20 lat ZABEZPIECZENIA

CZASOPISMO BEZPŁATNE
ISSN: 1505-2419 DWUMIESIĘCZNIK NR 5(123)/2018

AXIS COMMUNICATIONS

JEDNA, której potrzebujesz.

JEDEN adres IP
JEDEN interfejs z podwójnym podglądem
JEDEN mechanizm PTZ - dwa bispektralne strumienie wideo

www.axis.com/products/axis-q87-series

deLux
technology

Kolory nawet w ciemności

Nowa metoda tworzenia i kodowania obrazów opracowana przez Videotec zapewnia doskonałą reprodukcję barw nawet przy bardzo słabym oświetleniu obserwowanej sceny.

Kolorowa kamera, która pracuje przy oświetleniu 0,006 lx

Usprawnione funkcje PTZ

BEST CHOICE

Wyższa jakość, niższe ceny

Ex

APPROVED TYPE APPROVAL SCHEME

VIDEO SECURITY PRODUCTS

www.videotec.com

info@videotec.com

Made in Italy since 1986

VIDEOTEC

NOVUS®

FISHEYE

ZAWSZE WIESZ CO JEST GRANE

Z NOWYMI KAMERAMI TYPU „RYBIE OKO” NIE UMKNIE CI ŻADEN SZCZEGÓŁ

AAT HOLDING S.A.

PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA

www.aat.pl

SPIS TREŚCI

Case Study

Ochrona informacji

Nowa generacja czytników
Omnikey 5427CK

Asortyment firmy **HID Global** – lidera rynku kontroli dostępu i zabezpieczeń IT – został powiększony o czytniki **Omnikey 5427CK** drugiej generacji. Czytniki te różnią się od urządzeń pierwszej generacji tym, że bazują na natywnym wsparciu systemów operacyjnych Windows, iOS, Linux oraz Android i nie wymagają instalowania lub aktualizowania dodatkowych sterowników. Poza tym odczytują dodatkowo karty HITAG. Czytniki tego typu wspomagają administrowanie kartami zbliżeniowymi. Podłączane są do portu USB stacji roboczej administratora. Dzięki pracy w trybie emulacji klawiatury dane z karty mogą być pobierane i odpowiednio przekształcane w celu bezpośredniego wprowadzania do aplikacji, tak jakby były wprowadzane ręcznie, za pomocą klawiatury. Taki proces znacznie przyspiesza wprowadzanie numeru karty do aplikacji kontroli dostępu.

Czytniki obsługują karty pracujące na częstotliwości 125 kHz (np. Prox, EM) i 13,56 MHz (np. iClass, iClass SE, SEOS, Mifare, Desfire). Dzięki temu mogą być stosowane w obiektach, gdzie występują różne rodzaje kart. Pomocne są również w przypadku migracji systemu z przestarzałej technologii kart i czytników pracujących na częstotliwości 125 kHz na znacznie bardziej bezpieczną, pracującą na częstotliwości 13,56 MHz.

Czytniki Omnikey 5427 CK sprawdzają się zwłaszcza w systemach, w których zastosowano najnowszej generacji karty iCLASS Seos oraz karty zabezpieczone kluczami iCLASS Elite. Czytniki w wersji 5427 CK Bluetooth obsługują dodatkowo karty mobilne HID.

W celu uzyskania dodatkowych informacji można skontaktować się z platynowym partnerem HID – firmą **Alarmnet** (www.alarmnet.com.pl).

Bezpośr. inf. Krzysztof Borkiewicz
Alarmnet

Nowy kontroler Apollo

Firma **Apollo Security** – producent systemów kontroli dostępu – wprowadziła na rynek nowy, innowacyjny **kontroler sieciowy ASP-4**. Urządzenia te można grupować w klastry, w których jedno z urządzeń pełni funkcję głównego kontrolera systemu, jak i kontrolera drzwiowego, a pozostałe urządzenia pracują jako kontrolery podrzędne. W ramach jednego klastra można zgrupować do 32 kontrolerów. Jeden system kontroli dostępu może składać się z wielu klastrów. Każdy kontroler ASP-4 jest wyposażony w wiele procesorów – cztery mikrokontrolery PIC do zarządzania interfejsami komunikacyjnymi oraz moduł SOM z 1-gigabajtowym procesorem przemysłowym z jądrem Linux. Dzięki temu ASP-4 działa bardzo szybko z jednoczesnym zachowaniem stabilności. Rezultatem zastosowania takiej architektury jest też to, że pojedynczy kontroler może pracować samodzielnie, kontrolując dostęp nawet do miliona użytkowników kart, a przesłanie danych dotyczących 100 000 kart do pamięci kontrolera trwa poniżej 12 sekund!

Kontroler ma dwa ethernetowe porty sieciowe do komunikacji z jednostką nadrzędną i z pozostałymi urządzeniami w systemie, port USB oraz dwa wymienne interfejsy RS485 do szyfrowanej komunikacji z czytnikami OSDP i innymi urządzeniami peryferyjnymi.

Do kontrolera można podłączyć 16 czytników OSDP lub cztery czytniki Wiegand i 12 czytników OSDP. ASP-4 zapewnia najwyższy poziom zabezpieczenia przepływu danych – komunikacja jest szyfrowana z użyciem protokołu TSLv1.2 AES-128-SHA z dwukierunkowym uwierzytelnianiem. Całe urządzenie jest zbudowane z elementów przemysłowych, dostosowanych do pracy w temperaturze z zakresu od -40°C do +85°C.

Kontrolery ASP-4 pracują pod kontrolą systemu kontroli dostępu i monitorowania APACS w wersji 3.9 lub nowszej.

Dystrybutorem systemów kontroli dostępu Apollo w Polsce jest firma **Alarmnet**.

Bezpośr. inf.
Krzysztof Borkiewicz
Alarmnet

Monitoring do zadań specjalnych

Administratorzy infrastruktury krytycznej, duże przedsiębiorstwa, instytucje publiczne, placówki medyczne czy służby mundurowe potrzebują niezawodnych systemów monitorowania, funkcjonujących w każdym – także ekstremalnym – środowisku, tak aby utrzymywać odpowiedni poziom bezpieczeństwa bez zbędnego ryzyka po stronie zabezpieczającego. Potrzeby te rozumie firma **Axis Communications**, która wzbogaca swoją ofertę w nowe kamery kopułkowe ze znanej już serii **AXIS Q35**.

