuacji, ponieważ spełniają one postulat wymagania podstawowego – dotyczącego bezpieczeństwa pożarowego konstrukcji budynku.

Janusz Sawicki
IBP NODEX

Instytut Bezpieczeństwa Pożarowego

NODEX

www.IBPNODEX.pl

Niezależny Ośrodek Doradców i Ekspertów

- Organizujemy zaawansowane kursy specjalistyczne i szkolenia dedykowane z zakresu bezpieczeństwa pożarowego
- Kładziemy duży nacisk na ćwiczenia i zajęcia laboratoryjne
- Współpracuje z nami ponad trzydziestu wykładowców i specjalistów

Atrakcyjne zniżki dla Członków Wspierających Rozwój Instytutu!

- Posiadamy doskonale wyposażoną salę szkoleniową z własną komorą testową
- Wykonujemy ekspertyzy oraz opinie dotyczące zabezpieczeń przeciwpożarowych i ewakuacji
- Zajmujemy się doradztwem technicznym dla inwestorów, wykonawców i projektantów.

Instytut Bezpieczeństwa Pożarowego NODEX Sp. z o.o.
ul. Ks. J. Chrościckiego 93/105, 02-414 Warszawa
tel.: +48 22 203 59 21, fax: +48 22 203 58 31

www.IBPNODEX.pl

AlarmCalm
Kompletne rozwiązanie problemu fałszywych alarmów

Krzysztof Dembiński

Fałszywe alarmy pożarowe są poważnym problemem związanym z eksploatacją systemów sygnalizacji pożarowej. Osłabiają czujność personelu obsługującego system oraz pracowników, powodują kosztowne przestoje w zakładach produkcyjnych związane z ewakuacją pracowników, a w przypadku obiektów monitorowanych przez Państwową Straż Pożarną generują koszty związane z nieuzasadnionymi wezwaniami i odrywają strażaków od innych czynności

System sygnalizacji pożarowej Axis EN

Od początku procesu budowy instalacji systemu sygnalizacji pożarowej, czyli od momentu wykonania projektu, zaczyna się praca mająca na celu zapewnienie jego skutecznego działania oraz ograniczenie występowania fałszywych alarmów. Należy zadbać o odpowiednie rozmieszczenie i dobranie typów czujek, które mają być zastosowane w pomieszczeniach chronionych (w zależności od ich przeznaczenia), oraz stworzenie algorytmu działania systemu z uwzględnieniem warunków panujących w obiekcie, np. czasu potrzebnego na przyjęcie informacji i ich sprawdzenie przez obsługę. Następnie, podczas programowania działania systemu, należy zapewnić prawidłową realizację przyjętych założeń projektowych i zweryfikować ich poprawność podczas testów w trakcie uruchamiania systemu. Na etapie eksploatacji instalacji SSP należy zadbać o prawidłową konserwację zainstalowanych urządzeń.

Firma Advanced jest producentem systemu sygnalizacji pożarowej Axis EN. Aby umożliwić jeszcze większe ograniczenie liczby fałszywych alarmów przy zachowaniu wysokiej skuteczności wykrywania pożaru, wprowadziła na rynek rozwiązanie AlarmCalm.

Całość rozwiązania AlarmCam składa się z systemu sygnalizacji pożarowej Axis EN, oprogramowania Dynamix Tools i przycisku AlarmCalm.

Na zweryfikowanie alarmu, potwierdzenie go przez obsługę oraz sprawdzenie wykrytego zdarzenia potrzebny jest

czas. Niezależnie od tego, czy wykorzystywany jest mały system z jedną centralą i jedną pętlą dozorową czy rozbudowany system sieciowy, informacja musi być przesłana szybko. Jeśli w przypadku czasu potwierdzenia wynoszącego 60 sekund potrzebne jest 15 sekund na przesłanie informacji przez sieć, to 25% czasu zostaje stracone. Bardzo wydajna sieć Ad-Net zapewnia bardzo szybkie przesyłanie potrzebnych informacji.

Często warunkiem odpowiedniego zaprogramowania działania elementów systemu w celu ograniczenia występowania fałszywych alarmów jest uwzględnienie skomplikowanych zależności przyczynowo-skutkowych. Specjalny moduł Config Tool w oprogramowaniu systemu Axis EN pozwala łatwo i szybko stworzyć algorytm działania systemu z uwzględnieniem wszystkich opcji w celu wyeliminowania fałszywych alarmów.

Na pętli dozorowej SSP Axis EN instalowany jest adresowalny przycisk AlarmCalm, który umożliwia potwierdzenie zdarzenia i wydłużenie czasu weryfikacji przez przeszkolony personel bezpośrednio w miejscu jego wystąpienia. Przycisk jest wyposażony w diodę LED oraz wewnętrzny brzęczyk.

Fot. 1. Przycisk AlarmCalm

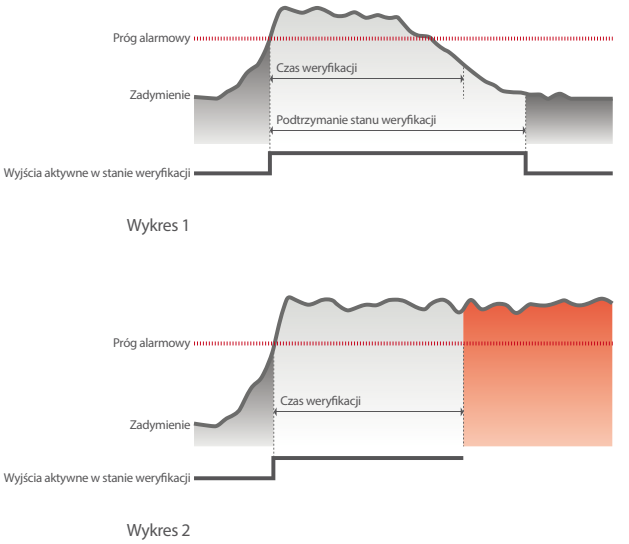
Weryfikacja alarmów i opóźnienia

System Axis EN, w którym są opcje weryfikacji alarmu i możliwe jest ustawianie opóźnień, dzięki którym uzyskuje się czas na wysterowanie wyjść, jest w prosty sposób konfigurowany w oprogramowaniu konfiguracyjnym. Podstawową różnicą między trybami pracy tego systemu jest moment jego przejścia w stan alarmu pożarowego. Przed przejściem w ten stan następuje weryfikacja alarmu, natomiast po przejściu system uruchamia procedurę związaną z opóźnieniami, dzięki którym jest czas na sprawdzenie przyczyny alarmu, oczywiście, jeśli taka procedura została zaprogramowana.

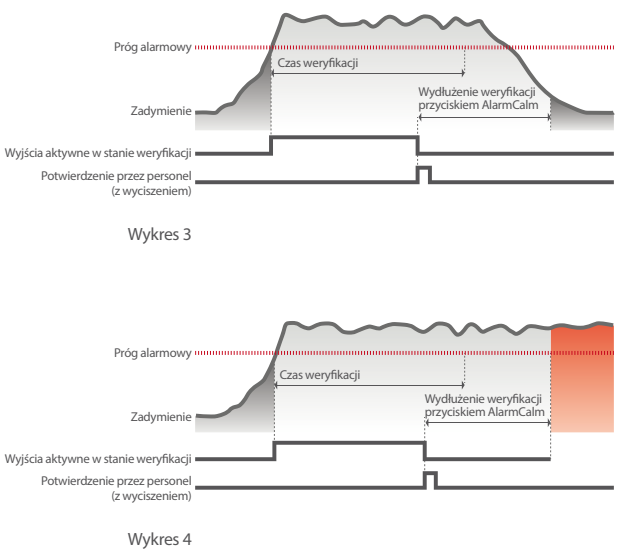
Weryfikacja może zostać włączona w jednym z dwóch trybów pracy – A lub B. W trybie A, po wykryciu przez dowolny detektor pożaru w okresie trwającym maksymalnie 60 sekund, następuje weryfikacja alarmu. W tym czasie centrala nie wyświetli alarmu pożarowego, zaś informacja o weryfikacji zostanie zapisana w pamięci zdarzeń.

Tryb B zapewnia dużą swobodę pod względem czasu i metody weryfikacji, a także umożliwia pełne zaprogramowanie działania wyjść i sygnalizatorów ostrzegawczych w trakcie weryfikacji. Informacja o alarmie i jego lokalizacji jest wyświetlana na panelu głównym centrali i dowolnie wybranych pozostałych centralach lub panelach wyniesionych w sieci przez cały okres weryfikacji.

Oprogramowanie Dynamix Tools pozwala zarządzać ustawieniami weryfikacji i czasów opóźnień i przypisywać te ustawienia do wirtualnych obszarów, które domyślnie pokrywają się z zaprogramowanymi w systemie strefami dozorowymi, ale mogą również być określone niezależnie i pokrywać wiele stref dozorowych i elementów lub tylko wybrane punkty systemu. Każda centrala obsługuje do 200 obszarów, co pozwala na zaprogramowanie maksymalnie do 40 000 obszarów w sieci central.



Rys. 1. Działanie mechanizmu weryfikacji bez potwierdzenia przyciskiem AlarmCalm



Rys. 2. Działanie mechanizmu weryfikacji z potwierdzeniem przyciskiem AlarmCalm

Dla każdego obszaru można zaprogramować niezależne parametry weryfikacji w celu eliminacji fałszywych alarmów. Można również pogrupować te obszary i zastosować wspólne ustawienia dla danej grupy.

Weryfikacja bez wywoływania alarmu pożarowego może następować na wielu obszarach równocześnie. Można zaprogramować maksymalną liczbę obszarów, na których równocześnie może nastąpić weryfikacja, zaś po zadziałaniu czujki z kolejnego obszaru system przejdzie w stan alarmu pożarowego.

Każda centrala systemu Axis EN umożliwia zaprogramowanie dziesięciu niezależnych sterowników czasowych. Dzięki temu można programować różne strategie redukcji fałszywych alarmów w zależności od pory dnia lub dnia tygodnia. Na przykład można zastosować różne parametry weryfikacji w ciągu dnia i nocy, zaś opóźnienia na sprawdzenie można wykorzystywać w różnych godzinach i (lub) dniach. Sterowniki można ustawić niezależnie dla każdego dnia tygodnia, co pozwala na włączenie różnych opcji weryfikacji lub zaprogramowanie różnych opóźnień na sprawdzenie w dni powszednie, w weekendy, w dzień i w nocy.

Rozwiązanie AlarmCalm umożliwia zmianę ustawienia czułości i trybów pracy detektorów w celu weryfikacji alarmu. Na przykład czujki multisensorowe mogą w tym celu zostać automatycznie przełączone w tryb, w którym pracują jako czujki temperatury.

Dla każdego obszaru jest dużo możliwych ustawień konfiguracyjnych. Możemy wybrać następujące opcje:

– weryfikacja dozwolona: tak/nie,
– wydłużenie czasu weryfikacji przyciskiem AlarmCalm: tak/nie,
– weryfikacja alarmu przez drugie urządzenie z tego obszaru: tak/nie,
– weryfikacja alarmu przez zmianę trybu pracy czujki: tak/nie.

Ustawień parametrów weryfikacji urządzeń na danym obszarze można dokonać bardzo szybko, wykorzystując opcję ustawień dla typów urządzeń wejściowych. W oprogramowaniu Axis EN Config Tool dostępna jest opcja ustawienia wspólnych parametrów weryfikacji dla wszystkich czujek

multisensorowych, optycznych, temperatury oraz pozostałych elementów wejściowych (przycisków ROP i wejść modułów). Można także wybrać opcję ustawienia parametrów weryfikacji indywidualnie dla każdego elementu danego typu.

W trybie weryfikacji można wysterować również sygnalizatory akustyczne, optyczne i wyjścia przekaźnikowe na każdym obszarze. Można szybko skonfigurować wszystkie urządzenia danego typu na raz albo skonfigurować każde urządzenie lub obwód niezależnie.

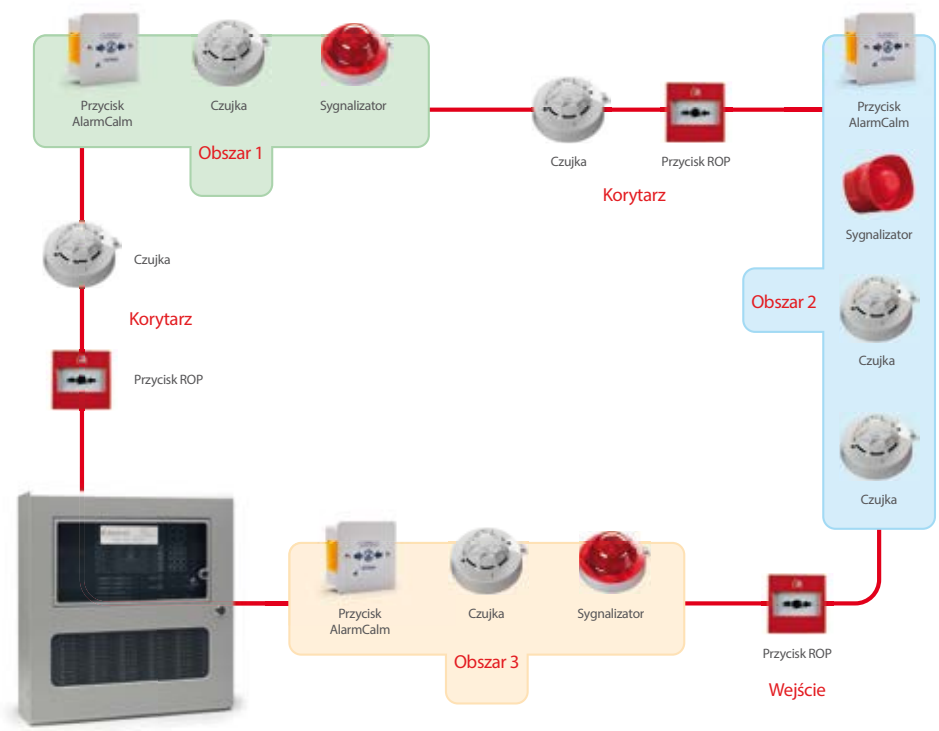
W trybie B weryfikacji alarmów AlarmCalm umożliwia ustawienie wielu parametrów czasowych. Weryfikacja rozpoczyna się wówczas, gdy ilość dymu w detektorze przekroczy założony próg alarmu lub zadziała inne urządzenie wejściowe. Podczas weryfikacji system aktywuje zaprogramowane na czas weryfikacji urządzenia wyjściowe. Dzięki możliwości ustawienia czasu podtrzymania stanu weryfikacji informacje o przebiegu weryfikacji są wyświetlane na wyświetlaczu centrali sygnalizacji pożarowej wystarczająco długo, aby mogły być odczytane i sprawdzone.

nień systemowych. Można korzystać ze sterowników czasowych dla różnych nastaw w poszczególnych dniach i godzinach oraz określić maksymalną liczbę obszarów, na których dozwolone jest opóźnienie zadziałania wyjść w czasie sprawdzania. Równie proste jest również ustawienie wejść, dla których opóźnienia będą aktywne – można ustawić wszystkie urządzenia wejściowe danego typu lub każde z nich indywidualnie.

Dzięki możliwości łatwego zadeklarowania koincydencji sygnałów na danym obszarze można w razie potrzeby zapewnić wysterowanie wyjść z pominięciem czasów opóźnienia na sprawdzenie.

Każda centrala systemu sygnalizacji pożarowej Axis EN ma na płycie czołowej cztery przyciski, których działanie jest programowane. Jedną z opcji działania może być również potwierdzenie weryfikacji na dowolnym obszarze.

Opcje weryfikacji są ustawiane dla każdej centrali oddzielnie i mogą być dowolnie zmieniane bez wpływu na działanie pozostałych central pracujących w tej samej sieci. Domyślnie informacje o weryfikacji będą wyświetlane na wszystkich cen-



Rys. 3. Przykładowa konfiguracja sprzętowa SSP Axis EN z AlarmCalm

Jeśli przyczyna alarmu (np. zadymienie) ustąpi przed upływem czasu weryfikacji, system powróci do normalnej pracy po upływie czasu podtrzymania.

Jeśli zadymienie po upływie czasu weryfikacji będzie nadal przekraczało próg alarmu, system sygnalizacji pożarowej Axis EN przejdzie w stan pełnego alarmu. Zależności czasowe zostały przedstawione na wykresach 1–4.

Dzięki możliwości zaprogramowania różnych stylów działania wyjść i sygnalizatorów (40 różnych stylów dla każdej centrali) można skonfigurować je w taki sposób, aby można było łatwo rozróżnić poszczególne etapy weryfikacji i opóźnień.

Ustawianie dodatkowych opóźnień weryfikacyjnych odbywa się w dokładnie taki sam prosty sposób jak ustawianie opóź-

tralach. W razie potrzeby można łatwo skonfigurować listę urządzeń w sieci, na których te informacje będą pokazywane.

Przykładowe rozwiązanie konfiguracyjne

W pomieszczeniach kuchennych restauracji hotelowych czy stołówek zakładowych bardzo często instalowane są czujki temperatury w celu uniknięcia fałszywych alarmów w przypadku chwilowo unoszącego się dymu z przypalonej patelni lub kłębów pary podczas gotowania.

Przyjmijmy, że w przykładowej kuchni pracuje się w godzinach od 7:00 do 20:00 w dni robocze i od 8:00 do 22:00 w soboty i niedzielę. W oprogramowaniu Config Tool programujemy odpowiednie okna czasowe. Korzystając ze zdefiniowanych

już okien czasowych, na czas pracy w kuchni umożliwiamy weryfikację. Ustawiamy tryb pracy czujek multisensorowych w taki sposób, by w godzinach pracy w kuchni czułość była niska, a poza godzinami pracy średnia. Na czas pracy w kuchni włączamy weryfikację poprzez zmianę trybu pracy czujki na tylko temperaturowy i wyłączamy na ten czas część optyczną. Programujemy czas weryfikacji – np. określamy, że będzie on wynosił 90 sekund i będzie można wydłużyć go przyciskiem AlarmCalm o kolejne 300 sekund. W trakcie weryfikacji powinna uruchomić się sygnalizacja akustyczno-optyczna w pomieszczeniu kuchni, przy czym po potwierdzeniu przyciskiem AlarmCalm część akustyczna zostanie wyłączona, a sygnał optyczny będzie emitowany przez cały czas weryfikacji.

W ten sposób w godzinach pracy w kuchni, czyli w czasie, kiedy przebywa tam personel, detektory działają z obniżoną czułością. Przeszkoleni pracownicy wiedzą, że w przypadku chwilowego zadymienia powinni potwierdzić zdarzenie przyciskiem AlarmCalm i przewietrzyć pomieszczenie. Poza godzinami pracy kuchni weryfikacja jest wyłączona i ustawiona jest wyższa czułość detektorów, dzięki czemu reakcja pracowników odpowiedzialnych za obsługę systemu sygnalizacji pożarowej może być szybka.

Zainstalowanie przycisku AlarmCalm bezpośrednio na pętli dozorowej nie zwiększa w istotny sposób kosztów instalacji. Zastosowanie AlarmCalm umożliwia szybką reakcję personelu obecnego w miejscu wystąpienia zdarzenia bez konieczności angażowania pracowników obsługujących centralę systemu sygnalizacji pożarowej, która może być umiejscowiona w znacznej odległości od kuchni. Można zatem uniknąć kosztownych przestojów związanych z alarmami ewakuacyjnymi.

Innymi pomieszczeniami, w których można wykorzystać bogate możliwości konfiguracji systemu Axis EN w celu ograniczenia fałszywych alarmów, są wszelkiego rodzaju warsztaty. Bardzo często wykonuje się w nich czynności takie jak cięcie, szlifowanie czy spawanie. Aby nie obniżać na stałe czułości systemu sygnalizacji pożarowej w takich pomieszczeniach, możemy skorzystać z wielu możliwych nastaw konfiguracyjnych i zapewnić optymalną, dostosowaną do panujących warunków ochronę.

AlarmCalm to jedno z kilku innowacyjnych rozwiązań firmy Advanced z dziedziny systemów sygnalizacji pożarowej. W ofercie producenta jest również między innymi LifeLine, czyli system powiadamiania osób niesłyszących o pożarze, a także TouchControl – dotykowy panel wyniesiony obsługujący aktywne mapy. Inne nowości, które pojawią się w ofercie w niedalekiej przyszłości, to np. Dynamix Smoke – rozwiązanie przeznaczone do współpracy z systemami wentylacji i oddymiania.

W celu uzyskania szczegółowych informacji na temat rozwiązania AlarmCalm i systemu sygnalizacji pożarowej Axis EN zapraszamy do kontaktu z naszą firmą.

Krzysztof Dembiński
P.U.I. Zeto-Projekt

55-075 Bielany Wrocławskie
ul. Kolejowa 20
tel.: 71 3110591
www.zeto-projekt.com.pl

Advanced
The Standard in Fire Systems

NAJWYŻSZY POZIOM OCHRONY

SYSTEM SYGNALIZACJI POŻARU

Axis EN

ZETO-PROJEKT

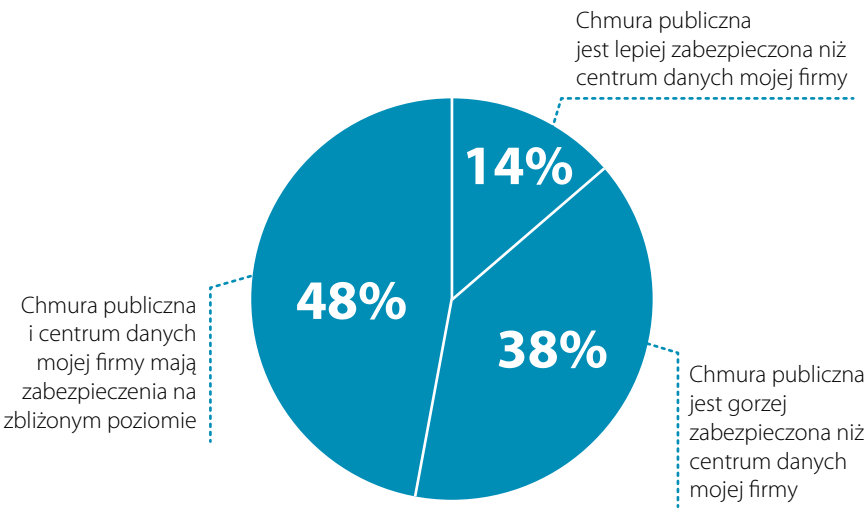
WYŁĄCZNY PARTNER FIRMY ADVANCED NA TERENIE POLSKI:
P.U.I. ZETO-PROJEKT SP. Z O. O.
UL. KOLEJOWA 20, 55-075 BIELANY WROCŁAWSKIE
WWW.ZETO-PROJEKT.COM.PL
BIURO@ZETO-PROJEKT.COM.PL

Bezpieczeństwo informacji w chmurze
(część 2)

dr inż. Marek Blim

W podsumowaniu poprzedniego artykułu cyklu przedstawiono jedynie fragmentaryczne wyniki przeprowadzonej w polskich przedsiębiorstwach ankiety dotyczącej wykorzystania możliwości chmury obliczeniowej (ang. *cloud computing*) w polskich firmach. Spójrzmy na nie z perspektywy statystyki europejskiej

Według najnowszych danych Eurostatu (dot. III kwartału 2016 r.) Polska jest jednym z trzech krajów, które korzystają z cloud computing (CC) w najmniejszym stopniu. W Europie dane w chmurze przetwarza co piąta firma (20% firm), ale w Polsce ten odsetek wynosi zaledwie 6%. Najwięcej firm (51%) korzysta z chmury obliczeniowej w Finlandii, 40% przedsiębiorców wykorzystuje tę technologię we Włoszech, 39% w Szwecji, a 38% w Danii. W pierwszej dziesiątce państw wykorzystujących CC zmieściły się jeszcze Holandia, Irlandia, Wielka Brytania, Chorwacja, Belgia i Słowacja. Nasz kraj znalazł się na szarym końcu europejskiego rankingu Eurostatu. Gorsza okazała się jedynie Rumunia (5%). Zajęliśmy przedostatnie miejsce ex *aequo* z Łotwą (6%). Wyprzedzają nas m.in. Węgry, Bułgaria i Grecja (8%). Według danych Eurostatu firmy w Europie wykorzystują CC przede wszystkim do usług prostych: poczty elektronicznej (66%) oraz przechowywania plików (53%). W nieco mniejszym stopniu do hostowania baz danych (39%), aplikacji – biurowych (34%) lub wspierających zarządzanie finansami (31%) – oraz systemów CRM (21%). W Polsce sposoby wykorzystania są podobne. Nieznacznie różnią się jedynie liczby. „Wyniki badań w Polsce wskazują, że z CC najczęściej korzystają przedsiębiorstwa z branży IT, zaś najrzadziej firmy z sektora przemysłu (17%), branży transportowej i dystrybucyjnej (15%) oraz budowlanej (14%)”[1].



Rys. 1. Ocena bezpieczeństwa CC wg polskich firm

Rozwiązania chmurowe mogłyby się upowszechnić, gdyby nie obawy dotyczące korzystania z tej techniki. Przedsiębiorcy na co dzień używający chmury przyznają, że boją się przede wszystkim o bezpieczeństwo danych (wskazuje na to aż 57% dużych i 38% małych firm). Zniechęcają ich również kwestie prawne (odpowiednio 46% i 31%) oraz wysokie koszty takich usług (po 32%). Obawy dotyczą także braku wystarczającej wiedzy niezbędnej do korzystania z usług chmurowych (wskazuje na to aż 32% małych firm), problemów ze zmianą operatora oraz ryzyka braku dostępu do danych. Aż 46% dużych firm za jedną z barier uznaje brak informacji na temat rzeczywistej lokalizacji danych przetwarzanych w chmurze. Kwestia bezpieczeństwa danych w chmurze stanowi dziś zasadniczą przeszkodę do dalszej ekspansji tej techniki informatycznej, co obrazuje wynik polskiej ankiety (rys. 1)[2].

