CZASOPISMO BEZPŁATNE
ISSN: 1505-2419 DWUMIESIĘCZNIK NR 4(128)/2019

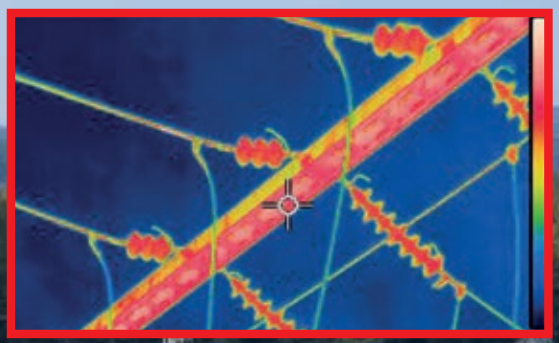
ZABEZPIECZENIA

Kolorowy obraz w ciemności

W kamerach Full-color Dahua Technology!

alhua TECHNOLOGY

VIDEOTEC



Ulisse evo Thermal

ULISSE EVO THERMAL to nowa kamera termowizyjna PTZ z funkcjami radiometrycznymi, przeznaczona do pracy w prewencyjnych systemach nadzoru wizyjnego w trybie 24/7.

Znajduje zastosowanie w systemach do wykrywania pożaru w obiektach infrastruktury krytycznej, w kolejnictwie, a także w ruchu drogowym i ulicznym.

ONVIF | S Q

IP66/IP67 IP68 | TYPE 4X TYPE 6P | PoE+ | IP

VIDEOTEC

VIDEO SECURITY PRODUCTS

www.videotec.com

Made in Italy

RACS 5 LT

Ekonomiczna wersja systemu RACS 5 dla zastosowań w małych i średnich obiektach

- Uproszczona konfiguracja i obsługa systemu
- Bezpłatny program zarządzający VISO LT
- Współpraca z dowolnymi urządzeniami systemu RACS 5 (MCT lub MCX)
- Współpraca z ekonomicznymi wersjami kontrolerów MC16 (seria MC16-LT)
- Obsługa czytników serii PRT (Roger)
- Obsługa czytników z interfejsem Wiegand
- Obsługa zamków bezprzewodowych serii RWL (Roger)
- Możliwość migracji do wyższych wersji systemu (RACS 5 ST lub RACS 5 EX)

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

roger®
Intelligence for Building

SPIS TREŚCI

Nowości produktowe

Wydarzenia, informacje

Normalizacja

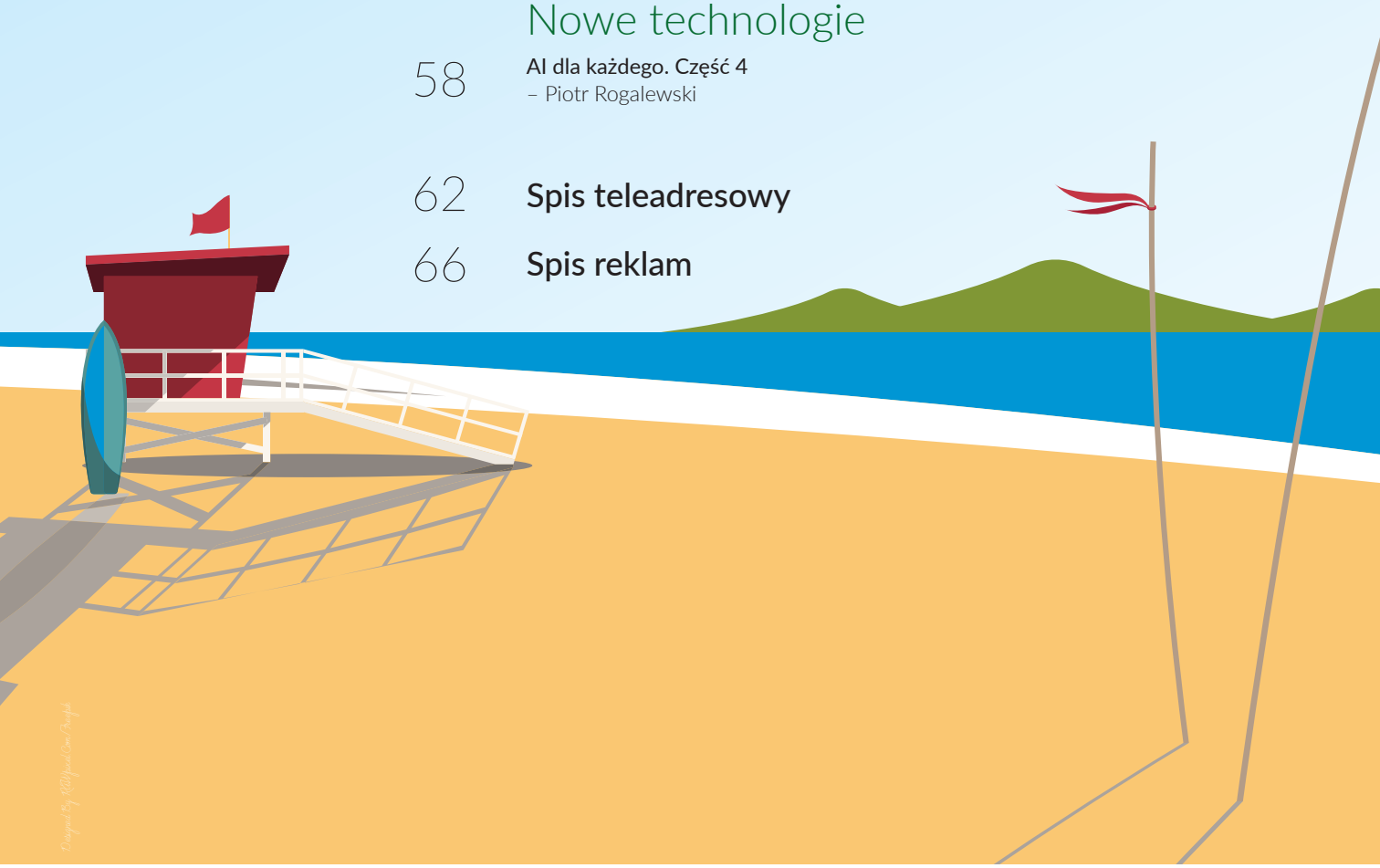
Kontrola dostępu

Telewizja dozorowa

Radiokomunikacja

Ochrona przeciwpożarowa

Nowe technologie



Zarządzalny przełącznik T2600G-28MPS firmy TP-Link

Przełącznik **T2600G-28MPS** to wydajny zarządzalny przełącznik **L2+** przeznaczony do budowy profesjonalnych sieci w małych i średnich firmach.

T2600G-28MPS został wyposażony w 24 porty PoE 10/100/1000 Mb/s zgodne ze standardami 802.3at/af, mogące łącznie dostarczyć 384 W mocy, co umożliwia podłączenie punktów dostępowych, telefonów IP oraz kamer IP. Urządzenie to pozwala zasilić urządzenia odbiorcze o poborze mocy do 30 W na każdy port.

Takie funkcje jak harmonogram PoE czy priorytet portów pozwalają na efektywniejsze zarządzanie zasobem mocy przełącznika. Ponadto przełącznik ma cztery osobne gniazda SFP, które umożliwiają bardziej uniwersalne wykorzystanie urządzenia w sieci.

W tworzeniu bezpiecznej sieci przydatne są liczne funkcje zarządzające – 802.1Q VLAN, izolacja portów, mirroring portów, STP/RSTP/MSTP, agregacja portów (LACP), funkcja kontroli przepływu 802.3x, ACL, funkcje L2+, tj. routing statyczny, oraz Quality of Service (QoS, od L2 do L4).

T2600G-28MPS jest prosty w obsłudze i zarządzaniu. Zarządzanie urządzeniem może odbywać się na różne sposoby, np. poprzez intuicyjny graficzny interfejs użytkownika (GUI) w przeglądarce internetowej lub interfejs linii poleceń (CLI). Transferowane pakiety mogą być szyfrowane metodą SSL lub SSH. Obsługa protokołów SNMP (1/2/3) oraz RMON umożliwia przełącznikowi przekazywanie istotnych informacji dotyczących statusu oraz wychwytywanie nieprzewidzianych zdarzeń.

Produkt jest objęty pięcioletnią gwarancją.

Więcej informacji na temat T2600G-28MPS jest dostępnych na stronie internetowej www.tp-link.com.pl.

Bezpośr. inf. Joanna Dąbek
Grayling Poland
joanna.dabek@grayling.com
www.tp-link.com.pl

Mechaniczne zamki do szafek
KitLock KL10

Chcąc spełnić oczekiwania klientów instytucjonalnych, **Firma ATLine sp.j. Sławomir Pruski** powiększa swój asortyment zamków szyfrowych, wprowadzając mechaniczny zamek do szafek **KitLock KL10**. Jest to nowość w ofercie producenta, która bez opóźnień trafia na polski rynek. W porównaniu z zamkami elektronicznymi mechanizm nowego zamka jest prosty. Ma on podstawowe funkcje, a jego cena jest niższa.

Zamki do szafek KitLock KL10 to pierwsze blokady mechaniczne z serii KitLock przeznaczonej do zamykania szaf, szafek i komód. Mogą być zamontowane jako nowe instalacje lub zamiast istniejących zamków baskwilowych.

Zamki KitLock KL10 są trwałe i łatwe w użyciu. Zmiana lub zresetowanie kodu nie wymaga demontażu zamka. Zamek można otwierać również za pomocą opcjonalnego klucza nadrzędnego. Główną różnicę pomiędzy nową a klasyczną linią zamków elektronicznych stanowią tryby pracy. KL10 działa tylko w trybie prywatnym, który służy do powtarzalnego otwierania z wykorzystaniem tego samego kodu. Taki zamek można zastosować na przykład w szafce pracowniczej lub szkolnej. Zabezpieczenie miejsca do przechowywania rzeczy dla jednej osoby jest jego typowym wykorzystaniem.

Zamek ma kolor czarny i elegancki wygląd. Obudowa jest wykonana z wytrzymałego stopu cynku. Klawiaturę do wprowadzania kodu obsługuje się intuicyjnie – każdy z nas zna podobny mechanizm z teczek, walizek czy kłódek. Umożliwia on ustawienie jednej z 10 000 możliwych kombinacji. Mechaniczna blokada KitLock KL10 powstała z myślą o takich miejscach zastosowania jak szkoły i małe biura, gdzie potrzebne są proste zamki szyfrowe, np. do szafek.

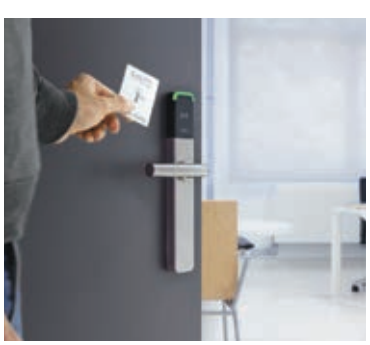
Bezpośr. inf. Maciej Prelich
Firma ATLine sp.j. Sławomir Pruski

@saltosystems

PLATFORMA KONTROLI DOSTĘPU NOWEJ GENERACJI

Nowoczesna technologia, która zapewnia użytkownikom maksymalną swobodę wyboru typu i liczby punktów dostępu, a także poziomu bezpieczeństwa.

Tworzymy inteligentne, kontrolowane elektronicznie budynki bez klucza.



SALTO SYSTEMS SP. Z O.O.
Oddział w Polsce
ul. 17 Stycznia 45A
02-146 Warszawa
Tel. 609 017 777
www.saltosystems.pl

SALTO
inspiredaccess

Bramki sensoryczne Argus
firmy dormakaba

Nowoczesne biuro to już nie tylko miejsce, w którym pracujemy, lecz przestrzeń dająca możliwość zachowania własnej indywidualności. Wszystkie firmy chcą zaprezentować się z jak najlepszej strony, dbając o elegancji wystrój w swych obiektach, który stanowi o ich prestiżu. Bramki sensoryczne Argus wywierają niezapomniane pierwsze wrażenie już od samego wejścia do holu. Wraz ze strefą recepcyjną stają się reprezentacyjną częścią budynku.

Argus to modułowy system, który można dostosować do potrzeb klientów. Oferowane są trzy rodzaje bramek Argus – **Argus 40** (o długości 1200 mm, przeznaczone do zastosowania tam, gdzie jest mało miejsca, stanowiące podstawowe zabezpieczenie), **Argus 60** (o długości 1650 mm, których wygląd można bardziej zmienić, zapewniające wysoki poziom zabezpieczenia) i **Argus 80** (o długości 1660 mm, z elegancką obudową, zapewniające wysoki poziom zabezpieczenia). Szerokość bramki może wynosić 650 mm, 900 mm lub 1000 mm, a także – zgodnie z wymogami amerykańskimi – 915 mm. Odpowiednio dobrany kąt otwarcia skrzydeł zapewnia bezproblemowe przemieszczenie się osób na wózku inwalidzkim lub transport bagażu. Argus może również zostać wyposażony w zintegrowany moduł ewakuacyjny, który nie wymaga dodatkowych badań i certyfikacji, a największa liczba punktów sensorycznych zapewnia wysoki poziom bezpieczeństwa. Wszystkie bramki są wyposażone w listwy sensoryczne, a nie pojedyncze czujniki. Dodatkowym uzupełnieniem jest oświetlenie zwiększające funkcjonalność bramki. Czerwone i zielone światło prowadzi przez korytarze w zależności od uprawnień. Dzięki nowoczesnemu wzornictwu i spójnemu designowi poręczy bramka wygląda tak, jakby była wykonana z jednego kawałka materiału. Czytnik można zainstalować w poręczy, pod szkłem, co uchroni go przed zużyciem na skutek przykładania tysięcy kart identyfikacyjnych dziennie. Instalowanie czytnika nie wymaga dodatkowych zmian konstrukcyjnych. Maksymalne wymiary czytnika to 150 mm długości, 90 mm szerokości i 30 mm głębokości. Typowa ikona RFID, która może być podświetlana na zielono i czerwono, czytelnie wskazuje pozycję czytnika. Argus jest także liderem, jeśli chodzi o liczbę cykli międzyawaryjnych – wersja 650 mm została przetestowana dla ośmiu, a wersja 900 mm dla sześciu milionów przejść.

Bezpośr. inf. Wioleta Osuch
dormakaba Polska
dormakaba.pl@dormakaba.com
www.dormakaba.pl

dormakaba

securex®
POLAND

Międzynarodowe Targi Zabezpieczeń

ZAPRASZA mtp GRUPA

21-23.04.2020
POZNAŃ

www.securex.pl

Międzynarodowe Targi Poznańskie

ZABEZPIECZ SWÓJ SUKCES!

Ekonomiczna wersja systemu RACS

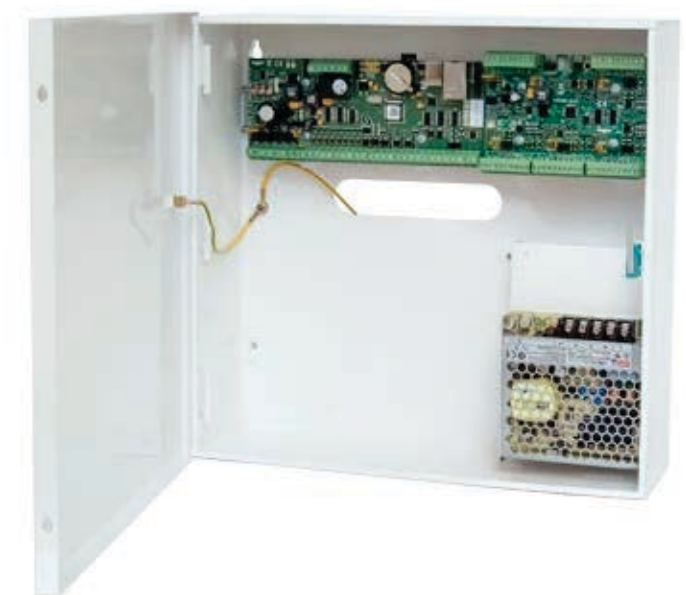
RACS 5 LT jest ekonomiczną, ograniczoną funkcjonalnie wersją systemu RACS 5 przeznaczoną do zastosowania w małych i średnich instalacjach, od których wymaga się tylko typowych funkcji związanych z elektroniczną kontrolą ruchu osób.

Do obsługi systemu RACS 5 LT służy program **VISO LT**. Program ten charakteryzuje się uproszczonym interfejsem graficznym, który z jednej strony redukuje zakres wiedzy potrzebnej do jego użytkowania, a z drugiej skraca czas potrzebny na konfigurację systemu. W systemie RACS 5 LT mogą być wykorzystane dowolne urządzenia systemu RACS 5, a także ekonomiczne wersje kontrolerów serii MC16 o oznaczeniu *MC16-LT*. Kontrolery MC16-LT są zgodne sprzętowo ze standardowymi kontrolerami serii MC16 i mogą, jeśli zajdzie taka potrzeba, zostać zaktualizowane do wyższych wersji systemu (ST lub EX) przez zakup dodatkowych licencji.

Oprócz funkcji kontroli dostępu system RACS 5 LT oferuje funkcje sterowania automatyką budynkową oraz sprzętową integrację z systemem alarmowym, która umożliwia sterowanie nim z poziomu terminali dostępu, a także prezentację stanów stref alarmowych na terminalach dostępu. Oprogramowanie zarządzające systemem umożliwia monitorowanie jego pracy w czasie rzeczywistym, monitorowanie osób przebywających w dowolnie zdefiniowanych strefach obiektu, pomiar czasu przebywania użytkowników w tych strefach, a także rejestrację zdarzeń w związku z rejestracją czasu pracy. W ramach integracji z kamerami CCTV możliwa jest rejestracja zdjęć oraz filmów powiązanych ze zdarzeniami, a także podgląd na żywo obrazów z kamer.

Bezpośr. inf. ROGER

Zestawy urządzeń do kontroli dostępu przeznaczone do systemu RACS 5



Zestawy urządzeń do kontroli dostępu to fabrycznie skompletowane i zmontowane w jednej metalowej obudowie urządzenia, które stanowią zasadniczy komponent sprzętowy służący do budowy systemu elektronicznej kontroli przejść. Oferowane są zestawy przeznaczone do obsługi jednego, dwóch, trzech lub czterech przejść. W skład zestawu, oprócz metalowej obudowy, wchodzi moduł kontrolera, zasilacz sieciowy oraz, opcjonalnie, ekspander linii we/wy.

Zestawy zostały zaprojektowane w taki sposób, aby umożliwić dwustronną kontrolę każdego z dozorowanych przejść wraz z obsługą czujnika stanu skrzydła drzwi, przycisku wyjścia, zamka elektrycznego oraz sygnalizatora alarmowego. Przyjęto zasadę, że zestaw musi zabezpieczać prąd zasilania na poziomie 1 A oraz miejsce na akumulator rezerwowy o pojemności nie mniejszej niż 3 Ah na każde obsługiwane przejście. Akumulator jest doładowywany stabilizowanym prądem i zabezpieczony przed głębokim rozładowaniem, a jego stan naładowania jest dozorowany elektronicznie.

Zestawy nie zawierają czytników, które dobiera się stosownie do wymagań dotyczących danej instalacji. Do zestawów można dołączyć zarówno czytniki serii MCT (RS485), jak i czytniki z interfejsem Wiegand, przy czym w tym ostatnim przypadku ich liczba jest ograniczona do czterech.