Operatorzy kamer – obserwujący granice państwa i miejsca publiczne, sieci transportowe lub przesyłowe, centra logistyczne i magazynowe czy zaawansowane procesy produkcyjne w sektorach strategicznych – potrzebują narzędzi łączących jakość z odpornością na warunki środowiskowe – od ultraniskiej temperatury, przez wstrząsy, po oddziaływanie czynników biochemicznych. Na rynku istnieje kilka specjalnych rozwiązań, ale seria AXIS Q35 z pewnością warta jest szczególnej uwagi.

Seria AXIS Q35 to stałopozycyjne kamery kopułkowe przeznaczone do montażu wewnątrz lub na zewnątrz pomieszczeń, charakteryzujące się wysokimi parametrami w zakresie optyki, a także odpornością na niekorzystne warunki pogodowe i akty wandalizmu. AXIS Q3518-LVE wykorzystuje najwyższej jakości

przetwornik obrazów o rozdzielczości 4K, a AXIS Q3517-SLVE – 5 Mpx. Obie wersje mają funkcję Wide Dynamic Range (WDR) – Forensic Capture, która zapewnia zbalansowaną jakość obrazu w scenach o dużej zmienności oświetlenia, a także funkcję Lightfinder umożliwiającą uzyskanie czytelnego obrazu nawet przy najsłabszym oświetleniu. Kamery obsługują korekcję dystorsji beczkowatej i mają obiektyw zmiennoogniskowy, z którego można korzystać podczas obserwacji. Nowe modele mają również wielokrotnie nagradzaną funkcję Zipstream, która identyfikuje szczegóły z właściwą dokładnością, przy jednoczesnym zmniejszeniu zapotrzebowania na przepustowość sieci o średnio połowę lub więcej.

Kamery AXIS Q35 mogą pracować stabilnie w temperaturach ekstremalnych, tj. od -50°C do +60°C. Ponadto AXIS Q3517-SLVE ma obudowę ze stali nierdzewnej, która jest odporna na korozyjne działanie soli, detergentów i innych chemikaliów. Kamery AXIS Q3518-LVE i AXIS Q3517-SLVE mają klasę odporności na udary IK10+ i mogą wytrzymać uderzenia o energii 50 J. Elektroniczna stabilizacja obrazu zapewnia stabilny obraz nawet podczas intensywnych wibracji.

W przypadku urządzeń serii Q35 dostępne są preinstalowane systemy AXIS Motion Guard, AXIS Fence Guard i AXIS Loitering Guard do tzw. proaktywnego nadzoru. Jest też możliwość dodawania dynamicznych nakładek wprowadzających dodatkowe informacje do kanału wizyjnego, np. z prognozą pogody. Dostępne są zewnętrzne czujniki, podłączane do portów wejściowych, wyzwalające alarmy lub inicjujące inne działania. Istnieje możliwość podłączania do wyjść kamery przekaźników i innych urządzeń peryferyjnych, służących np. do włączania i wyłączania świateł blokowania i odblokowywania drzwi. Kamery mogą być zasilane metodą PoE przez kabel sieciowy. Kamery Q35 są łatwe do zainstalowania, głównie dzięki asystentowi poziomowania, automatycznemu obracaniu, zdalnej regulacji ogniskowej obiektywu i kalibracji ostrości.

Zaawansowane testy potwierdziły, że kamery z nowej serii sprawdzą się w najbardziej wymagających warunkach, niezależnie od tego, czy chodzi o światło, pogodę czy surowe środowisko. Jakość obrazu umożliwia najskuteczniejszą z możliwych identyfikację ludzi, obiektów i pojazdów, a preinstalowane narzędzia analityczne zapewniają doskonałe wsparcie proaktywnego nadzoru. Unowocześniona seria AXIS Q35 doskonale nadaje się do monitorowania infrastruktury krytycznej, monitoringu miejskiego, nadzoru lotnisk, stacji kolejowych, portów, zakładów opieki zdrowotnej, zakładów przemysłowych z branży farmaceutycznej i spożywczej – powiedziała Petra Bennermark, globalny menedżer produktu w firmie Axis Communications.

Kamery AXIS Q3518-LVE i AXIS Q3517-SLVE są dostępne w dystrybucji od sierpnia tego roku.

Bezpośr. inf. Axis Communications

PNM-7000VD

tandem z wymiennymi obiektywami

Hanwha Techwin wprowadza do oferty nowy model kamery tandemowej z dwoma przetwornikami Full HD typu **PNM-7000VD**, która znakomicie nadaje się do monitorowania rozległych obszarów lub miejsc, w których powinny być zainstalowane dwie kamery mające różne pola obserwacji.

Oba moduły kamerowe są całkowicie niezależne od siebie i można w nich indywidualnie ustawić poziomy i pionowy kąt widzenia, tryb korytarzowy, strefy prywatności oraz wszystkie parametry obrazu (liczba klatek na sekundę, poziom kompresji etc.). Każdy z modułów kamerowych można wyposażyć w jeden z czterech kompatybilnych obiektywów: SLA-2M2.400D (2,4 mm), SLA-2M3600D (2,8 mm), SLA-2M2800D (3,6 mm) lub SLA-2M6000D (6 mm).

Kamera obsługuje kodeki H.265, H.264 oraz MJPEG. Maksymalna częstotliwość odświeżania to 60 kl./s. Dostępna jest funkcja WiseStream II i możliwa jest cyfrowa korekcja zniekształceń krawędziowych. Kamera może pracować w trybie dzień/noc. To wszystko w połączeniu z funkcją WDR o dynamice 150 dB gwarantuje doskonały obraz w każdych warunkach oświetleniowych.