1. Zalety i wady chmur obliczeniowych

Ewolucja sposobu przetwarzania danych, której obecnym etapem jest chmura obliczeniowa, dotyczy nie tyle zmiany sposobu dokonywania obliczeń (jest to głównie ich – jakże szeroka – wirtualizacja), ile podejścia do tej pracy. Obecnie dzięki CC uzyskujemy szybkość, dostępność i skalowalność przy jednoczesnym wyeliminowaniu wielu uciążliwości związanych z korzystaniem ze sprzętu (zasilanie, chłodzenie, ochrona środowiska).

Rys. 2. Uproszczony diagram przedstawiający chmurę obliczeniową

Ten nieco schematyczny rysunek odnosi się w swej treści do podstawowych modeli CC (wg NIST są to: IaaS, PaaS, i SaaS). Obecnie oferowany jest dużo szerszy zakres usług – w praktyce jest to XaaS, czyli „wszystko jako usługa” oferowane w chmurze.

Do niewątpliwych zalet chmury należą skalowalność, dostępność, wydajność, łatwe zarządzanie, elastyczność, niezawodność, ekologiczność i niezależność sprzętowa klienta.

1) "Chmura obliczeniowa w polskim e-biznesie. Raport e24cloud", http://it-manager.pl/chmura-obliczeniowa-w-polskim-e-biznesie-raport-e24cloud/ (stan z 20.07.2017).

2) "Bezpieczeństwo chmur publicznych z perspektywy polskich organizacji", http://www.computerworld.pl/whitepaper/2832-Bezpieczenstwo-chmur-publicznych-z-perspektywy-polskich-organizacji.html (stan z 20.07.2017).

1.1. Skalowalność

Każdy użytkownik chmury na pewno doceni swobodę i pozytywne aspekty dynamicznego przydzielania zasobów, gdy tylko okażą się potrzebne. Dzięki skalowalności nie trzeba płacić za utrzymanie infrastruktury „na wszelki wypadek". Oczywiście za wykorzystaną dodatkową moc obliczeniową chmury czy obsługę większej liczby transakcji trzeba zapłacić, ale większy wydatek jest równoważony wzrostem zysku wynikającym z obniżonych kosztów wzmożonego ruchu.

1.2. Dostępność

Usługi w chmurze są dostępne za pośrednictwem praktycznie każdego komputera podłączonego do Internetu. W tradycyjnym modelu korzystania z aplikacji instalowanych na stanowiskach pracy i licencjonowanych zależnie od ich liczby uzyskanie podobnej funkcjonalności jest po prostu niemożliwe. Warto też pamiętać o tym, że w przypadku programów działających jako usługi w chmurze użytkownik nie musi się martwić o to, czy sprzęt, z którego korzysta, ma odpowiednią wydajność.

1.3. Wydajność

Centra obliczeniowe (farmy komputerowe), będące największymi chmurami publicznymi, oferują moc nieosiągalną dla nawet najbardziej rozbudowanej stacji roboczej. Nie bez znaczenia jest też wzrost szybkości wynikający ze skalowania i dynamicznego przydzielania zasobów. To, że wzrost obciążenia nie powoduje przestojów, również przekłada się na efektywność działania danej firmy.

1.4. Łatwe zarządzanie

Łatwe zarządzanie ma związek z dostępnością. Firma korzystająca z kompleksowego zestawu usług w chmurze może nimi zarządzać za pomocą wygodnego w obsłudze oprogramowania i pojedynczego punktu, z którego można zawiadywać całością (aplikacjami w chmurze, przechowywanymi w niej danymi, oferowanymi instancjami[3] itp.). Nie ma potrzeby tworzenia różnych końcówek administracyjnych do zarządzania poszczególnymi serwerami, macierzami dyskowymi itp.

1.5. Elastyczność

Dzięki chmurom rozwój użytkowości technik informatycznych jest prostszy niż w klasycznym ujęciu. Zamiast kupować nowe serwery, dbać o ich prawidłową konfigurację, zgodność z istniejącymi rozwiązaniami itp., można skorzystać z gotowych usług CC.

1.6. Niezawodność

Budowanie bezpiecznej infrastruktury zapewniającej nieprzerwane działanie kosztuje bardzo wiele, tymczasem dostawcy usług w chmurze bardzo podkreślają niezawodną infrastrukturę swoich centrów danych – jest ona nie tylko zaletą, ale wręcz koniecznością, bo warunkuje sukces biznesowy inwestycji. W tradycyjnym modelu korzystania z aplikacji awaria jednego z komputerów w firmie zmniejsza ogólną wydajność. W przypadku chmury jest inaczej. Serwery w centrach danych również się psują, ale zadania realizowane przez jednostki, które uległy awarii, są natychmiast przejmowane przez inne maszyny.

1.7. Ekologiczność

Ekologiczność oznacza w tym przypadku bardziej efektywne wykorzystanie pamięci, mocy obliczeniowej i przestrzeni na dane, co przekłada się na mniejsze zużycie zasobów naturalnych (energii, paliw itp.) niż w tradycyjnym IT. Dodatkowym atutem są grupowe rozwiązania klimatyzacyjne (chłodnie kominowe).

1.8. Niezależność sprzętowa klienta

Jedną z zalet CC jest brak zależności od sprzętu. Komputer czy tablet to tylko klient, interfejs, dzięki któremu można korzystać z usług, które „gnieżdżą się" na serwerach w chmurze. Uszkodzenie lokalnego sprzętu nie skutkuje utratą danych czy brakiem dostępu do usług. Zaletą jest też łatwiejsze monitorowanie wydajności i optymalizacji naszych aplikacji czy infrastruktury wirtualnej, wielodostęp do wspólnych zasobów (współpraca), niezawodność czy bezpieczeństwo (choć bywa ono kwestionowane i zależy od wielu czynników).

Wykorzystanie CC w firmie ma również wady, które są opisane w następnych podpunktach.

1.9. Bezpieczeństwo

Jedną z większych zalet chmur jest ich skalowalność, jednak stwarza ona pewne ryzyko, np. w przypadku serwisu internetowego, ze względu na stosowany w chmurach model obliczeń. Przykładem mogą być ataki DDoS polegające na masowym generowaniu wywołań mających na celu przeciążenie i w rezultacie czasowe unieruchomienie wybranych serwerów. Gdy dane są przetwarzane tradycyjnie (w firmie, w jej centrum danych), taki atak w najgorszym razie powoduje zablokowanie serwerów danej firmy, ale gdy chodzi o duże, bardzo wydajne centra danych, w których zasoby są dynamicznie alokowane według potrzeb usługobiorcy, DDoS może być bardzo kosztowny. Z bezpieczeństwem wiąże się też kwestia lokalizacji danych. W tradycyjnym modelu przetwarzania ich właściciel najczęściej ma nad nimi pełną kontrolę, bowiem wszystkie znajdują się na dyskach komputerów i serwerach firmowych. W przypadku modelu cloud computing dane, podobnie jak wykorzystywana aplikacja, znajdują się w chmurze, na której działanie – jeżeli jest to chmura publiczna – właściciel danych nie ma żadnego wpływu.

1.10. Ograniczone rozwiązania

Usługi dostarczane z chmury mają kompleksowy charakter i nie wymagają od osoby z nich korzystającej wiedzy na temat niezbędnej infrastruktury, konfiguracji itp., ale jakże często zapominamy o tym, że zakres tych usług jest ograniczony i faktycznie narzucony przez dostawcę (np. trudno sobie wyobrazić środowisko online do pracy grupowej IBM LotusLive działające w chmurze Microsoftu), zaś korzystając z aplikacji instalowanych lokalnie, mamy pełną swobodę wyboru rozwiązania. Takie ograniczenie to tylko jeden aspekt problemu. Trzeba też pamiętać o tym, że aplikacje są stale rozwijane i aktualizowane.

3) Instancja w przypadku CC to dyspozycyjny wirtualny oprogramowany „komputer" o 15–20 GB pamięci.

Można np. wyobrazić sobie sytuację, w której usługodawca wprowadza jakąś nową funkcję danej usługi, jednak nowość okazuje się zbędna dla niektórych firm lub wręcz przeszkadza w pewnych działaniach. To oczywiście uproszczony przykład, ale pokazuje problem swoistego uzależnienia użytkownika chmury od nieuzgadnianych z nim rozwiązań wprowadzanych przez usługodawcę. Na ogół uważa się, że prywatne dane użytkowników nie powinny być powierzane zewnętrznym firmom, bo takie przekazanie danych oznacza, że, chcąc mieć do nich dostęp, uzależniamy się od zamkniętych rozwiązań opracowanych przez ludzi, na których pracę nie mamy żadnego wpływu. Poza tym nie ma żadnej gwarancji, że ceny oferowanych usług nie wzrosną, gdy praca w wielu firmach zostanie ściśle zintegrowana z chmurami. Oczywiście opisane powyżej ograniczenie związane z dostarczanymi rozwiązaniami nie dotyczy chmur prywatnych, w których sami jesteśmy dostawcami rozwiązań dla siebie.

1.11. Wydajność

Wydajność centrów obliczeniowych przetwarzających dane w chmurach jest nieosiągalna nawet dla wielu firm, a więc tym bardziej dla użytkowników indywidualnych. Faktyczna wygoda korzystania z poszczególnych rozwiązań jest jednak ograniczona szybkością transmisji danych pomiędzy komputerem użytkownika a chmurą. Nawet najszybsze centrum danych niewiele zmieni, jeśli czas reakcji programu działającego online będzie fatalny za sprawą łącza o małej przepustowości. Warto też mieć na uwadze, że nawet najszybsze powszechnie dostępne łącza internetowe zapewniają transfer danych, który jest dużo wolniejszy niż w przypadku komunikowania się aplikacji z komponentami sprzętowymi komputera, na którym jest uruchomiona. W rezultacie, choć moc obliczeniowa pojedynczej stacji roboczej jest dużo mniejsza niż moc dowolnego centrum obliczeniowego, istnieje bardzo wiele programów, które jeszcze długo będą działać szybciej, gdy zostaną uruchomione lokalnie. Trudno wyobrazić sobie (przynajmniej na razie) np. aplikację użytkową lub grę generującą obraz 3D w czasie rzeczywistym i w całości działającą w chmurze. Jeśli jednak przepustowość łączy indywidualnych użytkowników będzie mierzona w gigabitach na sekundę, możliwe będzie działanie tych programów w całości w chmurze (próbowano, czego przykładem jest OnLive Game Service[4]).

1.12. Ograniczenia indywidualnego użytkownika

Nie wszyscy indywidualni użytkownicy mogą sobie pozwolić na dysponowanie stałym dostępem do Internetu za pośrednictwem szybkiego i stabilnego łącza – tak jak duże firmy. Brak połączenia jest tożsamy z brakiem dostępu do usług zapewnianych przez chmurę. Samo połączenie również nie wystarczy. Jeśli nie będzie ono stabilne i szybkie, korzystanie z serwisów będzie utrudnione, co może zniechęcić użytkownika. Drugą kwestią jest bezpieczeństwo. Oczywiście możemy liczyć na to, że zaufani usługodawcy zapewnią nam wysoki poziom zabezpieczeń sprzętowych i systemowych, ale nie zmieni to faktu, że przechowujemy własne, czasami newralgiczne dane na obcych serwerach, całkowicie przekazując innym kontrolę nad nimi. Już zdarzały się duże wpadki, nawet poważnym graczom, takim jak Dropbox czy Google Drive. Bezpieczeństwu danych zagrażają nie tylko ataki z zewnątrz. Jeśli zdecydujemy się na korzystanie z darmowych dysków sieciowych, powinniśmy najpierw dokładnie przeczytać regulamin świadczenia usługi, by sprawdzić, na co pozwolimy świadczeniodawcy, powierzając mu swoje dane. Zachęcam do zapoznania się z regulaminami CC oraz przemyślenia, jakie pliki chcemy trzymać w chmurze i czy rozsądny będzie automatyczny upload naszych prywatnych zdjęć na Google+, OneDrive czy Dropbox.

2. Bezpieczeństwo informacji w chmurze a polskie prawo

W polskich warunkach trzeba wyraźnie rozdzielić użytkowników chmury. Każdy użytkownik musi zaakceptować wszystkie rodzaje ryzyka, gdy decyduje się na zawarcie umowy z usługodawcą. Oczywiście sam decyduje o zakresie i sposobie korzystania z usługi. Użytkownik indywidualny sam w pełni decyduje o swoim korzystaniu z CC. Przedsiębiorca prywatny (właściciel firmy) może być po części użytkownikiem indywidualnym, ale na ogół jest on depozytariuszem powierzonych mu lub przetworzonych danych decydujących o operacyjnym „być albo nie być" w zarządzanej przez niego firmie. W przypadku użytkownika publicznego przepisy i zobowiązania ustawowe jednoznacznie określają zakres korzystania przez niego z usług w CC (pomimo jego możliwości decyzyjnych).

W odniesieniu do podmiotu publicznego obowiązuje „dekalog chmuroluba", czyli dziesięć zasad stosowania usług chmurowych przez administrację publiczną wg wskazań GIODO[5]. Bezpieczeństwo danych w chmurze jest zróżnicowane. W chmurze publicznej i przypisanej (ang. *dedicated cloud*) ma ono związek z:

- dostępem osób trzecich do danych w procesie ich przekazywania, przechowywania i wykorzystywania,
- bezpieczeństwem fizycznym i technicznym samego centrum danych chmury obliczeniowej (farmy serwerów),
- pewnością utylizacji zasobu w momencie rezygnacji z usługi,
- bezpieczeństwem systemów/oprogramowania/przemieszczania.

W chmurze prywatnej i specjalnej ma ono związek z:

- ochroną fizyczną i techniczną centrum danych (kontenera),
- bezpieczeństwem danych użytkowników (ochroną dostępu),
- bezpieczeństwem danych w czasie konserwacji i (lub) awarii.

4) OnLive Game Service był uruchomioną w 2010 roku chmurą typu PaaS, w której klientom oferowano całą platformę przystosowaną do gier. Całość obliczania odbywała się w serwerowniach OnLive. Następnie obraz na żywo był przesyłany do użytkownika. Przeniesienie przetwarzania na potężne maszyny w klastrze sprawiło, że oferowane tytuły można było uruchomić na starym notebooku, tablecie lub smartfonie, a nawet – uwaga – na telewizorze (za pomocą specjalnej przystawki podłączanej do telewizora i Internetu). Potrzebne były jednak specjalne, szybkie szerokopasmowe łącza. Serwis zaprzestał funkcjonowania w 2015 r.

5) http://www.giodo.gov.pl/259/id_art/6271/j/pl (stan z 20.07.2017).

Potwierdzeniem przestrzegania narzuconych przez prawo[6] zasad bezpieczeństwa dotyczących CC są odpowiednie certyfikaty. Powinniśmy pamiętać, że mówimy przede wszystkim o wymaganiach prawnych dotyczących użytkownika (przepisach administracji publicznej i „dekalogu chmuroluba"), które mogą znacząco różnić się od obowiązków prawnych dostarczyciela usługi CC (np. *common law* w Wielkiej Brytanii).

3. Polskie odniesienia do problemu bezpieczeństwa informacji

Polskie serwerownie pod względem bezpieczeństwa znajdują się obecnie na 17. miejscu na 30 przebadanych w corocznym badaniu Data Centre Risk Index organizowanym przez Cushman & Wakefield. Jak na nasz region nie jest to wynik zły – instytucja zakwalifikowała krajowe centra do grupy średniego ryzyka, razem z Francją (14. miejsce), Szwajcarią (11. miejsce) i Singapurem (15. miejsce).

Miejsce	Indeks	Państwo	Koszty energii	Łącze	Prowadzenie biznesu
1	100	USA	3	1	3
2	89,53	Wielka Brytania	21	2	5
3	82,29	Szwecja	15	10	10
4	81,29	Niemcy	19	4	15
5	81,16	Kanada	4	11	13
6	79,63	Hong Kong	27	3	2
7	79,47	Islandia	8	29	11
8	79,45	Norwegia	13	19	4
9	78,74	Finlandia	11	22	8
10	78,37	Katar	1	30	21
...	...	...	...	...	...
17	67,43	Polska	18	16	24

Tab. 1. Bezpieczeństwo polskich serwerowni w rankingu światowym
Źródło: Data Centre Risk Index Cushman & Wakefield

Przywołując dane dotyczące polskich obiektów I&CT, nie zapominajmy, że dotyczą one opcjonalnie wszelkich usług oferowanych w ramach big data center, razem z rozwiązaniami o charakterze firmowych serwerowni (nie są to jeszcze chmury prywatne, ale odbiegają standardami dostępu od VPS).

Warto pamiętać, że mamy rodzimego lidera usług przechowywania danych w postaci firmy Oktawave, która w niezależnych testach przeprowadzonych przez CloudHarmony pokonała m.in. Amazon Web Services oraz Microsoft Azure.

4. Podsumowanie

Pozostaje jeszcze kwestia fizycznego miejsca przechowywania danych i ich fizycznego zabezpieczenia. Poruszę ją w kolejnej części.

Opracował dr inż. Marek Blim

6) W przypadku procesów finansowo-księgowych jest to certyfikat SAS 70 typu II przyznawany przez Amerykański Instytut Biegłych Rewidentów (American Institute of Certified Public Accountants – AICPA) i będący w przypadku CC potwierdzeniem wprowadzonej i utrzymywanej wewnętrznej kontroli bezpieczeństwa danych (głównie rachunkowych).

Bibliografia

1) *Bezpieczeństwo biznesu w XXI wieku*, praca zbiorowa, wyd. SASMA EUROPE, Warszawa 2014.
2) Handzel Z., *Cloud computing – czyli chmura obliczeniowa i możliwości jej wykorzystania w mediach*, „Problemy Zarządzania" vol. 11, nr 4 (44), wyd. UW, Warszawa 2013.
3) Konarski X., *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, wyd. Difin, Warszawa 2004.
4) Kępa L., Tomasik P., Dobrzyński S., *Bezpieczeństwo systemu e-commerce*, wyd. Helion, Gliwice 2012.
5) Mateos A., Rosenberg J., *Chmura obliczeniowa. Rozwiązania dla biznesu*, wyd. Helion, Gliwice 2011.
6) Michalak A., *Ochrona tajemnicy przedsiębiorstwa. Zagadnienia cywilnoprawne*, wyd. Kantor Wydawniczy ZAKAMYCZE, Kraków 2006.
7) Siwicki M., *Ochrona praw autorskich, bezpieczeństwa systemów informatycznych, danych osobowych i tajemnicy komunikacyjnej w chmurach obliczeniowych*, „Prokuratura i Prawo" nr 5/2015, s. 109–127.
8) Spraul V. A., *Jak działa oprogramowanie*, wyd. Helion, Gliwice 2016.

Netografia

1) http://it-manager.pl/chmura-obliczeniowa-w-polskim-e-biznesie-raport-e24cloud/ (stan z 14.05.2017).
2) www.3s.pl/pl/17,serwery-i-cloud.html (stan z 14.05.2017).
3) www.computerworld.pl/news/Dlaczego-chmura-sie-w-Polsce-nie-udaje,405741.html (stan z 14.05.2017).
4) www.cyberdefence24.pl/526022,jak-chronic-infrastrukture-krytyczna-nowe-rekomendacje-nist (stan z 14.05.2017).
5) www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_PL.pdf (stan z 14.05.2017).
6) www.giodo.gov.pl/259/id_art/6271/j/pl (stan z 14.05.2017).
7) www.hbrp.pl/a/chmura-obliczeniowa-bilans-korzysci-i-zagrozen/36ypu9gW (stan z 14.05.2017).
8) ww.piit.org.pl/documents/10181/268830/Definicja_rodzaje_chmur_obliczeniowych_oraz_poziomy_uslug_-_Dorota_Grudzien-Molenda_HP.pdf (stan z 14.05.2017).
9) www.spidersweb.pl/2013/11/tencent-10-tb-za-darmo.html (stan z 14.05.2017).
10) www.spidersweb.pl/2015/11/jaka-chmure-wybrac-dysk-google-mega.html (stan z 14.05.2017).

DSC

PowerSeries neo

JEDEN SYSTEM – WSZECHSTRONNA INSTALACJA

- Hybrydowy system alarmowy - przewodowy, bezprzewodowy lub mieszany
- Szybki montaż
- Elastyczna rozbudowa systemu dzięki bezprzewodowej technologii PowerG
- Nowy intuicyjny interface menu instalatora
- Aplikacja mobilna Neo Go (Android/iOS)

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

RACS 5

Skalowalny system kontroli dostępu i automatyki budynkowej

Stacje robocze systemu

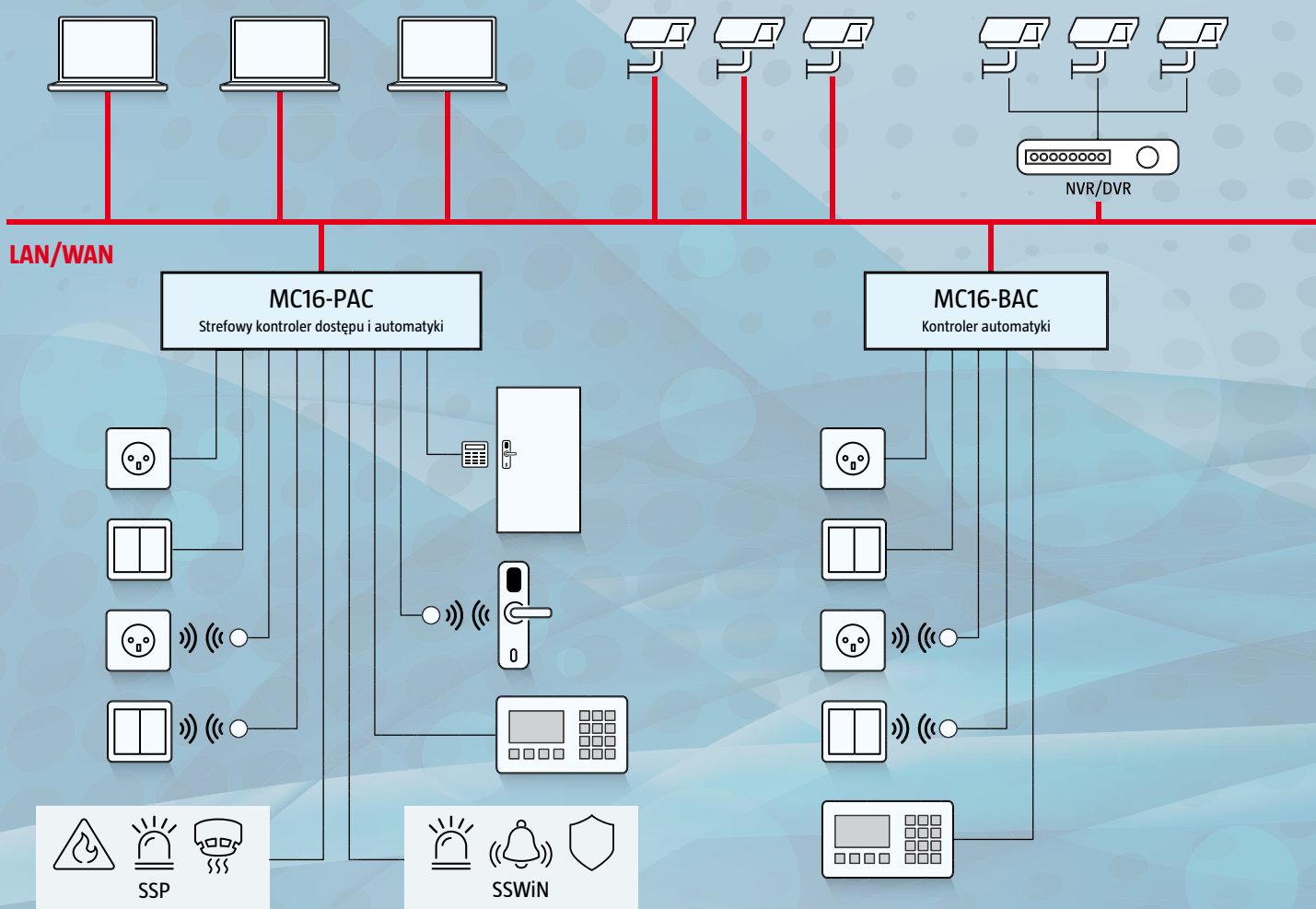
- obsługa systemu z poziomu wielu stacji roboczych
- opcja logowania przez usługę Active Directory
- partycje logiczne systemu zarządzane przez osobnych operatorów
- monitorowanie systemu online
- zdalne sterowanie dostępem i innymi funkcjami systemu
- rejestracja działań operatorów
- zarządzanie użytkownikami bez przerywania pracy systemu

Kamery ONVIF

- podgląd na żywo z kamer IP zgodnych z standardem ONVIF

Rejestratory NVR/DVR

- obsługa rejestratorów HIKVISION
- obsługa rejestratorów DAHUA
- podgląd na żywo obrazu z kamer
- podgląd filmów i zdjęć zapisanych w rejestratorach



Kontrola dostępu i automatyki budynkowej

- obsługa przejść przewodowych
- obsługa przejść bezprzewodowych RACS AIR (ROGER)
- obsługa przejść bezprzewodowych APERIO (ASSA ABLOY)
- obsługa przejść bezprzewodowych SALLIS (SALTO)
- rejestracja czasu pracy
- raportowanie stanów automatyki
- sterowanie automatyką z poziomu terminali systemu
- możliwość załączenia wymogu autoryzacji dla dowolnej akcji wykonywanej w systemie
- sceny świetlne
- bezprzewodowe wyjścia mocy
- optoizolowane wejścia bezprzewodowe
- integracja sprzętowa z systemem alarmowym
- prezentacja stanu systemu alarmowego na terminalach kontroli dostępu
- sterowanie stanem systemu alarmowego z poziomu terminali dostępu
- integracja sprzętowa z systemem p.poż.
- wielofunkcyjne wejścia parametryczne w tym Dual Wiring
- wielofunkcyjne wyjścia z rozróżnieniem priorytetu i sposobu modulacji
- możliwość definiowania globalnych akcji w systemie w odpowiedzi na wybrane zdarzenia
- sterowanie zasilaniem elektrycznym za pośrednictwem czytnika z kieszenią