Zastosowanie zestawów upraszcza zarówno projektowanie systemu, jak i jego instalację, minimalizując ryzyko wystąpienia problemów wynikających z nieprawidłowego doboru sprzętu. Zestawy zostały zoptymalizowane pod kątem ekonomicznego doboru obudów oraz zasilaczy sieciowych.

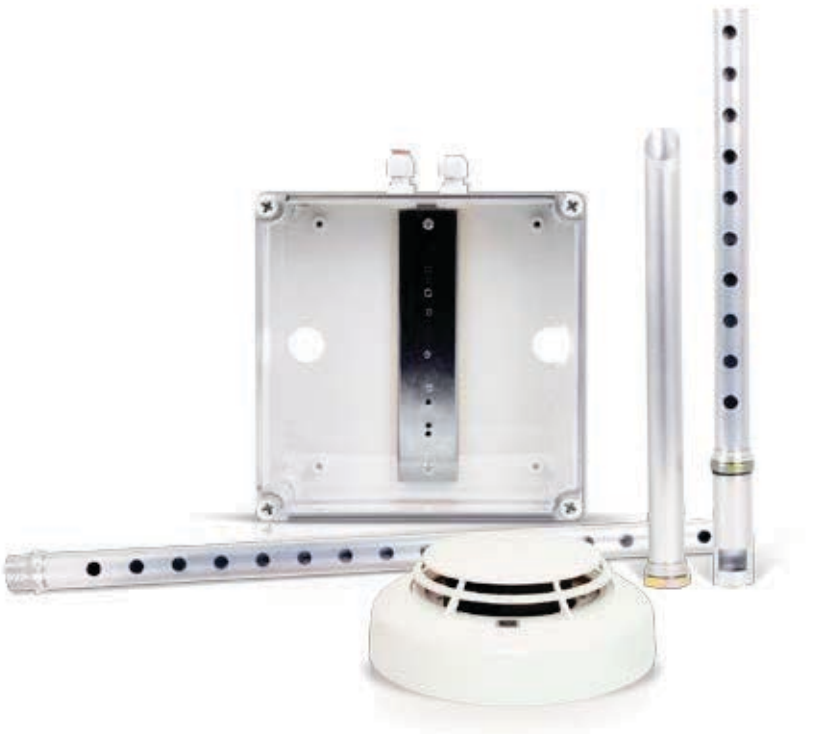
Cena zestawu odpowiada sumie cen jego elementów składowych.

Zestawy są wykorzystywane głównie w rozproszonych instalacjach, w których urządzenia kontrolujące przejścia są zwykle montowane w ich pobliżu. Wariant rozproszony zapewnia dużą stabilność działania kontroli dostępu ze względu na podział instalacji na grupy od jednych do czterech drzwi obsługiwanych przez niezależne zestawy kontroli dostępu. Dodatkowo w wariancie tym zwykle nie ma potrzeby stosowania przewodów o większych przekrojach, gdyż długości połączeń kablowych pomiędzy kontrolerem a urządzeniami współpracującymi (czytnikami, zamkami, czujnikami, przyciskami) są relatywnie małe, co redukuje zarówno koszt użytych kabli, jak i koszt ich rozprowadzenia.

Bezpośr. inf. ROGER

Kanałowa czujka dymu DUO-6046K

nowość w ofercie firmy POLON-ALFA



Systemy wentylacji i klimatyzacji są niezbędnymi elementami nowoczesnych obiektów. Bardzo ważne jest szybkie wykrycie zadymienia wewnątrz kanałów wentylacyjnych, gdyż dzięki temu jest szansa na reakcję i wykluczenie rozprzestrzeniania się dymu pomiędzy pomieszczeniami poprzez system wentylacji.

Norma EN54-27 określa wymagania dotyczące detekcji pożaru w kanałach wentylacyjnych, jako że wykrycie zadymienia wewnątrz kanałów wentylacji nie jest łatwe. Ze względu na warunki pracy systemu wentylacji, w tym obecność kurzu, pyłu, pary wodnej, zmienną wilgotność, a także dużą prędkość przepływu powietrza stosowanie czujek dymu we wnętrzu kanału jest wykluczone.

Zadymienie i pożar w kanałach wentylacyjnych skutecznie wykrywają czujki kanałowe **DUO-6046K** lub **DUR-40K**, które współpracują z oferowanymi przez **POLON-ALFA** systemami sygnalizacji pożarowej **POLON 6000**, **POLON 4000** lub **IGNIS**.

Czujka DUO-6046K jest oferowana w zestawie z gniazdem G-40, osłoną, rurkami zasysającymi o różnej długości i rurką wylotową. Jest to zestaw DUO-6046K. W zestawie DUR-40K jest czujka DUR-40, a pozostałe elementy są takie same.

Czujki kanałowe DUO-6046K oraz DUR-40K sprawdzą się w wykrywaniu zagrożeń pożarowych w każdym współczesnym obiekcie. W ich nowoczesnych konstrukcjach zastosowano rozproszeniowy dualny (DUO-6046K) lub ultrafioletowy (DUR-40K) sensor dymu, ograniczając do minimum podatność na fałszywe alarmy. Dodatkowo, dzięki doborowi odpowiedniego trybu pracy, czujki umożliwiają korekcję progu reakcji na zadymienie, dzięki czemu system jest odporny na zwodnicze czynniki, takie jak chwilowe zapylenie, które może wystąpić wewnątrz kanałów doprowadzających powietrze.

Czujka DUO-6046K uzyskała certyfikat 1438-CPR-0652.

Właściwości czujki DUO-6046K:
- zakres prędkości powietrza w kanale 1–20 m/s;
- długość bazowych rurek: 240 mm (zasysanie) i 240 mm (wylot);
- długości opcjonalnych rurek zasysających: 600 mm, 900 mm i 1200 mm;
- współpraca z systemami POLON 6000, POLON 4000 (DUO-6046K), IGNIS 1000 i IGNIS 2000 (DUR-40K);
- wykrywanie pożarów kategorii TF2D, TF4D, TF8D.

Zalecana wysokość zabezpieczanego kanału to 440–2400 mm.

Bezpośr. inf.
Krzysztof Marchlewski
POLON-ALFA
www.polon-alfa.pl

ULISSE EVO THERMAL

Prewencyjna ochrona obwodowa w trybie ciągłym

ULISSE EVO THERMAL jest kamerą termowizyjną PTZ przeznaczoną do stosowania w wizyjnych systemach dozorowych służących do prewencyjnej obserwacji obszarów miejskich, obiektów infrastruktury krytycznej, środków transportu lub infrastruktury drogowej i kolejowej. Może także mieć zastosowania związane z wykrywaniem pożarów.

Kamera termowizyjna w wersji podstawowej umożliwia pomiar temperatury obserwowanych obiektów na podstawie danych z czterech centralnych pikseli obrazu. W wersji zaawansowanej pomiar może się odbywać w dowolnie wybranym punkcie obrazu. Funkcje radiometryczne umożliwiają określenie granicznych temperatur, których przekroczenie powoduje alarm.

Kamery ULISSE EVO THERMAL mogą pracować w nieprzyjaznych warunkach środowiskowych i temperaturach od -40°C do +65°C. Stopnie ochrony IK10 i IP66/IP67/IP68, NEMA typ 4X i NEMA typ 6P gwarantują maksymalną odporność na kurz i niesprzyjającą pogodę, silne udary mechaniczne i akty wandalizmu.

Kamery ULISSE EVO THERMAL odznaczają się bardzo wysoką odpornością na korozję, osiągniętą dzięki odpowiedniej obróbce powierzchni elementów aluminiowych oraz zastosowaniu technopolimerów.

Kamera ULISSE EVO THERMAL ma podłużny kształt. Jej konstrukcja łączy w sobie maksymalną wytrzymałość i niezawodność z bardzo ograniczoną wagą. Oznacza to łatwy i szybki montaż, a tym samym niższe koszty instalacji i konserwacji.

Kamery ULISSE EVO mogą być instalowane na różne sposoby, nawet w pozycji odwróconej, typowej dla szybkoobrotowych kamer kopułowych, z użyciem różnych dostępnych wysięgników i zamocowań, w celu spełnienia wszystkich wymagań instalacyjnych. Wysięgniki są wyposażone w szybkozłączki do podłączania kabli ethernetowych oraz sterujących, dzięki czemu prace instalacyjne są

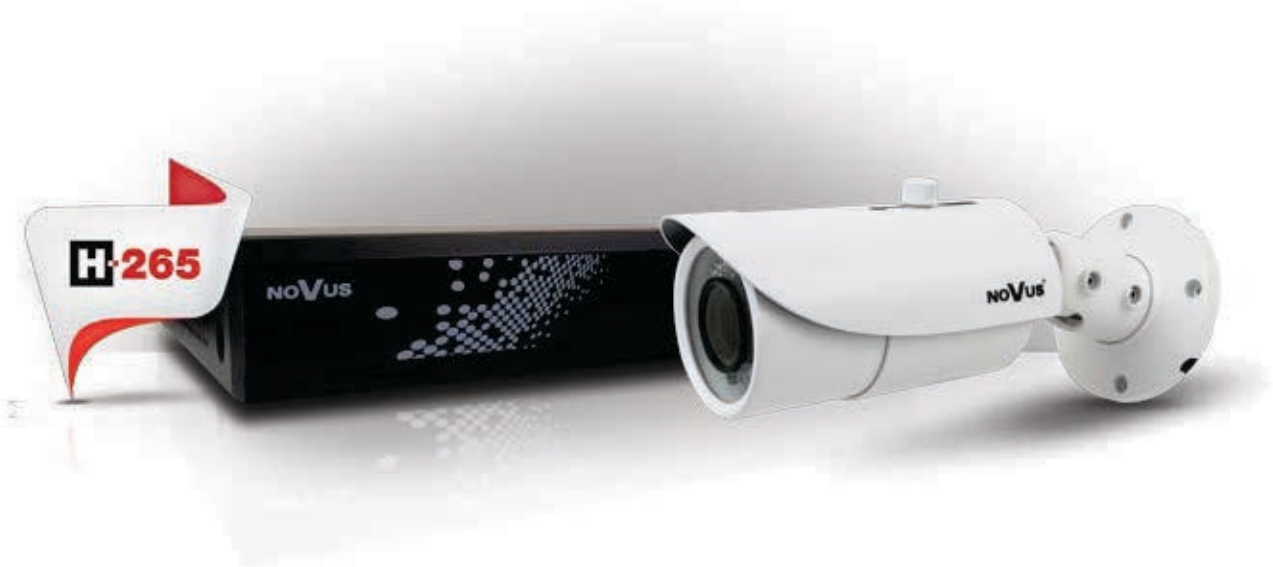
znacznie ułatwione. Kamery pracują bezobsługowo i nie wymagają konserwacji.

Kamery ULISSE EVO THERMAL są dostępne w dwóch standardowych kolorach, szaro-białym i czarnym, aby dopasowanie ich do konkretnego miejsca instalacji było łatwiejsze.

Bezpośr. inf. Videotec
www.videotec.com
Informacje dot. sprzedaży: sales@videotec.com
Kontakt z mediami:
Martina Panighel
martina.panighel@videotec.com
Tłumaczenie: Andrzej Walczyk

Rejestratory AHD

umożliwiające kompresję H.265 i obsługujące kamery o rozdzielczości do 8 Mpx



Zastosowany algorytm **kompresji H.265** umożliwia optymalizację danych strumienia wizyjnego i tym samym lepsze wykorzystanie archiwum, szczególnie w przypadku kamer o wysokich rozdzielczościach. Ponadto zachowano możliwość pracy z wykorzystaniem algorytmu kompresji H.264 w przypadku mniej wydajnych urządzeń peryferyjnych wykorzystywanych w systemie wizyjnym, np. komputerów z zainstalowanym oprogramowaniem **NHDR-5000Viewer**.

Nowe modele rejestratorów będą obsługiwały kamery o rozdzielczościach nawet do **8 Mpx** i stanowiły równą pod względem jakości alternatywę dla systemów IP, posiadając zarazem zalety systemów analogowych, do których należy prostota instalacji i konfiguracji, a także niewygórowana cena.

Wybrane modele rejestratorów mają funkcje inteligentnej analizy treści obrazu. Wykrywają przekroczenie linii, wejście do strefy oraz pozostawienie albo zniknięcie obiektu.

Wszystkie modele są hybrydowe. Umożliwiają dodatkowo pobieranie nawet ośmiu strumieni IP (do 8 Mbps na strumień) lub pracę w trybie IP i zamianę sygnałów analogowych na strumienie cyfrowe. Rejestratory korzystają z inteligentnych funkcji kamer serii 4000.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Nowe funkcje rejestratorów z serii NVR4000IP

Dotychczas dostępne modele rejestratorów z serii 4000 **NVR-4116-H1**, **NVR-4308P8-H1** oraz **NVR-4204P4-H1PIR** zostały wzbogacone w nowe funkcje, które znacznie zwiększają ich użyteczność w wizyjnych systemach dozorowych.

Kamery z wbudowanymi czujkami PIR we współpracy z wymienionymi rejestratorami pozwalają wyeliminować wpływ takich niekorzystnych zjawisk w obserwowanej scenie jak padające snopy światła z reflektorów przejeżdżających aut lub poruszanie się krzewów i drzew pod wpływem wiatru. Dzięki temu możliwe jest ograniczenie liczby fałszywych alarmów i zaoszczędzenie przestrzeni w archiwum.

Rejestratory pozwalają zobrazować nie tylko strumienie z kamer ale również strumienie RTSP z innych rejestratorów serii 4000 lub AHD. Dzięki tej funkcji można przygotować punkty zdalnego nadzoru wybranych strumieni wizyjnych bez wykorzystania jednostki komputerowej.

Dodatkowo wprowadzono funkcję detekcji dźwięku oraz funkcję sygnalizacji sabotażu w przypadku przestawienia lub zasłonięcia kamery.

Podczas lokalnego podglądu na żywo lub odtwarzania obrazów archiwalnych operator może oznaczać interesujące fragmenty i opisywać znaczniki oraz w szybki sposób je wyszukiwać w zarchiwizowanym materiale.

W celu zabezpieczenia nagrań pojedyncze zdjęcie lub krótki film ukazujący przebieg zdarzenia może zostać automatycznie przesłany na dyski sieciowe Google Drive lub Dropbox po uprzednim podaniu adresu e-mailowego. Ponadto dane na tych wirtualnych dyskach mogą być nadpisywane.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Kamery Dahua z serii 5

Kamery **Dahua DH-IPC-HDBW5442EP-ZE z serii 5** należą do kolejnej generacji kamer sieciowych spełniających wysokie wymagania jakościowe. Zostały wyposażone w przetwornik 4 Mpx 1/1.8" CMOS, dzięki czemu liczba detali rozróżnianych w obrazie jest jeszcze większa niż w poprzednich modelach. Dzięki wysokiej czułości użytkownik może liczyć na efektywną pracę kamer w trudnych warunkach oświetleniowych. Nie bez znaczenia jest również zastosowany obiektyw o sile światła F1.8 i ogniskowej regulowanej w zakresie od 2,7 mm do 12 mm. W nowych kamerach nie tylko zastosowano inny niż w urządzeniach poprzedniej generacji przetwornik. Zwiększono do 1 GB pojemność pamięci RAM, co umożliwia wykorzystanie bardziej zaawansowanych algorytmów analizy treści obrazu. Od teraz, kamery z serii 5000 pozwalają na korzystanie z algorytmów sztucznej inteligencji.

Oprócz znanych już funkcji, takich jak detekcja przekroczenia linii, wykrycie intruza i wykrycie zniknięcia lub pojawienia się obiektu, seria 5 umożliwia wykrywanie twarzy wraz z analizą ich obrazów. Na tej podstawie można ocenić wiek i płeć obserwowanej osoby, stwierdzić, że nosi okulary, zarost lub próbuje zamaskować twarz. Detekcja intruzów jest jeszcze skuteczniejsza niż wcześniej dzięki klasyfikacji obiektu (człowiek/pojazd). Oprócz tego kamery z serii 5 zyskały funkcję dostępną wcześniej tylko w najwyżej serii Ultra. Mowa o zliczaniu osób wchodzących, wychodzących i przebywających w zdefiniowanej strefie. Nowość w przypadku serii 5 polega na wykorzystaniu wcześniej wspomnianych algorytmów AI, które umożliwiają osiągnięcie niespotykanej do tej pory dokładności wyników analizy. Kolejną nowością w serii 5 jest funkcja cyfrowej redukcji efektu mgły na obrazie. Bez zmian pozostaje ilość i przepływność generowanych strumieni wizyjnych. Kamery z serii 5 umożliwiają generowanie trzech niezależnych strumieni – pierwszego o maksymalnej rozdzielczości 4 Mpx, pomocniczego o rozdzielczości D1 i trzeciego, który może mieć rozdzielczość Full HD.

Oczywiście użytkownik może korzystać ze wszystkich najpopularniejszych metod kompresji obrazu, w tym z najnowszego kodeka H.265, który pozwala na jeszcze wydajniejszą kompresję bez znacznej utraty jakości obrazu.

Kamery z serii 5 są wyposażone w estetyczne wandaloodporne obudowy o odporności na udary mechaniczne IK10 oraz odporności na wilgoć i kurz IP67.

Bezpośr. inf. Maciej Pietrzak
Dahua Technology Poland

Caesar

system kontroli dostępu dla wymagających

Firma **Dahua Technology** ma w swojej ofercie szereg rozwiązań służących do kontroli dostępu. Na szczególną uwagę zasługują sieciowe kontrolery z serii **Caesar**. Ze względu na swoją pojemność, funkcjonalność i otwartość na integrację system ten docenią ci, którzy oczekują czegoś więcej niż tylko kontroli stanu drzwi.

Aktualnie seria Caesar składa się z trzech urządzeń: **ASC2204C-H** (kontroler *master* obsługujący cztery przejścia jednostronnie kontrolowane, 200 000 użytkowników i 150 000 zdarzeń), **ACS2104B-T** (kontroler *slave*, podkontroler czterech przejść jednostronnie kontrolowanych) i **ASC2102B-T** (kontroler *slave*, podkontroler dwóch przejść dwustronnie kontrolowanych). Każdy z kontrolerów typu *slave* obsługuje 20 000 użytkowników i 30 000 zdarzeń. Do kontrolera *master* można podłączyć przez magistralę CAN szesnaście podkontrolerów *slave*. Każdy ze sterowników jest wyposażony w porty RS485 i Wiegand do obsługi czytników oraz zaciski do obsługi czujników stanu drzwi, przycisków wyjścia, stanów alarmowych i elementów ryglujących. Przypisanie konkretnych funkcji do konkretnych wejść znajdujących się na płytach urządzeń bardzo upraszcza proces konfiguracji kontrolerów.

Pojedynczy kontroler *master* może obsłużyć szesnaście podkontrolerów, co umożliwia zbudowanie struktury złożonej z 68 przejść. Taka topologia ma szereg zalet, np. wykorzystuje tylko jeden adres IP dla 68 przejść i obsługuje sprzętowo globalną funkcję *anti-passback* oraz funkcję śluzy. Wszystkie globalne funkcje są realizowane bez udziału serwera, dzięki czemu proces ten przebiega niezwykle szybko i nie jest obciążony ryzykiem utraty tych funkcji na skutek przerwania połączenia ze stacją nadzorującą. Dodatkowo kontroler główny jest wyposażony w dwie niezależne karty sieciowe i może być zintegrowany z platformami programowymi innych dostawców.

Pełna oferta firmy Dahua Technology jest dostępna pod adresem http://pl.dahuasecurity.com/pl.