Niewątpliwą zaletą PNM-7000VD jest pojedynczy interfejs sieciowy i jeden adres IP do obsługi obu modułów. Całość jest uzupełniona przez zestaw algorytmów analizy treści obrazów, obejmujących (dla każdego modułu indywidualnie): detekcję sabotażu, detekcję kierunkową, detekcję pyłu lub mgły, barierę wirtualną, wykrywanie wałęsania się, wykrywanie wejścia na dany obszar lub wyjścia z danego obszaru, wykrywanie pojawienia się albo znikania obiektu, detekcję twarzy oraz detekcję ruchu z filtrowaniem ruchów elementów otoczenia. PNM-7000VD ma obudowę o klasie szczelności IP66, z certyfikatem udarowym IK10.

Zaszyfrowanie plików konfiguracyjnych i plików oprogramowania układowego, a także programowana retencja danych na kartach SD (osobne dla obu modułów) czyni z kamery PNM-7000VD produkt ułatwiający klientom spełnienie wymagań RODO.

Bezpośr. inf. Piotr Rogalewski
Hanwha Techwin Europe

CENTRALE AUTOMATYKI POŻAROWEJ

www.mercor.com.pl

mercor®

Dostarczamy bezpieczeństwo

certyfikat CNBOP-PIB

niezawodna jakość

CENTRALE STERUJĄCE

CENTRALE ZASILAJĄCE

budowa modułowa

CENTRALE WYKRYWANIA POŻARU

ZASILACZE DO URZĄDZEŃ PRZECIWPOŻAROWYCH

Rejestratory sieciowe serii 6000
kompatybilne z platformą NMS

Cieszące się dużym uznaniem klientów rejestratory sieciowe **serii 6000** zostały zintegrowane z platformą **NMS** (Novus Management System) – profesjonalnym rozwiązaniem przeznaczonym do dozoru wizyjnego.

Opisywane rejestratory to już kolejna seria urządzeń, po rejestratorach hybrydowych AHD marki NOVUS, wykorzystująca rozbudowany graficzny interfejs użytkownika platformy NMS. Czyni to aplikację NMS wszechstronnym narzędziem do budowy rozległych systemów monitorowania wizyjnego, dodatkowo łączącym różne standardy sygnału wizyjnego (AHD i inne). Wszechstronność rozwiązania NMS wynika m.in. z możliwości obserwacji obrazów na sześciu monitorach w maksymalnym podziale 6x6. Umożliwia to dowolne zobrazowanie strumieni wizyjnych, czego inne sieciowe rejestratory nie gwarantują.

Rejestratory są odnajdywane w sieci lokalnej za pomocą wbudowanej wyszukiwarki i automatycznie dodawane do systemu. Nie ma limitu liczby podłączonych urządzeń. Jedyne ograniczenia mogą wynikać z ogólnej wydajności sprzętowej oraz sieciowej infrastruktury.

NMS wykorzystuje mechanizm przełączania strumieni wizyjnych w zależności od tego, czy obrazy z kamer są wyświetlane w podziale czy na pełnym ekranie. Dotyczy to zarówno bieżących obrazów z kamer, jak i obrazów z zapisanego materiału wizyjnego. Rejestracja strumieni wizyjnych może być dokonywana zarówno w rejestratorze, jak i w aplikacji NMS, co daje możliwość redundantnego gromadzenia nagrań.

Rejestratory kolejnych generacji, w tym rejestratory sieciowe z planowanej serii 2000, również zostaną zintegrowane z platformą NMS.

Bezpośr. inf. Patryk Gańko
AAT Holding

NOVUS

3000 SERIA IP • 6000 SERIA IP

NOVUS IP NMS Compatible ONVIF

SKUTECZNE ROZPOZNAWANIE TWARZY

W REJESTRATORACH SERII 6000 W POŁĄCZENIU Z KAMERAMI SERII 3000

AAT HOLDING S.A.

PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA

www.aat.pl

Wandaloodporna kamera szybkoobrotowa IP marki NOVUS

Klasa wandaloodporności kamery **NVIP-3DN3630SD/IRH-2** to **IK10**. Ta wandaloodporność dotyczy nie tylko korpusu kamery i uchwytu, ale również głowicy uchylno-obrotowej z poliwęglanowym zabezpieczeniem modułu kamerowego oraz wbudowanego promiennika podczerwieni.

Zastosowana matryca CMOS Sony Exmor R Starvis o rozdzielczości 3 Mpx w połączeniu z trzydziestokrotnym obiektywem o ogniskowej regulowanej w zakresie 4,5–135 mm umożliwia efektywną obserwację rozległych obszarów i rozpoznawanie drobnych szczegółów sceny.

Kamera generuje wysokiej jakości obraz nawet w złych warunkach oświetleniowych dzięki zastosowaniu przetworników Sony Exmor R Starvis, potocznie określanych mianem *Starlight*.

Uzupełnieniem wysokoczułej matrycy CMOS jest wbudowany promiennik podczerwieni o zasięgu 180 m, który składa się z dziesięciu diod LED o dużej mocy, podzielonych na sekcje. Kąt świecenia dynamicznie się zmienia w zależności od aktualnej długości ogniskowej obiektywu.

Kamera została wyposażona w gniazdo dla karty microSD o pojemności do 128 GB. Na karcie może być dokonywany zapis ciągły oraz alarmowy, inicjowany przez inteligentne funkcje analizy treści obrazu, lub zapis pojedynczych obrazów, w przypadku którego określony jest interwał czasowy. Aktywacja wybranego wejścia alarmowego (jednego z siedmiu dostępnych, typu NO/NC) również może skutkować lokalnym zapisem obrazu na karcie SD.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Obsługa pokoju hotelowego
w systemie RACS 5