Kontrola automatyki budynkowej

- raportowanie stanów automatyki
- sterowanie automatyką z poziomu terminali systemu
- możliwość załączenia wymogu autoryzacji dla dowolnej akcji wykonywanej w systemie
- sceny świetlne
- bezprzewodowe wyjścia mocy
- optoizolowane wejścia bezprzewodowe
- wielofunkcyjne wejścia parametryczne w tym Dual Wiring
- wielofunkcyjne wyjścia z rozróżnieniem priorytetu i sposobu modulacji
- możliwość definiowania globalnych akcji w systemie w odpowiedzi na wybrane zdarzenia
- sterowanie zasilaniem elektrycznym za pośrednictwem czytnika z kieszenią

Baza danych

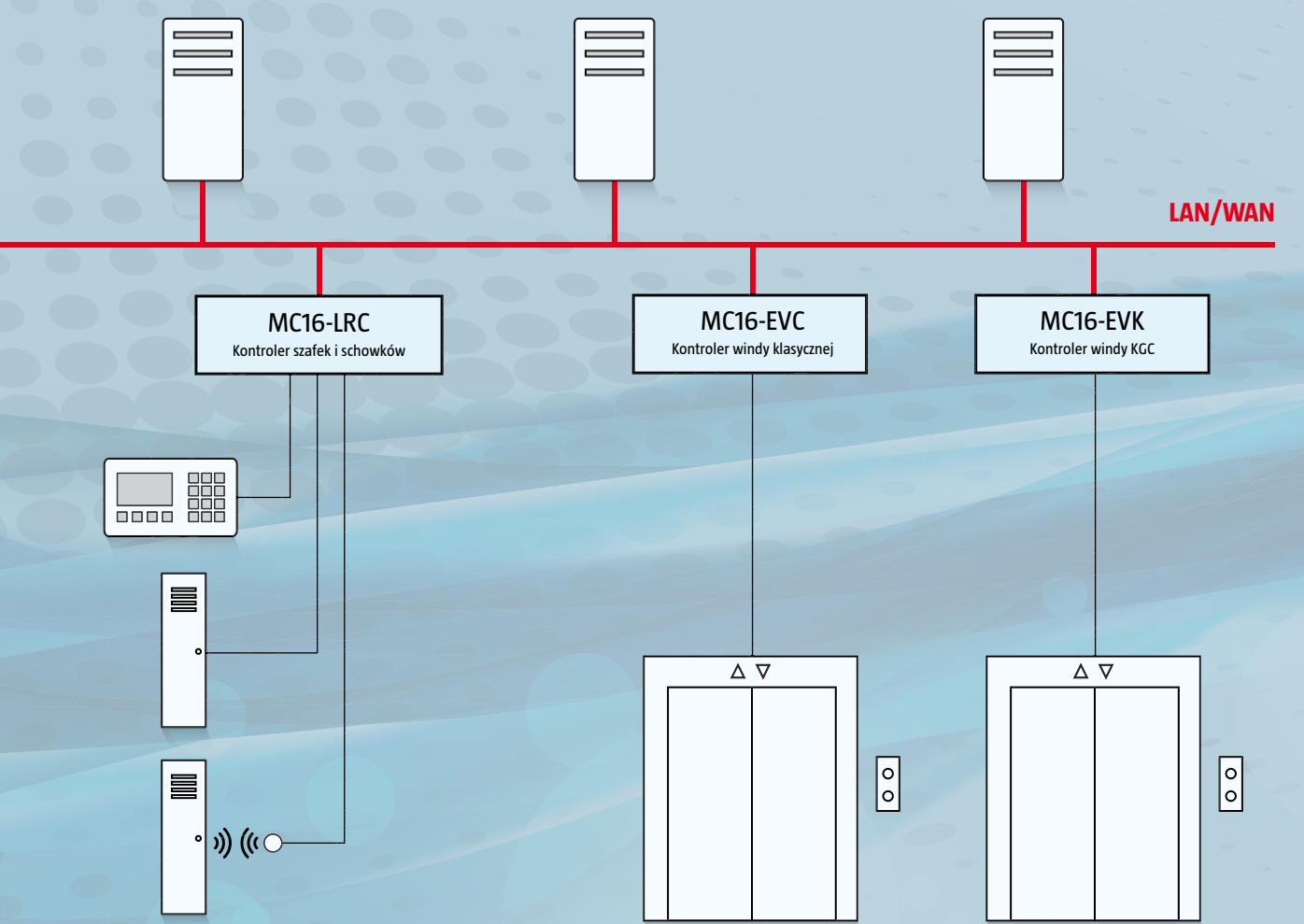
- serwerowa baza danych MS SQL Server
- plikowa baza danych MS SQL Compact

Serwer komunikacyjny

- usługa systemu operacyjnego Windows
- obsługa komunikacji z kontrolerami systemu
- ciągły proces pobierania zdarzeń i aktualizacji rejestru zdarzeń
- sterowanie funkcjami globalnymi
- obsługa komend i poleceń zdalnych
- szyfrowana komunikacja

Serwer integracji

- usługa systemu operacyjnego Windows
- komunikacja w technologii WCF
- API do bazy danych systemu
- API do poleceń zdalnych
- API do zarządzania użytkownikami systemu
- dostęp do funkcji serwera integracji z poziomu dedykowanej aplikacji mobilnej



Kontrola dostępu do szafek i schowków

- kontrola dostępu do szafek i schowków
- obsługa zamków przewodowych
- obsługa zamków bezprzewodowych RWL-3 (RACS AIR)
- podział szafek na grupy obsługiwane z poziomu osobnych terminali

Kontrola dostępu w windach klasycznych

- obsługa 64 pięter
- czytnik montowany w kabinie
- harmonogramy dostępu
- kalendarze wyjątków

Kontrola dostępu w windach KONE

- obsługa 128 pięter
- rozróżnienie typów przywołania windy
- obsługa terminali poza kabiną windy
- obsługa terminali w kabinie windy
- harmonogramy dostępu
- kalendarze wyjątków

Prowadzenie audytu

zarządzania bezpieczeństwem organizacyjno-technicznym obiektów (część 2)

dr inż. Andrzej Wójcik

W pierwszej części artykułu przedstawione zostały ogólne zasady prowadzenia audytu, dotyczące m.in. planowania audytu, doboru audytorów, przedmiotu, etapów i sposobów audytowania oraz dystrybucji raportu. W tej części artykułu poruszony zostanie istotny problem, jakim jest określenie kryteriów audytu

Zgodnie z definicją kryteria audytu mogą zawierać odniesienia dotyczące polityki bezpieczeństwa, procedur, norm, wymagań prawnych, wymagań odnoszących się do systemów zarządzania, wymagań kontraktowych, praktyk charakterystycznych dla danego sektora oraz inne wymagania biznesowe. W przypadku systemów zarządzania bezpieczeństwem organizacyjno-technicznym obiektów możemy skorzystać z gotowych, uznanych wzorców zawartych w normach zarządzania bezpieczeństwem informacji, przede wszystkim w normie ISO/IEC 27001:2013 (wydanie PN-ISO/IEC 27001:2014).

Czy można skorzystać z normy dotyczącej bezpieczeństwa informacji w przypadku zarządzania bezpieczeństwem obiektów? Odpowiedź jest jednoznaczna: tak, ponieważ zgodnie z definicją obiekt jest zasobem informacyjnym niezbędnym do realizacji procesów biznesowych, np. procesu zarządzania bezpieczeństwem organizacyjno-technicznym. Oczywiście ten proces jest jednym z wielu procesów zarządzania obiektem, do których należy m.in. zarządzanie eksploatacją, serwisem, podatnościami technicznymi, wszelkimi zmianami organizacyjno-technicznymi czy też ryzykiem.

Co ważne, cytowana norma służy do certyfikacji systemów zarządzania bezpieczeństwem informacji i zawarte w niej wymagania i kryteria są niezbędne do sprawdzenia, czy wdrożony system zarządzania spełnia wymagania dotyczące szeroko rozumianego bezpieczeństwa informacji.

Analogicznie można stosować kryteria zawarte w normie ISO/IEC 27001:2013 w celu przeprowadzenia audytu bezpieczeństwa obiektu – oczywiście po uwzględnieniu i uzupełnieniu wymagań branżowych zawartych w technicznych normach alarmowych.

Połączenie wymagań zawartych w normie ISO/IEC 27001:2013 oraz wymagań zawartych w normach alarmowych daje audytorowi bardzo skuteczne narzędzia do badania bezpieczeństwa zarządzania oraz poprawności funkcjonowania infrastruktury bezpieczeństwa w audytowanym obiekcie.

Normatywne podstawy zarządzania bezpieczeństwem informacji

W celu wykorzystania możliwości opracowania kryteriów audytu należy zapoznać się z normami zarządzania bezpieczeństwem informacji.

Najważniejsze z nich to:

1) ISO/IEC 27001:2013 (wydanie PN-ISO/IEC 27001:2014) *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*. Ta norma jest uwzględniana podczas certyfikowania systemów zarządzania bezpieczeństwem informacji. W dalszej części artykułu zostaną omówione jej podstawowe zapisy.
2) ISO/IEC 27002:2013 (wydanie PN-ISO/IEC 27002:2014) *Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji.* Ta norma jest przeznaczona dla firm oraz innych organizacji, jako podstawa wyboru zabezpieczeń w ramach procesu wdrażania systemu zarządzania bezpieczeństwem informacji (SZBI) z uwzględnieniem ISO/IEC 27001 lub jako wytyczne dla przedsiębiorstw wdrażających powszechnie akceptowane zabezpieczenia informacji. Norma jest również przeznaczona do stosowania w ramach rozwoju branżowych wytycznych dotyczących zarządzania bezpieczeństwem informacji z uwzględnieniem środowiska, w którym występują specyficzne zagrożenia dla bezpieczeństwa informacji, np. przy projektowaniu i instalacji systemów alarmowych.

Należy pamiętać, że podstawą prawidłowego zarządzania bezpieczeństwem jest szacowanie ryzyka – systematyczne i zgodne z przyjętą metodyką zarządzania bezpieczeństwem w danym przedsiębiorstwie. W przypadku systemów zarządzania

bezpieczeństwem informacji zastosowanie mają m.in. dwie normy: PN-ISO 31000 *Zarządzanie ryzykiem – Zasady i wytyczne*. W tej normie podane są zasady i ogólne wytyczne dotyczące zarządzania ryzykiem oraz norma PN-ISO/IEC 27005:2010 *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.* Pierwsza z nich może być stosowana przez każdy podmiot gospodarczy i administracyjny w ciągu całego okresu jego działalności i w odniesieniu do każdego typu ryzyka, bez względu na jego charakter oraz konsekwencje. Norma nie jest stosowana na potrzeby certyfikacji. Jest zbiorem wskazówek dotyczących zarządzania ryzykiem w systemie bezpieczeństwa informacji. Druga z wymienionych norm określa dobre praktyki oraz daje wskazówki dotyczące planowania i wdrażania wspomnianego systemu.

Wybrane terminy i ich definicje

Aby zrozumieć zasady funkcjonowania systemów bezpieczeństwa informacji (w obiektach), trzeba poznać terminy, które stanowią wspólny język opisujący procesy i zasoby mające wpływ na bezpieczeństwo. Informację traktujemy jako aktyw (zasób), który, podobnie jak inne ważne aktywa biznesowe, ma dla przedsiębiorstwa, instytucji czy organizacji wartość i dlatego należy go odpowiednio chronić. Poniżej podane są wybrane definicje terminów z zakresu bezpieczeństwa informacji.

System zarządzania bezpieczeństwem informacji (SZBI) – część systemu zarządzania, stosowana w związku z ryzykiem biznesowym w celu ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. System zarządzania obejmuje strukturę organizacyjną, polityki, działania związane z planowaniem, zakresy odpowiedzialności, praktyki, procedury, procesy i zasoby.

Aktywa (zasoby) – to wszystko, co ma wartość dla przedsiębiorstwa.

Zagrożenie – potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji.

Podatność – słabość aktywu lub grupy aktywów, która może przyczynić się do zaistnienia (zmaterializowania się) zagrożenia.

Zdarzenie związane z bezpieczeństwem informacji – to określony stan systemu (w tym alarmowego), usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.

Incydent związany z bezpieczeństwem informacji – pojedyncze zdarzenie lub serię niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji i mogą w konsekwencji spowodować znaczne straty lub wręcz przerwać proces biznesowy.

Skutki – rezultat niepożądanego incydentu.

Prawdopodobieństwo – stopień pewności, że incydent (zdarzenie) się zdarzy.

Ryzyko – prawdopodobieństwo, że podatność aktywu lub aktywów oraz istniejące zagrożenie spowodują w efekcie straty (materialne i niematerialne) albo zniszczenie aktywów.

Zabezpieczenie – praktyka, procedura lub inny mechanizm redukujący ryzyko.

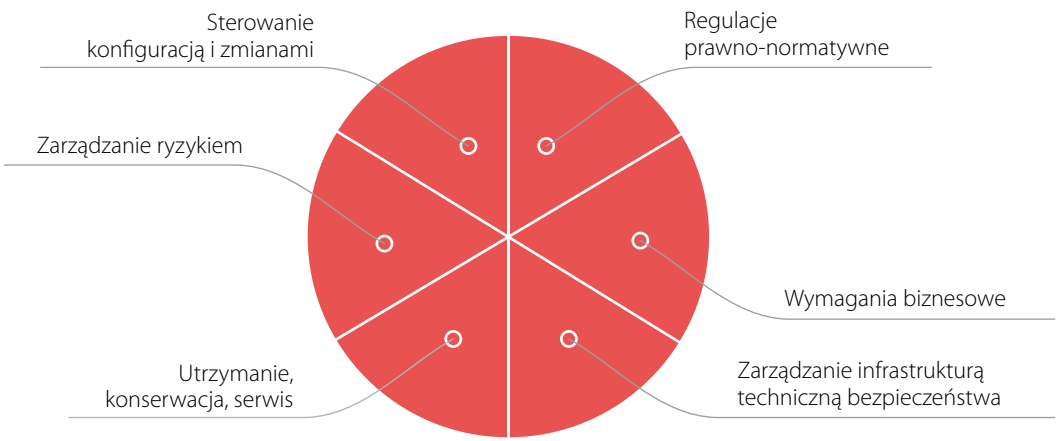
System zarządzania bezpieczeństwem obiektu (SZBO)

SZBO stanowi część wykorzystywanego przez przedsiębiorstwo systemu zarządzania, który jest stosowany z powodu istnienia ryzyka biznesowego, w celu ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa obiektu. SZBO obejmuje infrastrukturę techniczną, strukturę organizacyjną, politykę oraz działania związane z planowaniem, eksploatacją, konserwacją i serwisem, zakresy odpowiedzialności, praktyki, procedury, procesy i zasoby.

Obszary zarządzania za pomocą SZBO

Zarządzanie za pomocą systemu zarządzania bezpieczeństwem obiektu dotyczy przede wszystkim następujące obszary:

- obszar prawno-normatywny, który obejmuje wszystkie regulacje prawno-normatywne, jakim podlega obiekt i podmioty go użytkujące lub powiązane;
- obszar wymagań biznesowych, który dotyczy zobowiązania zawarte w umowach między zainteresowanymi stronami, które korzystają z obiektu lub w jakiś inny sposób są z nim biznesowo powiązane (np. w umowach dotyczących czynności serwisowych i konserwacyjnych przeprowadzanych przez strony trzecie, w umowach dotyczących dzierżawy pomieszczeń, w których przetwarzane



Rys. 1. Zasadnicze elementy składowe SZBO

są informacje niejawne itd.);
– obszar technicznej infrastruktury bezpieczeństwa, który obejmuje szeroko rozumiane systemy zabezpieczenia technicznego, ochrony środowiska, komunikacyjne i teleinformatyczne;
– obszar zarządzania utrzymaniem obiektu (serwisem, konserwacją), który obejmuje zarządzanie eksploatacją i administrowanie obiektem w celu zapewnienia ciągłości działania systemów organizacyjno-technicznych obiektu zgodnie z wymaganiami prawno-normatywnymi (np. dokumentowanie serwisu i przeglądów systemów alarmowych);
– obszar zarządzania ryzykiem, który dotyczy procedury szacowania ryzyka i plan postępowania z ryzykiem w celu zapewnienia optymalnej ochrony obiektu przed zagrożeniami wszystkich możliwych kategorii;
– obszar nadzoru nad konfiguracją i zmianami w obiekcie i jego infrastrukturze, który obejmuje tworzenie dokumentacji opisującej zmiany (rejestru zmian), jakie w trakcie eksploatacji wystąpiły w obiekcie (np. modernizacja systemów alarmowych, która powinna znaleźć swoje odzwierciedlenie w dokumentacji powykonawczej systemu).

Opisane wyżej obszary zarządzania za pomocą SZBO pokazują, że należy sprawdzić poprzez przeprowadzenie audytu, czy infrastruktura w obiekcie jest technicznie zabezpieczona i czy panują w nim bezpieczne warunki środowiskowe. Warto odwołać się w tym miejscu do zapisów opisanej wcześniej normy zarządzania bezpieczeństwem informacji ISO/IEC 270001:2013.

Struktura normy ISO/IEC 27001:2013

Można wyodrębnić następujące fazy wdrażania systemu zarządzania bezpieczeństwem informacji:

1) Planowanie. Należy ustalić zakres, cele, zasoby, zadania i zaplanować, jak przeprowadzić szacowanie ryzyka w celu zapewnienia uzyskania oczekiwanego funkcjonowania SZBI.
3) Wykonanie. Należy wykonać niezbędne działania, np. przeprowadzić analizę ryzyka i postępowanie z ryzykiem, zabezpieczyć informacje technicznie, organizacyjnie i prawno-normatywnie.
3) Sprawdzenie. Należy zapewnić (poprzez stosowanie wskaźników i pomiarów, audyt i kontrolę zarządzania), że zaspokojono potrzeby zainteresowanych stron w zakresie funkcjonowania systemu zarządzania bezpieczeństwem informacji.
4) Działanie. Należy dokonać przeglądu wyników pomiarów i w razie potrzeby podjąć odpowiednie kroki w celu udoskonalenia Systemu Zarządzania Bezpieczeństwem Informacji lub korekty niezgodności. Nowa wersja normy ISO/IEC 27001:2013 bazuje na modelu ciągłego doskonalenia. Nie ma w niej jednoznacznego odniesienia do cyklu PDCA i znanego wszystkim rysunku modelu PDCA. Wynika to stąd, że chociaż model PDCA jest nadal stosowany, można także stosować inne metody realizacji ciągłego doskonalenia.

Struktura normy

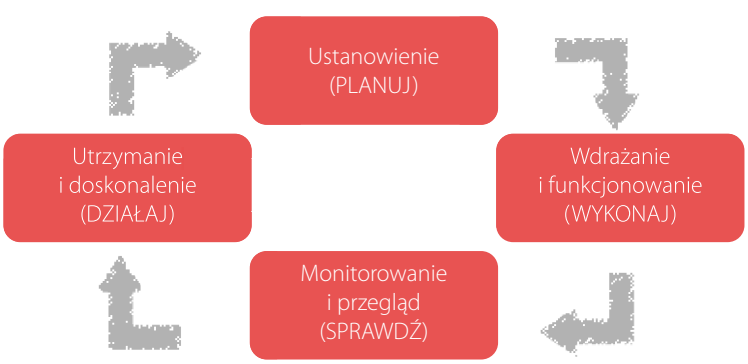
Poniżej znajduje się opis rozdziałów normy w ujęciu zgodnym z modelem PDCA.

Faza planowania (ustanowienia)

Rozdział 4. (*Kontekst organizacji*) dotyczy określenia czynników zewnętrznych i wewnętrznych, jakie powinna uwzględnić organizacja, aby osiągnąć cel swego działania, i takie, które wpływają na jej zdolność do uzyskania efektywnego działania systemu zarządzania bezpieczeństwem informacji. Ważny jest zakres SZBI, a także zrozumienie kontekstu organizacji oraz oczekiwań zainteresowanych stron.

W rozdziale 5. (*Przywództwo*) opisane są wymagania dotyczące najwyższego kierownictwa, które powinno ustanowić i zatwierdzić dokument – politykę bezpieczeństwa informacji, zapewnić odpowiednie zasoby, w tym zasoby ludzkie, wspierać działania mające na celu bezpieczeństwo.

Rozdział 6. (*Planowanie*) dotyczy planowania wszelkich działań odnoszących się do ryzyk i szans osiągnięcia założonych celów mających związek z bezpieczeństwem organizacji.



Rys. 2. Model PDCA (Plan-Do-Check-Act)

W rozdziale 7. (*Wsparcie*) jest mowa o tym, że organizacja powinna zapewnić odpowiednie zasoby, niezbędne kompetencje osób zaangażowanych w funkcjonowanie SZBI oraz wiedzę pracowników i stron współpracujących w zakresie bezpieczeństwa, a także określić zasady przepływu informacji, komunikacji oraz dokumentowania informacji.

Faza wykonywania (wdrażanie i funkcjonowanie)

W rozdziale 8. (*Działania operacyjne*) jest mowa o tym, że organizacja powinna zaplanować, wdrożyć i nadzorować

czynności potrzebne do spełnienia wymagań dotyczących bezpieczeństwa informacji, w tym planowanie i nadzór operacyjny, szacowanie ryzyka oraz postępowanie z ryzykiem.

Faza sprawdzania (monitorowanie i przegląd)

W rozdziale 9. (*Ocena funkcjonowania*) jest mowa o tym, że organizacja powinna ocenić wyniki działań na rzecz bezpieczeństwa informacji oraz skuteczność systemu zarządzania bezpieczeństwem informacji. Powinna określić, co należy mierzyć i monitorować, ustalić metody monitorowania i pomiaru, nadzorować, mierzyć, analizować, oceniać, przeprowadzać audyty wewnętrzne w zaplanowanych odstępach czasu w celu dostarczenia informacji o tym, czy system zarządzania bezpieczeństwem informacji jest zgodny z wymaganiami organizacji, a także dokonywać przeglądu SZBI w zaplanowanych odstępach czasu w celu zapewnienia jego stałej przydatności, adekwatności i skuteczności.

Faza działania

Rozdział 10. (*Doskonalenie*) dotyczy zagadnień związanych z ciągłym doskonaleniem oraz badania przydatności, adekwatności i skuteczności systemu zarządzania bezpieczeństwem informacji. Doskonalenie obejmuje także działania korygujące, które mają na celu wyeliminowanie niezgodności.

Stosowanie zabezpieczeń normatywnych

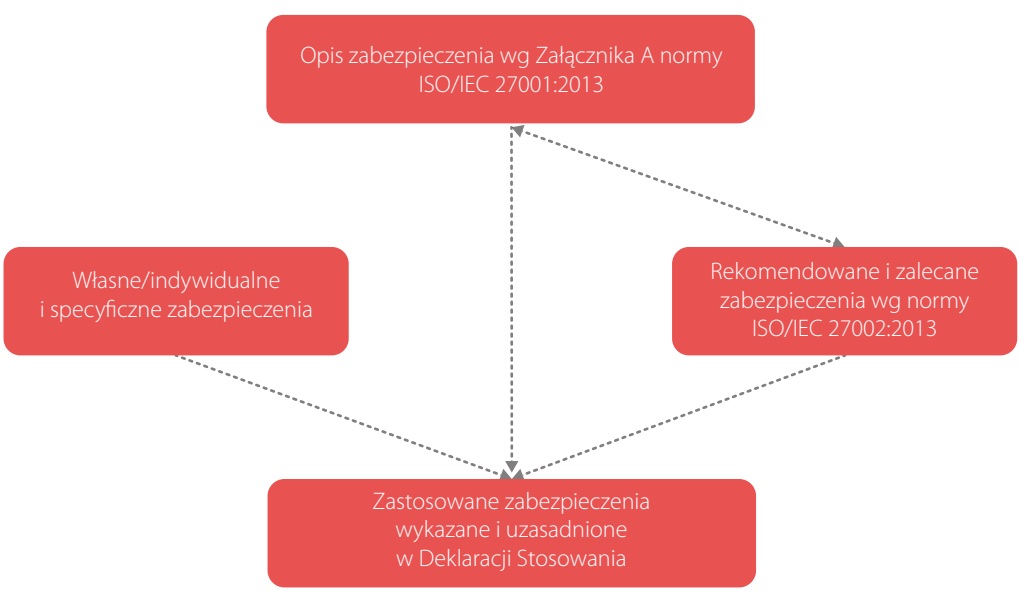
W normie zawarty jest wzorcowy wykaz celów stosowania zabezpieczeń, a w załączniku A wymienione są zabezpieczenia.