Bezpośr. inf. Grzegorz Michalski
Dahua Technology Poland
e-mail:
grzegorz.michalski@dahuatech.com

Walne zgromadzenie Polskiego Związku Pracodawców Ochrona

podsumowanie

11 czerwca 2019 r. w hotelu Warszawianka w Jachrance odbyło się **XXXI Walne Zgromadzenie Sprawozdawczo-Wyborcze Polskiego Związku Pracodawców Ochrona**.

Podczas tegorocznych obrad zatwierdzono sprawozdanie finansowe za 2018 rok, wręczono grawertony z okazji 10-, 15-, 20-, i 25-lecia działalności firm członkowskich oraz wybrano prezesa i zarząd na kolejne cztery lata. Po raz drugi prezesem Polskiego Związku Pracodawców Ochrona został Tomasz Wojak, pełniący również funkcję prezesa zarządu firmy SERIS Konsalnet Security.

Polski Związek Pracodawców Ochrona zrzesza 91 agencji ochrony, a 12 firm wspiera jego działalność. Współpracuje z różnymi instytucjami państwowymi i administracji publicznej, uczestniczy w tworzeniu nowych przepisów prawnych, a wszystko po to, aby wyznaczyć nowe standardy w branży ochrony osób i mienia i wesprzeć działalność firm zajmujących się ochroną.

Podczas tegorocznego walnego zgromadzenia można było zasięgnąć porad prawnych u przedstawicieli Enodo Advisors – firmy zajmującej się doradztwem podatkowym.

Wśród prelegentów byli przedstawiciele Federacji Przedsiębiorców Polskich oraz Komendy Głównej Policji.

Tematem prelekcji były wyzwania dla branży ochrony, m.in. problemy z pozyskaniem nowych pracowników i ich zatrudnieniem na atrakcyjnych warunkach. Przedstawiono sytuację na rynku ochrony w Europie i w Polsce. Polscy pracownicy ochrony zarabiają coraz więcej, a największe zapotrzebowanie na nich jest wciąż w obiektach handlowych. Większość jest zatrudniania na podstawie umowy o pracę.

Omówiono również zasady wdrożenia Pracowniczych Planów Kapitałowych oraz nadchodzące zmiany w prawie zamówień publicznych.

Spotkaniu towarzyszyła wystawa produktów i usług. Na zakończenie wszyscy goście mieli okazję biesiadować przy grillu.

Serdecznie dziękujemy za możliwość wzięcia udziału w spotkaniu, a zarządowi Polskiego Związku Pracodawców Ochrona życzymy powodzenia w osiąganiu wyznaczonych celów, rozwoju i sukcesów.

Zapraszamy do obejrzenia fotorelacji ze spotkania (https://www.zabezpieczenia.com.pl/fotogalerie).

Ela Końka

Bosch Partners Day 2019

podsumowanie

14 maja br. w Folwarku Łochów odbyła się kolejna edycja **Bosch Partners Day** zorganizowana przez dział **Bosch Security and Safety Systems** firmy **Robert Bosch**. W spotkaniu wzięło udział prawie 140 przedstawicieli firm partnerskich.

Konferencja rozpoczęła się od przedstawienia Rafała Rudzińskiego – nowego prezesa firmy Robert Bosch w Polsce, który objął stanowisko na początku bieżącego roku. W swoim wystąpieniu Rafał Rudziński zwrócił uwagę na wskaźniki wzrostu w 2018 roku, które wskazują m.in. na zwiększenie obrotów firmy, wzrost zatrudnienia i coraz większe wydatki na badania i rozwój.

W skład grupy Bosch w Polsce wchodzą cztery spółki: Robert Bosch, BSH Sprzęt Gospodarstwa Domowego, Bosch Rexroth i sia Abrasives. Zatrudnionych jest około 7000 pracowników. Na terenie Polski znajduje się osiem fabryk i trzy centra badań i rozwoju.

Poza zintegrowanymi systemami zabezpieczeń wykorzystywanymi na całym świecie firma ma na swoim koncie również takie innowacyjne rozwiązania jak autonomiczne taksówki, wodorowe ogniwa paliwowe do samochodów ciężarowych i osobowych, a także czujniki MEMS wykorzystywane m.in. w smartfonach, dronach i konsolach do gier.

Ze względu na ochronę klimatu firma Robert Bosch planuje znaczne zmniejszenie emisji dwutlenku węgla od 2020 roku.

W dalszej części konferencji Krzysztof Góra – dyrektor handlowy działu Bosch Security and Safety Systems odpowiedzialny za rynek w Polsce, w Czechach, na Słowacji i na Ukrainie omówił wzrost gospodarczy i zmiany na świecie, które mają wpływ na rynek budowlany i wzrost sprzedaży systemów zabezpieczeń w Polsce.

W 2018 roku Bosch Security and Safety Systems odnotował wzrost sprzedaży we wszystkich krajach w regionie SEP i wygrał ponad 1100 przetargów. Polski oddział zajął trzecie miejsce pod względem sprzedaży w regionie EMEA i pierwsze miejsce w sprzedaży SAP.

Krzysztof Góra zaprezentował projekty zrealizowane z partnerami Bosch Security and Safety Systems na terenie Polski. Systemy zabezpieczeń Bosch sprawdzają się zarówno w dużych przedsiębiorstwach przemysłowych czy kompleksach biurowych, jak i w apartamentowcach i muzeach.

W dalszej części konferencji odbyły się prezentacje nowych produktów, w tym innowacyjnych stałopozycyjnych kamer kopułkowych z serii FLEXIDOME IP Starlight 8000i oraz kompaktowych kamer z serii IP 3000 do zastosowań wewnątrz i na zewnątrz budynków, a także omówiono unikatowe cechy systemu Paviro.

Jakub Bednarz przedstawił wytyczne dotyczące planowania i instalacji czujek kanałowych. Omówił przykłady systemów sygnalizacji pożarowej Bosch działających w magazynach oraz w przedsiębiorstwach przemysłowych. W siedzibie firmy Robert Bosch w Warszawie jest dostępna nowoczesna sala szkoleniowa, w której można zapoznać się z funkcjonowaniem zainstalowanych tam systemów.

Jerzy Ciszewski z IBP Nodex omówił organizację alarmowania i sposoby sterowania urządzeniami automatyki przemysłowej, a przedstawiciel firmy Kaspersky zagadnienia związane z bezpieczeństwem danych w Internecie rzeczy.

Konferencja zakończyła się uroczystą kolacją i galą, którą poprowadził znany prezenter telewizyjny i radiowy Tomasz Kammel. Podczas kolacji rozdano nagrody za wyniki sprzedaży w 2018 roku oraz promowanie rozwiązań marki Bosch na rynku systemów zabezpieczeń.

Serdecznie dziękujemy za spotkanie i życzymy całemu zespołowi Bosch Security and Safety Systems powodzenia i sukcesów.

Zapraszamy do obejrzenia fotorelacji na naszej stronie internetowej (https://www.zabezpieczenia.com.pl/fotogalerie).

Ela Końka

Czwarta edycja seminarium
podsumowanie

18 czerwca w warszawskim Centrum Nauki Kopernik odbyła się kolejna edycja **seminarium Videotec & CBC Poland**. Spotkanie zgromadziło ponad 50 uczestników – integratorów, projektantów systemów zabezpieczeń technicznych, osób odpowiedzialnych za techniczne aspekty zabezpieczenia obiektów o specjalnych wymaganiach, a także inwestorów i przedstawicieli administracji publicznej.

Spotkania organizowane przez firmy partnerskie są już na stałe w kalendarzu imprez branżowych. W tym roku, w ramach czwartej edycji, uczestnicy mieli okazję posłuchać o najnowszych rozwiązaniach i możliwościach systemów CCTV marki Videotec oraz GANZ przeznaczonych do zastosowania w obiektach infrastruktury krytycznej i inteligentnym mieście.

– *Miejsce spotkania wybraliśmy nieprzypadkowo. Centrum Nauki Kopernik to instytucja, której celem jest popularyzacja i rozwijanie nauki. Wspólnym naszym obszarem zainteresowania jest obserwacja całego świata. Naukowcy skupiają się na obserwacji gwiazd, a my dzisiaj skupimy się na obserwacji za pomocą prezentowanych kamer* – powiedział na wstępie Krzysztof Skowroński, Branch Manager w CBC Poland.

W trakcie seminarium Alessandro Franchini i Matteo Abrahamsohn z firmy Videotec w trzech blokach tematycznych opowiedzieli o przeszłości i planach firmy, seriach produktowych i kryteriach doboru kamer, zaprezentowali najnowsze rozwiązania Videoteca oraz podali najciekawsze referencje i przykłady wdrożeń.

Krzysztof Skowroński z CBC Poland zaprezentował najnowsze funkcje oprogramowania VMS Ganz CORTROL, które jako niezwykle wszechstronne i rozbudowane narzędzie, mające szereg zaawansowanych funkcji i dodatków, może stanowić centralny ośrodek systemu wspomagania inteligentnego miasta. Bierne systemy telewizji dozorowej są zastępowane nowoczesnymi rozwiązaniami, które zmieniają je w aktywne narzędzia do zarządzania funkcjonowaniem i ochroną miasta.

Na specjalnie przygotowanych stoiskach zaprezentowano wybrane rozwiązania oferowane przez firmy Videotec i CBC Poland. W trakcie przerw uczestnicy mogli zapoznać się z oprogramowaniem Ganz CORTROL VMS oraz zobaczyć, jak działa ULISSE EVO – wszechstronna kamera PTZ o nowoczesnym i niespotykanym wyglądzie, zapewniająca najwyższy poziom bezpieczeństwa monitorowanych obszarów miejskich,

Videotec & CBC Poland

obiektów infrastruktury krytycznej, środków transportu, infrastruktury drogowej i kolejowej. Wykorzystana w ULISSE EVO autorska metoda kodowania obrazów DELUX powoduje, że zarówno w dzień, jak i w nocy kamera wytwarza barwne obrazy, które są wyraźne i pełne szczegółów, a szereg dodatkowych funkcji, konstrukcja i wyposażenie obudowy oraz konkurencyjna cena czynią to rozwiązanie wyjątkowo atrakcyjnym.

W trakcie spotkania nie zabrakło też czasu na podsumowania. Współpraca firm Videotec i CBC Poland trwa nieprzerwanie od 22 lat. CBC Poland jako partner zrzeszony w programie Videotec Executive Club oferuje swoim klientom dostęp do znakomitych produktów, specjalną politykę rabatową oraz silne wsparcie projektowe i posprzedażowe. Firma ta po raz kolejny została czołowym sprzedawcą produktów Videoteca, potwierdzając tym samym swoją mocną i ugruntowaną pozycję na polskim rynku.

Zwieńczeniem spotkania był pokaz w planetarium Niebo Kopernika. Organizatorzy zaprosili swoich gości na obsypaną nagrodami produkcję *Na skrzydłach marzeń*, dzięki której można było zbliżyć się na chwilę do gwiazd, pojeździć łazikiem na Marsie i zajrzeć do wnętrza stacji kosmicznej.

Więcej informacji na temat prezentowanych rozwiązań znajduje się na www.cortrol.eu/pl oraz www.videotec.com.

Zapraszamy do obejrzenia fotorelacji na stronie internetowej https://www.zabezpieczenia.com.pl/fotogalerie.

Bezpośr. inf. Dagmara Dąbrowska
CBC Poland

NIST rekomenduje specyfikację ONVIF jako nowy standard dla FBI

Andrea Gural

ONVIF jest globalną organizacją zajmującą się standaryzacją urządzeń przeznaczonych do stosowania w wizyjnych systemach dozorowych opartych na protokole IP. Organizacja ta ogłosiła, że format plików stosowany do eksportowania materiału wizyjnego z rejestratorów sieciowych zgodnych z najnowszą specyfikacją ONVIF jest standardowym formatem zalecanym przez Narodowy Instytut Norm i Technologii (NIST) do eksportowania i odtwarzania nagrań z wizyjnych z systemów dozorowych.

W projekcie badawczym zleconym przez FBI, mającym na celu usprawnienie działań organów ścigania w dochodzeniach kryminalistycznych, NIST współpracował z ONVIF w celu ujednolicenia formatu plików przeznaczonych do eksportu obrazów, który spełniałby nowe minimalne wymagania FBI w zakresie interoperacyjności podczas korzystania z materiałów wizyjnych pochodzących z różnych systemów dozorowych. Pliki te są często eksportowane w różnych zastrzeżonych formatach, co utrudnia organom ścigania gromadzenie, korelowanie i analizowanie materiałów dowodowych. Taka sytuacja miała miejsce na maratonie bostońskim w 2013 r., w czasie którego nastąpił terrorystyczny atak bombowy. Ponad 120 analityków FBI przeanalizowało ponad 13 000 filmów przed odkryciem kluczowych dowodów. Rekomendacja NIST jest opublikowana jako *NISTIR 8161 wersja 1*, która zastępuje wersję 0.

Ujednolicony format plików zalecany przez ONVIF umożliwi organom ścigania, a także użytkownikom prywatnym, szybsze i skuteczniejsze przeprowadzanie badań kryminalistycznych z wykorzystaniem materiałów wizyjnych dokumentujących zaistniałe incydenty, pochodzących z różnych źródeł, zarówno prywatnych, jak i publicznych. Ujednolicony format eksportowanych plików będzie również częścią nowych globalnych standardów, które zostaną opublikowane w tym roku przez Międzynarodową Komisję Elektrotechniczną (IEC).

– *Jest to duży krok w kierunku wykorzystania obszernych materiałów dowodowych gromadzonych przez wizyjne systemy dozorowe oparte na protokole IP. W przypadku poważnych incydentów materiały te mogą być udostępnione organom ścigania oraz innym użytkownikom oczekującym szybkiego i łatwego dostępu do plików wizyjnych* – powie-

dział Per Björkdahl, przewodniczący komitetu sterującego ONVIF. – *Byliśmy bardzo zadowoleni z tego, że mogliśmy zaoferować nasze kompetencje, zwłaszcza specjalistyczną wiedzę naszych ekspertów technicznych, dra Hansa Buscha i Stefana Andersona, i że nasza praca na rzecz interoperacyjności została doceniona przy tworzeniu globalnych standardów wykorzystywanych przez służby bezpieczeństwa i prawników.*

Per Björkdahl

Raport NIST dotyczy szczegółów technicznych, takich jak zalecenie używania MP4 jako standardowego formatu plików, oraz opisuje obsługę kodeków wizyjnych H.264, jak przyszłych wariantów tych kodeków, co ma na celu zachowanie odpowiedniej jakości obrazu. Wyeksportowane pliki muszą zawierać znormalizowane znaczniki czasu UTC, które odpowiadają każdej klatce wizyjnej, wraz z dodatkowymi informacjami pochodzącymi z wiarygodnego źródła określającego czas rejestracji i eksportu plików. Ujednolicony format plików pozwoli na eksportowanie danych dotyczących sprzętu, na którym zostało utworzone nagranie, nazwy operatora eksportującego pliki itp., a także na umieszczenie w pliku wizyjnym cyfrowego podpisu w celu uwiarygodnienia materiału dowodowego.

Organizacja ONVIF została założona w 2008 roku i jest czołowym, uznanym forum branżowym dbającym o interoperacyjność urządzeń wizyjnych opartych na protokole IP. Organizacja ma zasięg globalny i zrzesza znane firmy zajmujące się produkcją kamer i innych składników wizyjnych systemów dozorowych, a także systemów kontroli dostępu. Dotychczas ponad 12 000 produktów uzyskało certyfikat zgodności ze specyfikacją ONVIF. Wśród tych certyfikatów rozróżnić można profil S dla standardowych urządzeń wizyjnych, profil G dla urządzeń peryferyjnych, profil C dla urządzeń służących do kontroli ruchu pieszego i zarządzania zdarzeniami, profil Q dla urządzeń przeznaczonych do szybkiej instalacji, profil A dla urządzeń stosowanych w systemach kontroli dostępu i profil T dla zaawansowanych technicznie urządzeń wizyjnych. ONVIF kontynuuje współpracę ze swoimi członkami w celu dalszej poprawy interoperacyjności sieciowych urządzeń wizyjnych pochodzących od różnych dostawców.

Szczegółowe informacje na temat produktów zgodnych ze specyfikacją ONVIF oraz firm członkowskich biorących udział w pracach tej organizacji są dostępne na stronie www.onvif.org.

Andrea Gural
Eclipse Media Group on behalf of ONVIF
Tłumaczenie: Andrzej Walczyk

Bezpieczeństwo w systemach kontroli dostępu

Andrzej Walczyk

Systemy kontroli dostępu są znane i używane od dziesięcioleci. Tak jak wszystkie dziedziny techniki, podlegają one ciągłej ewolucji. Pierwsze systemy, które można już nazwać elektronicznymi, pojawiły się w latach siedemdziesiątych zeszłego stulecia. Działanie kart identyfikacyjnych opierało się na wykorzystaniu tak zwanego efektu Wieganda oraz protokołu komunikacyjnego o tej samej nazwie

Budowa kart identyfikacyjnych Wieganda

Pierwsze karty identyfikacyjne były podobne pod względem rozmiarów do wizytówki lub karty kredytowej. Ich zasada działania była bardzo prosta. W ich wnętrzach zatopione były stalowe druciki. Rdzeń każdego drucika był wykonany z materiału miękkiego magnetycznie, a płaszcz z materiału twardego magnetycznie. Tak przygotowane druciki miały bardzo stabilną charakterystykę magnesowania, którą zawdzięczały wspomnianemu wcześniej efektowi Wieganda, czyli zjawisku fizycznemu występującemu w materiałach magnetycznych, którego opis wykracza poza ramy tego artykułu. Wystarczy stwierdzić, że wprowadzenie kodu polegało na odpowiednim namagnesowaniu kolejnych drucików. Odczyt następował podczas przeciągnięcia karty przez szczelinę w czytniku.