W ramach systemu **RACS 5** wprowadzono do oferty specjalistyczny kontroler dostępu **MC16-HRC** przeznaczony do obsługi pokojów hotelowych. Kontroler ten jest odmianą standardowego kontrolera dostępu MC16-PAC, w której dostępne są dodatkowe funkcje przeznaczone do sygnalizacji typowych życzeń gościa hotelowego oraz do sterowania automatyką pokoju. Pokój hotelowy jest obsługiwany przez kontroler we współpracy z czytnikiem korytarzowym (MCT82M-IO-HR), kieszenią na kartę (MCT82M-IO-CH) oraz dotykowymi panelami funkcyjnymi (MCT82-FK-HR). System pozwala na sterowanie i umożliwia gościowi hotelowemu zamawianie usług lub sygnalizowanie typowych życzeń, np. zamówienie jedzenia, prośbę o pomoc w przeniesieniu bagażu, prośbę o posprzątanie, wezwanie pomocy, wezwanie obsługi oraz sygnalizację komunikatu „nie przeszkadzać". Sygnalizacja usług hotelowych oraz stanów automatyki może być na bieżąco monitorowana z poziomu programu zarządzającego VISO. Czytnik korytarzowy ma cztery wskaźniki LED przeznaczone do sygnalizacji wybranych zamówień usług hotelowych oraz przycisk dzwonka. System rozpoznaje numer karty włożonej do kieszeni i – w zależności od uprawnień – włącza dopływ prądu w pokoju, uruchamia określone urządzenia i umożliwia wybrane usługi. Przyciski funkcyjne na panelach dotykowych są zwykle wykorzystywane do sterowania oświetleniem, w tym scenami świetlnymi, oraz do sterowania sygnalizacją hotelową. Kontroler MC16-HRC jest oferowany w czterech wersjach, które umożliwiają obsługę od jednego do czterech pokojów. Terminale serii MCT przeznaczone do instalacji w pokojach są również dostępne w wersji podtynkowej ze szklanym panelem frontowym, która jest estetyczna i bardzo trwała. Ze względu na wymagania dotyczące bezpieczeństwa urządzenia systemu RACS 5 wykorzystywane w hotelach są oferowane wyłącznie w wersji z obsługą szyfrowanych sektorów pamięci kart MIFARE.

Bezpośr. inf. ROGER

Kamery Full Color firmy Dahua Technology

kolorowy obraz całodobowo i całotygodniowo

Dahua Technology, czołowy producent systemów dozoru wizyjnego, oferuje nowe kamery do monitoringu miejskiego, które charakteryzują się bardzo wysoką światłoczułością.

Kamery z serii **Full Color** zostały wyposażone w przetworniki Sony Starvis o wysokiej czułości, dzięki którym możliwe jest śledzenie obiektów przy słabym oświetleniu. Przetwornik zapewnia bardzo dobrą jakość obrazu w zakresie widzialnym i w bliskiej podczerwieni. Wysoka czułość oraz niski poziom szumów umożliwiają całodobową rejestrację kolorowego obrazu. W połączeniu z ulepszonymi kolorowymi filtrami mozaikowymi RGB zapewniają bardzo dobre odwzorowanie kolorów bez konieczności dalszego przetwarzania.

Przysłona obiektywu F1.0 umożliwia czterokrotnie lepsze wykorzystanie dostępnego światła niż w konwencjonalnych kamerach z obiektywami o przysłonie F2.0, a nowy układ soczewek lepiej redukuje aberrację chromatyczną, która również ma wpływ na ostrość obrazu.

Kamery HDCVI:

HAC-HFW2249T-I8-A

HAC-HFW2249E-A

HAC-HDW2249T-A

Fot. Rodzina kamer Full Color firmy Dahua Technology

Kamery IP:

IPC-HFW4239T-ASE

IPC-HDBW4239R-ASE

Fot. Rodzina kamer Full Color firmy Dahua Technology

Kamery Full Color nie mają podświetlaczy pracujących w podczerwieni, dlatego są przeznaczone do zastosowania przede wszystkim tam, gdzie już są zewnętrzne źródła światła, czyli w muzeach, barach, kasynach, na ulicach itp. Dzięki brakowi promienników IR kamery są dużo mniej dostrzegalne dla obserwowanych osób. Pobór mocy takiej kamery wynosi tylko 4 W – ponad dwa razy mniej niż w kamerach z oświetlaczami.

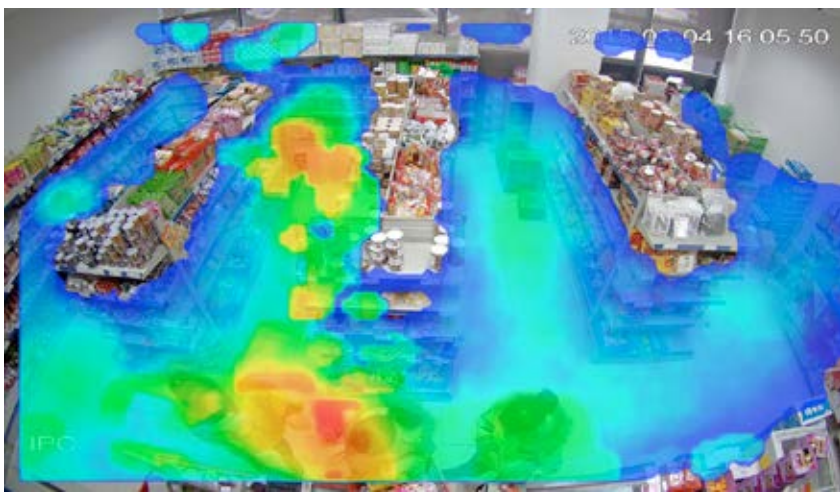
W ofercie firmy Dahua Technology są zarówno analogowe, jak i sieciowe kamery z serii Full Color. Wszystkie wytwarzają kolorowy obraz o jakości Full HD w trybie ciągłym, a wersje analogowe także kodują ścieżkę dźwiękową z wykorzystaniem sygnału z wbudowanego mikrofonu. Kamery sieciowe są wyposażone w gniazdo kart SD, a dzięki zasilaniu metodą ePoE dane można przesyłać na dystans nawet 800 m.

Bezpośr. inf. Ewelina Pułka
Dahua Technology Poland
Opracowanie: Redakcja

Kamera firmy Dahua Technology
z funkcją liczenia osób

Jakość obrazów z kamer IP jest coraz lepsza i mają one coraz więcej funkcji, takich jak zaawansowana analiza obrazu. W związku z tym nie tylko spełniają swoją podstawową funkcję, jaką jest dozór wizyjny, ale również odgrywają coraz ważniejszą rolę w działaniach marketingowych, np. w sklepach. Funkcją niezwykle pożądaną przez działy marketingu w obiektach handlowych jest zliczanie klientów. Z myślą o tym firma **Dahua Technology**, czołowy dostawca zabezpieczeń technicznych, opracowała kamerę **IPC-HDW8341X-3D**.