Stosowane zabezpieczenia obejmują:

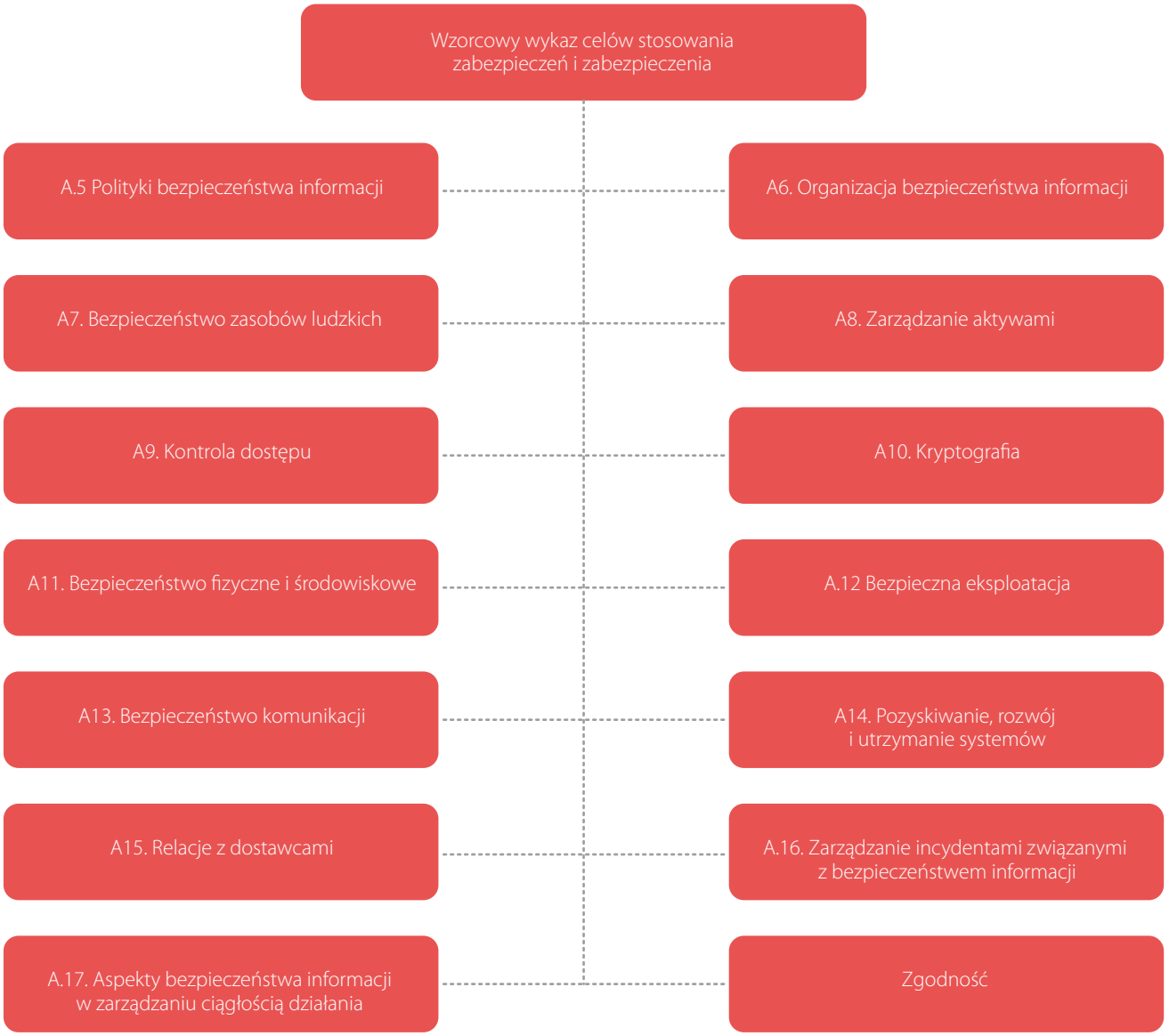
- rekomendowane i zalecane zabezpieczenia zawarte w normie ISO/IEC 27002:2013,
- własne (indywidualne) i specyficzne zabezpieczenia wymagane w związku z działalnością danego przedsiębiorstwa, instytucji czy organizacji, np. ochrona informacji przed ulotem elektromagnetycznym czy podsłuchem.

Poniżej opisany został wzorcowy wykaz celów stosowania zabezpieczeń i stosowane zabezpieczenia wg Załącznika A normy ISO 27001:2013 obejmuje następujące rozdziały numerowane wg normy:

- A.5 *Polityki bezpieczeństwa informacji* – wskazanie działań kierownictwa, którymi jest wskazanie wytycznych działań mających na celu bezpieczeństwo informacji zgodnie z wymaganiami biznesowymi oraz właściwymi normami prawnymi i regulacjami oraz wspieranie tych działań;
- A.6 *Organizacja bezpieczeństwa informacji* – wskazówki dotyczące sposobu ustanowienia struktury zarządzania w celu zainicjowania oraz nadzorowania wdrażania i eksploatacji systemu bezpieczeństwa informacji;
- A.7 *Bezpieczeństwo zasobów ludzkich* – określenie sposobu na to, by pracownicy i kontrahenci rozumieli swoją odpowiedzialność i byli odpowiednimi kandydatami do wypełnienia ról, które są dla nich przewidziane;
- A.8 *Zarządzanie aktywami* – pokazanie, w jaki sposób identyfikuje się aktywa organizacji i określa właściwą odpowiedzialność dotyczącą ich ochrony;
- A.9 *Kontrola dostępu* – wskazówki dotyczące sposobu ograniczenia dostępu do informacji i środków przetwarzania informacji;
- A.10 *Kryptografia* – podanie sposobu zapewnienia właściwego i skutecznego wykorzystania kryptografii do ochrony poufności, autentyczności lub integralności informacji;
- A.11 *Bezpieczeństwo fizyczne i środowiskowe* – podanie sposobu zapobiegnięcia nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom informacji i środków przetwarzania informacji należących do organizacji;
- A.12 *Bezpieczna eksploatacja* – określenie wymagań, które zapewnią poprawną i bezpieczną eksploatację środków przetwarzania informacji;
- A.13 *Bezpieczeństwo komunikacji* – rozdział dotyczący ochrony informacji w sieciach oraz wspomagających je środkach przetwarzania informacji;
- A.14 *Pozyskiwanie, rozwój i utrzymanie systemów* – rozdział, w którym jest mowa o tym, że bezpieczeństwo informacji powinno być zapewnione w systemie



Rys. 3.



Rys. 4.

informacyjnym w całym cyklu jego życia (dotyczy to również systemów informacyjnych dostarczających usług w sieciach publicznych);
- A.15 *Relacje z dostawcami* – rozdział dotyczy potrzeby zapewnienia ochrony aktywów organizacji udostępnianych dostawcom;
- A.16 *Zarządzanie incydentami związanymi z bezpieczeństwem informacji* – rozdział, w którym jest mowa o tym, że potrzebne jest spójne i skuteczne podejście do zarządzania incydentami związanymi z bezpieczeństwem informacji – z uwzględnieniem informowania o zdarzeniach i słabościach oraz sposobach ich rozwiązywania;
- A.17 *Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania* – rozdział, w którym jest mowa o tym, że celem zabezpieczenia jest zapewnienie ciągłości bezpieczeństwa informacji w systemach zarządzania;
- A.18 *Zgodność* – rozdział, w którym jest mowa o tym, że zgodność z prawem i zawartymi umowami ma na celu uniknięcie naruszenia zobowiązań prawnych, regulacyjnych lub umownych związanych z bezpieczeństwem informacji oraz innych wymagań dotyczących bezpieczeństwa.

Podsumowanie

W tej części poznaliśmy podstawowe obszary zarządzania bezpieczeństwem obiektów w ujęciu zapisów i wymagań normy zarządzania bezpieczeństwem informacji ISO/IEC 27001.

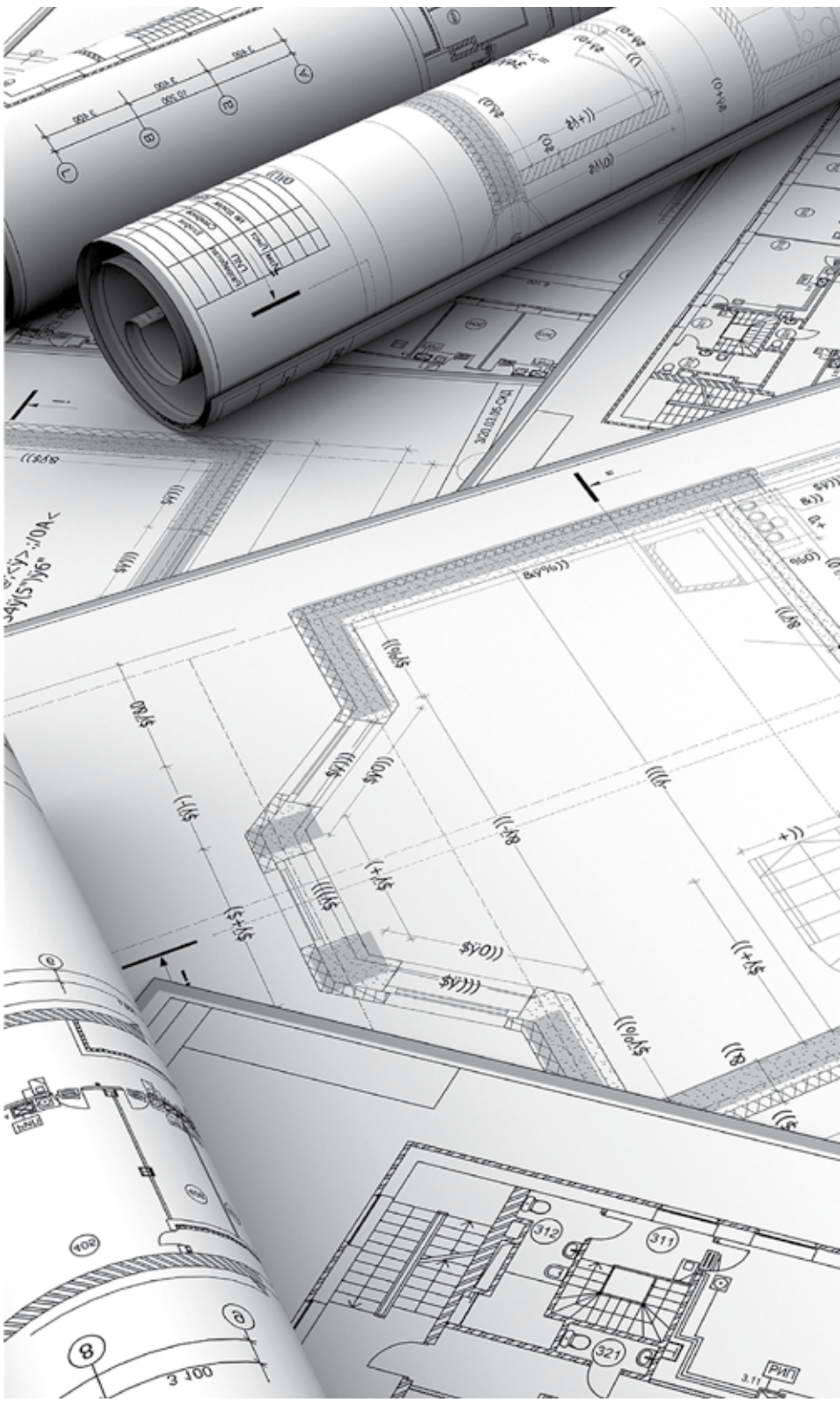
Zapoznaliśmy się z modelem wdrażania normy, jej strukturą, celami oraz sposobami zabezpieczenia. Jest to ważna wiedza dla audytora, który musi kierować się obiektywnymi wytycznymi audytowania bezpieczeństwa obiektów. Wspomniano także kilkakrotnie o zarządzaniu ryzykiem. Następny artykuł będzie dotyczył szacowania ryzyka w zarządzaniu bezpieczeństwem obiektów w ujęciu cytowanych w artykule norm.

Opracował
dr inż. Andrzej Wójcik
ekspert i rzeczoznawca
ds. bezpieczeństwa technicznego i ochrony informacji
audytor ds. bezpieczeństwa biznesu
andrzej@esinstal.pl

Projektuj
z firmą Hanwha Techwin

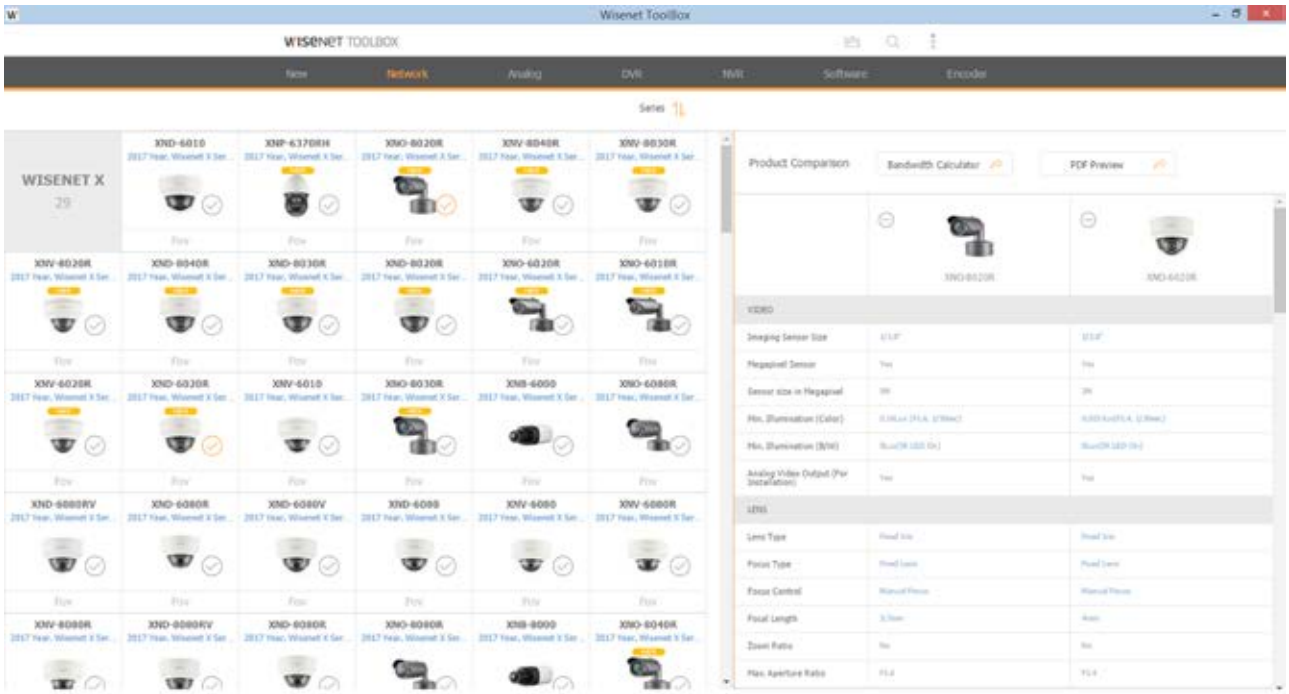
Piotr Rogalewski

Wysokiej jakości sprzęt i oprogramowanie to podstawa profesjonalnego i skutecznie działającego systemu telewizji dozorowej. Ale zanim taki system zostanie uruchomiony, potrzeba wiele pracy – od wyboru urządzeń i wstępnej koncepcji, przez obliczenia pasma sieciowego i pojemności dysków, modelowanie pola widzenia kamer, ustalenie budżetu mocy etc., aż po finalny projekt i samą instalację. Na każdym etapie Hanwha Techwin wspiera dystrybutorów, projektantów i instalatorów nie tylko wiedzą i doświadczeniem swoich pracowników, ale także darmowymi aplikacjami narzędziowymi i wieloma materiałami informacyjnymi



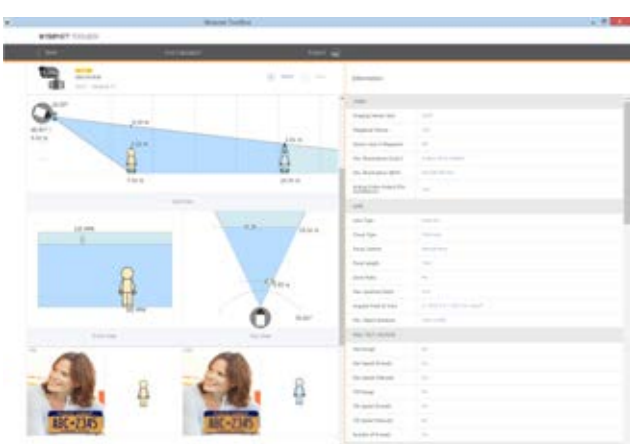
WiseNet Toolbox – trzy w jednym

Nasi klienci, którzy mieli okazję korzystać ze sprzętu Samsung Techwin, pamiętają zapewne takie aplikacje narzędziowe jak Product Selector, Field of View Claculator i Bandwidth Calculator. Obecnie wszystkie te narzędzia zintegrowano w jednej intuicyjnie obsługiwanej aplikacji WiseNet Toolbox, która ma wiele nowych funkcji. WiseNet Toolbox to baza aktualnych produktów firmy Hanwha Techwin. Kliknięcie zdjęcia odpowiedniego produktu skutkuje wyświetleniem kompletnej listy parametrów w postaci tabeli, którą można zapisać w formacie PDF lub wydrukować. Przeniesienie kilku produktów w obręb pola porównywania powoduje wyświetlenie ich danych technicznych we wspólnej tabeli. Dzięki temu można szybko ocenić różnice i podobieństwa, a zestawienie wyeksportować do pliku PDF lub wydrukować. Tak przygotowany materiał można przedstawić klientowi, aby szczegółowo wyjaśnić różnice w funkcjach i cenach poszczególnych produktów. Bogaty zestaw filtrów pozwala zawęzić obszar poszukiwań zgodnie z zadanymi kryteriami. Na przykład szukając wybranej kamery sieciowej, możemy wskazać produkty o rozdzielczości 2 Mpix



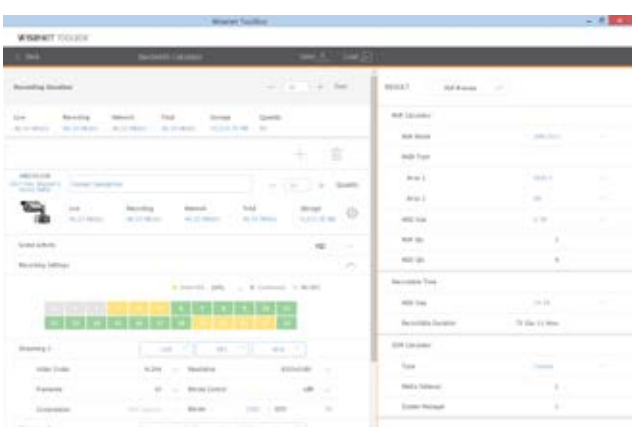
Fot. 1. WiseNet Toolbox – wybór produktów

i z funkcją WDR, w obudowach kopułkowych o klasie szczelności IP66, z promiennikiem podczerwieni. Aplikacja automatycznie dostosuje listę produktów do aktualnie włączonych filtrów, a także podpowie, jakie akcesoria montażowe można zastosować (np. akcesoria do aktualnie oglądanej kamery). Jest wiele kryteriów filtracji, m.in. rodzaj obudowy, rozdzielczość obrazu, prędkość transmisji, rodzaj kompresji, wejścia/wyjścia alarmowe, sposób zasilania, obsługa kart SD i wiele, wiele innych. Nie jest potrzebne połączenie z Internetem. Dostępny jest też tryb wyszukiwania na podstawie symboli produktów, który bardzo ułatwia zapoznanie się z aktualną ofertą, zwłaszcza nowym klientom.



Fot. 2. WiseNet Toolbox – kalkulacja pola widzenia

Kliknięcie pola *FOV* pod fotografią kamery przełącza aplikację w tryb obliczania pola widzenia. Za pomocą suwaków można zmieniać wysokość montażu kamery, jej poziomy i pionowy kąt widzenia, ogniskową, wymiary obserwowanej sceny oraz odległość obiektu od kamery. Niezależnie od tego, który z parametrów jest modyfikowany, pozostałe wartości są przeliczane automatycznie i na bieżąco. W dolnej części okna wyników pokazywany jest poglądowy obraz o jakości zgodnej z aktualnie wybranymi ustawieniami. „Gęstość" obrazu, podawana w pikselach na metr, pozwala ocenić, jakie kryterium obserwacji będzie spełniał modelowany obraz (może umożliwiać identyfikację, rozpoznanie, detekcję albo obserwację ogólną).



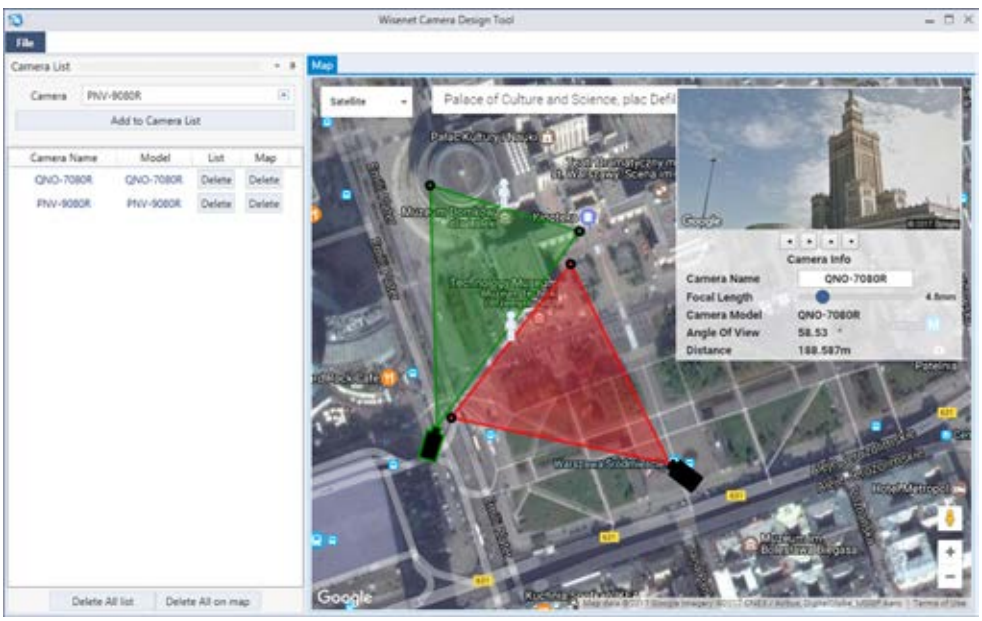
Fot. 3. WiseNet Toolbox – obliczanie pasma i pojemności dysków

Kliknięcie ikony z symbolem wykresu znajdującej się w górnej części okna powoduje przejście w tryb obliczania pasma sieciowego i pojemności dysków twardych.

Dla każdej grupy kamer można wybrać ich liczbę, sposób ustawienia poszczególnych strumieni danych, parametry kompresji, harmonogram rejestracji etc. W polu obliczeń automatycznie pojawiają się informacje o przewidywanym paśmie sieciowym, o przepływnościach strumieni wizyjnych generowanych przez poszczególne grupy kamer oraz oszacowanej liczbie dysków twardych i ich niezbędnej do zapisania obrazu zgodnie z podanymi kryteriami łącznej pojemności.

Camera Design Tool – narzędzie do wizualnej symulacji obrazu z wybranego modelu kamery

Modelowanie pola widzenia za pomocą poglądowego rysunku w aplikacji WiseNet Toolbox jest niewątpliwie bardzo pomocne. Co jednak zrobić, jeśli chcemy zobaczyć, jak będzie wyglądał obraz z kamery w rzeczywistości? W takim przypadku można skorzystać z narzędzia Camera Design Tool oraz usługi Google Street View. Wystarczy wskazać wybraną



Fot. 4. Camera Design Tool w działaniu

kamerę na liście modeli kamer Hanwha, umieścić ją w pożądanym miejscu na mapie oraz ustawić ogniskową obiektywu i kąt obserwacji, aby zobaczyć obraz niemal dokładnie taki, jaki będzie widoczny z docelowej, rzeczywistej kamery.

Można też zrobić odwrotnie – na obrazie ulicy na Street View wskazać to, co chcemy obserwować, a następnie odczytać ogniskową obiektywu. Ze względu na wykorzystanie map Google do prawidłowego działania aplikacji Camera Design Tool wymagane jest połączenie z Internetem.

WiseNet Network Design Tool – rysunki, wykresy, emulacje

Ta aplikacja to ukłon w stronę projektantów i integratorów systemów. Umożliwia ona m.in. wykonanie szczegółowego schematu instalacji z wykorzystaniem gotowych, predefiniowanych symboli dla urządzeń i oprogramowania firmy

Fot. 5. WiseNet Network Design Tool

Hanwha Techwin. Filtrowanie biblioteki produktów (analogicznie jak w aplikacji WiseNet Toolbox), podgląd wszystkich parametrów aktualnie zaznaczonego urządzenia, określanie rodzaju połączeń (100 Mbps, 1 Gbps itd.), adresowania w sieci IP, parametrów transmisji, rozdzielczości, kompresji etc. to tylko niektóre ważne funkcje. Aby tworzenie rysunków było szybsze, można określać grupy urządzeń (np. zamiast umieszczania na rysunku 10 kamer wystarczy utworzenie grupy urządzeń i przypisanie jej wartości liczbowej). Wbudowany moduł raportowania automatycznie tworzy szczegółową listę urządzeń, która po uzupełnieniu o ceny jednostkowe staje się automatycznie skalkulowanym, gotowym kosztorysem systemu. Na szczególną uwagę zasługuje funkcja symulacji zajętości pasma, realizowana w postaci wykresu uzupełnionego tabelą wartości. Dla każdego elementu systemu (kamer, rejestratorów, oprogramowania etc.) podawane są szczegółowo przewidywane wartości (w Mbps) – zarówno dla transmisji przychodzącej, jak i wychodzącej (np. emulacja jednoczesnego zapisu i odtwarzania obrazu w rejestratorze). Sam schemat oraz wszystkie wyniki obliczeń i symulacji można zapisać na dysku w plikach programów Excel lub Word, w formacie PDF lub wydrukować. Całość jest uzupełniona przez moduł emulacji pracy, który już na etapie rysunku i konfiguracji wykryje nieprawidłowości i poinformuje np. o braku połączenia kamery z rejestratorem, zbyt małej pojemności dysków w stosunku do oczekiwanej długości archiwum, błędach w adresach IP etc.