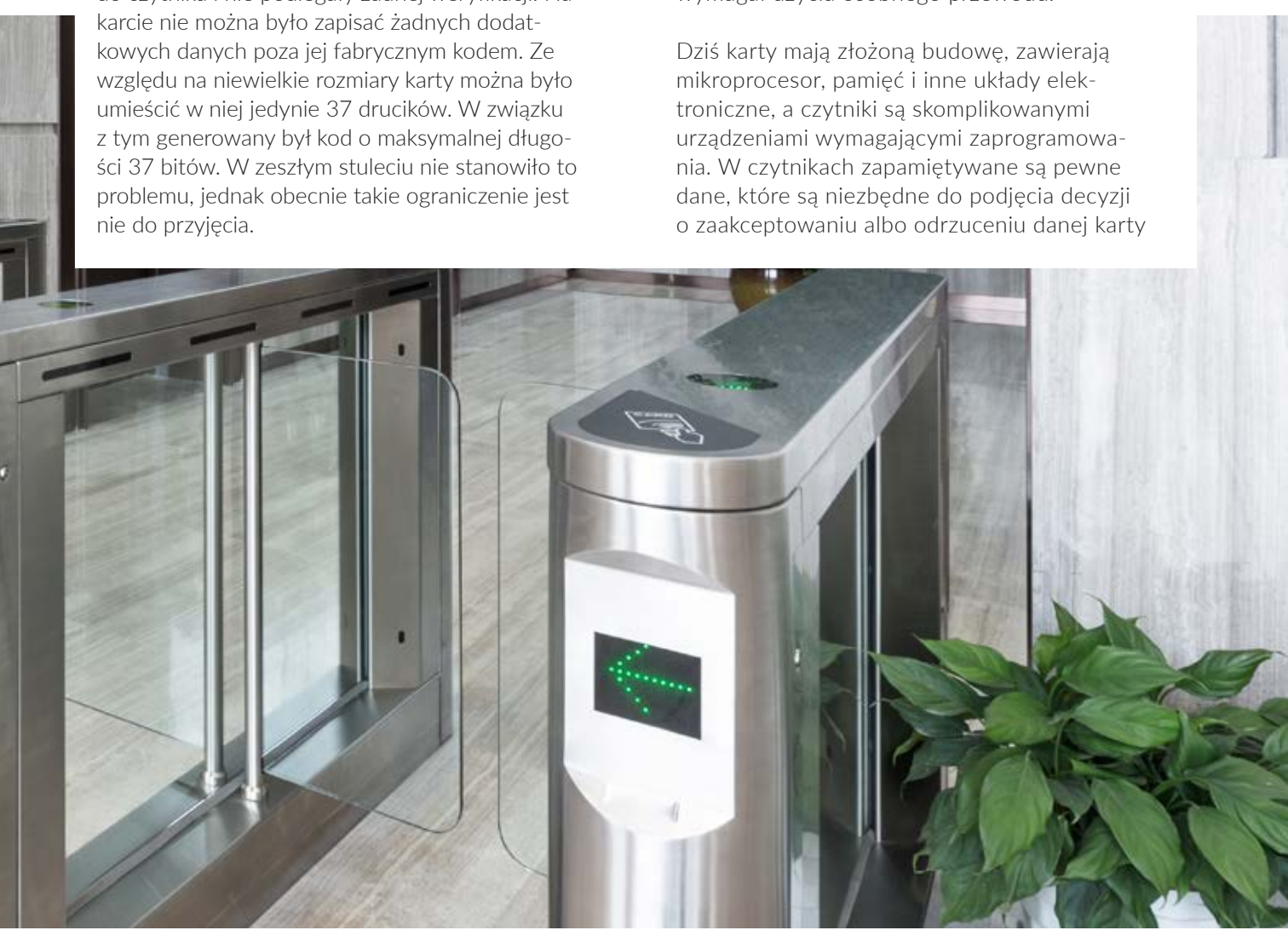
Komunikacja między kartą a czytnikiem była jednokierunkowa. Dane były przenoszone z karty do czytnika i nie podlegały żadnej weryfikacji. Na karcie nie można było zapisać żadnych dodatkowych danych poza jej fabrycznym kodem. Ze względu na niewielkie rozmiary karty można było umieścić w niej jedynie 37 drucików. W związku z tym generowany był kod o maksymalnej długości 37 bitów. W zeszłym stuleciu nie stanowiło to problemu, jednak obecnie takie ograniczenie jest nie do przyjęcia.

Protokół Wieganda i konsekwencje jego stosowania

Do komunikacji między czytnikami a kontrolerami drzwiowymi wykorzystywany był protokół Wieganda, opracowany specjalnie w tym celu. W latach, w których powstawały pierwsze systemy kontroli dostępu nie kładziono nacisku na bezpieczeństwo. Nikt nie zastanawiał się, czy kartę Wieganda można podrobić, nikt nie rozpatrywał sytuacji, w której włamywacz rozcina kable i podłącza do systemu jakieś obce urządzenia.

Zasadniczo protokół Wieganda wykorzystuje transmisję szeregową z użyciem dwóch przewodów sygnałowych i przewodu masowego, jednak do połączenia czytników z kontrolerami stosowane były kable kilkunastożyłowe. Każdy z elementów czytnika, to znaczy dioda świecąca się światłem czerwonym, dioda świecąca się światłem zielonym, brzęczyk, przycisk, styk antysabotażowy i inne podobne elementy, wymagał użycia osobnego przewodu.

Dziś karty mają złożoną budowę, zawierają mikroprocesor, pamięć i inne układy elektroniczne, a czytniki są skomplikowanymi urządzeniami wymagającymi zaprogramowania. W czytnikach zapamiętywane są pewne dane, które są niezbędne do podjęcia decyzji o zaakceptowaniu albo odrzuceniu danej karty



identyfikacyjnej. Sam protokół komunikacyjny Wieganda nie zmienił się jednak od dziesięcioleci.

Z natury protokołu Wieganda wynika, że transmisja danych trwa tylko w chwili, gdy ktoś przykłada kartę do czytnika. Przez pozostały czas czytnik znajduje się w stanie czuwania i żadna transmisja nie zachodzi. Gdy czytnik jest w stanie czuwania, przewody sygnałowe interfejsu Wieganda przyjmują wysoki stan logiczny. Inaczej mówiąc, są pod napięciem 5 V wymuszanym przez kontroler. Jeśli w takiej sytuacji ktoś odetnie przewody sygnałowe, do kontrolera nie jest wysyłana informacja, że czytnik jest odłączony. Co więcej, po odcięciu przewodów można w to samo miejsce podłączyć inny, odpowiednio zaprogramowany czytnik – z kodami znanymi włamywaczowi. Pozostaje jeszcze skopiowanie głównego kodu karty, ale dobrze przygotowany włamywacz i z tym sobie poradzi.

Kolejnym zagrożeniem w przypadku systemu kontroli dostępu jest możliwość podsłuchania transmisji radiowej między kartą identyfikacyjną a czytnikiem. Przestępca może tego dokonać na znaczną odległość, więc pozostaje niezauważony. Potrzebuje odpowiednio skonstruowanego odbiornika radiowego oraz laptopa z odpowiednim oprogramowaniem. Dzięki takiemu wyposażeniu może przechwycić kod zapisany na karcie i przygotować własny duplikat.

Modyfikacje czytników Wieganda

Z biegiem czasu opisane powyżej wady systemów kontroli dostępu stały się bardzo uciążliwe, co zmusiło konstruktorów do modyfikacji konstrukcji czytników i kart identyfikacyjnych. Postęp w dziedzinie elektroniki i miniaturyzacja urządzeń mikroprocesorowych umożliwiły wprowadzenie szyfrowania transmitowanych danych. Już na początku tego stulecia czołowi producenci czytników i kart identyfikacyjnych zastosowali szyfrowanie interfejsu radiowego. Od tego momentu przechwycenie danych metodą podsłuchu stało się bezużyteczne.

Niestety sam protokół Wieganda nie uległ modyfikacji. We współczesnych kontrolerach liczba przewodów łączących czytniki z kontrolerami została ograniczona do sześciu, ale to nie rozwiązało problemów związanych z bezpieczeństwem. Niektórzy producenci opracowali własne protokoły transmisji szeregowej i zastosowali magistralowe połączenie czytników, jednak pojawił się problem z kompatybilnością. Projektanci byli zmuszeni do stosowania wszystkich urządzeń wchodzących w skład systemu jednej marki, co w wielu sytuacjach stanowiło poważne ograniczenie funkcjonalności.

Dopiero pojawienie się otwartego protokołu OSDP rozwiązało większość opisanych problemów.

Protokół OSDP

OSDP (od ang. *Open Supervised Device Protocol*) to otwarty protokół stosowany do dwukierunkowej komunikacji między urządzeniami w systemach bezpieczeństwa. OSDP szyfruje połączenie między czytnikiem a kartą zbliżeniową oraz między czytnikiem a kontrolerem, dzięki temu próba podsłuchania transmisji radiowej lub przechwycenia danych transmitowanych drogą kablową jest bezużyteczna. Protokół utrzymuje stałe połączenie między czytnikiem a kontrolerem, więc każda próba odłączenia lub uszkodzenia czytnika jest natychmiast wykrywana.

Do połączenia czytnika z kontrolerem wystarcza jedna para przewodów, jednakże ze względu na konieczność doprowadzenia zasilania i realizacji funkcji pomocniczych przeważnie stosowanych jest sześć przewodów. Transmisja jest znacznie szybsza niż w starszych rozwiązaniach, co powoduje, że system szybciej reaguje na zbliżenie karty do czytnika.

Żeby protokół OSDP mógł być wykorzystany, zarówno kontrolery, jak i czytniki muszą być do tego przystosowane. Ze względu na zalety tego protokołu jego popularność ciągle rośnie i czołowi producenci systemów kontroli dostępu wprowadzają go do swoich urządzeń.

Protokół OSDP nie tylko zapewnia szyfrowanie danych transmitowanych w obrębie systemu, lecz ma także inne, dotychczas niedostępne funkcje. Za jego pomocą można transmitować dane

konfiguracyjne do czytników. W dużych, wielo-obiektowych systemach jest to bardzo użyteczna funkcja. Przykładowo, jeśli z jakichś powodów konieczna jest zmiana kodów we wszystkich czytnikach, można jej dokonać z poziomu stanowiska operatorskiego, bez konieczności podchodzenia do każdego z czytników z osobna i odwiedzania odległych obiektów objętych działaniem systemu.

Protokół OSDP umożliwia utworzenie w systemie tak zwanego bezpiecznego kanału transmisyjnego, zaszyfrowanego za pomocą AES-128, który znajduje zastosowanie w obiektach o szczególnym znaczeniu i jest akceptowany przez instytucje rządowe wielu krajów. Ze względu na to, że współczesne systemy kontroli dostępu często obejmują swoim zasięgiem obiekty rozmieszczone w różnych częściach świata, ta cecha protokołu OSDP nabiera szczególnego znaczenia.

Gdy OSDP nie wystarcza

W większości przypadków, szczególnie w obiektach cywilnych, poziom bezpieczeństwa uzyskiwany dzięki zastosowaniu protokołu OSDP można uznać za wystarczający, jednakże w obiektach specjalnych, rządowych lub wojskowych konieczne jest zastosowanie silniejszych zabezpieczeń. Jednym z nich jest wprowadzenie dodatkowych kluczy do kart identyfikacyjnych i do czytników. W efekcie uzyskuje się symetryczne kodowanie transmisji radiowej między kartą a czytnikiem. Wprowadzanie kluczy odbywa się w procesie programowania kart i czytników. Stanowi to kolejny poziom zabezpieczenia, gdyż oprócz kodu zapisanego w karcie musi zgadzać się klucz szyfrujący.

Dalsza poprawa poziomu bezpieczeństwa jest możliwa dzięki umieszczeniu w czytnikach odpowiednio zaprogramowanych modułów SAM (od ang. *Secure Access Module*), z wyglądu przypominających zwykłe karty SIM. Czytniki muszą być do tego przygotowane. Muszą zawierać odpowiednie gniazda, w których umieszcza się moduły SAM. Obecnie wielu producentów produkuje takie czytniki.

Moduły SAM zawierają zestaw 128 kluczy szyfrujących, które są wykorzystywane w sposób losowy. Te same klucze muszą być wprowadzone do oprogramowania zarządzającego systemem oraz do kart zbliżeniowych. Ta ostatnia czynność przebiega automatycznie, w momencie przygotowywania kart dla użytkowników systemu.

Siła zabezpieczenia z użyciem modułów SAM bierze się z zastosowania dwóch składników. Po pierwsze wprowadzone klucze są długie, mogą mieć nawet 256 bitów, więc skuteczność szyfrowania jest wysoka. Po drugie klucze są wybierane w sposób losowy i nigdy nie wiadomo, który z nich jest aktualnie w użyciu.

W systemie działają zatem trzy rodzaje zabezpieczeń, które uzyskuje się dzięki zastosowaniu protokołu OSDP, dodatkowych kluczy w czytnikach i kartach identyfikacyjnych, a także modułów SAM.

Ktoś mógłby podać w wątpliwość sens stosowania aż tak silnych zabezpieczeń, jednakże we współczesnym świecie należy się liczyć z pewnymi dotychczas nie występującymi zagrożeniami. Nie chodzi tu o zwyczajne zabezpieczenia antywłamaniowe czy o kontrolę dostępu na terenie przeciętnego budynku. W takim przypadku wystarczą podstawowe zabezpieczenia. Są jednak obiekty specjalne, takie jak biura konstrukcyjne korporacji przemysłowych, laboratoria badawcze, obiekty przemysłowe o specjalnym znaczeniu, biurowce rządowe i obiekty wojskowe, do których może próbować włamać się nie zwykły złodziej, lecz doskonale wyszkolony i wyposażony wywiadowca, którego zadaniem jest zdobycie określonych informacji. Tej klasy specjalista dysponuje zarówno wiedzą, jak i sprzętem, a systemy zabezpieczające mają przeszkodzić mu w działaniu na skutek czasochłonności ich pokonywania.

Wiadomo, że każde zabezpieczenie można pokonać – to tylko kwestia użycia odpowiednich środków. Na wszystko potrzebny jest jednak odpowiedni czas. Żaden włamywacz nie może pozwolić sobie na manipulowanie przy systemie przez kilkanaście godzin w celu odszyfrowania danych. Właśnie dlatego zastosowanie silnych zabezpieczeń elektronicznych ma sens.

Andrzej Walczyk

Bezprzewodowe zamki
zwiększają możliwości kontroli dostępu

ASSA ABLOY

W miarę jak ochrona budynków staje się coraz bardziej inteligentna, wzrasta zapotrzebowanie na elektroniczne systemy kontroli dostępu. Przez długi czas podstawą były przewodowe systemy kontroli dostępu i drzwi antywłamaniowe. W budynkach z rozległymi systemami elektronicznymi mechanicznie zamykane drzwi pozostawały niekontrolowane, niechronione i z pewnością nie były „inteligentne". Działanie mechanicznych zamków nie mogło być kontrolowane. Na szczęście najnowszej generacji zamki bezprzewodowe mogą łatwo je zastąpić i zostać bezproblemowo zintegrowane z niemal każdym systemem kontroli dostępu

Fot. 1. Dzięki integracji interfejsów ten sam nośnik danych uwierzytelniających może być wykorzystywany do otwierania garażu i wejścia do budynku.

Niedawny branżowy sondaż – przywołany w raporcie Wireless *Access Control Report 2018* przygotowanym przez firmę ASSA ABLOY i IFSEC Global – wskazuje na wzrost zainteresowania integracją. Ponad 90 procent ankietowanych specjalistów z branży sugeruje, że łączenie systemów zabezpieczeń ze sobą (i z innymi inteligentnymi systemami w budynku) zyskało na znaczeniu w ostatnich kilku latach.

53 procent respondentów uważa, że łatwe połączenie z CCTV, urządzeniami alarmowymi, systemem rejestracji czasu pracy, oświetleniem oraz systemami ogrzewania, wentylacji i klimatyzacji mogłoby skłonić ich do zastosowania nowego produktu bardziej niż jakikolwiek inny czynnik. 43 procent powiedziało, że zachęciłaby ich do tego łatwa integracja z istniejącymi systemami kontroli dostępu. Skąd jednak to zainteresowanie integracją? Jakie są jej zalety?

Po co integrować?

Im mniej interfejsów systemów zabezpieczających, tym łatwiej je obsługiwać, a więc jest też mniej nauki ich obsługi. Integracja przynosi korzyść użytkownikom budynków. Ten sam nośnik danych uwierzytelniających może być wykorzystywany do otwierania garażu i wejścia do budynku, w którym mieści się biuro, a także do uzyskiwania dostępu do laptopa czy do uiszczenia opłaty za obiad.

> Integracja jest powtarzającym się tematem rozmów wśród specjalistów z branży.

Integracja systemów nie tylko ma na celu bezpieczeństwo ludzi, pomieszczeń i wyposażenia – przyczynia się też do zwiększenia skuteczności działań biznesowych. Na przykład połączenie zarządzania zasobami ludzkimi z kontrolą dostępu sprawi, że inteligentne karty dostępowe będą mogły być automatycznie unieważniane, gdy

> Ponadczasowość rozwiązania jest dla nabywcy ważna.

Fot. 2. Bezprzewodowe zamki Aperio odczytują poświadczenia z urządzeń mobilnych.

pracownicy odejdą z pracy, co ułatwi zarządzanie kadrami i zmniejszy koszty ogólne.

Większość ankietowanych na potrzeby Wireless *Access Control Report 2018* (58 procent) wierzy, że w przypadku systemów kontroli dostępu bardzo ważne jest używanie otwartych standardów w celu uzyskania elastyczności tych systemów i możliwości ich długoletniego wykorzystywania. Ponadto 91 procent uznało to za ważne przynajmniej w pewnym stopniu.

Czy twój system będzie można dostosować do zmian w działalności biznesowej i czy możliwe będą zmiany jego funkcji? Czy możesz usprawnić funkcjonowanie systemu kontroli dostępu za pomocą odpowiednich komponentów, które coś do niego wniosą?

Sposób na usprawnienie systemu kontroli dostępu

Zastosowanie dodatkowych zamków mechanicznych może być drogie i skutkować uciążliwą eksploatacją. Są jednak alternatywne rozwiązania, które można szybko, łatwo i tanio wdrożyć, pozwalające zapomnieć o kluczach i kłopotach związanych z zarządzaniem nimi. Mowa o bezprzewodowych urządzeniach Aperio – zasilanych bateryjnie zamkach ze zintegrowanymi czytnikami RFID.

Wspomniany raport przytacza prognozy dotyczące rynku bezprzewodowych urządzeń do systemów kontroli dostępu, przewidujące wzrost na poziomie około 8 procent rocznie do 2025 roku. Łatwa i niedroga integracja urządzeń bezprzewodowych z pewnością napędza ten wzrost.

System Aperio ma otwartą architekturę, jest elastyczny i modułowy. Ci, którzy już wdrożyli przewodowy system kontroli dostępu i chcą objąć nim więcej drzwi, uważają, że najwłaściwsze są rozwiązania bezprzewodowe.

Integracja jest bezproblemowa i zwiększa możliwości istniejącego systemu dzięki urządzeniom, które będą skutecznie działać przez długie lata. Zarządzający bezpieczeństwem operują drzwiami wyposażonymi w Aperio za pomocą tego samego interfejsu co w przypadku zainstalowanego systemu przewodowego. Użytkownik korzysta z jednej inteligentnej karty identyfikacyjnej umożliwiającej dostęp do wszystkich drzwi. Karta może mieć też inne funkcje, np. służyć do płacenia na stołówce czy do wypożyczania książek w bibliotece, co jest równie łatwe do uzyskania.

> Zamki Aperio współpracują z niemal każdym systemem kontroli dostępu – od ponad stu różnych producentów.

Co zrobić, jeśli w systemie zabezpieczeń wykorzystywane są mechaniczne klucze, a nie ma elektronicznej kontroli dostępu? Zastosowanie bezprzewodowych zamków, takich jak Aperio, również w tym przypadku może być właściwym rozwiązaniem. Zasilane bateryjnie wkładki z czytnikami RFID, klamki i zamki mogą być

zainstalowane jako nowy system kontroli dostępu lub rozszerzać istniejącą instalację przez bezprzewodowe połączenie nowych drzwi ze starym systemem. Personel nie musi wymieniać swoich kart. Nikt nie musi używać więcej niż jednego identyfikatora.

Zamki Aperio współpracują z niemal każdym systemem kontroli dostępu – od ponad stu różnych producentów. Są energooszczędne, gdyż baterie wystarczą na 40 000 otwarć drzwi (zazwyczaj na dwa lata), zanim trzeba będzie je wymienić.