Kamera została wyposażona w dwa obiektywy ustawione pod różnymi kątami w celu analizowania obrazu w trzech wymiarach. Dzięki temu unikamy problemów związanych z dwuwymiarowym analizowaniem obiektów przez kamery konwencjonalne. Częstym problemem kamer z funkcją analizy dwuwymiarowej było błędne zliczanie osób, które znajdowały się blisko siebie – osoby te mogły zostać potraktowane jako jeden obiekt. Kamery firmy Dahua bez problemu separują obiekty, które znajdują się blisko siebie. Jednym słowem – tłum nie jest im straszny. Kamera IPC-HDW8341X-3D ma dwa przetworniki Starlight o rozdzielczości 3 Mpx, dzięki czemu uzyskuje lepszą światłoczułość. Dzięki funkcjom BLC i WDR z łatwością dostosowuje się do lokalnych warunków oświetleniowych. Refleksy i cienie, które mogą być skutkiem złego oświetlenia lub próby oślepienia kamery za pomocą latarki, zostają zniwelowane, aby obraz był jak najlepszej jakości. W kamerze IPC-HDW8341X-3D liczenie osób



następuje dopiero po przekroczeniu strefy i jej opuszczeniu. Zwiększono tym samym wiarygodność otrzymywanych wyników. Dzięki możliwości zliczania osób w danej strefie kamera znajdzie zastosowanie w sklepach. Zaalarmuje nas np. wtedy, gdy liczba osób w kolejce przekroczy określoną wartość. Dostaniemy informację o tym, że trzeba uruchomić dodatkową kasę. Funkcje map ciepła pomogą śledzić kupujących i dostosować dane dotyczące strategii sprzedaży zgodnie z preferencjami klientów.

Kamera daje także możliwość generowania raportów. Możemy automatycznie uzyskać wykresy i wyeksportować je w formacie BMP lub CSV.

Aby w pełni wykorzystać możliwości kamery IPC-HDW8341X-3D firmy Dahua Technology, należy ją zamontować na wysokości od 2,2 m do 5 m. Kamera powinna być zawieszona centralnie nad obserwowanym obszarem.

Bezpośr. inf.
Agnieszka Gołędowska
Dahua Technology Poland
Opracowanie: Redakcja

Ochrona przeciwpożarowa modernizowanych obszarów
za pomocą systemu WES

W funkcjonujących obiektach bezpieczeństwo ludzi zapewniają m.in. działające systemy przeciwpożarowe, jednak wiele z nich jest modernizowanych lub rozbudowywanych. Dotyczy to na przykład centrów handlowych. Zmiany mogą być przeprowadzane po to, by nadążyć za konkurencją, przyciągnąć więcej klientów dzięki zmianie aranżacji wnętrz lub zwiększenia powierzchni sprzedażowej. Modernizacje mogą być przeprowadzane bez przerywania funkcjonowania obiektów, ale zastosowane w nich systemy nie pracują wówczas zgodnie z założonymi dla nich scenariuszami. Możliwe jest też czasowe wyłączenie systemu ochrony przeciwpożarowej na czas modernizacji. W takich przypadkach można skorzystać z mobilnego systemu detekcji pożarowej WES.

W ostatnim czasie firma **Geo-Kat** we współpracy z firmą **GardaTech** postanowiła sprawdzić możliwości systemów **WES+** oraz **WES³** w istniejących obiektach, jeszcze przed planowanymi modernizacjami.

– Zauważyliśmy, że w zabezpieczeniach przeciwpożarowych istniejących obiektów występuje poważna luka. Na etapie projektowym opracowywane są scenariusze pożarowe, warianty alarmowania i ewakuacji uzależnione od miejsca wykrycia pożaru. Te założenia mają sens jedynie do pierwszej przebudowy, rozbudowy lub modernizacji. Najbardziej zagrożona przestrzeń jest pozbawiana ochrony, zanim jeszcze zaczną się poważ-

ne roboty budowlane. Demontuje się dźwiękowe systemy ostrzegawcze, system sygnalizacji alarmów pożarowych, często opróżniona zostaje sekcja tryskaczowa lub jej fragment. W takiej przestrzeni rozpoczną się roboty budowlane, w tym prace niebezpieczne pod względem pożarowym. Tymczasem za prowizorycznym wydzieleniem z folii ludzie będą zostawiać swoje dzieci w kinie, robić zakupy, przekonani, że wszystko działa, że są bezpieczni. A nie są! Systemy bezpieczeństwa w najbardziej zagrożonym obszarze właśnie zostały świadomie wyłączone. Cała misterna koncepcja bezpieczeństwa pożarowego obiektu właśnie runęła, dlatego tak ważne było dla nas sprawdzenie możliwości zastosowania systemu WES w istniejących centrach handlowych. Próby zakończyły się pełnym sukcesem. Za pomocą kilku urządzeń udaje się objąć ochroną najdalsze miejsca w centrach handlowych o powierzchni kilkudziesięciu tysięcy metrów kwadratowych. Kolejne próby GardaTech i Geo-Kat zamierzają przeprowadzić w szpitalach. W wyniku już przeprowadzonych prób potwierdzamy: to jest system, który zapewnia bezpieczeństwo ludziom w funkcjonujących obiektach w trakcie przebudowy – powiedział Kamil Ciszewski z firmy GardaTech.

Jeżeli chcesz bezpiecznie przeprowadzić modernizację swojego obiektu, powinieneś skorzystać z dodatkowej ochrony, jaką może zapewnić system WES.