WiseNet Device Manager – ułatwienie dla instalatorów

Narzędzie to pozwala na automatyczne wyszukanie podłączonych urządzeń IP, nawet gdy ich adresy należą do innej podsieci. Ponadto możliwe są operacje grupowe (na wybranych lub wszystkich urządzeniach jednocześnie), np. przypisywanie adresów IP, wykonywanie kopii zapasowej konfiguracji urządzeń i przywracanie tej konfiguracji, synchronizacja

czasu, konfiguracja parametrów wizyjnych dotyczących profili transmisji i kompresji w kamerach, diagnostyka połączeń, konfiguracja transmisji multicast czy aktualizacja oprogramowania układowego. To ostatnie zadanie może być wykonane o dokładnie wyznaczonym czasie, a także w trybie sekwencyjnym – po to, by proces aktualizacji systemu miał minimalny wpływ na ciągłość jego działania.

Fot. 6. WiseNet Device Manager w trybie podglądu obrazu i analizy pasma

Dla każdego urządzenia dostępne jest okno podglądu „na żywo" wraz z generowanymi w czasie rzeczywistym wykresami ilustrującymi liczbę generowanych klatek na sekundę i ruch aktualnie generowany w sieci. Możliwe jest także wyeksportowanie do pliku programu Excel mapy konfiguracji wszystkich zaznaczonych urządzeń, co jest nieocenioną pomocą dla osób administrujących systemem.

Online Updater – zawsze na czasie

Ciągły rozwój produktów Hanwha Techwin, wprowadzanie nowych funkcji, modeli i technik, wymaga aktualizacji parametrów i listy urządzeń, obsługiwanych przez opisywane tu narzędzia. Aby ułatwić to zadanie, stworzono aplikację Online Updater, która automatycznie sprawdza dostępność nowych wersji narzędzi, pobiera je i instaluje.

WiseNet Toolbox w wersji mobilnej – narzędzia w kieszeni

Wersja mobilna aplikacji WiseNet Toolbox działa niemal identycznie jak opisana wyżej wersja dostosowana do komputerów PC. Wersja mobilna ma inny interfejs użytkownika – dostosowany do urządzeń mobilnych. Wersję przeznaczoną do zainstalowania w systemie Android można pobrać w sklepie Google Play, natomiast wersja dostosowana do systemu iOS jest dostępna w sklepie App Store.

Fot. 7. WiseNet Toolbox w wersji mobilnej

WiseNet Installation

WiseNet Installation to aplikacja mobilna, którą stworzono specjalnie dla instalatorów kamer sieciowych Hanwha. Po instalacji kamer IP konfigurację przeprowadza się zazwyczaj z użyciem komputera i przeglądarki internetowej lub narzędzi konfiguracyjnych (np. opisanego w tym artykule programu WiseNet Device Manager). Inna metodą jest wykorzystanie serwisowego wyjścia analogowego, w które wyposażone są wybrane modele kamer Hanwha Techwin. Co jednak zrobić w przypadku, gdy pod ręką nie ma monitora, a użycie laptopa na drabinie jest uciążliwe (i oczywiście niezgodne z zasadami BHP)? WiseNet Installation umożliwia wstępne skonfigurowanie każdej z kamer za pomocą smartfonu lub tabletu. Do gniazda USB kamery należy podłączyć moduł Wi-Fi i połączyć się za jego pośrednictwem z aplikacją. WiseNet Installation współpracuje z kamerami Hanwha Techwin z serii WiseNet X wyposażonymi w złącze Micro USB, do którego można podłączyć moduł Wi-Fi USB za pomocą standardowego konwertera Micro USB/USB.

Co jeszcze?

Efekty działania opisanych aplikacji narzędziowych mogą stanowić doskonałe uzupełnienie dokumentacji projektowej lub powykonawczej, dzięki czemu instalator spędzi mniej czasu przy przysłowiowej papierkowej robocie, a klient końcowy otrzyma bardziej kompletne i szczegółowe informacje o swoim systemie.

Hanwha Techwin oferuje także wiele niezwykle przydatnych materiałów i kanałów informacyjnych, m.in. biblioteki interaktywnych symboli dla Microsoft Visio umożliwiające modelowanie pola widzenia kamer na mapach i podkładach architektonicznych, listę dysków twardych, które zostały przetestowane w laboratorium firmy Hanwha i są zalecane do współpracy z poszczególnymi rejestratorami NVR i DVR, wiele różnego rodzaju poradników i dokumentów inżynierskich, a także specjalistyczny kanał na portalu YouTube pod nazwą *HanwhaTechwinEurope*. Można nas znaleźć także na Twitterze i Linkedinie.

Wszystkie narzędzia oraz inne przydatne dla projektantów i instalatorów materiały można bezpłatnie pobrać ze strony *hanwha-security.eu* (sekcja *Wsparcie*). Więcej informacji można uzyskać u autoryzowanych dystrybutorów i bezpośrednich przedstawicieli firmy Hanwha Techwin w Polsce.

Piotr Rogalewski
Hanwha Techwin Europe

WISENET

- Najwyższej jakości sprzęt i oprogramowanie od jednego producenta
- Idealny obraz z WDR 150 dB, doskonałą czułością i stabilizacją żyroskopową
- Kompresja H.265 i technologia WiseStrem dla najlepszej efektywności transmisji i zapisu
- RAID-5/6, rejestracja awaryjna Failover n+1, automatyczne odzyskiwanie danych ARB
- Zaawansowana analityka obrazu w kamerach dzięki Open Platform
- Szyfrowane oprogramowanie układowe i pliki konfiguracyjne dla najlepszej ochrony systemu
- Bogaty zestaw aplikacji narzędziowych dla wsparcia projektantów i instalatorów
- 5-letnia gwarancja w programie partnerskim STEP

5 YEAR PARTNER'S WARRANTY

Hanwha Techwin

www.hanwha-security.eu

Obraz o rozdzielczości 4 MPX w telewizji analogowej

Patryk Gańko

„Kiedy wydawało się, że analogowe systemy telewizyjne zostaną całkowicie wyparte z rynku przez systemy IP, pojawiły się rozwiązania, dzięki którym obraz w telewizji analogowej może mieć wysoką rozdzielczość (Analog High Definition). Główne ograniczenie, jakim jest niska rozdzielczość obrazu i związana z nią słaba rozróżnialność szczegółów, zostało wyeliminowane”. Powyższym wstępem rozpocząłem artykuł poświęcony opisowi systemów AHD firmy NOVUS, opublikowany w numerze 3 magazynu *Zabezpieczenia* z czerwca 2015 roku. Po upływie dwóch lat nastąpił nowy etap rywalizacji systemów cyfrowych i analogowych

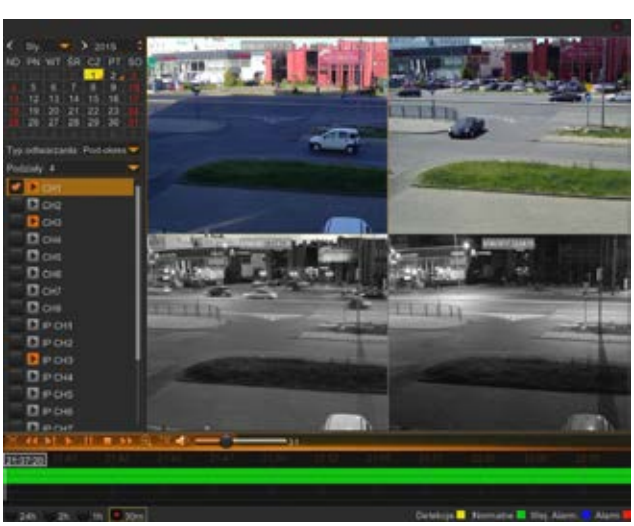
Dotychczasowy wzorzec w postaci kamer o rozdzielczości Full HD (1920x1080) został zastąpiony kamerami o rozdzielczości 4 Mpx (2592x1520). Zdecydowana większość kamer cyfrowych ma rozdzielczość 4 Mpx lub wyższą. W związku ze wzrostem rozdzielczości kamer IP stworzono system AHD marki NOVUS w wersji 3.0, w którym wytwarzany jest obraz o rozdzielczości 4 Mpx. W niniejszym artykule scharakteryzuję urządzenia stosowane w tym systemie. Wszystkie opisane poniżej modele rejestratorów generacji 3.0 obsługują funkcję Multistandard, tzn. mogą być stosowane we wszystkich analogowych systemach telewizyjnych dostępnych na rynku. Dzięki możliwości pracy w trybie AHD 4 Mpx, TVI 4 Mpx oraz CVI 4 Mpx rejestratory można zastosować w każdym analogowym systemie telewizji dozorowej bez konieczności sprawdzenia, jakiego rodzaju sygnał generują kamery. Uniwersalność tego rozwiązania wynika również z kompatybilności z systemami analogowymi 960H.

Rejestratory mogą pracować w trybie hybrydowym, umożliwiając równoczesne podłączenie kamer analogowych i kamer IP. Maksymalna rozdzielczość kamer IP wynosi 2688x1520.

Rys. 1

Pracujący w trybie hybrydowym 16-kanałowy rejestrator NHDR-4M5316AHD może obsługiwać maksymalnie 16 kanałów analogowych o rozdzielczości 4 Mpx i maksymalnie osiem kanałów IP. W przypadku modelu ośmiokanałowego NHDR-4M5308AHD tryb hybrydowy pozwala na dodatkową rejestrację czterech kanałów IP, natomiast w trybie IP, przy wyłączonych kanałach analogowych, istnieje możliwość rejestracji maksymalnie dwunastu kanałów IP. Szczegółowy opis wszystkich trybów pracy poszczególnych rejestratorów jest zawarty w kartach katalogowych urządzeń.

Rejestratory w wersji 3.0 umożliwiają zapis z prędkością do 15 kl./s dla każdego kanału o rozdzielczości 4 Mpx i 25 kl./s dla niższych rozdzielczości. Przy średniej przepływności strumienia



Rys. 2

wizyjnego równej 6 Mbit/s dla kanałów analogowych i IP ogromnym wyzwaniem jest zapewnienie odpowiedniego czasu archiwizacji. W modelach ośmio- i szesnastokanałowych można zamontować do dwóch dysków twardych, a każdy z nich może mieć maksymalną pojemność 8 TB. Dodatkowo wszystkie modele zostały wyposażone w złącze e-SATA do podłączenia zewnętrznych macierzy dyskowych. W rekomendowanym kompatybilnym urządzeniu NV-5000EST-H4 można zamontować cztery dyski o sumarycznej pojemności 32 TB. Tak rozszerzona pamięć jest zarządzana poprzez menu rejestratora w ten sam sposób jak wewnętrzne dyski. Rejestratory umożliwiają indywidualne przyporządkowanie kanałów do wybranych dysków. Dzięki temu można zróżnicować wielkość archiwum dla wybranych kanałów w zależności od pojemności dysku twardego i liczby przyporządkowanych do niego kamer. W celu poprawy bezpieczeństwa danych rejestracja obrazów z kamer może być zdublowana na dwóch lub więcej dyskach, tzn. możliwy jest zapis lustrzany. W takim trybie rejestracji awaria jednego z dysków nie powoduje utraty danych (Rys. 3).

Rys. 3

Rys. 4

W wyniku cyfrowej obróbki sygnału analogowego wszystkie modele rejestratorów tworzą dodatkowy strumień wizyjny o niższej rozdzielczości (do wyboru m.in. CIF, VGA, D1). Służy to przede wszystkim do redukcji obciążenia sieci przy połączeniach mobilnych w trybie podglądu na żywo i odtwarzania.

W celu optymalnego wykorzystania archiwum w rejestratorach zaimplementowano funkcję zmiany parametrów rejestrowanych strumieni wizyjnych dla zdarzeń alarmowych. Pozwala to na rejestrację strumieni wizyjnych o niskiej jakości w przypadku braku zdarzeń alarmowych i o wysokiej jakości w przypadku wystąpienia zdarzeń alarmowych (wykrycia ruchu, aktywacji wejścia alarmowego).

Bezpieczeństwo procesu archiwizacji zostało poprawione dzięki analizowaniu zagrożeń, tzn. czynników mogących zakłócić bezawaryjną pracę dysku, poprzez odbieranie komunikatów dyskowych SMART w rejestrze zdarzeń rejestratora (Rys. 4).

W celu sprawnego wyszukiwania zarejestrowanych zdarzeń zaimplementowano funkcję odtwarzania dowolnego strumienia wizyjnego z różnych okresów, w wielu oknach podziału. Pozwala to na redukcję czasu pracy osób obsługujących system (Rys. 2).

Rejestrator współpracuje z monitorami z wejściami HDMI i VGA. Maksymalna rozdzielczość wyświetlanego obrazu jest równa 4K, czyli 3840x2160 pikseli.

Asortyment oferowanych rejestratorów uzupełniają dwie 4-megapikselowe kamery nowej generacji – wandaloodporna kamera kopułowa NVAHD-4DN3202V/IR-1 oraz kamera w obudowie NVAHD-4DN3202H/IR-1 (Rys.1). W przypadku powszechnie stosowanego kabla koncentrycznego o impedancji falowej 75 Ω zasięg podczas transmisji sygnału z kamer 4 Mpx wynosi 350 m. Sygnał ma charakter analogowy, dlatego możliwa jest transmisja graniczna na większą odległość, ale wiąże się to z pogorszeniem jakości i rozdzielczości obrazu. Składowe wysokoczęstotliwościowe takiego sygnału, odpowiadające za odwzorowanie najmniejszych detali obrazu, są najsilniej tłumione. W przypadku kabla koncentrycznego RG6 zasięg ten jest większy i wynosi 500 m. Nie zaleca się stosowania kabla UTP do transmisji sygnału ze względu na ograniczony zasięg takiej transmisji i brak kompatybilnych konwerterów.

Powyższe kamery mogą być konfigurowane z poziomu rejestratorów z wykorzystaniem protokołu COAX, co upraszcza proces regulacji kamer. Równolegle z kamerami, w celu zapewnienia prostego i szybkiego montażu, wprowadzone zostały adaptery montażowe.

Nie sposób obecnie wyrokować, jak w przyszłości ukształtuje się relacja między systemami IP oraz analogowymi. Ważną przyczyną popularności systemów analogowych jest – obok niższej ceny – to, że nie jest potrzebna wiedza na temat budowy sieci, a także prostota instalacji. W przypadku systemów składających się z maksymalnie szesnastu kamer z pojedynczym punktem nadzoru systemy AHD jeszcze długo pozostaną korzystną alternatywą dla systemów IP.

Patryk Gańko
AAT HOLDING

AHD TECHNOLOGY by NOVUS®

MULTI STANDARD

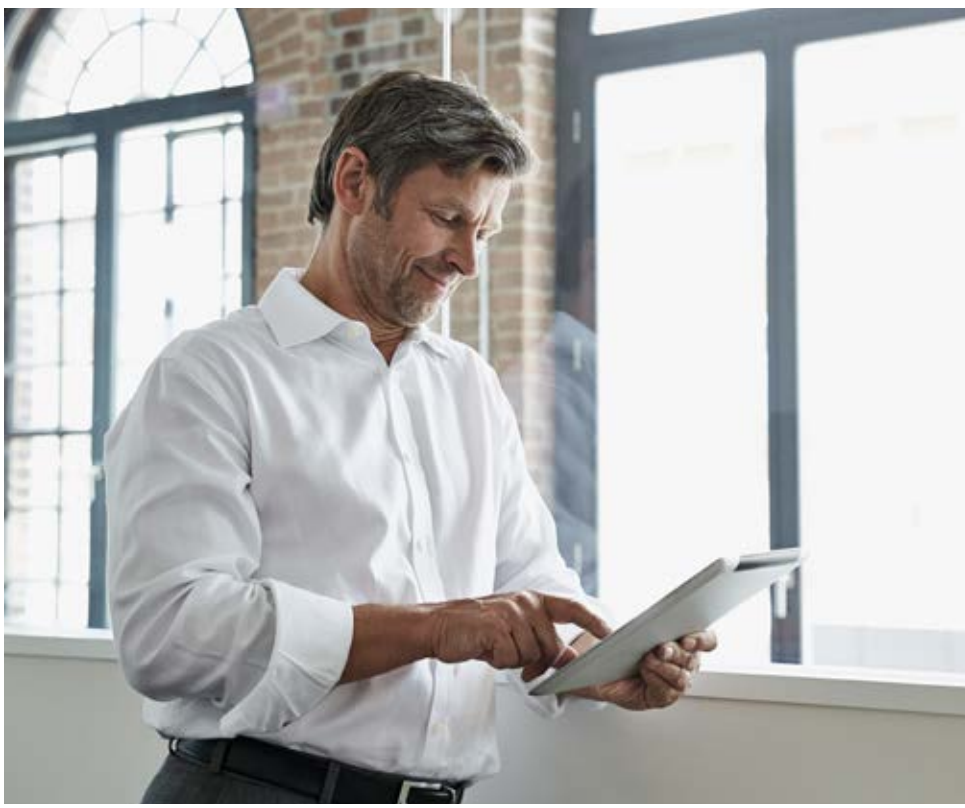
MULTISTANDARD – JEDNA KAMERA WIELE MOŻLIWOŚCI PODŁĄCZENIA

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

Remote Services firmy Bosch
usługi zdalnego nadzoru i konserwacji

Jakub Bednarz

Internet rzeczy (ang. *Internet of things* – IoT) podlega dynamicznemu rozwojowi i obejmuje coraz szerszy zakres urządzeń. Inteligentne urządzenia pomiarowe czy linie produkcyjne, a nawet sprzęty domowe stają się współczesnym standardem. Zdalny dostęp do informacji, na którym oparta jest koncepcja IoT, pozwala podejmować szybkie i trafne decyzje, zwiększa wydajność pracy oraz poprawia jej komfort. Wszystko to po to, aby zoptymalizować przebieg różnych procesów i wykonywane zadania oraz szybciej podejmować właściwe decyzje na podstawie aktualnych danych



Systemy bezpieczeństwa stanowią podstawę automatyki nowoczesnych budynków. Aby w pełni efektywnie nimi zarządzać, potrzebne są narzędzia do łatwej analizy danych. Obecnie zadanie to pełnią systemy BMS (Building Management System) oraz SMS (Security Management System), ale wymagają one obsługi i ciągłej obecności obsługujących je osób. Udostępnianie bieżących informacji firmom zewnętrznym – zajmującym się instalacją czy konserwacją systemu – było dotychczas zaniedbywane. Związane z tym wydłużenie czasu instalacji czy opóźnienie reakcji serwisowej może spowodować niezadowolenie klienta końcowego. Czy można temu zaradzić?

Remote Services to pakiet trzech usług zapewniających stały dostęp do aktualnych informacji dotyczących m.in. systemów sygnalizacji pożarowej.

Remote Connect

Remote Connect to usługa zdalnego połączenia się z centralą systemu sygnalizacji pożarowej. Dzięki niej z dowolnego miejsca, w którym jest dostęp do sieci można połączyć się i uzyskać bieżące informacje na temat pracy systemu (pełny podgląd ekranu kontrolera). Narzędzie to znajduje zastosowanie na każdym z etapów życia systemu. Podczas instalacji umożliwia programowanie centrali pożarowej nie tylko w bezpośrednim kontakcie z nią, ale również zdalnie, w dowolnym miejscu –

Rys. 1. Remote Connect

przez Internet. Dzięki temu w przypadku powiększenia instalacji i objęcia nią kolejnych stref budynku aktualizację i testy programu centrali można przeprowadzić na obszarze, którego te zmiany dotyczą. W znacznym stopniu przyśpiesza to programowanie centrali. Dostępna jest również funkcja *Automatyczne sczytywanie*, dzięki czemu ponowne sczytywanie i wykrywanie błędów w okablowaniu pętli dozorowej jest możliwe w dowolnym miejscu w budynku, bez konieczności przemieszczania się do pomieszczenia, w którym znajduje się centrala, i z powrotem. Dzięki usłudze Remote Connect i funkcji *Zapal diodę LED* możliwa jest również ręczna aktywacja diody w wybranej czujce. Dzięki temu łatwo można zweryfikować czy opis czujki w programie jest zgodny z miejscem jej instalacji. Narzędzie to ułatwia również konserwację systemu. W razie wystąpienia awarii pracownik serwisu może w dowolnym miejscu przeanalizować problem zgłaszany przez centralę dzięki możliwości zdalnego wglądu w szczegóły dotyczące usterki. Umożliwia to ograniczenie wyjazdów, dotychczas potrzebnych ze względu na konieczność ustalenia przyczyny problemu, i przygotowanie się do naprawy już podczas pierwszej wizyty w obiekcie. Modyfikacje istniejącego systemu – np. dodawanie czujek w środku pętli dzięki wymienionym narzędziom instalacyjnym – również stają się szybsze.

Remote Maintenance

Usługa zdalnego serwisu to narzędzie dostępne w chmurze

Rys. 2. Remote Maintenance

przez portal WWW. Szczegółowe informacje na temat systemu, obejmujące między innymi listę zainstalowanych urządzeń wraz ze szczegółami dotyczącymi ich aktualnego stanu, są dostępne za pośrednictwem dowolnych urządzeń typu smartfon czy tablet i przeglądarki internetowej. Użytkownik może uzyskiwać raporty serwisowe, które są generowane na podstawie informacji automatycznie zbieranych przez system, m.in. zawierających numery seryjne czujek i dotyczących stopnia ich zabrudzenia. Znacznie ogranicza to czas potrzebny na tworzenie dokumentacji i raportów, a użytkownik końcowy zyskuje wiarygodne i aktualne dane.

Remote Alert

Remote Alert to usługa, która zapewnia stały i natychmiastowy dostęp do informacji na temat pracy systemu. W przypadku wystąpienia zdarzenia alarmowego, awarii lub utraty łączności z chmurą danych określeni użytkownicy otrzymują automatyczne powiadomienia SMS oraz e-mail. Serwis jest w stanie zareagować natychmiast po wystąpieniu problemu, niezależnie od obecności obsługi w budynku. Użytkownik końcowy

Rys. 3. Remote Alert

wie, czy system pracuje poprawnie, a w przypadku wykrycia zagrożenia pożarowego natychmiast otrzymuje informacje.

Jakub Bednarz
Bosch Security Systems

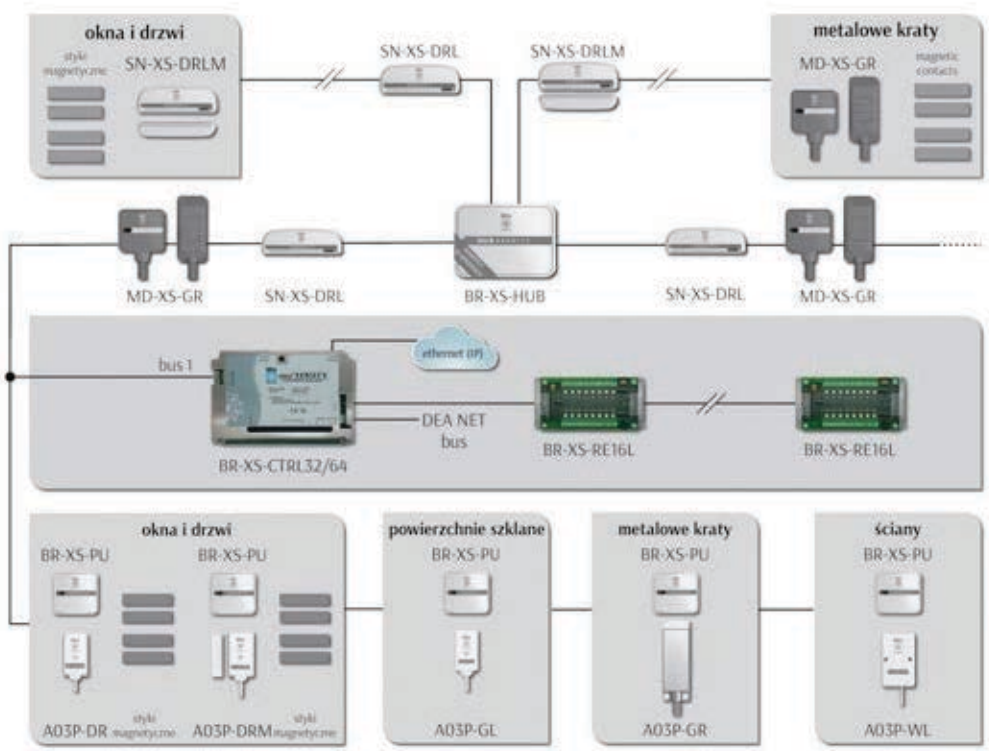
Zasada działania zapalniczki, a sprawne systemy wykrywania włamań na terenie budynku

Maciej Prelich

Zabezpieczenie biura czy prywatnej posesji oraz przestrzeni wewnątrz budynków, szczególnie tych wysokich, gdzie chroniona infrastruktura jest tylko częścią biura, jest wyzwaniem. Najważniejszym kryterium wyboru systemu jest jego skuteczność, jednak musi on być również przystosowany do połączenia z innymi systemami w budynku. Możliwe, że każde biuro będzie stanowiło osobny fragment systemu lub element większej infrastruktury całego budynku

Istnieje wiele systemów zabezpieczających. Najprostsze z nich to zamki szyfrowe, jednak w przypadku biur i cennej infrastruktury ważne jest zastosowanie systemów o znacznie większej skuteczności. Innym klasycznym rozwiązaniem może być system wizyjny, jednak wymaga on integracji z innymi urządzeniami.

W celu ochrony przed intruzami w budynku potrzebne jest zabezpieczenie szczególnie wrażliwych elementów, takich jak okna, drzwi, świetliki czy metalowe kraty. Jedna z metod detekcji wtargnięcia do budynku wykorzystuje zjawisko piezoelektryczne, które zostało po raz pierwszy zbadane przez braci Pierre'a i Jacques'a Curie w roku 1880. Zjawisko to zaczęto wykorzystywać w praktyce dużo później. W 1917 roku Paul Langevin wraz ze współpracownikami stworzyli pierwszy ultradźwiękowy detektor łodzi podwodnych składający się z miniaturowych kryształów kwarcu umieszczonych pomiędzy dwiema stalowymi płytkami oraz hydrofonu, który odbierał sygnały akustyczne w wodzie. Innym popularnym przedmiotem wykorzystującym to zjawisko jest zapalniczka. Po naciśnięciu przycisku powstaje iskra, która zapala paliwo.