– *Proces modernizacji łatwo rozpocząć* – powiedział Matthias Weiß, Aperio Product Manager w ASSA ABLOY EMEA. – *Zarządzający systemem bezpieczeństwa lub budynkiem musi tylko skontaktować się ze swym dostawcą urządzeń do kontroli dostępu. Możemy zmodernizować prawie każdy system.*

Aperio integruje elementy systemu kontroli dostępu

Zainstalowanie bezprzewodowych zamków jest tańsze niż przewodowe połączenie większej liczby drzwi z systemem, ponieważ nie wymaga okablowania lub inwazyjnego montażu. Nie ma też potrzeby wymiany wszystkich części drzwi. Na przykład można łatwo i szybko wymienić klamki mechaniczne na bezprzewodowe klamki Aperio ze zintegrowanymi czytnikami RFID, aby objąć więcej drzwi systemem kontroli dostępu.

Urządzenia Aperio z wbudowanymi czytnikami RFID mogą być wykorzystane w niemal każdej sytuacji. Zamki Aperio zabezpieczają zarówno wewnętrzne, jak i zewnętrzne drzwi – od pożarowych i ewakuacyjnych do tych w salach spotkań, laboratoriach i biurach (drewniane, szklane czy aluminiowe drzwi nie stanowią problemu). Oferta obejmuje zarówno same wkładki, jak i kompletne zamki do zabezpieczanych drzwi, a ponadto nową bezprzewodową klamkę ze zintegrowanym czytnikiem RFID, która niedawno wygrała w kategorii Access Control Product of the Year na targach Intersec. Zamki Aperio są kompatybilne ze wszystkimi powszechnie stosowanymi profilami – „euro", francuskimi, fińskimi, skandynawskimi i szwajcarskimi. Z istniejącym systemem mogą być połączone online, offline lub obydwiema metodami.

Fot. 3. Poświadczenia mobilne wykorzystywane w systemach hotelowych.

Opracował na podstawie materiałów firmy ASSA ABLOY Paweł Karczmarzyk

System kontroli dostępu MATRIX firmy dormakaba

Rafał Tamborski

dormakaba jest firmą o globalnym zasięgu. Oferuje rozwiązania z zakresu kontroli dostępu i rejestracji czasu pracy, terminale ewakuacyjne, zamki elektryczne, elektrozaczepy, zwory, okucia do szkła, okucia antypaniczne, automatyczne drzwi przesuwne, bramki sensoryczne, drzwi obrotowe, szklane ściany przesuwne, mobilne ściany przesuwne, a także wkładki mechaniczne i zamki hotelowe

Jednym z oferowanych przez firmę dormakaba systemów kontroli dostępu i rejestracji czasu pracy jest MATRIX. Można go dostosować do niemal każdych wymogów bezpieczeństwa oraz wielkości przedsiębiorstwa. Na system ten składa się oprogramowanie MATRIX do kontroli dostępu i rejestracji czasu pracy oraz sprzęt do kontroli dostępu, rejestracji czasu pracy i zarządzania czasem pracy.

Oprogramowanie MATRIX

Oprogramowanie MATRIX służy do kontroli dostępu, rejestracji czasu pracy i zarządzania drogami ewakuacyjnymi. Jest nowoczesne i skalowalne, to znaczy w zależności od potrzeb można dobrać potrzebne moduły oprogramowania. Mogą z niego korzystać zarówno małe, jak i duże przedsiębiorstwa. W biurowcach, w których pomieszczenia wynajmują różne firmy, można na przykład wydzielić w ramach jednego systemu kilka podsystemów, do których będą mieć dostęp tylko określeni wynajmujący, z zachowaniem wspólnego wejścia głównego lub przejścia z bramkami sensorycznymi (które również są w ofercie) przy recepcji.

Fot. 1. Interfejs oprogramowania MATRIX (responsywny interfejs, widok administratora, widok użytkownika)

Użytkownik ma dostęp do oprogramowania poprzez standardową przeglądarkę internetową (np. MS Explorer, Mozilla Firefox, Google Chrome, Safari), co upraszcza obsługę systemu. Wystarczy, że komputer jest w sieci firmowej, a użytkownik ma odpowiednie uprawnienia. Ponadto wszelkie aktualizacje oprogramowania realizowane są tylko na serwerze, a nie na każdym komputerze użytkownika.

Kolejną zaletą jest to, że interfejs użytkownika jest responsywny (fot. 1c.), czyli wyświetlana w przeglądarce zawartość zmienia się w zależności od urządzenia, na którym dane są wyświetlane. Dzięki temu można korzystać z oprogramowania zarówno na standardowym komputerze, jak i na tablecie czy smartfonie.

Językiem w interfejsie oprogramowania jest domyślnie ustawiony język w przeglądarce. Oczywiście do dostępnych w oprogramowaniu języków należy język polski.

Po zalogowaniu się administrator widzi wszystkie dostępne w menu funkcje (fot. 1a. – widok administratora). Użytkownik widzi tylko te elementy menu, do których powinien mieć dostęp (fot. 1b. – widok użytkownika). Jeżeli użytkownik użyje przycisku „ulubione", to bardzo szybko może wyświetlić to okno dialogowe, z którego korzysta najczęściej.

W mniejszych firmach, w których pracuje maksymalnie 100 osób i w których potrzebna jest obsługa maksymalnie 100 drzwi, administrator może zezwalać na dostęp do pomieszczeń, korzystając z uproszczonego planu zamykania. W oknie „plan zamykania" wyświetlą się nagłówki kolumn, które są nazwami pomieszczeń, oraz nagłówki wierszy, które są imionami i nazwiskami osób wprowadzonymi do systemu kontroli dostępu. W każdej komórce jest pole wyboru (*check box*). Zaznaczenie właściwego pola na styku nazwy pomieszczenia oraz imiona i nazwiska, a następnie zapisanie tego działania będzie skutkowało zezwoleniem na dostęp. Odznaczenie pola poskutkuje cofnięciem zgody na dostęp. Nieprzypisane nikomu pomieszczenia będą oznakowane kolorem czerwonym. Dla większych przedsiębiorstw wygodniejsze będzie wykorzystywanie profili dostępu. Na profile dostępu składają się informacje o dostępie do poszczególnych drzwi (np. drzwi do pomieszczenia działu IT), stref pomieszczeń użytkowych (np. hali produkcyjnej), czasie, w którym możliwy jest dostęp (zgodnym z ustalonym planem dostępu, np. od poniedziałku do piątku w godzinach od 8:00 do 19:00). Jeżeli jest to potrzebne, dla wybranej osoby można dodać specjalne uprawnienia do dostępu do danej strefy, pomieszczenia lub do drzwi.

Architektura oprogramowania zapewnia przedsiębiorstwu bezpieczeństwo. Obsługiwane są bazy danych H2 i MS SQL Express w przypadku firm mniejszych oraz MS SQL lub Oracle w przypadku większych przedsiębiorstw. Środowiskiem serwera jest MS Windows, a serwerem Apache Tomcat.

Dla partnerów i integratorów systemów ważne jest to, że instalacja oprogramowania jest bardzo prosta i trwa kilka minut.

Warto wspomnieć o możliwości integracji z systemami bezpieczeństwa i automatyki budynkowej poprzez serwer OPC (otwarty standard komunikacyjny), interfejsy do systemów sygnalizacji włamania i napadu (OII – od ang. *open intrusion interface*) oraz interfejsy do nadrzędnych systemów zarządzania zasobami firmy (ERP – od ang. *enterprise resource planning*), takie jak na przykład certyfikowany interfejs do systemu SAP ERP.

Rys. LEGIC connect

Można rejestrować czas pracy pracowników w firmie, zarówno w biurowym, zmianowym, jak i mieszanym trybie pracy, lub przesyłać nieobrobione dane dotyczące rejestracji czasu pracy do innych systemów, gdzie będą one podlegały dalszej obróbce.

REST API (REST – od ang. *representational state transfer*, API – od ang. *application programming interface*) zaimplementowany w systemie MATRIX umożliwia innym firmom komunikowanie się z nim w prosty sposób.

Prawie każdy z nas posiada smartfon. Dlaczego nie używać go jak karty zbliżeniowej? Można otwierać przejścia za pomocą telefonu. Z oprogramowaniem MATRIX i sprzętem dormakaba jest to możliwe.

dormakaba ma funkcję LEGIC connect do bezpiecznego przesyłania uprawnień do dostępu na smartfony. Dzięki aplikacji Door by dormakaba użytkownik, który ma odpowiednie uprawnienia dostępowe, może jednym naciśnięciem otworzyć wybrane pomieszczenie. Możliwe jest wysyłanie użytkownikom uprawnień do dostępu do poszczególnych pomieszczeń w dowolnym miejscu na świecie, w jednej chwili.

Sprzęt firmy dormakaba i nie tylko

Oprogramowanie jest jednym z elementów systemu. Innym równie ważnym elementem jest wydajny i bezpieczny sprzęt.

Należy pamiętać o właściwym połączeniu oprogramowania i sprzętu. dormakaba ma różne możliwości, zależne od sytuacji:

- połączenie online, czyli wykorzystanie okablowania, w różnych wariantach i topologiach, np. RS485, LAN;
- połączenie bezprzewodowe, z użyciem bezpiecznego łącza ZigBee, wykorzystujące bramki bezprzewodowe i okucia lub czytniki bezprzewodowe;
- możliwość przenoszenia uprawnień na karcie AoC (Access on Card); informacje o punktach dostępu oraz czasie, przez który dostęp jest możliwy, zapisywane są na karcie zbliżeniowej przez czytnik nabiurkowy, czytnik podłączony online, terminal aktualizujący uprawnienia lub terminal systemu do rejestracji czasu pracy Terminale do rejestracji czasu pracy są podłączane poprzez LAN.

Na sprzęt dormakaba składają się okucia i wkładki elektroniczne, wkładki mechatroniczne, zamki szafkowe, czytniki i kontrolery, terminale do rejestracji czasu pracy i terminale ewakuacyjne.

Kontrolery do systemu MATRIX można zamówić w wersji do montażu w racku lub w wersji naściennej. Mają one bardzo istotną funkcję – w przypadku utraty połączenia z serwerem komunikują się między sobą, dzięki czemu np. funkcja *anti-passback* jest cały czas realizowana w danej strefie, nawet jeżeli czytniki są podłączone do kilku różnych kontrolerów.

Czytniki online są dostępne w różnych wariantach, np. czytnik przystosowany do pracy na zewnątrz, o klasie szczelności IP66, lub tzw. czytnik zdalny, w przypadku którego elektronika montowana jest po stronie bezpiecznej, wewnątrz pomieszczenia chronionego, a głowica czytająca na zewnątrz pomieszczenia.

Okucia i wkładki cyfrowe można zamówić w różnych wersjach w zależności od rodzaju drzwi, bardzo dobrze sprawdzają się wszędzie tam, gdzie prowadzenie okablowania może być kłopotliwe, np. w zabytkowym budynku podlegającym konserwatorowi zabytków czy w biurowcu, podczas reorganizacji, jeżeli takie prace mogą być uciążliwe dla innych.

Terminale do rejestracji czasu pracy można skonfigurować w zależności od potrzeb. Różnią się one wymiarami i funkcjami.

Wszystkie oferowane urządzenia cechuje ponadczasowe wzornictwo, niezawodność i bezpieczeństwo.

Firma dormakaba nie zmusza klientów do stosowania tylko jej własnych urządzeń. Poprzez konwertery można podłączyć do kontrolerów dormakaba czytniki innych producentów, a oprogramowanie do obsługi czytników PGH (niemieckiego producenta komponentów systemów kontroli dostępu i rejestracji czasu pracy) jest zainstalowane bezpośrednio w kontrolerach z firmwarem TP4 (TP4 to oprogramowanie sprzętowe do kontrolerów w systemie MATRIX).

Terminale ewakuacyjne dormakaba są zintegrowane w oprogramowaniu MATRIX. Można sterować drogami ewakuacyjnymi z jednego miejsca.

Fot. 2. Terminal ewakuacyjny SafeRoute

Więcej informacji mogą Państwo uzyskać w firmie dormakaba Polska, na stronie www.dormakaba.pl lub na firmowym stoisku na konferencji SPIN.

Rafał Tamborski
dormakaba Polska
e-mail: rafal.tamborski@dormakaba.com
tel. kom.: 663 379 001

Okucie elektroniczne c-lever air jest równie płaskie jak okucie mechaniczne i pozwala kontrolować dostęp do właściwych pomieszczeń w odpowiednim czasie. Używane jest na drzwiach wewnętrznych i działa autonomicznie tzn. w drzwiach nie jest wymagane okablowanie, ponieważ okucie zasilane jest dwoma standardowymi bateriami. Najważniejsze cechy produktu to:

- Najbardziej płaskie okucie
- Czarna lub biała obudowa
- Wersja wąska do drzwi profilowych i wersja szeroka do drzwi pełnych
- Łatwa instalacja i szybka wymiana mechanicznego okucia drzwiowego
- Wybór szerokiej gamy mediów dostępowych: karta, brelok, klucz RFID, a także smartfon

www.dormakaba.pl

Odkryj nowe okucie c-lever air

dormakaba

AXIS 200

Krótka historia pierwszej na świecie kamery sieciowej

Axis Communications

Nikt nie ma recepty na sukces, ale, poznawszy historie większości globalnych osiągnięć technologicznych, można dojść do wniosku, że przełomowe wynalazki i innowacje tworzą entuzjastycznie nastawieni i zaangażowani ludzie z pomysłem, zapałem do pracy oraz wyczuciem czasu i przyszłych trendów. Nie inaczej było w przypadku pierwszej na świecie kamery sieciowej. Wszystko zaczęło się od pewnej podróży do Kraju Kwitnącej Wiśni...

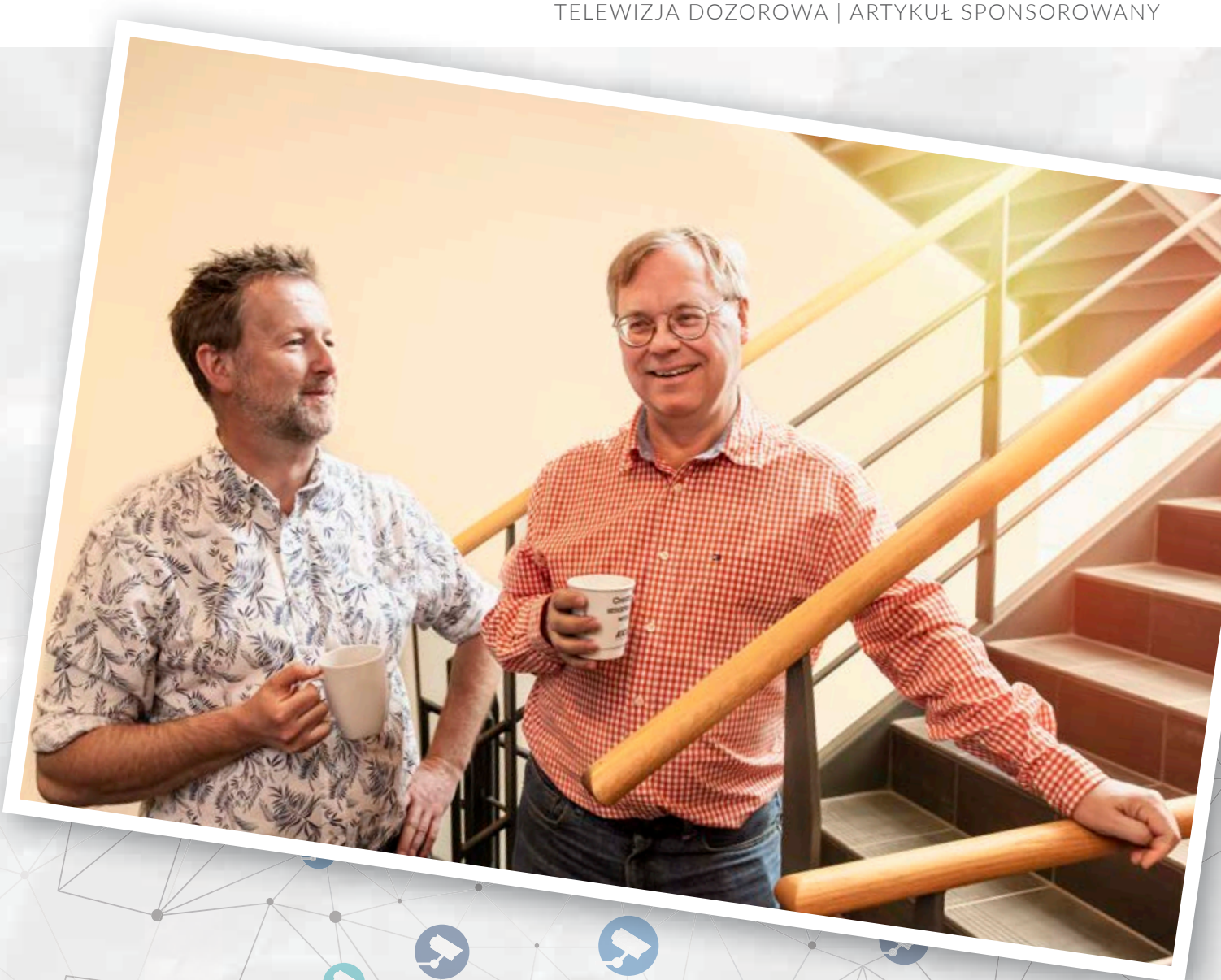
Powrót do przeszłości

Cofnijmy się w czasie do początku lat 90., kiedy to Martin Gren, współzałożyciel firmy Axis Communications, udał się w służbową podróż do Tokio, na spotkanie z potencjalnymi klientami. Jeden z nich zaprosił go do współpracy przy dystrybucji kamer analogowych, ale Gren uważał, że te produkty nie znajdą odbiorców. Wówczas padła propozycja, by podłączyć je do sieci internetowej – japoński kontrahent wiedział bowiem, że szwedzka firma pracuje nad innowacjami w zakresie rozwiązań sieciowych. Obie strony dostrzegły potencjał tego pomysłu.

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

Mamy to!

Warto pamiętać, że cały proces opracowywania kamery sieciowej, czyli takiej, która jednocześnie odbiera dane sterujące od operatora i przesyła z powrotem wytworzone obrazy, odbywał się w czasie, gdy sieć internetowa nie była powszechnie znana i używana. Internet wykorzystywały głównie wyspecjalizowane firmy i instytucje. Zespół inżynierski firmy Axis Communications musiał zatem zbudować produkt możliwy do wykorzystania przy ówczesnym stanie techniki.



– *To był szalony czas* – powiedział Carl-Axel. – *Mogłeś mieć naprawdę fajnego szefa, może nawet miałeś modem i komputer z procesorem 200 MHz, ale jego wydajność była tak niska, że nie pozwalała na oglądanie ruchomych obrazów – transmitowana była jedna klatka co 17 sekund (lub trzy klatki na minutę). Zrobiliśmy więc tyle, ile mogliśmy*. Martin Gren dodał z kolei, że działania firmy opierały się przede wszystkim na analizie potencjału. – *Stworzyliśmy innowacyjny produkt nie dlatego, że poznaliśmy aktualny rynek, ale dlatego, że mogliśmy po prostu zrobić coś całkowicie nowego, co będzie rozwiązaniem na przyszłość.*

Wreszcie, 17 września 1996 r. w Atlancie, tuż po igrzyskach olimpijskich, ciężka praca zaowocowała i po raz pierwszy uruchomiono kamerę sieciową zwaną AXIS 200. Kto był pierwszym klientem? Martin Gren podkreśla, że model biznesowy był oparty na relacjach B2B, w których budowaniu istotne były wzajemne referencje, pomoc techniczna i oczywiście wskazówki od użytkowników końcowych. – *Jednym z nich był Steve Wozniak, drugi założyciel Apple, który jako pierwszy udzielił nam wsparcia przez telefon. Okazało się, że miał całkiem udany zestaw AXIS 200* – powiedział Martin.