Marcin Malinowski
Geo-Kat
info@wesfire.com.pl
Opracowanie: Redakcja

Potwierdzanie tożsamości w systemie RACS5
za pomocą urządzeń mobilnych

Poza standardowymi metodami potwierdzania swojej tożsamości, takimi jak użycie karty zbliżeniowej oraz kodu PIN, system **RACS 5** umożliwia użytkownikom wykorzystanie w tym celu urządzeń mobilnych (smartfonów lub tabletu). W przypadku tej formy identyfikacji kod identyfikatora może być przekazany do czytnika za pośrednictwem NFC, Bluetooth LE (BLE) lub sczytany z ekranu urządzenia przenośnego (na ekranie wyświetlony zostaje kod QR). Logowanie z wykorzystaniem NFC oraz QR wymaga zbliżenia urządzenia mobilnego do czytnika na odległość kilku centymetrów. W przypadku korzystania z BLE urządzenie mobilne może znajdować się w odległości nawet do kilku metrów od czytnika, co umożliwia wykorzystanie tej formy identyfikacji do obsługi wjazdów na parkingi i bram – nie trzeba zbliżać identyfikatora do czytnika. Kod identyfikatora mobilnego jest przechowywany w urządzeniu mobilnym w postaci tzw. klucza elektronicznego REK (Roger Electronic Key). Klucz REK to zaszyfrowany plik zawierający kod identyfikatora użytkownika, a także dodatkowe informacje określające warunki wykorzystania klucza. Taki klucz można utworzyć lokalnie – w aplikacji mobilnej RMK (Roger Mobile Key) – lub otrzymać od administratora systemu RACS 5 – w tym przypadku jest przesyłany drogą elektroniczną. Użytkownik może posiadać wiele kluczy REK i używać ich, w zależności od potrzeb, do logowania się na różnych przejściach lub w różnych punktach rejestracji RCP. Identyfikacja mobilna może być stosowana jako uzupełnienie tradycyjnych metod logowania się z użyciem karty zbliżeniowej lub PIN-u albo zastępować te metody. Aplikacja RMK jest dostępna w wersjach dostosowanych do systemów Android oraz iOS. Obecnie logowanie się z wykorzystaniem urządzeń mobilnych jest możliwe na terminalu MD70 (QR, BLE) oraz na terminalach MCT88M-IO i MCT80M-BLE (NFC, BLE).

Bezpośr. inf. ROGER

15 lecie
Kongresu Pożarnictwa
podsumowanie

26 lipca 2018 r. na PGE Narodowym w Warszawie odbył się Kongres Pożarnictwa „**Fire Security Expo 2018**". Firma **DND Project**, która jest organizatorem od 15 lat, po raz kolejny udowodniła, że warto przeznaczyć jeden dzień wakacji na branżowe spotkanie. W tegorocznym kongresie wzięło udział prawie 1000 uczestników.

Kongresowi towarzyszyły wystawy Fire Expo 2018 i Security Expo 2018, w których wzięło udział 59 firm.

Organizatorzy zaprosili do współpracy wielu ekspertów, rzeczoznawców ds. zabezpieczeń przeciwpożarowych, przedstawicieli uczelni z całego kraju (m.in. ze Szkoły Głównej Służby Pożarniczej, z Politechniki Warszawskiej, Politechniki Poznańskiej, Politechniki Łódzkiej, Politechniki Wrocławskiej, z Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej – Państwowego Instytutu Badawczego im. Józefa Tuliszkowskiego, ze Stowarzyszenia Wykonawców Dachów Płaskich i Fasad DAFA, z Instytutu Bezpieczeństwa Pożarowego NODEX, BSI Group Polska i z wielu innych branżowych instytucji, dzięki którym powstał bardzo bogaty w treść program.

W tym roku kongres był podzielony na cztery panele tematyczne. Pierwszy z nich był poświęcony aspektom projektowania

systemów przeciwpożarowych. W drugim poruszono zagadnienia integracji i współdziałania systemów bezpieczeństwa budynków, kontroli nad rozprzestrzenianiem się pożaru, bezpieczeństwa instalacji i certyfikacji systemów wykrywania pożarów. W kolejnym panelu mówiono m.in. o strategiach ochrony przeciwpożarowej, bezpieczeństwie pożarowym hal i magazynów oraz o Building Information Modelling (BIM). W ostatnim odbyła się debata ekspertów, podczas której dyskutowano na temat „nowych warunków technicznych ochrony przeciwpożarowej budynków" – rok po nowelizacji przepisów.

Podczas kongresu odbyły się również warsztaty pożarowe zorganizowane przez firmy POLON-ALFA i Bosch oraz Szkołę Główną Służby Pożarniczej. Na warsztatach omówiono dobre praktyki w zarządzaniu bezpieczeństwem pożarowym.

Kongres Pożarnictwa od 15 lat cieszy się uznaniem w branży. W trakcie tegorocznej edycji poza prelekcjami i warsztatami odbyły się również liczne pokazy, testy produktów oraz konsultacje.

Uczestnicy kongresu wybrali dwie firmy, które otrzymały nagrody za najlepszą prezentację i najlepsze stoisko:
- GAZEX (statuetka za najlepszą prezentację na Kongresie Pożarnictwa „Fire Security Expo 2018"),
- SMAY (statuetka za najlepsze stoisko na Kongresie Pożarnictwa „Fire Security Expo 2018").

Przyznano również statuetki za innowacyjne technologie i rozwiązania techniczne w dziedzinie ochrony przeciwpożarowej. Otrzymały je następujące firmy:
- Blachy Pruszyński – za lekkie ściany osłonowe na bazie kaset stalowych (nagroda Fire Product Award Expo 2018),
- APC by Schneider Electric – za zasilacz Easy UPS 3S do zasilania systemów o znaczeniu krytycznym (nagroda Security Product Award Expo 2018).

Z okazji 15-lecia Kongresu Pożarnictwa przyznano:

– nagrodę specjalną Fire Safety Education Leader 2018 dla Szkoły Głównej Służby Pożarniczej za działalność w zakresie kształcenia kadry oficerskiej dla potrzeb dynamicznego rozwoju ochrony przeciwpożarowej i bezpieczeństwa cywilnego,

– nagrodę specjalną Fire Safety Leader 2018 dla CNBOP-PIB za działalność w zakresie badań i certyfikacji na rzecz rozwoju bezpieczeństwa pożarowego, ochrony pracy i ratownictwa.

Na zakończenie kongresu odbyło się losowanie nagród dla uczestników.