Rys. 1. Schemat systemu Xensity

Detekcja drgań za pomocą czujek piezoelektrycznych polega na przetworzeniu sił działających na przetworniki na napięcie elektryczne. Rysunek 2 przedstawia schemat działania takiej czujki.

Czujki z elementami piezoelektrycznymi znajdują zastosowanie w układach służących do pomiaru sił, amplitudy drgań, prędkości ruchu lub ciśnienia. Ten szeroki zakres zastosowań jest rezultatem ich wielu zalet. Rozwój technologii produkcji materiałów piezoelektrycznych jest związany z ich właściwościami mechanicznymi. Wartość modułu Younga tych materiałów jest relatywnie duża, podobnie jak w przypadku metali. Mimo iż czujki piezoelektryczne są elementami reagującymi na ściskanie, nie wykazują one trwałych odkształceń nawet w przypadku długiego oddziaływania znacznych sił ściskających. Niektóre z materiałów piezoelektrycznych mogą pracować w temperaturze dochodzącej do 1000°C. Dodatkowo czujniki są niewrażliwe na pole elektromagnetyczne i promieniowanie korpuskularne, co umożliwia ich stosowanie w trudnych warunkach środowiskowych.

Dzięki swoim zaletom materiały piezoelektryczne mają wiele zastosowań. Są wykorzystywane m.in. w urządzeniach medycznych, akcelerometrach w telefonach komórkowych, urządzeniach służących do ochrony perymetrycznej, czujnikach w silnikach Diesla, drukarkach i mikroskopach. Pokonywanie zabezpieczeń mechanicznych jest związane z wywoływaniem drgań, a efekt piezoelektryczny jest bardzo pomocny w ich wykrywaniu.

Od lat czujki piezoelektryczne są z powodzeniem stosowane w systemach ochrony perymetrycznej obiektów o podwyższonym ryzyku, takich jak bazy wojskowe, lotniska czy elektrownie. Pionierem w tej dziedzinie jest firma DEA, która, bazując na wieloletnim doświadczeniu, wprowadza również system ochrony wnętrz budynków Xensity, który wykorzystuje tę technikę. System ten pracuje niezawodnie dzięki indywidualnej identyfikacji czujek (Point ID) umożliwiającej dokładną lokalizację intruzów. Ważne są także funkcje autodiagnostyczne czujek. Ponadto system może być zdalnie zarządzany poprzez sieć IP oraz można go połączyć z wcześniej wdrożonym, innym systemem alarmowym.

Xensity wykorzystuje czujki piezoelektryczne do ochrony drzwi, okien, świetlików i metalowych krat. Informuje o wstrząsach, próbach rozbicia, otwarcia lub przecięcia. Wszystkie czujki są adresowalne. Każda z nich zawiera przetwornik piezoceramiczny, który dzięki specjalnie opracowanym algorytmom

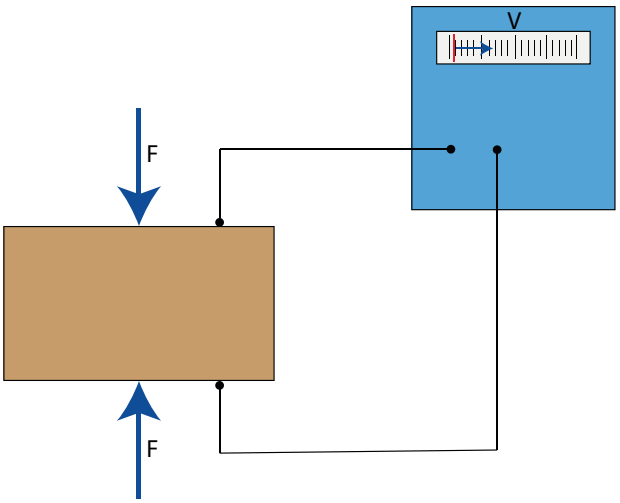
pozwala osiągnąć bardzo wysoką czułość detekcji oraz odporność na fałszywe alarmy. Rysunek 1 przedstawia schemat przykładowej instalacji.

Warto zauważyć, że czujki zostały skonstruowane tak, aby uwzględniać różnorodność materiałów stosowanych w budownictwie. Te przeznaczone do ochrony okien nadają się do każdego rodzaju szkła, w tym szkła hartowanego, laminowanego szkła klejonego oraz szyb kuloodpornych. Opcjonalny interfejs pozwala zabezpieczyć ściany żelbetowe, sejfy oraz szafy pancerne. Czujki są instalowane po wewnętrznej stronie zabezpieczanych obiektów, co utrudnia działania sabotażowe.

Komunikacja między czujkami jest możliwa dzięki specjalnym płytkom kontrolnym. Najbardziej skomplikowany wariant pozwala na zarządzanie 128 czujkami. Dzięki temu możliwa jest łatwa konfiguracja i monitorowanie systemu za pomocą komputera podłączonego lokalnie lub skonfigurowanego do pracy zdalnej. Niezależnie od połączenia system umożliwia kalibrację czujek, kontrolę ich statusu, wgląd w historię alarmów oraz monitorowanie pracy.

System Xensity może być podłączony do innych urządzeń za pomocą opcjonalnego interfejsu XS-PU oraz umożliwia zarządzanie zewnętrznymi sygnałami alarmowymi pochodzącymi z innych systemów.

Interfejs użytkownika został zaprojektowany w sposób maksymalnie ułatwiający szybką obsługę systemu oraz łatwy dostęp do najważniejszych informacji. Stan systemu oraz wszystkich podłączonych elementów (czujek, interfejsów, rozszerzeń przekaźnikowych) może być zwizualizowany w postaci drzewa lub macierzy. W oknie związanym z danym elementem widoczny jest zestaw narzędzi do kalibracji, programowania oraz testowania każdej z czujek. Konfiguracja umożliwia uwrażliwienie lub uniewrażliwienie czujek (każdej z osobna) na różnego rodzaju pobudzenia, w tym słabe uderzenia, silne uderzenia, sabotaż linii, sabotaż obcym polem magnetycznym oraz alarm ze styków sabotażowych. Ponadto oprogramowanie pozwala ustawić poziom czułości detekcji, poziom ochrony oraz manualnie uruchomić procedury autodiagnostyczne dla każdej z czujek.



Rys. 2. Schemat działania czujki piezoelektrycznej

Maciej Prelich
Firma ATLine sp.j. Sławomir Pruski

dahua TECHNOLOGY

4K Now Available over COAX

Leading end-to-end 4K Ultra HD over Coax

HDCVI 4.0 4K

- Kamera kompaktowa 4K: doskonała jakość obrazu dzięki przetwornikowi Starlight+ o rozmiarze 4/3”
- Kamery tulejowe i kopułowe 4K: zasięg podczerwieni 100m / 50m, wysoki stopień ochrony IP67 i IK10
- Wieloprzetwornikowa kamera panoramiczna: widok 180° oraz obraz 3x 2 Mpx jednocześnie
- Kamera Fisheye 4K: panoramiczny widok 360°, 10 trybów prostowania obrazu z HCVR
- HCVR: kompatybilność wsteczna ze wszystkimi kamerami HDCVI
- Transmisja do 500 m przez RG59 oraz do 300 m przez CAT5e, łatwość rozbudowy istniejących systemów

HAC-HF3805G
4/3’’ 4K HDCVI
Kamera Starlight+

HAC-HFW3802E-Z
4K HDCVI WDR
Kamera tulejowa IR

HAC-PFW3601-A180
4K HDCVI Multi-sensor
Kamera Panoramiczna IR

HAC-EBW3802
4K HDCVI
Kamera Fisheye IR

HAC-HDBW3802E-Z
4K HDCVI WDR
Kamera kopułowa IR

HCVR7000-4K
Rejestrator 4K HDCVI

CE FC RoHS 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

Ewolucja
popularnych systemów alarmowych

Michał Konarski

Obserwując branżę systemów alarmowych, trudno od razu dostrzec istotne zmiany funkcji lub techniki w sprzęcie obecnym w porównaniu do sprzętu sprzed 10–15 lat. Mimo iż zmiany nie są tak dynamiczne jak chociażby w przypadku telewizji dozorowej, nie można powiedzieć, że branża się nie rozwija

Jak wyglądał typowy system alarmowy dla indywidualnego użytkownika instalowany na początku XXI wieku? Mógł składać się z centrali alarmowej wyposażonej w dialer telefoniczny. Do tej centrali podłączone były klawiatury z diodami LED lub (w wariancie „rozbudowanym") z tekstowym wyświetlaczem LCD. Mógł zawierać czujki ruchu PIR, dualne czujki PIR+MW oraz przeznaczone do ochrony obwodowej kontaktronowe czujki otwarcia drzwi i okien. Urządzeniem sygnalizującym naruszenie obiektu był sygnalizator optyczno-akustyczny z palnikiem ksenonowym.

dysponuje wielokrotnie większą mocą obliczeniową niż topowy komputer biurkowy z początku XXI wieku. A jak na tym tle wypada typowy współczesny system alarmowy?

Przede wszystkim zmianie ulega sposób interakcji człowieka z systemem. Wciąż główną rolę pełni klawiatura – takie rozwiązanie doskonale sprawdza się w praktyce, głównie ze względu na bezpieczeństwo. Obecnie raczej nie stosuje się klawiatur z diodami LED. Są stosowane tylko w najprostszych systemach. Sprawdzały się dość dobrze w systemach typu „włącz/wyłącz", ale poprawne ustawienie daty i godziny było uciążli-

W tym czasie na ulicach wciąż jeździło sporo polonezów, a golf III wywoływał niemałe wrażenie. W kieszeni podążającego za trendami spoczywała nokia 3310, z której należało korzystać raczej oszczędnie, ponieważ koszty połączeń były wciąż niemałe. Szczytem techniki domowej był komputer z procesorem Pentium IV i monitorem kineskopowym.

17 lat później hybrydowe modele aut nie robią na nikim szczególnego wrażenia, a współczesny smartfon klasy średniej

wym zadaniem wymagającym sięgania po instrukcję. Manipulatory z wyświetlaczami tekstowymi również powinny powoli odchodzić do lamusa, a ich miejsce mogą zająć dużo bardziej czytelne i bardziej intuicyjne w obsłudze modele z graficznym interfejsem użytkownika. Wprawdzie podstawowa rola klawiatury w systemie alarmowym pozostała niezmieniona, ale wygodny interfejs graficzny ułatwia użytkownikowi korzystanie z bardziej rozbudowanych funkcji systemu. Wygodna

obsługa nie jest zarezerwowana wyłącznie dla dużych i kosztownych systemów z kolorowymi panelami dotykowymi, ale staje się dostępna nawet w prostszych i tańszych systemach. Taka zmiana staje się możliwa dzięki stale rosnącym możliwościom mikrokontrolerów – serc cyfrowych urządzeń takich jak manipulator. W porównaniu ze sterowaniem świecącymi diodami czy obsługą wyświetlaczy tekstowych wyświetlanie grafiki (ikon czy pełnoekranowych, interaktywnych menu ułatwiających programowanie) wymaga nie tylko znacznie większej pamięci, ale także większej szybkości przetwarzania. Wszystko to jest potrzebne, by uzyskać atrakcyjny interfejs, który będzie szybko reagować na polecenia użytkownika.

Mówiąc o interakcji użytkownika z systemem, nie sposób przemilczeć komunikacyjnej „rewolucji", która faktycznie już się odbyła. Dziś już niewiele osób korzysta prywatnie z tradycyjnej linii telefonicznej (PSTN) w celu utrzymywania kontaktu z innymi. Tę rolę przejęła bardzo rozpowszechniona telefonia komórkowa (GSM). Nie tylko zmienia się technika łączności, ale również ewoluował sposób dostępu do informacji. Nowoczesne telefony komórkowe przyzwyczaiły swoich użytkowników do łatwego dostępu do wszelkich informacji w dowolnej chwili i w każdym miejscu.

Naturalną konsekwencją tych zmian stały się również oczekiwania użytkowników dotyczące interakcji z systemem alarmowym. Proste poinformowanie o alarmie za pomocą połączenia telefonicznego lub lakonicznego SMS-a – za pośrednictwem „uniwersalnego" nadajnika GSM przyłączonego do centrali – często nie jest już dla użytkowników wystarczające. Świadomi użytkownicy coraz częściej oczekują szczegółowych informacji, a także możliwości zdalnego sterowania swoim systemem. Taką funkcję mogą zaoferować jedynie systemy z wbudowanym komunikatorem GSM oraz te, które są przystosowane do wyposażenia w specjalistyczne, opcjonalnie podłączane komunikatory komórkowe. Przysłowiową „wisienką na torcie" mogą być funkcje zarządzania kartami bezabonamentowymi typu prepaid, dzięki którym można radykalnie ograniczyć koszty utrzymania systemu powiadamiania, utrzymując przy tym kontrolę nad kontem powiązanym z kartą SIM.

Przejście na całkowicie cyfrowy sposób łączności, jakim jest komunikacja przez sieć GSM/GPRS, niesie za sobą również zmianę w zakresie komunikacji systemu alarmowego ze stacją monitorującą. Trzeba przyznać, że wcześniej wykorzystywane w tym celu protokoły wymagające komutowanego połączenia i przesyłające informację w postaci dźwięku wciąż są w użyciu, głównie z powodu ich szerokiego rozpowszechnienia i w miarę dobrej standaryzacji. Większe możliwości oferują jednak systemy w pełni cyfrowej transmisji wykorzystujące protokoły IP. Umożliwiają nie tylko przesyłanie rozszerzonych informacji diagnostycznych, ale także np. stosowanie szyfrowania w celu poprawy bezpieczeństwa i integralności przesyłanych danych. Takie rozwiązania są również dobrze uzasadnione ekonomicznie – większość operatorów sieci GSM ma w swojej ofercie dla dużych odbiorców atrakcyjne cenowo pakiety kart SIM przeznaczone do transmisji danych, których wykorzystanie staje się najtańszym sposobem na utrzymanie kanału łączności pomiędzy obiektem chronionym i stacją monitorowania alarmów.

Kolejną dużą zmianą, która w istotny sposób wpływa na systemy alarmowe, jest sposób połączenia elementów systemu. Do niedawna jedynie połączenie przewodowe, np. czujek, było traktowane jako pewne i niezawodne. Wynikało to w dużej mierze z mankamentów wczesnych technik bezprzewodowych stosowanych w systemach alarmowych. Jednokierunkowa łączność w „przeciążonym" (przez liczne nielicencjonowane urządzenia) paśmie 433 MHz, popularna w niedrogich, często amatorskich systemach, negatywnie wpłynęła na ocenianie łączy bezprzewodowych przez fachowców zajmujących się systemami zabezpieczeń. Na szczęście znacznie bardziej nowoczesne rozwiązania wykorzystujące dwukierunkową, nadzorowaną łączność w pasmie 868 MHz przywróciły zaufanie do łączności radiowej w systemach alarmowych. Dlaczego na szczęście? Odpowiednie ułożenie instalacji niezbędnej do funkcjonowania systemu alarmowego wymaga kosztownej i uciążliwej ingerencji w jego strukturę. Prawidłowe ułożenie okablowania w zasadzie jest możliwe jedynie przy okazji wykonywania gruntownego remontu, a i to wymaga od inwestora skontaktowania się w odpowiednim momencie z wykwalifikowanym instalatorem, który pomoże wykonać stosowny projekt instalacji. Rozwiązania stosowane na późniejszym etapie, często kompromisowe (projektowane pod kątem względnie łatwego rozmieszczenia okablowania, a nie zamontowania urządzeń we właściwych miejscach), dają równie kompromisowe rezultaty. Możliwość dużo szybszego i „czystszego" montażu urządzeń łączących się bezprzewodowo może w efekcie zaowocować systemem skuteczniejszym i bardziej niezawodnym.

Największą elastycznością charakteryzują się nowoczesne rozwiązania hybrydowe, łączące tradycyjne połączenia przewodowe tam, gdzie są one dostępne, i elementy komunikujące się bezprzewodowo w miejscach, gdzie nie zostało doprowadzone okablowanie. Takie systemy można łatwo dostosować do wymagań. W końcu kto chociaż raz nie miał do czynienia z tym, że idealnie dobrane na etapie stanu surowego miejsce montażu czujki zostało później zabudowane szafą?

Jakie będą kolejne, przyszłe kierunki rozwoju branży? Na pewno można spodziewać się jeszcze bardziej ścisłej integracji systemu alarmowego z urządzeniami mobilnymi, które stają się przedmiotami pierwszej potrzeby dla coraz większej liczby osób. Być może dzięki funkcjom mającym poprawić bezpieczeństwo (takim jak wbudowane czytniki biometryczne, systemy analizy obrazu czy systemy uwierzytelniające) nowoczesne smartfony staną się podstawowym narzędziem służącym do obsługi systemu alarmowego. Później branża alarmowa zapewne zamieni komunikację z wykorzystaniem GSM 2G na standard 3G lub 4G – w miarę wzrostu dostępności odpowiednich modułów komunikacyjnych. Nieuchronna staje się też tendencja do zwiększania liczby funkcji systemów.

Na powyższych przykładach widać wyraźnie, że branża ewoluuje. Zmiany nie są może tak dynamiczne jak w przypadku urządzeń powszechnego użytku, ale jest to spowodowane głównie dużo wyższymi wymaganiami dotyczącymi niezawodności systemów alarmowych. Kończy się żywotność systemów zainstalowanych 10–15 lat temu, dlatego być może warto rozważyć ich wymianę na urządzenia bardziej nowoczesne przy okazji remontu czy przeglądu okresowego. Prostsza i bardziej intuicyjna obsługa, a także większe możliwości komunikacyjne zrekompensują właścicielowi jednorazowy wydatek.

Michał Konarski

25 lat
największych w Polsce spotkań
projektantów, rzeczoznawców, instalatorów i konserwatorów systemów sygnalizacji pożarowej (Część 1)

mgr inż. Mariusz Radoszewski

Nie tak dawno temu odbyły się 20. Ogólnopolskie Warsztaty Systemy Sygnalizacji Pożarowej, a już w tym roku odbędzie się ich 25. edycja. I choć minęło dopiero pięć lat, obfitowały one w wiele niezwykle ważnych wydarzeń mających ogromny wpływ na rozwój firmy Polon-Alfa

Geneza warsztatów

W latach osiemdziesiątych ubiegłego wieku usługi związane z projektowaniem, instalowaniem i konserwacją instalacji sygnalizacji pożarowej świadczyły głównie Przedsiębiorstwa Handlowo-Techniczne Sprzętu Pożarniczego i Ochronnego „Supon". Nasz kraj był podzielony na dwanaście obszarów obsługiwanych przez 12 przedsiębiorstw należących do zjednoczenia Supon, mających siedziby w największych polskich miastach. Zjednoczenie prowadziło negocjacje z producentami i dostawcami wyrobów, którymi handlowało, np. sprzętu ochronnego BHP, gaśnic, a także urządzeń sygnalizacji pożarowej. Jego działalność objęła także np. podjęcie próby opracowania jednolitych wytycznych projektowania, wykonawstwa, odbioru i konserwacji instalacji i urządzeń SAP. Pierwszy taki materiał powstał w już 1984 roku.


1993


1995

1995

1998


2002

Podobną działalność, ale tylko w odniesieniu do systemów sygnalizacji pożarowej, prowadziło także zjednoczenie Polon dla swoich siedmiu zakładów.

Zjednoczenie Supon zapraszało co roku przedstawicieli ówczesnych krajowych producentów urządzeń sygnalizacji pożarowej – firm Polon i Telfa z Bydgoszczy – na coroczne spotkania projektantów i instalatorów celem omówienia bieżących problemów związanych z sygnalizacją pożarową oraz wysłuchania informacji na temat nowych urządzeń. W wyniku przemian społeczno-gospodarczych zjednoczenia Supon i Polon zostały rozwiązane, a wywodzące się z nich zakłady zaczęły się usamodzielniać. Niektóre z nich postanowiły się sprywatyzować, część nie miała pomysłu na funkcjonowanie w nowych warunkach i ogłosiła upadłość. Zwolnieni z nich lub odchodzący z branży specjaliści zaczęli zakładać własne firmy. Na polski rynek zaczęło napływać coraz więcej sprzętu z importu, więc krajowi producenci poczuli się zagrożeni konkurencją.

Wtedy właśnie w bydgoskim Polonie narodził się pomysł przejęcia roli organizatora corocznych spotkań firm instalujących i konserwujących, a przy okazji wypromowania wdrażanych nowości z zakresu sygnalizacji pożarowej. Na przełomie lat osiemdziesiątych i dziewięćdziesiątych kilka takich spotkań odbyło się w Ośrodku Wypoczynkowym firmy Polon-Alfa w Sokolu-Kuźnicy nad Zalewem Koronowskim. Na spotkania te zaproszeni byli także przedstawiciele drugiego producenta z Bydgoszczy – firmy Telfa.

Narodziny Ogólnopolskich Warsztatów „Zacisze"

Warunki w ośrodku w Sokolu-Kuźnicy niestety nie były najlepiej dostosowane do trzydniowych spotkań. Nieduża liczba miejsc noclegowych, dość spartańskie warunki, brak funkcjonującej kuchni oraz niewielka salka konferencyjna ograniczały liczbę uczestników do jednego z każdej firmy. Chętnych nieustająco przybywało, dlatego kierownictwo firmy Polon-Alfa podjęło decyzję o przeniesieniu spotkań do leżącego także nad Zalewem Koronowskim Ośrodka Doskonalenia Kadr Służby Więziennej „Zacisze" w Suchej koło Klonowa. Pierwsze spotkanie w nowym miejscu – pod nazwą *Ogólnopolskie Spotkanie Instalatorów Sygnalizacji Pożarowej* – odbyło się na początku października 1993 roku. Uczestniczyło w nim 107 osób z 67 firm z całej Polski. Z roku na rok liczba uczestników systematycznie wzrastała. Czwarte z kolei spotkanie, w 1996 roku, miało nową nazwę – *Ogólnopolskie Warsztaty Systemy Sygnalizacji Pożarowej „Zacisze"*. Spotkania o tej nazwie odbywały się aż do 2009 roku. Każde warsztaty były poświęcone innemu tematowi wiodącemu, a zbiory referatów wygłoszonych przez specjalistów były publikowane w broszurze, którą otrzymywał każdy uczestnik. W odbywających się w ośrodku Zacisze warsztatach uczestniczyło blisko 180 osób z branży zabezpieczeń przeciwpożarowych z całej Polski.

Początkowo warsztaty odbywały się wczesną jesienią, na przełomie września i października, natomiast od 1997 r., na prośbę uczestników, zostały przeniesione na pierwszą połowę

CDN

POLON-ALFA

czerwca. Mimo iż w pierwszych dniach października bywało nieraz chłodno, zawsze – czy to jesienią, czy wiosną – piękna sceneria Borów Tucholskich i Zalewu Koronowskiego przyczyniała się do niepowtarzalnej atmosfery spotkań i wywierała niezatarte wrażenia estetyczne.

W związku z modernizacją bazy lokalowej, a tym samym polepszeniem warunków pobytowych w Zaciszu, zmniejszeniu uległa liczba miejsc noclegowych. I choć Zacisze miało swój niepodważalny urok i unikalną atmosferę (którą do dzisiaj wspominają najstarsi bywalcy), musieliśmy podjąć trudną decyzję o zmianie miejsca organizowania warsztatów. Od 2010 roku imprezy są organizowane w atrakcyjnych hotelach i ośrodkach wypoczynkowo-rekreacyjnych na terenie całego kraju.

Fot. 1. Zbiory referatów z lat 1996–2016

Uczestników warsztatów gościła m.in. Dolina Charlotty, hotele Molo i Magellan nad Zalewem Sulejowskim, a przez ostatnie trzy lata GrandHotel Tiffi w Iławie. Zmiana miejsca przyniosła również zmianę nazwy spotkań na *Ogólnopolskie Warsztaty „Sygnalizacja i Automatyka Pożarowa SAP"*. W tym roku, z okazji 25-lecia naszych spotkań, zaprosiliśmy naszych przyjaciół na Zamek Biskupi w Janowie Podlaskim. Mamy nadzieję, że to wyjątkowe miejsce będzie sprzyjać świętowaniu tego pięknego jubileuszu.

Uczestnicy warsztatów

Początkowo uczestnikami warsztatów byli głównie przedstawiciele firm zakładających i konserwujących instalacje sygnalizacji pożarowej. Z biegiem czasu zaczęło w nich uczestniczyć coraz więcej projektantów instalacji, gdyż firmy usługowe z tej branży rozrastały się i zaczęły kształcić własnych projektantów. Przyjeżdżało wielu właścicieli firm, które świadczyły pełny zakres usług związanych z instalacjami sygnalizacji pożarowej, łącznie z dystrybucją. Wysoka ranga corocznych ogólnopolskich warsztatów sprawiła, że chęć uczestnictwa w imprezie zaczęli zgłaszać wszyscy zainteresowani zagadnieniami dotyczącymi ochrony przeciwpożarowej, m.in. rzeczoznawcy ds. ochrony przeciwpożarowej. Ograniczona liczba miejsc noclegowych w Zaciszu spowodowała, że byliśmy zmuszeni wprowadzić weryfikację uczestników. Informacje o warsztatach były wysyłane tylko do firm aktywnie z nami współpracujących, do większych odbiorców urządzeń oraz do tych, którzy posiadali autoryzację firmy Polon-Alfa. Zaczęli w nich uczestniczyć również zagraniczni dystrybutorzy naszych urządzeń. Z perspektywy czasu można zauważyć, że w warsztatach uczestniczy już kolejne (młodsze) pokolenie instalatorów i projektantów systemów sygnalizacji pożarowej. Wysoki poziom merytoryczny sprawił, że właściciele firm zaczęli chętnie zabierać ze sobą specjalistów pracujących w ich firmach.