W procesie wdrażania innowacji zawsze przychodzi czas ich weryfikacji. Kamerę sieciową AXIS także czekał taki test. – *Dwie sytuacje uświadomiły mi, że jesteśmy częścią wspaniałego projektu. Pierwsza była w zasadzie jeszcze przed uruchomieniem AXISA 200,*

kiedy odwiedziliśmy targi IFSEC w Anglii wiosną 1996 r. i zobaczyliśmy, że wszystkie tamtejsze urządzenia są analogowe. Wniosek był prosty – jesteśmy pionierami i wchodzimy na szczyt, którego nikt wcześniej nie zdobył. Drugi moment swoistego olśnienia nastąpił również na tych samych targach, ale w 1998 r. Zaprezentowaliśmy wtedy gotową kamerę i stało się jasne, że odbiorcy nie rozumieją do końca naszej idei i czeka nas praca nie tyle nad produktem, co nad zmianą świadomości użytkowników. Wielu z nich myślało, że tworzymy tanie kamery internetowe i sugerowało pokaz na innych targach – powiedział Martin.

Pierwsza sprzedaż i narodziny procesora ARTPEC

Dzięki doświadczeniom zdobytym na rozmaitych targach branżowych, takich jak IFSEC, założyciele firmy Axis Communications i pracujący dla niej inżynierowie zdali sobie sprawę, że czeka ich dużo pracy, ale z pewnością opłaci się ona w dalszej perspektywie, ponieważ nie mieli konkurencji, a istniejąca technika analogowa była przestarzała, podobnie jak sam model biznesowy branży dozoru wizyjnego.

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

W związku ze zwiększaniem się liczby zamówień postanowiono zainwestować w pierwszy w branży procesor przeznaczony do kamer sieciowych – ARTPEC-1, który umożliwiał kodowanie obrazu w czasie rzeczywistym (sama nazwa została wymyślona przez jednego z pracowników działu marketingu w Bostonie). – *Zainwestowanie w pierwszy chip ARTPEC było kluczowe, bo, gdyby nam się nie udało, moglibyśmy utracić firmę. Zdaliśmy sobie sprawę, że nie mamy wyjścia, i zrobiliśmy wszystko, by wykorzystać szansę* – wspominał Martin. Inwestycja opłaciła się – firma nie musiała długo czekać na pierwszą nagrodę za swój innowacyjny procesor. Gdy tworzyła jego kolejne wersje, oczekiwania rosły, więc musiała postarać się o szybszy rozwój. To z czasem przełożyło się na lepsze wyniki finansowe.

Nowatorskie wzornictwo i jego konsekwencje

Firma Axis Communications zmieniała kamery nie tylko wewnątrz, ale i na zewnątrz, aby uniknąć kształtów kojarzących się z masywnością i zarazem przystosować wygląd do większej funkcjonalności. To nietypowe wówczas podejście miało kilka skutków ubocznych. – *Kamera sieciowa AXIS trafiła wówczas na pierwsze strony wielu magazynów komputerowych, ponieważ wyglądała nietuzinkowo. Z drugiej strony mieliśmy niemałe problemy z wyprodukowaniem obudowy, która w pełni pasowałaby do kamery* – wyjaśnił Carl-Axel.

Ograniczenia biznesowe i nowy rozdział w historii firmy

Firma Axis Communications musiała zmierzyć się z nowymi wyzwaniami – dalszym rozwojem produktów, wchodzeniem na nowe rynki, inwestowaniem w kadry i planowaniem rozwiązań komplementarnych. Zespół nigdy nie zniechęcał się trudnościami.

– Porzucenie tego pomysłu nigdy nie wchodziło w grę. Najważniejsze było stworzenie takiej struktury organizacyjnej, aby nasz nowy dział był niezależny od reszty operacyjnych działów grupy Axis w stopniu umożliwiającym swobodną pracę nad nowymi pomysłami. Myślę, że w przeciwnym razie nigdy nie zaszlibyśmy tak daleko – podkreślił Martin. Zgadza się z tym także Carl-Axel: *– Byliśmy zespołem składającym się z 8–10 osób, który zarządzał całym działem kamer, całkowicie oddzielonym od pozostałych części firmy. Jednocześnie zawsze mogliśmy liczyć na wsparcie z ich strony, zwłaszcza gdy chodziło o nowe zakupy, organizację sprzedaży czy zarządzanie finansami.*

Niewątpliwym wyzwaniem było przekonanie kierownictwa do produktu, który w latach dziewięćdziesiątych praktycznie nie istniał na rynku i początkowo nie był dobrze odbierany przez branżę. Ówczesne innowacje polegały głównie na rozszerzeniach lub ulepszeniach już istniejących produktów. Do takich innowacji łatwiej było przekonać zarówno klientów, jak i zarząd.– *Podczas spotkania z zarządem Axisa próbowałem przekonać go, że tworzymy coś wielkiego. Niepewność została ostatecznie przezwyciężona, gdy pokazaliśmy, że do obejrzenia materiału z kamery można wykorzystać przeglądarkę internetową. To był prawdziwy przełom w grze! Rozwiązanie to przekształciło się później w serwer sieciowy umożliwiający obrazowanie na żywo. Ostatecznie umówiliśmy się z zarządem, że mamy sprzedać 10 000 sztuk w ciągu dwóch lat. Po tych dwóch latach osiągnęliśmy wynik 14 000 sztuk. Myślę, że to naprawdę niezły wynik* – stwierdził Martin. Liczby mówiły same za siebie, a Martin Gren dostał swój własny dział poświęcony kamerom. To był początek nowej ery dla firmy.

Mały krok firmy Axis Communications to olbrzymi skok dla branży dozoru wizyjnego

Na szczęście Martin i Carl-Axel nie pozwolili, aby przeszkody uniemożliwiły stworzenie urządzenia sieciowego AXIS 200. Urządzenie to, od którego wszystko się zaczęło, dało technologiczne i biznesowe podwaliny pod inteligentny monitoring, a także pod inne sieciowe systemy powiązane, tj. w zakresie analizy danych, kontroli dostępu i komunikacji głosowej. Imponujące jest to, jak połączenie dwóch pomysłów może doprowadzić do stworzenia takiego narzędzia jak AXIS 200, które w istocie na zawsze zmieniło rynek dozorowy. Nikt, nawet sam twórca-konstruktor, nie mógł wymarzyć sobie, że dwadzieścia trzy lata później kamera sieciowa przyczyni się do powstania nowych, między innymi tzw. inteligentnych rozwiązań.

Ci dwaj wynalazcy-pasjonaci kochają to, co robią. *– Pracuję w firmie Axis od ponad 25 lat i widziałem tu narodziny kamer termowizyjnych, kamer modułowych i radarów. Nadal mam tę samą rolę co inżynier programista, ponieważ jestem takim trochę szalonym wynalazcą, jak Disneyowski Diodak (oryg. Gyro Gearloose) z Kaczora Donalda. Nadal cieszy i nakręca mnie robienie nowych, ciekawych rzeczy, które mogą służyć wszystkim. Nie lubię tworzyć sztuki dla sztuki, bo to prowadzi do wynaturzeń. Kocham robić coś, co finalnie jest po prostu dobre i przydaje się klientowi* – podsumował z uśmiechem Carl-Axel.

Axis Communications

Rola anten w systemach monitorowania alarmów

na przykładzie produktów firmy Poynting. Część 1.

Wielokrotnie zdarza się, że użytkownicy systemów radiokomunikacyjnych kupują drogi sprzęt z nadzieją, że będzie on działał niezawodnie i zapewni niezakłóconą łączność radiową, jednak całkowicie zaniedbują anteny, które są często zastępowane kawałkiem drutu. Tymczasem prawda jest taka, że to właśnie anteny decydują o jakości połączenia radiowego.

Przykładem potwierdzającym prawdziwość powyższej tezy jest odbiór programu telewizyjnego w miejscu odległym od stacji nadawczej. Jeśli poziom odbieranego sygnału jest zbyt niski, kupno nowego telewizora nic nie da, natomiast wymiana anteny na lepszą lub zainstalowanie jej w dogodniejszym miejscu zasadniczo wpłynie na jakość odbieranego obrazu.

Poniższy opis ma charakter uniwersalny i odnosi się do wszystkich systemów radiokomunikacyjnych. W systemach monitorowania alarmów wykorzystuje się albo licencjonowane kanały radiowe w zakresie VHF lub UHF, albo telefonię komórkową i jej pochodne, takie jak łącza GPRS. Nierzadko wykorzystywane są łącza szerokopasmowe, służące do przesyłania obrazów z wnętrza i otoczenia chronionych obiektów. Mundurowe i cywilne służby bezpieczeństwa korzystają z systemów DMR i TETRA. Jak widać, sposoby wykorzystania transmisji radiowej w celu zapewniania ochrony są różne.

Obecnie monitorowanie alarmów nie ogranicza się do przesłania informacji o pobudzeniu którejś z czujek ruchu czy otwarciu okna. Często przekazywane są sygnały telemetryczne sygnalizujące innego rodzaju zagrożenia, na przykład wzrost temperatury czy ulatnianie się gazu. Nierzadko komunikacja jest dwukierunkowa, gdyż właściciel obiektu wyposażony w smartfon odbiera informacje o stanie systemu alarmowego, a wysyła sygnały sterujące automatyką budynkową. Wszystko to razem zmusza do zapewnienia niezawodnej, wolnej od zakłóceń łączności radiowej.

We wszystkich systemach radiokomunikacyjnych mamy do czynienia z szumami i zakłóceniami zniekształcającymi transmitowany sygnał. W systemach analogowych objawiało się to szumami i trzaskami nanoszącymi się na odbieraną informację głosową lub zniekształceniami obrazu telewizyjnego. W systemach cyfrowych, na których skupimy się w dalszej części artykułu, nadmierne szumy powodują błędy podczas dekodowania odbieranych danych lub całkowicie zrywają połączenie.

We współczesnych cyfrowych systemach radiokomunikacyjnych miarą jakości łącza radiowego jest stopa błędów BER (skrót od *bit error rate*). W idealnym przypadku BER = 0%. W zależności od rodzaju systemu graniczna, dopuszczalna wartość BER wynosi od kilku do kilkunastu procent. Jak widać, pojawianie się niewielkich błędów jest dopuszczalne, gdyż zostają one skorygowane przez protokoły transmisyjne i algorytmy obróbki danych.

O jakości odbioru radiowego decydują dwa czynniki: poziom odbieranego sygnału S oraz stosunek sygnału do szumu S/N.

Źródłem sygnału jest nadajnik radiowy, zaś źródłem szumu mogą być zjawiska naturalne – np. wyładowania atmosferyczne, szumy kosmiczne pochodzące zarówno ze słońca, jak i z głębi kosmosu – oraz szumy generowane przez urządzenia elektryczne używane przez człowieka. Szumy sumują się i są wprowadzane przez antenę do urządzenia odbiorczego wraz z użytecznym sygnałem. Urządzenie odbiorcze też nie jest idealne i podczas wzmacniania sygnału dodaje do niego swoje szumy. Jeśli odbierany sygnał jest zbyt słaby, szumy nad nim dominują i uniemożliwiają prawidłowe dekodowanie danych. Przez czułość urządzenia odbiorczego rozumie się najniższy poziom sygnału doprowadzanego do jego wejścia, przy którym zachowana jest pełna funkcjonalność tego urządzenia.

W praktyce pomiar S/N jest uciążliwy, gdyż nie można łatwo oddzielić sygnału od szumu. W związku z tym stosowany jest inny parametr zwany SINAD, definiowany jako stosunek sygnału i szumu do szumu.
SINAD = (S+N)/N.

By zdefiniować czułość cyfrowego urządzenia odbiorczego należy podać trzy parametry: poziom sygnału S mierzony w µV, stosunek sygnału do szumu S/N wyrażony w dB i stopę błędów B wyrażoną w procentach. Przykładowo, urządzenie odbiorcze może mieć czułość określoną w następujący sposób: 0,25 µV przy S/N = 12 dB i B = 5%.

W praktyce pomiar S/N jest uciążliwy, gdyż nie można łatwo oddzielić sygnału od szumu. W związku z tym stosowany jest inny parametr zwany SINAD, definiowany jako stosunek sygnału i szumu do szumu.
SINAD = (S+N)/N.

W tym momencie wracamy do zasadniczego tematu artykułu, czyli do anten. Antena jest jedynym elementem w torze radiokomunikacyjnym, który jest w stanie poprawić stosunek sygnału do szumu. Żadne układy wzmacniające nie są w stanie tego dokonać, gdyż wzmacnianiu podlega zarówno sygnał, jak i szum, czyli wartość S/N nie ulega poprawie. W praktyce o czułości urządzenia odbiorczego decydują jego szumy własne, których poziom powinien być jak najniższy. Zadaniem anteny jest dostarczenie możliwie niezakłóconego sygnału o poziomie wyższym niż czułość odbiornika.

Antena jest jedynym elementem w torze radiokomunikacyjnym, który jest w stanie poprawić stosunek sygnału do szumu.

Dobór anten do konkretnych zastosowań nie jest rzeczą prostą. Do tych samych urządzeń radiokomunikacyjnych zainstalowanych w różnych warunkach należy dobrać inne anteny. Jest to związane z propagacją fal radiowych, które inaczej zachowują się w otwartej przestrzeni, inaczej na obszarze gęsto zabudowanym lub przemysłowym, a jeszcze inaczej w terenie zalesionym.

Jeśli firma zajmująca się monitorowaniem alarmów chce zaopatrywać się w anteny u jednego producenta, powinna wybrać takiego, który oferuje szeroki asortyment wyrobów. Zasadnicze znaczenie ma jakość materiałów i staranność wykonania anten, gdyż są one wystawione na działanie niekorzystnych warunków środowiskowych. W następnej części artykułu opisane będą profesjonalne anteny radiokomunikacyjne firmy Poynting, które spełniają powyższe wymagania.

Poynting
Making wireless happen

Opracował na podstawie materiałów
firmy Poynting
Andrzej Walczyk

www.poynting.tech
e-mail: sales-europe@poynting.tech

NOVUS®

NIEZAWODNE PRZEŁĄCZNIKI – ZASILANIE PoE DO 250 m

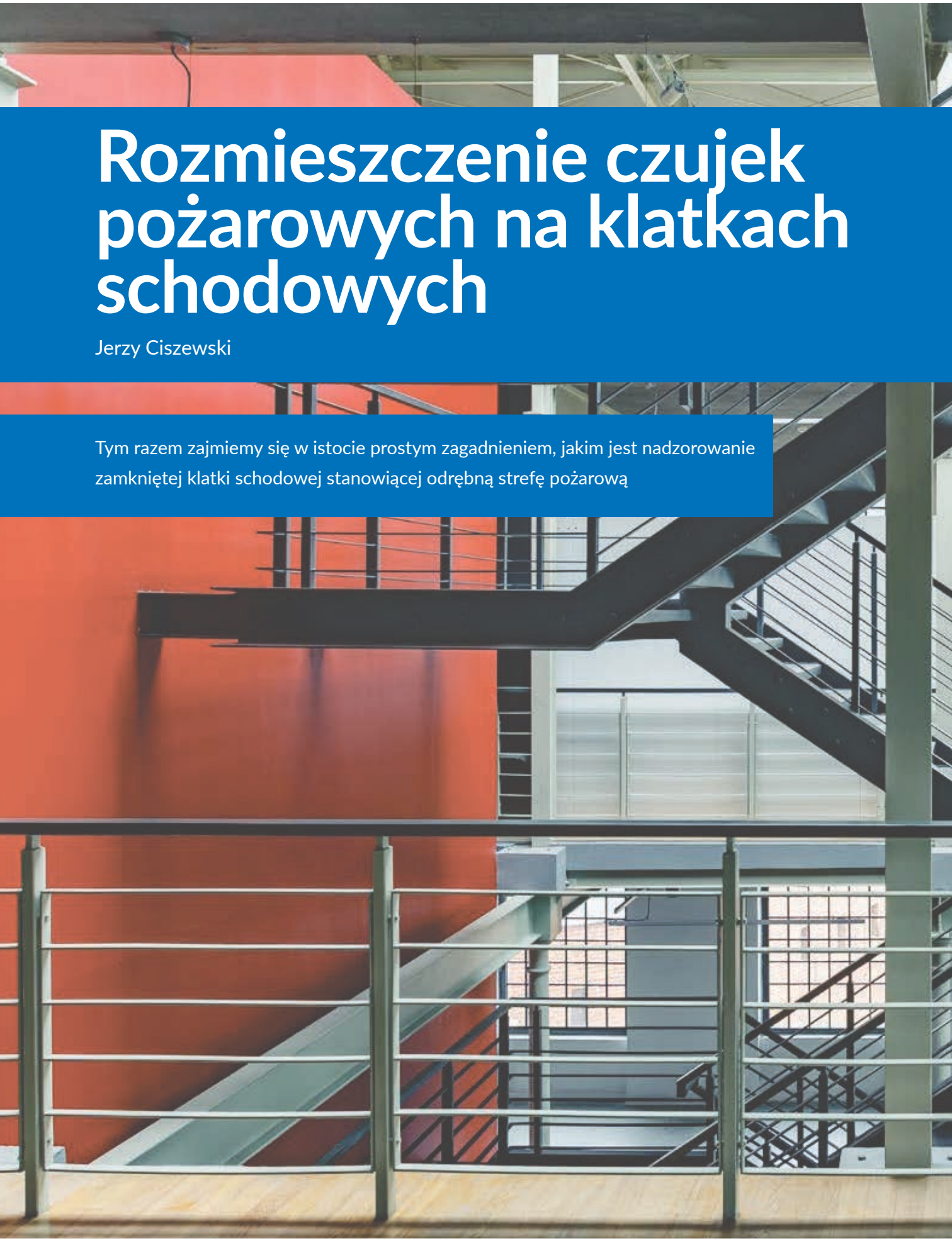
NAJLEPSZE ROZWIĄZANIA W ZAAWANSOWANYCH SYSTEMACH IP DUŻY BUDŻET MOCY DO 370 W

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

Rozmieszczenie czujek pożarowych na klatkach schodowych

Jerzy Ciszewski

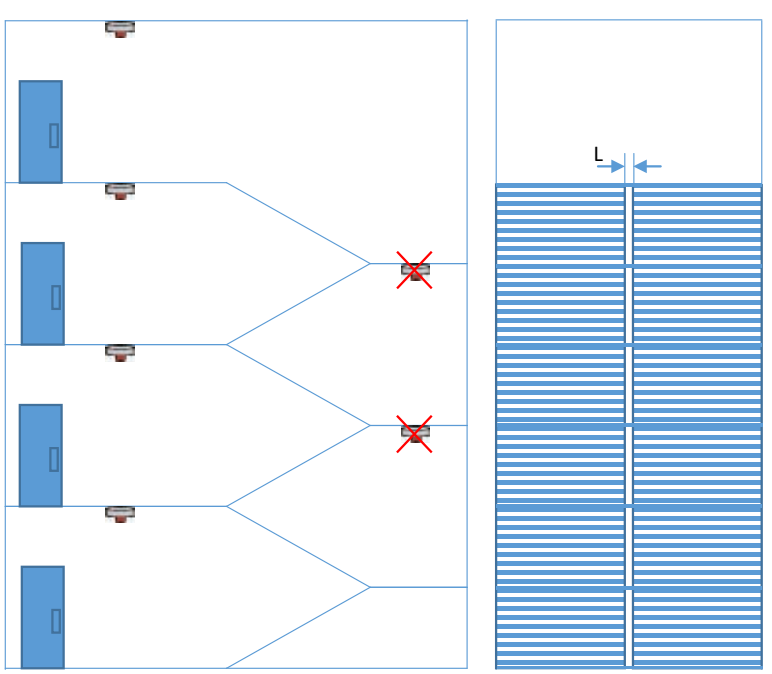
Tym razem zajmiemy się w istocie prostym zagadnieniem, jakim jest nadzorowanie zamkniętej klatki schodowej stanowiącej odrębną strefę pożarową



Nadzór klatki schodowej za pomocą czujek dymu jest zależny od jej tzw. pionowej drożności, czyli od oporów, jakie występują w czasie przemieszczania się dymu w kolumnie konwekcyjnej, wynikających z faktu istnienia obu biegów, a także odległości między biegami.