Bezpośr. inf. Ewa Dziatkowska, DND Project

Firmie DND Project bardzo dziękujemy za zaproszenie i możliwość uczestnictwa w kolejnej edycji Kongresu Pożarnictwa. Życzymy wielu sukcesów, pomyślności i wytrwałości w organizowaniu kolejnych branżowych wydarzeń.

Redakcja

Agencje ochrony wybierają systemy alarmowe pracujące w chmurze

Daniel Kamiński

Najwięksi gracze w branży usług monitorowania alarmów uważają, że do 2025 roku w Stanach Zjednoczonych tradycyjne systemy alarmowe zostaną wyparte przez rozwiązania, w których wykorzystuje się chmurę. Kiedy nastąpi to w Polsce? Z doświadczenia mogę powiedzieć, że 5–7 lat po zmianach w USA. Mamy więc 12–15 lat, żeby się do tego przygotować

Zdalny dostęp do systemów alarmowych za pomocą aplikacji mobilnych jest obecnie bardzo modny i chętnie podkreślany. Głównie dlatego, że zwiększa wygodę użytkowania systemów oraz daje poczucie kontroli nad chronionym obiektem. Dzięki nim agencje ochrony mogą obniżyć koszty eksploatacji oferowanych rozwiązań. Mogą też uzyskać wzrost przychodów dzięki uruchomieniu dodatkowych usług umożliwiających zdalne sterowanie systemami alarmowymi i zdobyć przewagę nad konkurencją. Przewiduje się, że w ciągu 12–15 lat tradycyjne systemy alarmowe zostaną zastąpione rozwiązaniami sieciowymi.

Zaskakujące wnioski wynikające z badań rynkowych

Badania rynkowe prowadzone przez firmę IHS jednoznacznie wskazują na to, że tradycyjne metody ochrony obiektów tracą na popularności. Prosta usługa polegająca na odbiorze sygnału alarmowego i wysłaniu grupy interwencyjnej jest obecnie świadczona głównie w krajach rozwijających się, np. w krajach Afryki Środkowej, w których potrzeba zapewnienia bezpieczeństwa nie jest zaspokojona. W innych krajach klienci oczekują komfortu i wygody. Z tego względu w krajach bardziej rozwiniętych, takich jak Stany Zjednoczone czy kraje Europy Zachodniej, dużo bardziej popularne są usługi mobilne oraz rozwiązania współtworzące tzw. inteligentny dom (ang. *smart home*).

Ta moda szybko zmierza również do nas i w ciągu najbliższych lat wypromuje nowe podejście do usług monitorowania. Chodzi o to, by klient miał poczucie kontroli nad własnym bezpieczeństwem, między innymi dzięki aplikacjom mobilnym służącym do nadzoru oraz zdalnego zarządzania systemami alarmowymi. Do tego potrzebne są urządzenia stale podłączone do Internetu oraz platformy pracujące w chmurze, zarządzające komunikacją z systemami alarmowymi, aplikacjami mobilnymi oraz programem do obsługi alarmów w centrum monitorowania.

Zdalny dostęp do systemów alarmowych podłączonych do Internetu

Wspomniane prognozy potwierdzają wpływ światowego trendu, który bywa określany mianem *connected life* i który przewiduje znaczący wpływ usług sieciowych i wzrostu dostępności Internetu na styl życia ludzi. Tego typu trendy mają wpływ również na sposób korzystania z systemów alarmowych. Coraz więcej producentów takich systemów dostarcza urządzenia mające dostęp do Internetu. Najczęściej są to modemy 2G/3G/4G, karty sieciowe oraz moduły Wi-Fi. Systemy zyskują możliwość bycia obsługiwanymi poprzez strony WWW, aplikacje mobilne czy też programy do obsługi alarmów.

Wspomniane tendencje biorą pod uwagę również producenci tradycyjnych nadajników służących do współpracy z wcześniej zamontowanymi systemami alarmowymi. Wiedzą oni, że na rynku istnieje wiele starych systemów, które trzeba będzie zmodernizować lub wymienić. Z tego względu przygotowują uniwersalne moduły komunikacyjne umożliwiające zdalne zarządzanie tradycyjnymi systemami alarmowymi. Wraz z nadajnikiem klienci otrzymują aplikacje mobilne oraz gwarancję integracji z programami do obsługi alarmów.

Rewolucja w działach technicznych firm ochrony

Korzystanie z systemów alarmowych mających dostęp do Internetu i pracujących w chmurze będzie miało duży wpływ na sposób ich uruchamiania u klientów. Etapy wdrażania systemu:

1. Rejestracja. Już podczas wizyty u klienta odbędzie się wstępna rejestracja jego danych w module CRM w chmurze. Dane klienta zostaną wprowadzone i przekazane do właściwych działów.

2. Kompletacja. Na tym etapie wypełniony zostanie arkusz konfiguracji, w którym podaje się liczbę chronionych pomieszczeń, nazwy tych pomieszczeń, liczbę otworów okiennych oraz drzwiowych, a także inne przydatne informacje. Na tej podstawie powstanie wstępna konfiguracja, która zostanie zarejestrowana w chmurze. Podane informacje zostaną wykorzystane podczas kompletacji urządzeń.
3. Montaż. Skompletowany i wstępnie skonfigurowany system zostanie przekazany monterowi, który nie będzie musiał go programować – system będzie uruchomiony zdalnie.
4. Uruchomienie. Informacje zebrane od klienta dotyczące nazw linii, partycji, czasów na wejście itp. zostaną zdalnie załadowane po pierwszym zarejestrowaniu się urządzeń w chmurze. Przeprowadzona zostanie zdalna diagnostyka, czyli sprawdzenie, czy baterie w czujkach są naładowane, czy poziomy sygnałów są właściwe oraz czy urządzenia komunikacyjne pracują prawidłowo.
5. Monitorowanie. Na tym etapie aktywowane zostaną aplikacje klienta i obiekt zostanie objęty usługą monitorowania.

Zaproponowany scenariusz wykorzystuje zalety wbudowanego komunikatora internetowego, korzystania z chmury oraz automatycznej wymiany danych pomiędzy CRM (dane klienta), WMS (magazyn) oraz programem do obsługi alarmów.