Tematy przewodnie warsztatów i publikacje zbiorów referatów

Na spotkaniach w pierwszych latach omawiano przede wszystkim problemy związane z dystrybucją (w owych czasach brak towarów na rynku ciągle jeszcze były normą) oraz nowe wdrożenia urządzeń do sygnalizacji pożarowej, przedstawiając ich parametry i funkcje. Traktowano to jako swego rodzaju szkolenia w tym zakresie.

Począwszy od 1996 roku każde spotkanie było poświęcone wybranemu tematowi przewodniemu, w ramach którego referenci starali się możliwie dogłębnie przedstawić dane zagadnienie. Tematyka wynikała z aktualnych zainteresowań środowiska oraz potrzeby pogłębienia wiedzy w określonym zakresie. Obejmowała ona wszystkie dziedziny szeroko rozumianej działalności w zakresie wykrywania pożaru, sygnalizacji i alarmowania oraz sterowania urządzeniami zabezpieczającymi, czyli tzw. automatykę pożarową.

W 2016 roku po raz pierwszy pojawiły się również panele dyskusyjne, które umożliwiły swobodną, otwartą dyskusję w nieco mniejszym gronie.

Referaty drukowane w postaci broszur otrzymywali wszyscy uczestnicy warsztatów, a pozostałe egzemplarze były dostarczane przede wszystkim do bibliotek szkół pożarniczych – w tym do Szkoły Głównej Służby Pożarniczej – oraz rozprowadzane wśród aktywnych projektantów i rzeczoznawców.

W roku 1999 wydano dodatkowo broszurę z tłumaczenia-

Fot. 2. Centrala sygnalizacji pożarowej CSP-35 z przystawką PCSP-35

mi projektu normy prEN 54-14 *Systemy sygnalizacji pożarowej – Wytyczne planowania, projektowania, instalowania, odbioru, użytkowania i serwisu* oraz wytycznych VdS 2496 *Sterowanie i uruchamianie stałych urządzeń gaśniczych*, które miały stanowić punkt wyjścia do opracowania polskich norm.

W 2002 roku, z okazji 10-lecia Warsztatów Zacisze, oprócz broszury na temat główny wydano dodatkowo dwie inne broszury – jedną zatytułowaną *Projektowanie instalacji SAP* a drugą z wybranymi referatami z 10 lat warsztatów w Zaciszu.

I choć broszury z materiałami zaczęto wydawać dopiero

Fot. 3. Jonizacyjna czujka dymu DIO-32A-2

w 1996 r., w sumie – w ciągu 25 lat warsztatów – i tak wydano 25 tomów materiałów. Stały się one ogromną skarbnicą fachowej wiedzy dla projektantów i instalatorów instalacji sygnalizacji i automatyki pożarowej. Należy zaznaczyć, że w wielu przypadkach materiały z warsztatów były jedynym źródłem fachowej literatury w tamtych czasach i były poszukiwane przez specjalistów z branży zabezpieczeń przeciwpożarowych.

Warto również wspomnieć, że w wydanych w 2011 roku *Wytycznych projektowania instalacji sygnalizacji pożarowej SITP WP-02:2010* w dużej mierze wykorzystano wiedzę przekazaną właśnie podczas warsztatów.

Prezentacja nowych opracowań firmy Polon-Alfa

Podczas każdych warsztatów przedstawiciele działu rozwoju lub działu marketingu firmy Polon-Alfa prezentowali nowe, przygotowane do wdrożenia lub ostatnio wdrożone urządzenia do systemów sygnalizacji pożarowej. Zwykle jednak prezentowano nowe urządzenia z wyprzedzeniem rocznym lub dwuletnim, gdy trwała ich obowiązkowa certyfikacja, aby w chwili uzyskania certyfikatu i uruchomienia produkcji zainteresowani mieli pełną informację o nowym produkcie.

Do początku lat dziewięćdziesiątych ubiegłego wieku w stałej produkcji firmy Polon-Alfa znajdowały się czujki szeregu 30 do central TELSAP 3 produkowanych w bydgoskich zakładach Telfa. Był to system konwencjonalny, eksportowany również do ZSRR.

Na pierwszym spotkaniu w Zaciszu w 1993 roku zaprezentowano nową konwencjonalną centralę sygnalizacji pożarowej CSP-35 wyprodukowaną w zakładzie Polon-Alfa. Był to przełom – Polon-Alfa stał się drugim w kraju producentem central sygnalizacji pożarowej. Przedstawiono także gniazdo adresowalne G-3AD współpracujące z czujkami szeregu 30 do pierwszej centrali adresowalnej TELSAP 2000 produkowanej w zakładach Telfa.

Fot. 4. Adresowalna centrala sygnalizacji pożarowej CSP-38 systemu ALFA 3800

Nowości pokazane w 1994 roku to nowa centrala adresowalna systemu monologowego CSP-35A i gniazda adresowalne G-35A, w których można było instalować produkowane dotąd czujki szeregu 30.

Fot. 5. Adresowalna centrala sygnalizacji pożarowej CSP-T2104 systemu TELSAP 2100

Rok 1995 przyniósł duże zmiany. W połowie roku firma Polon-Alfa stała się spółką pracowniczą, a jednocześnie amerykański koncern AT&T, który od trzech lat był właścicielem spółki Telfa, postanowił skoncentrować się wyłącznie na produkcji systemów telekomunikacyjnych i zrezygnował z produkcji systemów sygnalizacji pożarowej. Wykorzystał to Polon-Alfa. Przejął produkcję central adresowalnych TELSAP 2000 i osprzętu współpracującego oraz zobowiązał się w umowie dotyczącej przekazania do zagwarantowania obsługi

serwisowej i części zamiennych do znajdujących się w eksploatacji central TELSAP 3. Jednocześnie Polon-Alfa przejął z zakładów Telfa zespół konstruktorów, a także handlowców i marketingowców zajmujących się sygnalizacją pożarową, co doprowadziło do powstania prężnego zaplecza rozwojowego systemów sygnalizacji pożarowej.

Fot. 6. Optyczna czujka dymu DOR-2193

Na jesiennych warsztatach w 1995 roku zaprezentowano centrale rozszerzające system konwencjonalny o centrale CSP-36 dla małych obiektów i CSP-36/OT dla obiektów telekomunikacyjnych.

Rok 1996 przyniósł znaczny skok jakościowy. Podczas warsztatów zaprezentowano nowy adresowalny system dialogowy TELSAP 2100 z centralą CSP-T2104 i nowymi czujkami szeregu 2193 w gniazdach G-90, który powstał na bazie zmodernizowanej centrali sytemu TELSAP 2000. Po raz pierwszy pokazano centralę adresowalną CSP-38 z monologową komunikacją z czujkami szeregu 30 w gniazdach G-38A (system ALFA 3800). Ponadto zademonstrowano współpracujący z centralami konwencjonalnymi CSP-35 i CSP-36 zestaw do sterowania gaszeniem ZSG-35 składający się z pakietu instalowanego w centrali i połączonego z nim zewnętrznego bloku z wyjściami sterującymi i kontrolnymi.

Podczas warsztatów w 1997 roku firma Polon-Alfa zaprezentowała kompletny już, po certyfikacji, adresowalny system monologowy ALFA 3800 do średnich obiektów – centralę adresowalną CSP-38 oraz gniazda adresowalne zwykłe G-38A i zawierające izolator zwarć G-38AI do czujek szeregu 30.

W roku 1998 pokazano pierwszą z central konwencjonalnych systemu IGNIS 1000 – dwuliniową centralę IGNIS 1020. Centrale systemu IGNIS 1000 miały zastąpić centrale CSP-35 i CSP-36.

Prezentacja w roku 1999 obejmowała już dwie nowe centrale konwencjonalne – IGNIS 1020 i ośmioliniową IGNIS 1080. Pokazano też nową liniową czujkę dymu DOP-40 mającą odbiornik podczerwieni zintegrowany z nadajnikiem – w odróżnieniu od dotychczasowej czujki DOP-35 złożonej z osobnego nadajnika i osobnego odbiornika. Próby w testach pożarowych wykazały bardzo dużą przydatność tej czujki w całym zakresie pożarów testowych.

W roku 2000 został zapowiedziany nowy interaktywny system POLON 4000 z pierwszą centralą POLON 4800, która docelowo zastąpiła centralę TELSAP 2100. Pokazano również nową czujkę konwencjonalną szeregu 40 – optyczną czujkę dymu DOR-40 w nowym gnieździe G-40.

Koniec wieku nie oznaczał jednak końca organizowania warsztatów.

Dalsza część artykułu, opisująca wydarzenia z następnych lat, zostanie zamieszczona w kolejnym numerze *Zabezpieczeń*.

mgr inż. Mariusz Radoszewski
Polon-Alfa

Fot. 7. Centrale UCS

Fot. 8. Centrale 6000

AHD TECHNOLOGY by NOVUS®

NOVUS NA STRAŻY PORZĄDKU

DYNAMICZNA OBSERWACJA W TECHNOLOGII ANALOGOWEJ WYSOKIEJ ROZDZIELCZOŚCI

WYBIERZ KAMERĘ SZYBKOOBROTOWĄ AHD 1080P

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

25 lat
Polskiego Związku Pracodawców Ochrona

Barbara Bujak-Kowerczuk

Fot. Grzegorz Sawicki

Polski Związek Pracodawców Ochrona to dobrowolne, samorządne i niezależne zrzeszenie czołowych pracodawców z branży bezpieczeństwa w Polsce. Reprezentujemy firmy zatrudniające w sumie ponad 100 tysięcy pracowników. Już od 25 lat szczególną uwagę zwracamy na fakt, że ochrona osób i mienia jest nie tylko istotnym elementem życia gospodarczego, ale także ważnym elementem systemu bezpieczeństwa państwa

Podstawowe cele PZPO to:

1) Ochrona praw oraz reprezentowanie społecznych i gospodarczych interesów zrzeszonych członków wobec instytucji i administracji publicznej, związków zawodowych, mediów oraz samorządu terytorialnego, a także zleceniodawców i kontrahentów.
2) Tworzenie rozwiązań prawnych uwzględniających zarówno interesy zrzeszonych firm, jak i potrzeby i interesy usługobiorców oraz ich popularyzowanie.
3) Inicjowanie i rozpowszechnianie przedsięwzięć sprzyjających poprawie publicznego i indywidualnego bezpieczeństwa obywateli oraz ich mienia.
4) Wykazywanie stałej troski o jakość usług świadczonych przez przedsiębiorców zrzeszonych w Związku (profesjonalizm, zgodność z obowiązującymi przepisami prawa oraz zasadami sztuki i etyki zawodowej).
5) Wspieranie inicjatyw mających na celu ugruntowanie zaufania do pracodawców zrzeszonych w związku i ich pracowników, a także przekonania o wysokiej jakości usług świadczonych przez te przedsiębiorstwa.

Na stałe współpracujemy z Wydziałem Nadzoru nad SUFO Komendy Głównej Policji. Jesteśmy członkiem Federacji Przedsiębiorców Polskich. Związek posiada także Mobilny Punkt Konsultacyjny, w którym udziela pomocy prawnej i organizacyjnej członkom oraz prowadzi działalność doradczą i szkoleniową.

W ramach kreowania standardów, po analizie wnioskujących firm przez specjalnie powołaną komisję, wydajemy Certyfikat Jakości Usług Ochrony. Opracowaliśmy swój kodeks etyczny. Członkowie związku zobowiązują się do przestrzegania zawartych w nim zasad. Ponadto bierzemy aktywny udział w pracach Polskiego Komitetu Normalizacyjnego w zakresie bezpieczeństwa powszechnego, ochrony ludności oraz systemów alarmowych włamania i napadu.

Walne zgromadzenie i obchody 25-lecia działalności

Większość firm członkowskich, członkowie wspierający oraz liczni wystawcy i goście spotkali się 6 czerwca tego roku w hotelu Warszawianka w Jachrance na walnym zgromadzeniu i obchodach 25-lecia działalności Polskiego Związku Pracodawców Ochrona.

W pierwszej z trzech części programu dokonano podsumowania działań organów PZPO z ostatnich dwunastu miesięcy. Swoje sprawozdania przedstawili:

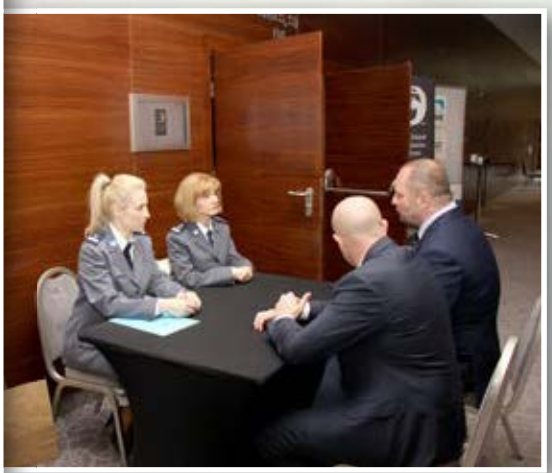
– prezes Tomasz Wojak (w imieniu zarządu);
– przewodniczący komisji rewizyjnej Rafał Stelmaszczyk (w imieniu komisji rewizyjnej; odczytał Adam Walenciak – członek tej komisji);
– przewodniczący Jerzy Leporowski (w imieniu komisji etyki).

W związku z brakiem uwag uczestników oraz pozytywną rekomendacją komisji rewizyjnej udzielono absolutorium zarządowi PZPO, a także zatwierdzono ww. sprawozdania oraz sprawozdanie finansowe organizacji.

Wśród kwestii merytorycznych omawianych w drugiej części dnia znalazły się statystyki i wnioski z kontroli Wydziału Nadzoru nad Specjalistycznymi Uzbrojonymi Formacjami Ochronnymi Biura Prewencji Komendy Głównej Policji, przedstawione przez mł. insp. Katarzynę Olejnik (naczelnik wydziału) oraz podinspektor Agnieszkę Jabłońską (eksperta wydziału). Odczytano także list Dariusza Minkiewicza, dyrektora Biura Prewencji KGP, dotyczący jubileuszu działalności związku. Ponadto delegaci mogli indywidualnie konsultować się z przedstawicielkami KGP przy stoliku eksperckim.

Zaproszenie do udziału w tej części spotkania przyjęli także przedstawiciele Głównego Inspektoratu Pracy – Anna Martuszewicz, wicedyrektor Departamentu Prawnego, i Wojciech Gonciarz, wicedyrektor Departamentu Prewencji i Promocji.

Anna Martuszewicz przedstawiła podsumowanie kontroli przedsiębiorstw z branży ochrony przeprowadzonych przez Inspekcję Pracy w latach 2015, 2016 oraz 2017. Kontrole dotyczyły przede wszystkim czasu pracy, braku stosunku pracy i wynagrodzeń dla pracowników oraz ustalania wynagrodzeń dla pracowników wykonawców zamówień publicznych. Uczestnicy walnego zgromadzenia zwrócili uwagę na naruszanie przepisów przez zamawiających, którzy akceptują ceny usług ochrony w przetargach publicznych nie obejmujące nawet podstawowych kosztów zatrudnienia pracowników realizujących usługę. Przedstawiciele Głównego Inspektoratu Pracy poinformowali jednak, że inspekcja nie jest uprawniona do weryfikacji procesu udzielania zamówień publicznych, i podkreślili, że obecnie kontrole przeprowadzane są także u wykonawców zamówień publicznych, między innymi w wyniku interwencji PZPO oraz innych organizacji pracodawców i pracowników. Wojciech Gonciarz przekazał uczestnikom treść listu Romana Giedrojcia, głównego inspektora pracy, skierowanego do uczestników spotkania z okazji 25-lecia PZPO. Następnie prezes PZPO Tomasz Wojak i członek zarządu Łukasz Koch omówili aktualną sytuację w branży ochrony. Ich wystąpienie miało interesującą formę interaktywnej prezentacji. Ostatnim punktem w tej części spotkania było omówienie działań i planów Federacji Przedsiębiorców Polskich przez Elizę Misiecką. Później odbyły się prezentacje rozwiązań technicznych przeznaczonych do wykorzystania w branży bezpieczeństwa.



Końcową częścią spotkania były uroczyste obchody 25-lecia działalności PZPO. Podczas wieczornej gali wyróżniono firmy członkowskie obchodzące jubileusze swojej działalności na rynku lub w związku oraz firmy wspierające, które także przyczyniają się do kreowania sukcesu organizacji. Spotkanie uatrakcyjnił występ skrzypaczki i pokaz barmański, a chętni mogli wziąć udział w walce o statuetkę Milionera Wieczoru przy stołach krupierskich. Nie zabrakło tortu i życzeń.

Jeszcze raz dziękujemy za udział zaangażowanym firmom członkowskim, firmom wspierającym, wystawcom oraz gościom. Zapraszamy do współtworzenia kolejnych organizowanych przez związek spotkań!

Barbara Bujak-Kowerczuk
sekretarz generalny PZPO

15 SPIN

15 lat tradycji Spotkań Projektantów Instalacji Niskoprądowych

Świętuj z nami
jubileusz 15-lecia SPIN:
flagowego wydarzenia
branży niskich prądów

27-28 września 2017

Nosalowy Dwór Resort & Spa | Zakopane

Dołącz do nas:

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

L O C K U S | 12 298 08 00 spin@lockus.pl

Rozmowa z Martinem Grenem,
współzałożycielem firmy Axis Communications

Właśnie został Pan uznany za najbardziej wpływową osobę z branży zabezpieczeń i ochrony przeciwpożarowej w prestiżowym rankingu IFSEC Global *Top 50 influencers in security & fire 2017*. **Czy to duże wyróżnienie?**

MG: Oczywiście, choć staram się nie przykładać wagi do tytułów czy nagród. Cieszę się, że moje przewidywania i analizy się sprawdzają, bo to utwierdza mnie w przekonaniu, że Axis Communications idzie dobrą drogą.

Kiedyś powiedział Pan, że trendy technologiczne są tak samo powtarzalne jak moda – po kilkunastu latach stare ubrania są znów modne. Czy wciąż może się Pan pod tym podpisać?

MG: Oczywiście, choć to spore uproszczenie. Stare idee i pomysły są często wykorzystywane na nowo i analizowane pod zupełnie innym kątem. Doskonałym przykładem jest Internet rzeczy (IoT), który wywodzi się ze sposobu wykorzystania komputerów określanych jako *thin servers*, popularnych w połowie lat 90. dwudziestego wieku. Jeżeli dziś zastanawiamy się nad tym, jak IoT wpłynie na branżę zabezpieczeń, możemy obejrzeć się za siebie i zobaczyć, jak *thin servers* zmieniły rynek dwadzieścia lat temu.

Czego zatem możemy się spodziewać?

MG: Coraz więcej urządzeń sieciowych wykorzystujących protokół IP nieuchronnie zastępuje starzejące się systemy analogowe. Producenci i dostawcy zabezpieczeń mają przed sobą trudne zadanie umożliwienia użytkownikom integracji nowych urządzeń i skutecznego zarządzania rosnącą ilością danych generowanych w ramach IoT – po to, aby stały się one użyteczne w biznesie.

Czy będą oferowane urządzenia podejmujące decyzje zamiast ludzi?

MG: Raczej urządzenia pomagające ludziom i wyręczające ich w niektórych zadaniach. Już dziś na podstawie obrazu z kamer system sam może ocenić, że kolejka do kasy w sklepie jest zbyt długa, i automatycznie wezwać dodatkowe osoby do obsługi, równocześnie wyświetlając na ekranach lub podając przez głośniki sieciowe komunikat o otwarciu dodatkowych stanowisk kasowych. Skoro już dziś jest to możliwe i coraz bardziej popularne, aż trudno sobie wyobrazić możliwości, które będziemy mieć za kilka lat.

Czy nowe zastosowania kamer wyeliminują współczesne zagrożenia?

MG: Odpowiednio użyta technika jest w stanie pomóc zmniejszyć zagrożenie, ale nie jest remedium na całe zło. Jako przykład mogę podać aplikacje do wykrywania pozostawionego bagażu. Taka aplikacja musi zaalarmować w przypadku wykrycia porzuconej walizki, ale nie powinna reagować na pozostawiony wózek sklepowy. A co w sytuacji, gdy walizka znajduje się w tymże wózku? Wiele mówi się o rozpoznawaniu twarzy, lecz obecnie takie aplikacje działają poprawnie przy ograniczonej bazie danych i w kontrolowanym środowisku – kamera znajdująca terrorystę na wypełnionym ludźmi stadionie to niestety wciąż science fiction.

Mówi Pan z perspektywy osoby, która jest związana z branżą od ponad 20 lat. Jak to się właściwie zaczęło?

MG: Pomysł na stworzenie pierwszej kamery sieciowej powstał podczas mojej podróży z jednym z potencjalnych klientów do Japonii. W tym samym czasie mój kolega, Carl-Axel Alm, zastanawiał się nad zbudowaniem systemu wideokonferencyjnego wykorzystującego protokół IP. Porozumieliśmy się i wspólnie zmieniliśmy nasze pomysły w rzeczywistość.

Tak powstała kamera AXIS 200?

MG: Tak i na początku nie był to produkt, który wykorzystywał pełnię dostępnych możliwości. Gdy wprowadziliśmy ją na rynek we wrześniu 1996 r., wytwarzała obraz o niskiej rozdzielczości z prędkością zaledwie jednej klatki na sekundę

i potrzebowała aż 17 sekund do wygenerowania pojedynczej klatki o rozdzielczości D1. To było praktycznie bezużyteczne w przypadku normalnych aplikacji dozorowych, ale ukazywało potencjalne przyszłe ukształtowanie rynku na którym dostępne były wówczas wyłącznie kamery analogowe.

To był początek rewolucji cyfrowej w monitoringu?

MG: Nie wiem czy rewolucji, ale z pewnością ewolucji. Choć muszę przyznać, że kamera AXIS 200 wywołała prawdziwy szok wśród technologicznych wizjonerów i guru z lat 90. – kilka lat temu spotkałem się ze Stevem Wozniakiem z Apple'a, który przyznał się, że wciąż trzyma swój stary egzemplarz AXISA 200. Zresztą na rynku też doceniono nasz pomysł. Miałem umowę z zarządem firmy – ustaliliśmy, że jeśli sprzeda się przynajmniej 10 000 egzemplarzy AXISA 200, zajmiemy się tym biznesem na poważnie i stworzymy oddział firmy zajmujący się rozwojem kamer sieciowych. Jak widać udało nam się.

Czy rozwój technologii i duże zapotrzebowanie na sieciowe rozwiązania z dziedziny zabezpieczeń w ostatnich 20 latach Pana zaskoczyły?

MG: „Dwadzieścia lat" brzmi jak „długi czas", ale dla mnie ten okres minął szybko. W 1996 roku nie przypuszczaliśmy, że będziemy w czołówce biorących udział w potężnej rewolucji związanej z rozwojem Internetu rzeczy. Dzisiaj na całym świecie zainstalowanych jest kilkadziesiąt milionów kamer IP. Dzięki możliwościom dawanym przez sieć możliwe stało się obserwowanie dużych obszarów za pomocą małej liczby urządzeń, co sprawia, że monitorowanie stało się dostępne praktycznie dla każdego miasta czy firmy. Z perspektywy lat widać doskonale, że do naszej branży można zastosować prawo Moore'a.

Wróćmy do teraźniejszości. Jakie główne wyzwania widzi Pan dziś przed naszą branżą?

MG: Przede wszystkim zapewnienie bezpieczeństwa urządzeń podłączonych do Internetu. Coraz częściej słyszymy o kolejnych atakach czy cyberzagrożeniach. Wierzę, że to w gestii producentów leży zapewnienie odpowiedniego oprogramowania i zabezpieczeń naszych urządzeń. Ważne jest także, aby użytkownicy mogli ufać swojemu dostawcy sprzętu i wiedzieli, że w przypadku wykrycia luki w zabezpieczeniach problem zostanie szybko rozwiązany. Dlatego tak istotna jest znajomość łańcucha dostaw producenta i jego kontrahentów, a w związku z tym również zaufanie do marki. Drugim kluczowym wyzwaniem jest odpowiednie wykorzystanie kamer i wszystkich inteligentnych urządzeń w ramach IoT. Wierzę, że tak popularne dziś określenie smart city to tak naprawdę rozwinięcie pojęcia safe city. Tylko w bezpiecznym miejscu ludzie będą czuć się na tyle komfortowo, aby w pełni korzystać z możliwości oferowanych przez technikę.

Jakie najważniejsze trendy mogące utrzymać się w najbliższych latach w branży zabezpieczeń mógłby Pan wymienić?

MG: Jest ich całkiem sporo. Nie wiem, czy mamy miejsce na wszystkie, więc skupię się na kilku. W związku z rosnącą liczbą urządzeń podłączonych do Internetu i gigantycznym przyrostem wielkości przesyłanych plików z pewnością rośnie zapotrzebowanie na technologie umożliwiające ograniczenie objętości przesyłanych danych, takie jak Axis Zipstream. To ograniczenie jest ważne również ze względu na zaawansowane funkcje analityczne, które coraz częściej realizowane są już w samych kamerach, a nie na serwerach. O cyberbezpieczeństwie już wspomniałem. Jest ono kluczowe dla wszystkich producentów i dostawców systemów. Ponadto w firmie Axis wierzymy w rozwój innych sieciowych urządzeń zabezpieczających, które nie osiągnęły jeszcze takiego poziomu rozwoju i w związku z tym również popularności jak kamery, zwłaszcza głośników IP czy urządzeń z zakresu kontroli dostępu. Jeśli zaś chodzi o same kamery, to ogromny potencjał widzę w urządzeniach wieloprzetwornikowych, wytwarzających obraz na podstawie danych pochodzących z różnego typu modułów optycznych (np. tradycyjny obraz wizyjny oraz termowizyjny), a także w rozwiązaniach wykorzystujących technikę radarową.