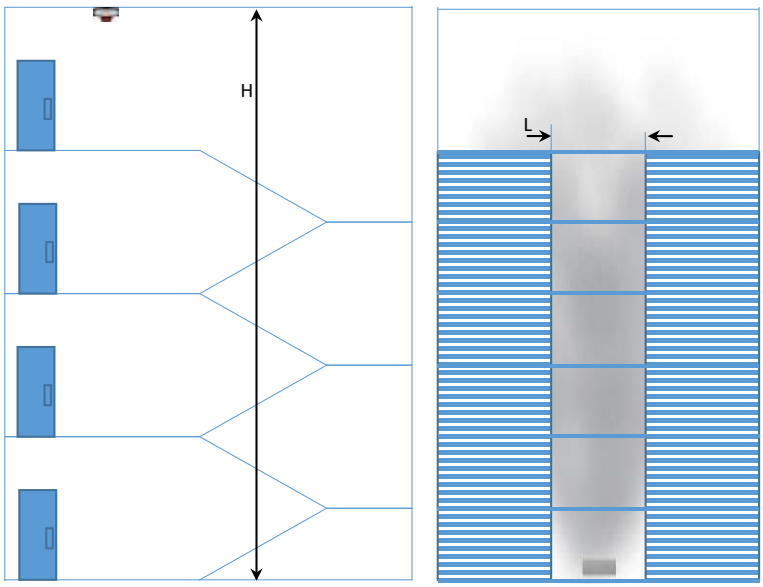
Aby umożliwić wczesną detekcję pożaru, można wstępnie przyjąć, że ukośne ustawienie obu biegów schodów i minimalna możliwa konstrukcyjnie odległość między biegami praktycznie uniemożliwiają przemieszczanie się dymu między piętrami. Takie założenie wymusza nadzór za pomocą czujek zainstalowanych na każdej kondygnacji, począwszy od najwyższej.

Nie przewiduje się instalowania czujek na stropach spoczników. Takie rozwiązanie jest zalecane w normie brytyjskiej BS 5839-1 (pkt 22.2.a).



Założenie: klatka schodowa jest zamknięta i stanowi odrębną strefę pożarową.

Rys. 1. Nadzór nad klatką schodową za pomocą czujek zainstalowanych na każdej kondygnacji



Rys. 2. Nadzór klatki schodowej za pomocą czujki zainstalowanej na granicznej wysokości H

Jeżeli odległość między biegami jest odpowiednio duża, istnieje jednak możliwość przemieszczania się dymu między biegami schodów z kondygnacji na kondygnację. W krańcowym przypadku opory w przemieszczaniu się gorącego powietrza mogą być na tyle małe, że w procesie projektowania można użyć maksymalnej dopuszczalnej wysokości instalowania czujek H, a więc ok. 12 m.

Fot. 1. Klatka schodowa o niskiej drożności pionowej. Mała, mniejsza niż 50 cm, odległość między biegami w dół i w górę

Nasuwa się w związku z tym pytanie: jaka jest ta graniczna odległość między biegami schodów? Jedynymi wytycznymi odnoszącymi się do projektowania, które dają odpowiedź na to pytanie, są wytyczne VdS.

Według VdS 2095:2010-05(07), pkt 6.2.7.1, ta odległość (l) powinna być większa niż 0,5 m.

Niespełnienie kryterium l (el)>0,5 m wymusza na projektancie zastosowanie nadzoru na każdej kondygnacji klatki schodowej (jak na rysunku 1).

W przypadku struktur nachylonych jak schody, schody ruchome i podobne, umieszczonych w przestrzeni pomieszczenia, opiszę sposób rozmieszczania czujek w artykule dotyczącym stropów ukośnych z uwzględnieniem artykułu opisującego nadzorowanie podestów.

Jerzy Ciszewski
IBP NODEX

Bibliografia

1. BS 5839-1:2002-2013 *Fire detection and fire alarm systems for buildings – Part 1: Code of practice for system design, installation, commissioning and maintenance.*
2. VdS 2095:2010-05(07) *VdS-Richtlinien für automatische Brandmeldeanlagen. Planung und Einbau.*

POLON-ALFA

PROJEKTUJEMY zgodnie ze sztuką

SYSTEMY SYGNALIZACJI POŻAROWEJ

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

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

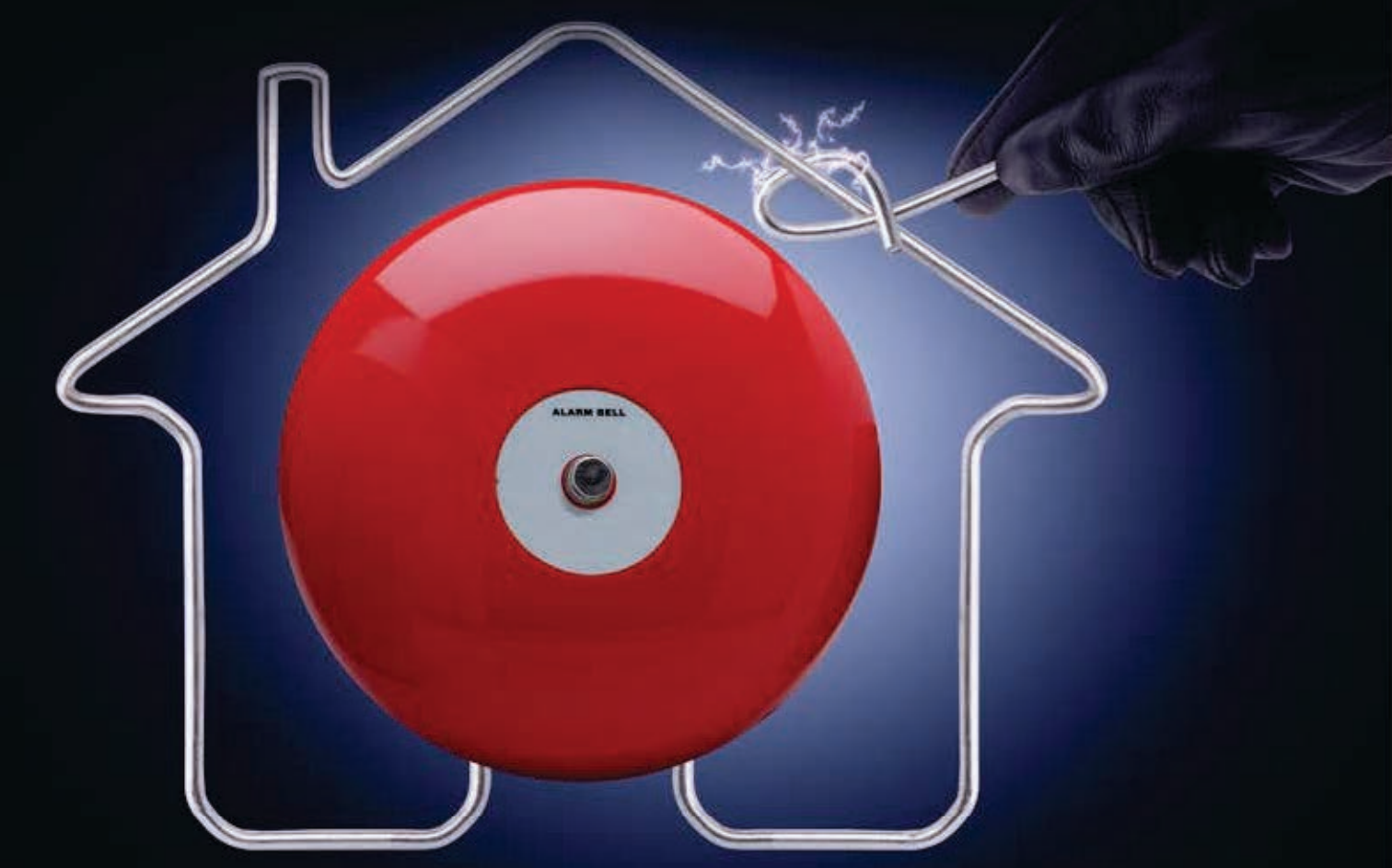
SYSTEM DETEKCJI GAZÓW SDG 6000

POLON-ALFA S.A.
85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.pl

Właściwa integracja systemów budynkowych

Jan Dziedzic

W fachowej (branżowej) literaturze, a zwłaszcza w Internecie, można znaleźć ogromną ilość informacji na temat integracji systemów budynkowych. Integrację systemów opisują, oferują i zachwalają przede wszystkim producenci systemów automatyki budynkowej, producenci oprogramowania przeznaczonego do integracji, a także sprzedawcy takich rozwiązań



W Polsce wspomnianą integrację zapoczątkowały w drugiej połowie lat 90. ubiegłego wieku trzy firmy: Johnson Controls, Honeywell i Siemens. Dysponując szerokim asortymentem własnych produktów (systemów automatyki budynkowej i bezpieczeństwa), firmy te zaoferowały swoim klientom systemy zintegrowane z wykorzystaniem własnego oprogramowania.

Gdy mówimy o integracji budynkowych systemów bezpieczeństwa, najczęściej myślimy o integracji systemu telewizji dozorowej z systemem kontroli dostępu oraz systemem sygnalizacji włamania i napadu. Ta integracja polega najczęściej na przełączaniu na monitor główny obrazu z kamery, która jest najbliżej miejsca danego zdarzenia (np. nieuprawnionego otwarcia drzwi czy uruchomienia przycisku alarmowego), co ma umożliwić ochronie uzyskanie większej ilości informacji o tym zdarzeniu lub jego sprawcy.

Jak jest realizowana i co daje personelowi w budynku i wezwanej straży pożarnej integracja systemu SAP i DSO z innymi działającymi albo przerywającymi działanie podczas alarmu pożarowego systemami, takimi jak system wentylacji czy kontroli dostępu? W niektórych materiałach pojawiają się informacje, jakoby dzięki integracji systemów przeciwpożarowych można było podjąć w trakcie alarmu pożarowego decyzję i wykonać związane z nią czynności w celu dostosowania działania systemów przeciwpożarowych do sytuacji w budynku, której nie przewiduje tzw. scenariusz pożaru. Czy na pewno? Niech za przykład posłuży jeden z istniejących budynków wysokich, bogato wyposażony w automatykę budynkową jednej z czołowych firm oraz w systemy bezpieczeństwa (telewizję dozorową, system kontroli dostępu) i systemy przeciwpożarowe (SAP, DSO, a także instalację tryskaczową). Wszystkie systemy budynkowe są ze sobą zintegrowane (za pomocą znajdującego się w pomieszczeniu ochrony komputera systemu integracji). Do personelu zajmującego się ochroną należy strażak dyżurny, którego głównym zadaniem jest reagowanie na alarmy pożarowe (weryfikacja przyczyny alarmu i adekwatne do danej sytuacji działania, w tym skasowanie fałszywego alarmu, uruchomienie alarmu II stopnia w przypadku pożaru i inne czynności – zależne od miejsca i skali zdarzenia).

Jeżeli np. na kondygnacji +6 zasygnalizowano alarm pożarowy I stopnia, centrala SAP włącza lampkę „Pożar", na jej wyświetlaczu można zobaczyć, jaka jest lokalizacja i źródło alarmu, drukarka centrali drukuje komunikaty z wyświetlacza, na monitorze systemu integracji pojawia się rzut kondygnacji z zaznaczonym urządzeniem zgłaszającym alarm (czujką), a drukarka systemu integracji drukuje komunikaty wyświetlane na monitorze (pomijam tu alarmy II stopnia, ponieważ te uruchamiają wszystkie funkcje przewidziane w scenariuszu pożarowym dla miejsca powstania alarmu). Strażak dyżurny odczytuje informacje z wyświetlacza centrali lub z wydruku, sprawdza na monitorze lokalizację alarmu, zabiera wydruk rzutu kondygnacji, naciska przycisk „Potwierdzenie" na centrali SAP i udaje się na kondygnację +6 w celu weryfikacji alarmu (może tam dojechać windą pożarową, która czeka na niego na parterze budynku). System integrujący systemy budynkowe może wyświetlić na monitorze obraz z kamery zlokalizowanej najbliżej źródła alarmu, co pomoże ochronie w działaniu. Pracownik ochrony pełniący dyżur w pomieszczeniu służącym do monitorowania może przekazać strażakowi informację o tym, czy

na monitorze widać dym lub płomienie. Jeżeli po przybyciu na kondygnację +6 strażak stwierdzi, że jest to pożar, ma nacisnąć przycisk pożarowy i wrócić do pomieszczenia ochrony, aby oczekiwać na przyjazd jednostek Państwowej Straży Pożarnej. Centrala SAP realizuje funkcje przewidziane w scenariuszu pożarowym. Trwa ewakuacja określonych kondygnacji budynku.

Jaka jest w tym momencie rola systemu integrującego systemy budynkowe (oprócz wyświetlenia na monitorze obrazu z kamery)? Żadna! Wszystkie funkcje sterujące – odblokowanie drzwi na drodze ewakuacyjnej, włączenie nadawania przez DSO ewakuacyjnych i ostrzegawczych komunikatów, wyłączenie wentylacji bytowej i włączenie wentylacji pożarowej (wentylatorów, klap itp.), sprowadzenie wszystkich wind na poziom parteru i zamknięcie bram pożarowych w garażu – są realizowane przez centralę SAP. Centrala ta steruje systemami (centralami systemów) i urządzeniami poprzez wyznaczone wyjścia sterujące z samej centrali (najczęściej dotyczy to systemu DSO) oraz moduły sterujące zainstalowane w pętlach dozorowych (w pobliżu sterowanych systemów lub urządzeń). Ponadto centrala SAP nadzoruje realizację sterowania i ewentualnie zgłasza awarię, jeśli jakieś urządzenie nie zadziałało poprawnie. Takie rozwiązanie (sterowania przez centralę SAP poprzez wyznaczone wyjście sterujące lub moduł do każdego urządzenia, w tym do pojedynczych drzwi objętych kontrolą dostępu czy każdej klapy pożarowej) nie tylko jest bardziej niezawodne w przypadku pożaru, ale także umożliwia łatwiejsze testy poprawności działania poszczególnych urządzeń podczas przeglądów i konserwacji.

Szybkie podejmowanie decyzji i wykonywanie odpowiednich działań (czyli włączanie lub wyłączanie urządzeń) nie może być skutecznie wykonane przez systemy integracji, promowane przez producentów sprzętu i oprogramowania, a także sprzedawców systemów budynkowych. Ani obsługa budynku, ani tym bardziej funkcjonariusze PSP nie znają na tyle systemów budynkowych, aby – na podstawie informacji wyświetlanych na monitorze systemu integracji budynkowej (nie wiadomo, jakich informacji) – bezpiecznie włączyć albo wyłączyć konkretne urządzenie lub system, zwłaszcza jeśli dane urządzenie uległo awarii, co sygnalizuje centrala SAP. Nawet w przypadku rozszerzenia zakresu ewakuacji osób przebywających w budynku na podstawie decyzji zarządcy obiektu lub kierującego działaniami ratowniczymi (w przykładowym budynku ewakuowana jest kondygnacja +6, garaż podziemny i najwyższa, techniczna kondygnacja) wykorzystuje się panel operatora systemu DSO, co na pewno zajmuje mniej czasu i jest bardziej niezawodne niż wyszukiwanie i klikanie odpowiednich ikon na monitorze systemu integracji.

Reasumując, najbardziej niezawodna i optymalna „integracja" systemów przeciwpożarowych budynku powinna polegać na połączeniu kablowym (najczęściej kablem pożarowym) wyjść sterujących oraz pętlowych modułów sterujących centrali/systemu SAP z właściwymi (pożarowymi) wejściami urządzeń wykonujących określone czynności (start/stop lub włącz/wyłącz) podczas alarmu pożarowego. Najkorzystniej jest, gdy jedno wyjście sterujące centrali SAP lub jeden sterujący moduł pętlowy steruje pojedynczym urządzeniem (jednymi drzwiami objętymi kontrolą dostępu, jedną klapą pożarową itp.), a nie grupą urządzeń (kilkorgiem drzwi objętych kontrolą dostępu na kondygnacji), a tym bardziej centralą systemu kontroli dostępu, kilkoma klapami pożarowymi, np. przez odłączenie zasilania grupy klap, itp.). Wszelkie inne systemy i urządzenia budynkowe mogą być ze sobą zintegrowane w dowolny sposób.

Jan Dziedzic

NOVUS®

NVIP-4H-6202M

6000 VSS IP

NOVUS IP

NMS Compatible

ONVIF

MOTOR ZOOM

ZOBACZ ISTOTNE SZCZEGÓŁY

KAMERA Z OBIEKTYWEM MOTOR-ZOOM I FUNKCJĄ AUTO-FOCUS

AAT HOLDING S.A.

PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA

www.aat.pl

AI dla każdego

Część 4

Piotr Rogalewski

Poprzednią część zakończyłem omówieniem podstaw działania perceptronu – najprostszej sieci neuronowej. Teraz nadeszła pora na wyjaśnienie najbardziej „magicznej" właściwości sztucznej inteligencji – tego, że sieci neuronowe potrafią się uczyć

Nauka nadzorowana (z trenerem) i ważenie danych

W poprzedniej części opisałem działanie sztucznego neuronu i mechanizmu wag. Dla przypomnienia, waga to fundamentalny element neuroplastyczności w sztucznych sieciach neuronowych. Waga to liczba, która określa ważność (wagę) wejścia, do którego jest przypisana. Im wyższa waga, tym większe znaczenie ma sygnał na wejściu i nawet jego niewielkie zmiany będą wywierać duży wpływ na sygnał na wyjściu neuronu. Im waga niższa, tym mniejsze znaczenie będą miały nawet duże wahania sygnału przypisanego do wejścia z taką wagą. Ale skąd sztuczny neuron „wie", jakie wagi są przypisane poszczególnym wejściom? Jedną z możliwości jest wcześniejsze, wstępne zaprogramowanie wag przez człowieka. Innym sposobem, spotykanym najczęściej w nienadzorowanym uczeniu się, jest losowanie wartości wag z ustalonego wcześniej zakresu. Manipulowanie wartościami wag na podstawie sygnału zwrotnego jest istotą procesu nauki w sztucznych sieciach neuronowych. Takim sygnałem zwrotnym jest błąd.

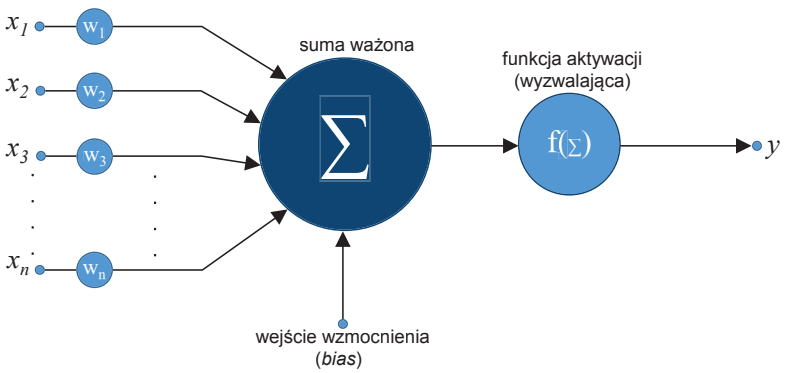
Mylić się jest rzeczą nie tylko ludzką

Człowiek nie jest doskonały i, jak mówi mądre powiedzenie, uczy się przez całe życie, choć niestety często na własnych błędach. Tak jednak działa jego mechanizm poznawczy. Dzięki temu, że uczymy się unikać takich błędów, które już kiedyś popełniliśmy, lub przynajmniej je minimalizować, rozwijamy się i stajemy się doskonalsi. To jedna z podstawowych sił napędowych ewolucji – rozwiązania lub osobniki słabe, które nie sprawdzają się lub nie radzą sobie w rzeczywistych warunkach są w sposób naturalny eliminowane na rzecz rozwiązań i osobników lepszych, silniejszych. Dokładnie ta zasada legła u podstaw algorytmu genetycznego[I], który został zdefiniowany przez Johna Henry'ego Hollanda w 1960 r[II]. Algorytm genetyczny należy do grupy algorytmów ewolucyjnych, czyli rozwiązań wzorowanych na ewolucji biologicznej, i jest stosowany tam, gdzie wymagana jest optymalizacja lub modelowanie obiektów bądź procesów. Sieć neuronowa jest doskonałym przykładem obiektu, który można modelować za pomocą algorytmów genetycznych. W jaki sposób działa taki algorytm? Na początku tworzona jest pewna liczba obiektów stanowiących populację startową. Obiekty z tej populacji mają ten sam zestaw parametrów, ale wartości tych parametrów dla populacji startowej są losowane. Następnie uruchamiany jest proces nauki, w którym obiekty populacji startowej wykonują założone zadanie, a ich parametry ulegają modyfikacjom na podstawie uzyskanych wyników. Kluczem do tych modyfikacji jest nauka na własnych błędach. Błędem w tym przypadku jest nieosiągnięcie oczekiwanego wyniku – im większe odchylenie, tym większy jest błąd. Posłużę się tu przykładem prostej gry w wyścigi, rozgrywanej na dwuwymiarowej planszy – wirtualnym torze wyścigowym. Populacja będzie się składać ze stałej liczby wirtualnych pojazdów, powiedzmy dziesięciu, a ich zadaniem będzie przejechanie przypisanych im wirtualnych torów w taki sposób, aby nie najechać na krawędź toru. Każdy pojazd jedzie po swoim własnym torze, takim samym jak tor każdego innego. Gra składa się z wielu wyścigów, które są powtarzane tak długo, aż któryś z pojazdów nauczy się pokonywać tor bezkolizyjnie i możliwie najszybciej. Oczywiście taki pojazd będzie zwycięzcą gry. Ewolucja obiektów populacji startowej będzie polegała na analizowaniu błędów popełnionych przez pojazdy – każde zetknięcie się z krawędzią toru będzie sygnałem zwrotnym dla neuronów sztucznej sieci neuronowej, informującym o konieczności modyfikacji parametrów jazdy w kolejnym wyścigu. Każdy z pojazdów ma ten sam zestaw właściwości i procedur. Właściwościami pojazdu są aktualna pozycja *X* i *Y*, bieżąca prędkość własna oraz aktualny kierunek jazdy. Procedurami pojazdu są natomiast skręt w lewo, skręt w prawo i zmiana prędkości. Pojazdy nie znają przebiegu trasy wyścigu i muszą go poznać. Każdy kolejny wyścig pozwala zebrać informacje o popełnionych błędach i tak zmodyfikować procedury sterowania pojazdem (wagi neuronów w poszczególnych warstwach sieci), aby ten sam błąd nie wystąpił podczas kolejnego wyścigu. Po każdym wyścigu mamy do czynienia z nową generacją pojazdów – bogatszą o doświadczenia poprzedniej generacji, dokładnie tak jak w procesie ewolucji naturalnej.

Wzmocnienie

Warto omówić przypadek działania systemu sztucznej inteligencji, w którym zachodzi konieczność zmiany progu zadziałania neuronu lub grupy neuronów, a jednocześnie zmiana wartości poszczególnych wag na wejściach jest niepożądana.

sygnał na wejściu *bias*, tym mniejsza czułość wejść synaptycznych neuronu. Innymi słowy, próg zadziałania funkcji aktywacji neuronu będzie przesuwał się w górę albo w dół w zależności od wartości sygnału na wejściu *bias*. W opisanym wyżej przykładzie z paletą barw nagłe zwiększenie jasności obrazu można skompensować,



Rys. 1. Sztuczny neuron z dodatkowym wejściem wzmocnienia *bias*. Graf.: P. Rogalewski

Przykładowo, w systemie rozpoznawania kolorów nagłe zwiększenie jasności obrazu na wejściu spowoduje przesunięcie się palety barw w stronę kolorów jaśniejszych, co dla systemu wytrenowanego przy zupełnie innej jasności może stanowić problem. Rozwiązaniem jest sztuczny neuron z dodatkowym wejściem wzmocnienia o nazwie *bias*, przedstawiony na rys. 1.

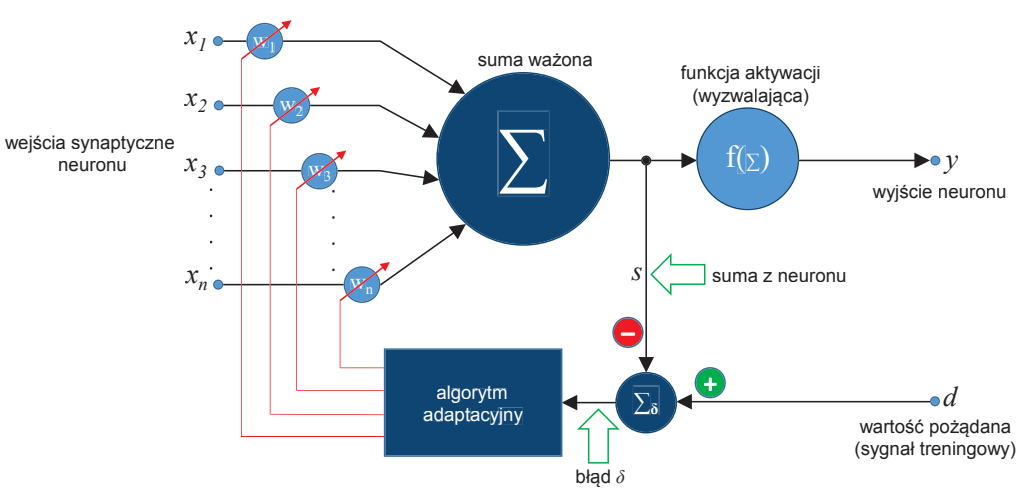
Im silniejszy sygnał jest podawany na wejście *bias*, tym większe będzie wzmocnienie sygnałów na wejściach synaptycznych (wszystkie te wejścia staną się bardziej czułe na sygnały wejściowe – w jednakowym stopniu) i odwrotnie – im słabszy

podając ujemny sygnał na wejście wzmocnienia w celu obniżenia czułości neuronów na poszczególne analizowane barwy.

Wsteczna propagacja błędu i reguła delta

Pozostaje odpowiedzieć na pytanie: skąd neuron wie, że popełnił błąd i jak duży był to błąd? Wyjaśnienie znajduje się na rys. 2.

Oprócz opisanych w poprzedniej części cyklu *AI dla każdego* standardowych wejść synaptycznych *x1… xn* i wyjścia *y* neuron posiada dodatkowe wejście *d*, do którego doprowadzony jest sygnał



Rys. 2. Neuron liniowy typu ADALINE z mechanizmem adaptacji wag. W celu uzyskania odpowiedniej czytelności rysunku pominięto wejście wzmocnienia *bias*. Graf.: P. Rogalewski

wzorcowy. Tego typu neuron jest adaptacyjnym neuronem liniowym nazywanym ADALINE (od ang. *Adaptive Linear Neuron*)[III]. Neuron jest nazywany liniowym, ponieważ jego funkcja aktywacji jest funkcją liniową. Sieć neuronowa składająca się z wielu neuronów ADALINE to MADALINE (od ang. *Many Adaptive Linear Neurons)*. Obecnie jest ona jednym z najpopularniejszych i najpowszechniej stosowanych typów sieci. Sygnałem wzorcowym *d* jest wartość, jaka jest oczekiwana na wyjściu neuronu w odpowiedzi na określony zestaw sygnałów wejściowych. Innymi słowy jest to pozytywny (jako wzorzec, nie matematycznie), wzorcowy sygnał „treningowy" (oznaczony na rysunku zielonym symbolem „+"), który „mówi" neuronowi, że to jest wartość, do której powinien dążyć. Neuron oblicza różnicę wartości sygnału treningowego *d* i wyliczonej przez siebie sumy ważonej *s* (na rysunku czerwony znak „-" określający sygnał typu negatywnego), określając tym samym wielkość błędu *δ* (delta). Proces ten to tzw. reguła delta stanowiąca fundament procesu uczenia neuronów. Reguła ta jest opisana wzorem:

$$\delta = d - s$$

Im większy błąd, tym większa wartość *δ*. Następnie wartość sygnału błędu *δ* jest przekazywana jako argument wejściowy dla algorytmu, który manipuluje wagami, dostrajając je tak, by wartość błędu na wyjściu neuronu zminimalizować. Im większy błąd, tym mocniejsze dostrojenie jest potrzebne. Cały proces uczenia neuronów sprowadza się właściwie do minimalizacji błędu średniokwadratowego w poszczególnych warstwach sieci i w pojedynczych neuronach. Jak łatwo zauważyć, błędy są w tym przypadku informacją biegnącą w kierunku przeciwnym do kierunku działania neuronu. Sygnały wejściowe *x* wejść synaptycznych ulegają propagacji, czyli biegną od lewej do prawej strony neuronu i „w głąb" sieci neuronowej. Informacje o błędach „podróżują" natomiast w przeciwną stronę – „w górę", między warstwami sieci (neurony przekazują sobie informację o błędach), jak i w samym neuronie (od prawej do lewej). Ta odwrócona wędrówka sygnałów to wsteczna propagacja błędu. Uczenie sieci uznaje się za zakończone, gdy wszystkie neurony w poszczególnych warstwach sieci dostroją swoje wagi tak, by na wyjściu generować sygnały jak najbardziej zbliżone do wzorców treningowych.

Co za dużo, to niezdrowo

W przypadku sztucznej inteligencji, podobnie jak w naturze, przesada nie jest wskazana. Przetrenowany sportowiec może nabawić się kontuzji i stracić motywację do dalszej ciężkiej pracy, zamiast osiągnąć lepszy wynik. Analogicznie, przetrenowana (ang. *overtrained*) sieć neuronowa będzie działać mniej efektywnie, a nawet niezgodnie z przewidywaniami[IV]. Często takie zjawisko nazywa się także nadmiernym dopasowaniem (ang. *overfitting*). Z czego to wynika? Jeśli opisana wyżej procedura manipulacji wagami zostanie wykonana zbyt precyzyjnie i wagi zostaną dostrojone zbyt „wąsko", bez odpowiedniej tolerancji, sieć będzie reagować zbyt „ostro" na dane wejściowe i w efekcie przez filtry klasyfikacji będzie przechodził tylko niewielki zbiór obiektów. Aby lepiej to wyjaśnić, wrócę do przykładu kota, który podałem w drugiej części (nr 2/2019 „Zabezpieczeń"). Gdyby sieć neuronowa została wytrenowana zbyt dużą liczbą zdjęć śpiących kotów zwiniętych w kłębek, nie byłaby w stanie prawidłowo rozpoznać kotów stojących na łapkach. Dobór materiału treningowego oraz określenie momentu, w którym należy zakończyć uczenie sieci, jest jednym z najtrudniejszych wyzwań dla twórców systemów sztucznej inteligencji.

W kolejnym artykule opiszę przykładowe rozwiązania implementujące sieci neuronowe i systemy *deep learning*.

Piotr Rogalewski

Przypisy:

I. Pojęcie algorytmu zostało wyjaśnione w drugiej części cyklu *AI dla każdego* („Zabezpieczenia" nr 2/2019).

II. D. E. Goldberg, *Genetic Algorithms in Search, Optimization, and Machine Learning*, Addison-Wesley Professional, Boston 1989.

III. B. Widrow, M. A. Lehr, *30 Years of Adaptive Neural Networks: Perceptron, Madaline, and Backpropagation*, (w:) *Proceedings of the IEEE*, vol. 78, nr 9, wrzesień 1990, s. 1415–1442.

IV. I. V. Tetko, D. J. Livingstone, A. I. Luik, *Neural Network Studies. 1. Comparison of Overfitting and Overtraining*, (w:) „Journal of Chemical Information and Computer Sciences", nr 35, wrzesień 1995, s. 826–833.

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

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

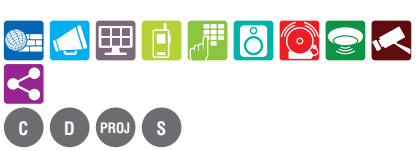
ALARMTECH POLSKA Sp. z o.o.
Oddział w Gdańsku
ul. Kielnieńska 115
80-299 Gdańsk
tel. 58 340 24 40; faks 58 340 24 49
e-mail: info@alarmtech.pl
www.alarmtech.pl

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

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

ASSA ABLOY POLAND Sp. z o.o.
ul. Iłżecka 24 bud. F
02-135 Warszawa
tel. 22 751 53 54; faks 22 751 53 56
e-mail: biuro@assaabloy.com
www.assaabloy.com.pl

ROBERT BOSCH Sp. z o.o.
ul. Jutrzenki 105
02-231 Warszawa
tel. 22 715 00 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. kom. 604 569 775
e-mail: brabork@braborklab.pl
www.braborklab.pl

bt electronics Sp. z o.o.
ul. Rybitwy 22
30-722 Kraków
tel./faks 12 410 85 10
e-mail: bte@bte.pl
www.bte.pl

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

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

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

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

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

EBS Sp. z o.o.
ul. Bronisława Czecha 59
04-555 Warszawa
tel. 22 518 84 00
e-mail: office@ebs.pl
www.ebssmart.com

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

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

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

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

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

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

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

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

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

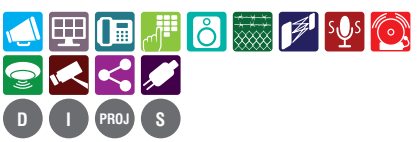
ul. Radzymińska 308, 03-694 Warszawa
tel. 22 676 78 40
e-mail: warszawa@eltrox.pl

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

ES-INSTAL Andrzej Wójcik
Al. gen. W. Sikorskiego 9 A/72 A
02-758 Warszawa
tel. kom. +48 501 277 513
e-mail: andrzejw@esinstal.pl
https://esinstal.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
Leszek Mitusiński
Włosań, ul. Świątnicka 88
32-031 Mogilany
tel. 12 256 50 25, 12 256 50 35;
faks 12 270 56 96
e-mail: biuro@gde.pl
www.gde.pl

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

B C D I PROD PROJ S

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

I PROJ

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

D PROJ S

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

C 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

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

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

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

PROD

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

D 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

ROGER Sp. z o.o. Sp. k.
Gościszewo 59
82-400 Sztum
tel. 55 272 01 32
faks 55 272 01 33
e-mail: roger@roger.pl
www.roger.pl

PROD PROJ

SCHRACK SECONET POLSKA Sp. z o. o.
Wilanów Office Park, bud. B1
ul. Adama Branickiego 15
02-972 Warszawa
tel./faks 22 33 00 620/624
e-mail: warszawa@schrack-seconet.pl
www.schrack-seconet.pl

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

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

ul. Św. Czesława 7 lok. 18, 61-575 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./faks 61 677 48 00
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. Ceramiczna 1A
86-005 Kruszyn Krajeński
tel. 52 522 32 38
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
e-mail: winkhaus@winkhaus.pl
www.winkhaus.pl

VIASAT MONITORING Sp. z o.o.
ul. Puławska 359
02-801 Warszawa
tel. 22 546 0 888; faks 22 546 0 619
e-mail: info@viasat.com.pl
www.viasat.com.pl

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

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

ul. Nowy rynek 2, 62-002 Suchy Las k/Poznania
tel. kom. 601 410 979, 601 203 664

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

Legenda

Kategorie*

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

Działalność*

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

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

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Paweł Karczmarzyk
Andrzej Walczyk

Korekta
Paweł Karczmarzyk

Dział marketingu i reklamy
Ela Końka

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

Współpraca
Marcin Buczaj
Piotr Czernoch
Marcin Pyclik

Projekt graficzny, skład i łamanie
Piotr Przybylski

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

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

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

Dostępne formy reklamy

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

Reklama na okładkach
pierwsza strona
druga strona
przedostatnia strona
ostatnia strona

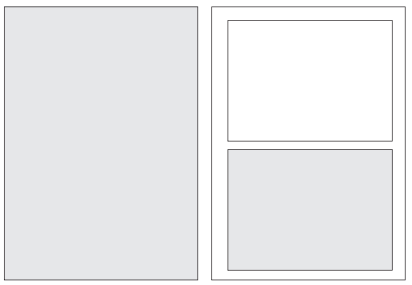
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie

Spis teleadresowy
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Ceny negocjujemy indywidualnie

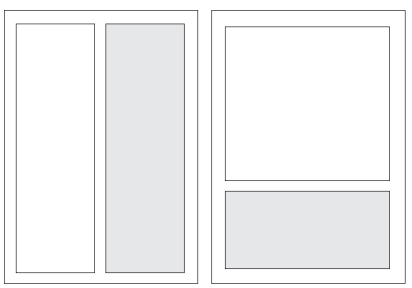
Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej http://www.zabezpieczenia.com.pl w dziale Reklama

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



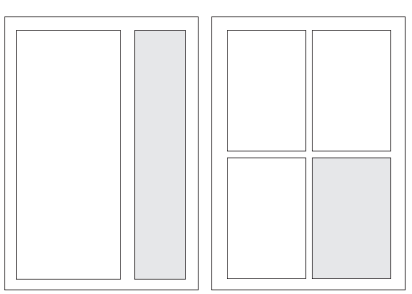
cała strona
(200 x 282 mm + 3mm spad)

1/2 strony
(170 x 125 mm)



1/2 strony
(83 x 260 mm)

1/3 strony
(170 x 80 mm)



1/3 strony
(54 x 260 mm)

1/4 strony
(83 x 125 mm)

Spis reklam

AST DO BRAM DRZWI OKIEN

2 GRADE

CZUJKI MAGNETYCZNE DO BRAM, DRZWI i OKIEN

TERAZ ZE STOPNIEM ZABEZPIECZENIA GRADE 2

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

FUJIFILM
Value from Innovation

HIGH-END CAMERA X TOP PERFORMANCE LENS

THE NEW FUJINON SX800. THE BEST OF BOTH.

With the new SX800, Fujinon combines both in one for the first time: camera and lens. For long range surveillance at the highest level with 40x optical magnification and constantly sharp images. **www.fujifilm.eu/fujinon. Fujinon. To see more is to know more.**

FUJINON