Dlaczego?

MG: Radar to urządzenie, które jeszcze do niedawna było wykorzystywane głównie przez wojsko i cywilne służby kontroli lotów. Dziś jest intensywnie rozwijane przez branżę motoryzacyjną i wykorzystywane do tworzenia inteligentnych czy autonomicznych samochodów. Radar pracuje niemalże w każdych warunkach pogodowych, choć oczywiście też ma swoje ograniczenia.

Czy na coś jeszcze zwróciłby Pan uwagę?

MG: Oczywiście nie można zapomnieć o rozwoju technologii produkcji samych kamer, który ma prowadzić do jednego – zapewnienia lepszego obrazu niezależnie od warunków obserwacji. Dziś rozdzielczość 4K to jeszcze nie standard, ale już jutro nim będzie. Technika WDR (ang. *Wide Dynamic Range*), ulepszona stabilizacja obrazu nawet w trakcie obrotu kamery, możliwość widzenia kolorów w ciemności czy rozwiązania ułatwiające montaż i regulację kamer to kolejne trendy, które będą definiować rozwój urządzeń do monitorowania.

Czy Pana zdaniem branża zabezpieczeń będzie nadal się rozwijać? Jeśli tak, to w jaki sposób?

MG: Dziś rynek zabezpieczeń w samych tylko Stanach Zjednoczonych jest wart 80 miliardów dolarów rocznie. Z tego około 80% to koszty ludzkie. Nowoczesny sprzęt i techniki mogą pomóc obniżyć te koszty – pracownicy ochrony nie będą musieli dokonywać cogodzinnego obchodu, a zamiast tego będziemy mogli wysyłać ich jedynie w przypadku naruszenia bezpieczeństwa, które zostanie wykryte przez kamerę czy radar. Takie wykorzystanie techniki może sprawić, że ta branża stanie się jeszcze bardziej dochodowa.

Martin Gren

szwedzki przedsiębiorca, konstruktor kamery sieciowej, współzałożyciel firmy Axis Communications – firmy o globalnym zasięgu działania, lidera w dziedzinie sieciowych rozwiązań przeznaczonych do nadzoru wizyjnego. Na International Fire and Security Conference & Exhibition (IFSEC) w roku 2013 i 2017 został uznany za najbardziej wpływową osobę z branży. Skonstruowana przez niego w 1996 r. kamera IP zrewolucjonizowała rynek zabezpieczeń, rozpoczynając przekształcanie systemów dozoru wizyjnego z analogowych w sieciowe.

Międzynarodowe Targi Poznańskie

securex®
POLAND

Międzynarodowe Targi Zabezpieczeń

23-26.04.2018
POZNAŃ

Zabezpiecz swój sukces!

www.securex.pl

Kontroler zintegrowany KaDe - KDH-KZ2000-IP-U/M

KaDe

32-bitowy procesor gwarantuje szybką i niezawodną pracę kontrolera, zwłaszcza w trybie monitorowania na żywo. Jest to kontroler jednego przejścia, które może być kontrolowane jedno- lub dwustronnie. Aby zrealizować kontrolę dwustronną, należy dołączyć do portu kontrolera drugi czytnik. Może to być również czytnik z klawiaturą. Kontroler wraz z czytnikiem z klawiaturą oferuje 4 tryby identyfikacji użytkownika: karta, kod dostępu, karta lub kod dostępu, karta+ kod dostępu. Każdy użytkownik może mieć swój indywidulany kod dostępu, również w trybie autonomicznym. Kontroler pracuje w trybie autonomicznym (programowanie z klawiatury) lub sieciowym pod programem nadzorczym **KaDe Premium Plus II**. Zalecany zasilacz to AWZ 200 z akumulatorem 7 Ah.

Urządzenie integruje w sobie następujące elementy:

- moduł kontrolera jednego przejścia
- czytnik kart zbliżeniowych:
  - w standardzie 125 kHz ISO Unique - model KDH-KZ2000-IP-U
  - w standardzie 13,56 MHz Mifare - model KDH-KZ2000-IP-M
- klawiaturę do wprowadzania kodu dostępu i programowania oraz przycisk dzwonkowy
- sygnalizator optyczny (diody LED) i akustyczny (brzęczyk)
- czujnik antysabotażowy

Nazwa parametru lub funkcji	Wartość parametru lub opis funkcji
Pojemność pamięci	
pamięć kart	20 000 (2 000 w trybie autonomicznym)
pamięć zdarzeń	50 000
pamięć alarmów	20 000
Parametry elektryczne	
napięcie zasilania	12 V_{DC}
pobór prądu	< 110 mA
odporność na przepięcia statyczne	tak
Parametry środowiskowe	
otoczenie	tylko do instalacji wewnątrz pomieszczeń
temperatura pracy	od +2°C do +55°C
wilgotność względna	0% – 95%
Porty komunikacyjne	
do połączenia z KaDe Premium Plus II	TCP
do podłączenia modułów rozszerzeń	RS485 (do wykorzystania w przyszłości)
Czytniki i karty	
zintegrowany w urządzeniu	na karty Unique, zasięg 5 – 10 cm (U) na karty Mifare, zasięg 2 – 5 cm (M)
dodatkowy	zgodny z 26(U)/34(M) bit Wiegand
format kart	ISO Unique (125 kHz) Mifare Classic (14443A) (13,56 MHz)
format kodów klawiatury czytnika dodatkowego	26(U), 34(M), 4–bitowy, bez buforowania
Linie dozorowe	3 x NO/NC
Wyjścia sterujące	3 (2 przekaźnikowe, 1 do dzwonka)

Producent:

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

tel. +48 22 546 05 46
e-mail: kontakt@aat.pl
www.aat.pl

Hybrydowa kamera szybkoobrotowa marki NOVUS NVIP-3DN3520SD/IRH-2-II

Kamera szybkoobrotowa NVIP-3DN3520SD/IRH-2-II może pracować równocześnie w trybie IP oraz analogowym o wysokiej rozdzielczości. Sterowanie urządzeniem odbywa się z użyciem protokołu TCP/IP (jak standardowych kamer IP), ale również w z użyciem interfejsu RS-485. Dodatkowo z poziomu rejestratorów AHD marki NOVUS kamera może być sterowana z użyciem protokołu COAX za pośrednictwem koncentrycznego o długości nie przekraczającej 300 m.

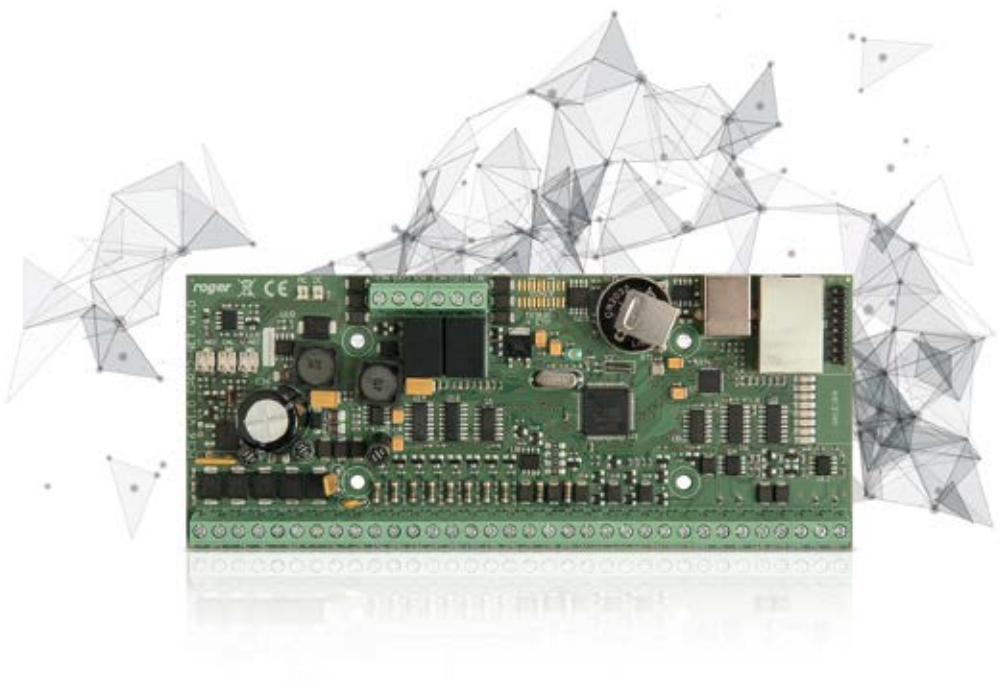
Nazwa parametru lub funkcji	Wartość parametru lub opis funkcji
Obraz	
Przetwornik obrazu	matryca CMOS, 1/2.8", SONY, 3 megapiksele
Czułość	4.0 lx/F1.6 – tryb kolorowy 0 lx (IR wł.) – tryb czarno-biały
Obiektyw	
Zmiennoogniskowy	krotność 20x
Zakres regulacji przysłony i ogniskowej	ogniskowa od 5,5 mm do 110 mm, przysłona od f=1:1,6 do f=1:3,5
Sieć	
Rozdzielczość obrazu	2048 x 1536 (QXGA), 1920 x 1080 (Full HD), 1280 x 720 (HD), 640 x 480 (VGA), 320 x 240 (QVGA
Kompresja obrazu	H.264, H.265, MJPEG
Zgodność z Onvif	profil S (Onvif 2.3)
OŚWIETLACZ IR	
Zasięg	do 100 m
INTERFEJSY	
Wyjście wizyjne	BNC, 1.0 V_{p-p}, 75 Ohm - Sygnał AHD/TVI 1080p
Wejścia/wyjścia audiogłosowe	1 x Jack (3.5 mm)/1 x Jack (3.5 mm)
Wejścia/wyjścia alarmowe	4 (NO/NC)/1 typu przekaźnikowego
Interfejs sieciowy	1 x Ethernet - złącze RJ-45, 10/100 Mbit/s
PARAMETRY INSTALACYJNE	
Stopień szczelności	IP 66 (szczegóły w instrukcji obsługi)
Zasilanie	24 V_{DC}/24 V_{AC}

Producent:

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

tel. +48 22 546 05 46
e-mail: kontakt@aat.pl
www.aat.pl

MC16-LRC
Kontroler dostępu do szafek



Kontroler **MC16-LRC** umożliwia realizację elektronicznej kontroli dostępu do szafek i schowków w ramach systemu kontroli dostępu i automatyki RACS 5. Kontroler może współpracować z dowolnymi, sterowanymi elektrycznie, zamkami przewodowymi lub z zamkami bezprzewodowymi RWL-3 (ROGER). Moduł kontrolera MC16-LRC jest zgodny sprzętowo z modułem kontrolera dostępu MC16-PAC i oferuje te same możliwości obsługi czytników i modułów rozszerzeń, co macierzysty kontroler MC16. Zasoby sprzętowe płyty głównej kontrolera umożliwiają obsługę do 8 szafek. W przypadku większej liczby szafek, konieczne jest dołączenie do kontrolera zewnętrznych ekspanderów wej/wyj. Użytkownik uzyskuje dostęp do szafki po identyfikacji na czytniku powiązanym z daną szafką. Możliwe jest takie skonfigurowanie systemu, w którym pojedynczy czytnik obsługuje wiele lub nawet wszystkie szafki. W takim wariancie konfiguracji, po rozpoznaniu użytkownika kontroler analizuje jego uprawnienia i otwiera te szafki, do których ma on uprawnienie. Zarówno zarządzanie systemem jak i monitorowanie systemu szafek realizowane jest z poziomu tego samego oprogramowania, co zarządzenie systemem kontroli dostępu do pomieszczeń. Obydwa systemy korzystają z tej samej bazy danych i tej samej listy użytkowników, co pozwala znacznie usprawnić ich zarządzanie. Kontroler MC16-LRC oferowany jest w 4 wersjach licencji umożliwiającej obsługę 8, 16, 32 lub 64 szafek.

Charakterystyka

- kontrola dostępu do szafek i skrytek
- 8 wejść parametrycznych
- 6 wyjść tranzystorowych
- 2 wyjścia przekaźnikowe
- wyjście zasilania 1 A
- wyjście zasilania 0,2 A
- współpraca z czytnikami RS485 (MCT), Wiegand, RACS CLK/DTA
- ekspandery we/wy dołączane przez RS485
- obsługa akumulatora
- zasilanie 18 V_{AC} lub 12 V_{DC}
- komunikacja Ethernet z szyfrowaniem
- zarządzanie z poziomu oprogramowania systemu RACS 5
- w zależności od licencji obsługa 8, 16, 32 lub 64 szafek

Producent: 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

RWL-3
Bezprzewodowy zamek szafkowy

Zamek szafkowy **RWL-3** umożliwia realizację bezprzewodowej kontroli dostępu do szafek i różnego rodzaju skrytek. Zamek RWL-3 może pracować w trybie autonomicznym (off-line) lub sieciowym (on-line). W trybie autonomicznym RWL-3 steruje dostępem do szafki zgodnie z konfiguracją wprowadzoną do pamięci zamka w trakcie jego programowania. Programowanie może być przeprowadzone manualnie za pomocą karty programującej lub przewodowo z poziomu programu RogerVDM. W trybie sieciowym, zamek jest połączony bezprzewodowo z kontrolerem dostępu, który zarządza dostępem do szafki i rejestruje na bieżąco zdarzenia związane z obsługą zamka, w tym stany alarmowe. W scenariuszu on-line, konfiguracja uprawnień dostępu jest realizowana z poziomu oprogramowania zarządzającego systemem RACS 5, które umożliwia elastyczne definiowanie zasad dostępu do szafek z uwzględnieniem kalendarzy, harmonogramów, poziomów dostępu i innych zaawansowanych mechanizmów stosowanych powszechnie w kontroli dostępu. Zamek RWL-3 składa się z czytnika zbliżeniowego montowanego na zewnątrz szafki oraz zasobnika na baterie zespolonego z mechanizmem ryglującym, który jest montowany wewnątrz szafki. Zamek wyposażony jest w czujnik położenia rygla oraz wejście do podłączenie zewnętrznego czujnika otwarcia drzwiczek. W przypadku wyczerpania baterii, zamek może być zasilony z zewnętrznego zasilacza podłączonego do czytnika zbliżeniowego.

Charakterystyka

- bezprzewodowy zamek szafkowy
- komunikacja bezprzewodowa IEEE 802.15.4/ 2.4 GHz
- wbudowany czujnik położenia rygla
- wejście do podłączenia zewnętrznego czujnika stanu drzwiczek
- identyfikacja użytkowników przy użyciu kart zbliżeniowych ISO/IEC 14443A/MIFARE® Ultralight/Classic/Plus/DESFire
- możliwość identyfikacji za pośrednictwem urządzeń mobilnych z systemem Android obsługujących komunikację NFC
- 4 wskaźniki LED oraz głośnik sygnalizacyjny
- zasilanie z trzech baterii AA
- typowy czas pracy 1 rok przy 10 odczytach dziennie
- sygnalizacja niskiego stanu baterii
- konfiguracja niskopoziomowa poprzez połączenie przewodowe lub bezprzewodowe z poziomu aplikacji RogerVDM
- wymiary panelu zewnętrznego (sz. x wys. x gł.): 44x113x20 mm
- wymiary panelu wewnętrznego (sz. x wys. x gł.): 65x132x22 mm
- obsługa drzwi lewych i prawych

Producent: 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

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

AGIS FIRE & SECURITY Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. 22 430 83 01
tel. kom. 604 290 185
faks 22 430 83 02
e-mail: lmarciniak@agisfs.com
www.agisfs.com

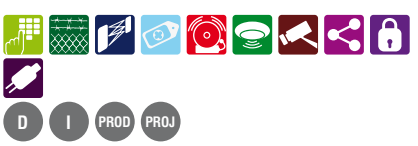
ALARMNET BORKIEWICZ Sp. J.
ul. Karola Miarki 20c
01-496 Warszawa
tel. 22 663 40 85
faks 22 833 87 95
e-mail: biuro@alarmnet.com.pl
www.alarmnet.com.pl

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

ALKAM SYSTEM Sp. z o.o.
ul. Bydgoska 10
59-220 Legnica
tel. 76 862 34 17
e-mail: alkam@alkam.pl
www.alkam.pl

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

FIRMA ATLINE SPÓŁKA JAWNA SŁAWOMIR PRUSKI
ul. Franciszkańska 125
91-845 Łódź
tel. 42 236 30 19
faks 42 655 20 99
e-mail: biuro@atline.pl
www.atline.pl



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

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

bt electronics Sp. z o.o.
ul. Dukatów 10
31-431 Kraków
tel. 12 429 36 16, 410 20 33
faks 12 410 85 11
e-mail: bte@bte.pl
www.saik.pl

D I PROD PROJ S

CAMSAT
Gralak Przemysław
ul. Ogrodowa 2a
86-050 Solec Kujawski
tel. 52 387 36 58
faks 52 387 36 58 w. 24
e-mail: camsat@camsat.com.pl
www.camsat.com.pl

D PROD

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: cbc@cbcpoland.pl
www.cbcpoland.pl

D PROD PROJ S

CMA MONITORING
Spółka z ograniczoną odpowiedzialnością Sp. k.
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. Świętochłowicka 3, 41-909 **Bytom**
tel. 32 388 0 950
faks 32 388 0 960
e-mail: bytom@cma.com.pl

ul. Zatorska 36, 51-215 **Wrocław**
tel. 71 342 03 78
tel. kom. 697 972 558
faks 71 341 16 26
e-mail: wroclaw@cma.com.pl

Biura handlowe:
ul. Skośna 12, 30-383 **Kraków**
tel. 12 260 13 96
tel. kom. 882 126 082
faks 12 260 13 95
e-mail: info@cma.com.pl

ul. Nowy rynek 2, 62-002 **Suchy Las k/Poznania**
tel. 61 861 40 51
tel. kom. 601 203 664, 601 410 979
faks 61 861 40 51
e-mail: poznan@cma.com.pl

ul. Hallera 140, lok. 124, 80-416 **Gdańsk**
tel. 58 345 23 24
tel kom. 693 694 339
e-mail: gdansk@cma.com.pl

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

D I PROD PROJ S

DAHUA TECHNOLOGY POLAND Sp. z o.o.
ul. Salsy 2, Lisbon Building, Lobby II
02-823 Warszawa
tel. 22 395 74 00
faks 22 395 74 10
e-mail: biuro.pl@global.dahuatech.com
www.dahuasecurity.com/pl

B C D PROD PROJ S

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

D I PROJ

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

D I PROJ

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

B C D PROD S

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

I PROJ

ELSTECH
os. Złota Podkowa 6/4
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.pl
ul. Główna 23
42-280 Częstochowa
tel. 34 341 14 61
tel. kom. 517 015 471
e-mail: sklep@eltrox.pl
www.eltrox.pl

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

ul. 6 sierpnia 14, 90-416 **Łódź**
tel. 42 632 31 24
e-mail: lodz@eltrox.pl

ul. Brynowska 65/4, 40-584 **Katowice**
tel. 32 203 50 73
e-mail: katowice@eltrox.pl

ul. Wybickiego 42A, 31-302 **Kraków**
tel. kom. 501 945 239
e-mail: krakow@eltrox.pl

ul. Dmowskiego 2/1, 45-365 **Opole**
tel. kom. 501 945 246
e-mail: opole@eltrox.pl

ul. Stablewskiego 31/3, 60-223 **Poznań**
tel. kom. 504 904 710
e-mail: poznan@eltrox.pl

ul. Wyszyńskiego 26, 70-203 **Szczecin**
tel. 91 434 78 72
e-mail: szczecin@eltrox.pl

ul. Remiszewska 1/7B, 03-550 **Warszawa**
tel. 22 676 78 40
e-mail: warszawa@eltrox.pl

ul. Łopuszańska 22, 02-220 **Warszawa**
tel. kom. 506 601 006
e-mail: warszawa2@eltrox.pl

ul. Komandorska 53R, 50-258 **Wrocław**
tel. kom. 503 127 533
e-mail: wroclaw@eltrox.pl

EUREKA SOFT & HARDWARE
ul. Rynek 13
62-300 Września
tel. 61 437 90 15
e-mail: biuro@eureka.com.pl
www.eureka.com.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
http://europeansecuritytrading.com/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.
Baltic Business Park
ul. 1-go Maja 38/39
71-627 Szczecin
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

D S

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

D I PROJ

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

D PROD PROJ S

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

PROD PROJ S

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

D

NUUXE RADIOTON Sp. z o.o.
ul. Olszańska 5H
31-513 Kraków
tel. 12 393 58 00
faks 12 393 58 02
e-mail: nuuxe@nuuxe.com
www.nuuxe.com

D I PROD PROJ S

POLON-ALFA
Spółka z ograniczoną odpowiedzialnością Sp. k.
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

PROD

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

D PROJ S

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

D I PROD PROJ S

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

D

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

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

D PROD S

SATEL Sp. z o.o.
ul. Budowlanych 66
80-298 Gdańsk
tel. 58 320 94 00
faks 58 320 94 01
e-mail: satel@satel.pl
www.satel.pl

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: warszawa@schrack-seconet.pl
www.schrack-seconet.pl

Oddziały:
ul. M. Gomółki 2, 80-279 **Gdańsk**
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- Systemy Alarmowe Sp. z o.o.
ul. Tatrzańska 8
60-413 Poznań
tel. 61 876 70 88
faks 61 875 03 03
e-mail: tap@tap.com.pl
www.tap.com.pl

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 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 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*

WIELOPUNKTOWY I WIELOGAZOWY SYSTEM DETEKCJI CO/LPG... NO_2... W GARAŻACH I PARKINGACH PODZIEMNYCH

JEŚLI MUSISZ STOSUJ ORYGINALNE

PRO-SERVICE®

Przedsiębiorstwo Wdrożeniowe Pro-Service© Sp. z o.o.
Os. Złotej Jesieni 4, 31-826 Kraków, Tel. 12 425 90 90
www.alarmgaz.com

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

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

Współpraca
Marcin Buczaj
Adam Bułaciński
Piotr Czernoch
Marcin Pyclik
Sławomir Wagner

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

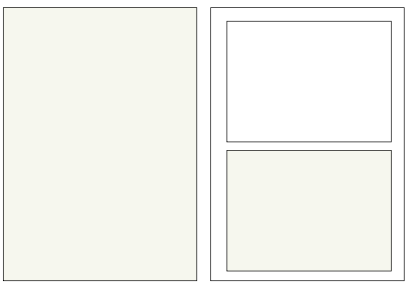
Wydawca
AAT HOLDING S.A.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

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

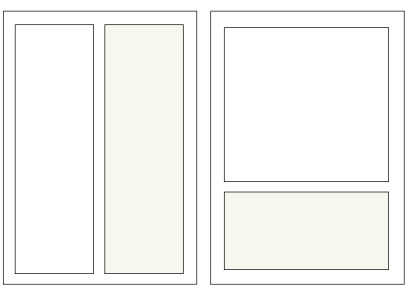


cała strona
(200 x 282 mm + 3mm spad)

1/2 strony
(170 x 125 mm)

Reklama na okładkach

pierwsza strona
druga strona
przedostatnia strona
ostatnia strona



1/2 strony
(83 x 260 mm)

1/3 strony
(170 x 80 mm)

Artykuł sponsorowany

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

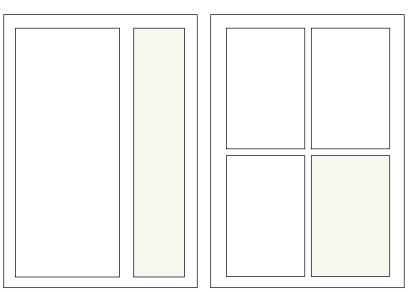
Spis teleadresowy

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



1/3 strony
(54 x 260 mm)

1/4 strony
(83 x 125 mm)

Spis reklam

AAT HOLDING	11, 45, 63, 79, 88, 89
AxxonSoft Polska	3
Bosch Security Systems	99
C&C Partners	14
Dahua Technology	14, 15, 69
DEKK Fire Solutions	6
Ela-compil	7
Firma ATline	68
Genevo	73
Gunnebo	38
Hanwha Techwin Europe	59
IBP NODEX	33
Impakt	10
International Water Mist Association	29
MOBOTIX	73
MTP-SECUREX	87
P.U.I. Zeto-Projekt	10, 39
Polon-Alfa	1, 7
Projekt BMS 2017	18
Proteng Systems	8
Przedsiębiorstwo Wdrożeniowe PRO-SERVICE	97
ROGER	46, 47, 90, 91
RST	8
Schrack Seconet Polska	9
SICUREZZA	100
SPIN Extra 2017	83
W2	9
Videotec	2

BOSCH
Technologia bliżej nas

Dla innych centrum handlowe to rozrywka.

Ty widzisz inteligentne dane, które pomogą zwiększyć sprzedaż.

Znajdź nas na **www.boschsecurity.pl**

JEDNO SŁOWO, WIELE ROZWIĄZAŃ

sferica.net

SICUREZZA

INTERNATIONAL SECURITY & FIRE EXHIBITION

TAM, GDZIE PRODUKTY I STRATEGIE TWORZĄ ROZWIĄZANIA

Fiera Milano, Rho

W DNIACH 15-17 LISTOPADA 2017 ROKU

www.sicurezza.it

WRAZ Z

SMART BUILDING EXPO

MIĘDZYNARODOWA SIEĆ

BRASEG BRAZILIAN TRADE SHOW FOR OCCUPATIONAL SAFETY AND HEALTH, AND FIRE PROTECTION
www.braseg.tmp.br

EXPOSEC INTERNATIONAL SECURITY FAIR
www.exposec.com.br

FISP INTERNATIONAL FAIR OF SAFETY AND PROTECTION
www.fispvirtual.com.br

POD PATRONATEM

Ministero della Difesa

CAMERA DI COMMERCIO MILANO

ZORGANIZOWANA PRZEZ

FIERA MILANO