Tego typu produkty dopiero się rozwijają, ale już teraz znacząco wpływają na obniżenie kosztów instalacji oraz uruchomienia obiektów. Dzięki nim można też ograniczyć ilość papierowych dokumentów i skrócić czas aktywacji obiektu.

Nowe usługi centrum monitorowania sposobem na zwiększenie przychodów

Wzrost cen abonamentów za monitorowanie alarmów jest spowodowany wzrostem ustawowej stawki minimalnej za godzinę pracy pracownika zajmującego się świadczeniem takiej usługi. Klientom trudno pogodzić się z podwyżkami, ponieważ w przypadku małej liczby fałszywych alarmów nie widzą działań firm, które je chronią. Co gorsza, często przestają korzystać z systemu alarmowego, chcąc uniknąć regularnych opłat.

Firmy trudniące się ochroną obiektów żalą się, że klienci nie rozumieją, iż abonament jest płacony za gotowość do interwencji w przypadku alarmu. Nie zdają sobie sprawy, że ta gotowość wynika z konieczności dysponowania całodobowym centrum monitorowania, załogami interwencyjnymi, a także z wykorzystania sieci telekomunikacyjnych do przesyłania informacji o zdarzeniach alarmowych. Przede wszystkim jednak wymaga utrzymania stałej obsady personelu w czasach, w których liczba wykwalifikowanych pracowników jest ograniczona.

Można jednak osiągnąć kompromis. Z pomocą przychodzą coraz popularniejsze rozwiązania polegające m.in. na podłączeniu systemów do Internetu, interakcji z systemami poprzez aplikacje mobilne, zwiększeniu możliwości systemów dzięki zintegrowaniu ich z urządzeniami wykorzystywanymi w inteligentnych domach.

Przede wszystkim należy doprowadzić do sytuacji, w której klient będzie chciał korzystać z systemu alarmowego i przestanie się go bać. Niezależnie od tego, czy system będzie sterowany pilotem czy za pomocą aplikacji mobilnej, trzeba z niego korzystać. Należy też zaoferować klientowi usługi, które umożliwią mu zdalne zarządzanie systemem alarmowym. Chodzi o to, by operatorzy centrum monitorowania zaczęli być traktowani jak własny personel klienta mający zdalny dostęp do jego biura, magazynu czy też domu. W uzasadnionych przypadkach będą mogli zdalnie włączać system alarmowy w dozór i wyłączać go z dozoru. Z czasem takie usługi staną się standardem, a firmy je realizujące zdominują rynek.

Kilka najprostszych przykładów to nocne dostawy leków do aptek, otwieranie i zamykanie bankomatów, gdy są zasilane gotówką, obsługa bram po godzinach pracy zakładów, weryfikacja godzin otwarcia sklepów lub punktów usługowych. W każdym z tych przypadków można wykonać usługi lokalnie, pod nadzorem pracownika ochrony, jednak poszukiwane są też alternatywne rozwiązania ze względu na wzrost kosztów ochrony. Taką alternatywą są pracownicy centrum monitorowania mający zdalny dostęp do systemów alarmowych pracujących w chmurze.

Aplikacje mobilne i opisy wdrożeń jako narzędzia sprzedażowe

Skąd klient ma wiedzieć, że centrum monitorowania obsługuje sieciowe systemy alarmowe i świadczy nowoczesne usługi zdalnego zarządzania chronionymi obiektami? Przecież każdy handlowiec może powiedzieć, że jego firma świadczy takie usługi.

Bardzo ważne jest postawienie na właściwe rozwiązania, czyli system alarmowy pracujący w chmurze, umożliwiający obsługę poprzez aplikacje mobilne oraz zintegrowany z programem do obsługi alarmów. Trzeba następnie stworzyć odpowiednią ofertę i udostępnić klientowi aplikacje mobilne, za pomocą których będzie mógł sam sterować systemem alarmowym. Już samo to działanie umożliwi zdobycie przewagi konkurencyjnej.

Następnie należy chwalić się opisami wdrożeń rozwiązań, które doprowadziły do obniżenia kosztów ochrony w poszczególnych firmach. Dzięki temu zbuduje się wizerunek eksperta branżowego, co pozwoli wyróżnić się na rynku. Nie trzeba się obawiać, że konkurencja skopiuje przepis na sukces. Wybór rozwiązania i integracja z programem do obsługi alarmów, a następnie przygotowanie oferty zajmie konkurencji tyle czasu, że firma wytworzy standard rynkowy i zyska przewagę.

Podsumowanie

Zaprezentowany scenariusz wymaga od firm trudniących się ochroną zmiany podejścia do systemów alarmowych oraz usług monitorowania. Wymusza też zmianę lub przebudowę programów biznesowych realizowanych w firmie, a także zdaje się potwierdzać, że nie ma ucieczki przed usługami chmurowymi. Jednocześnie wskazuje drogę, która umożliwi nie tylko utrzymanie się na rynku, ale nawet zdominowanie go. Ważne jest budowanie wizerunku eksperta poprzez opisywanie wdrożeń zakończonych sukcesem i promowanie prac nad tworzeniem branżowych standardów nowo kreowanych usług. Istotne jest informowanie klienta o korzyściach, jakie uzyska dzięki zastosowaniu zdalnego nadzoru nad technicznymi rozwiązaniami zastosowanymi w jego obiekcie. Czy jesteśmy gotowi na takie zmiany? W krajach, które były na to gotowe, model ochrony mocno się zmienił. Nie ma tam załóg interwencyjnych ani centrów monitorowania. Są za to firmy informatyczne, które udostępniają dla klientów chmurę przeznaczoną do samodzielnego monitorowania alarmów. Samodzielne zarządzanie jest akceptowalne, jeżeli interwencje są okazjonalne. Sterowaniem systemem – o różnych porach dnia i nocy – mogą zajmować się operatorzy centrów monitorowania. Uważam, że polskie firmy trudniące się ochroną mogą już teraz uruchamiać opisane usługi, szczególnie jeśli chcą przygotować się na nadchodzące zmiany.

Daniel Kamiński

Alert Control
ALARMY POD KONTROLĄ

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

Zabezpieczenia
w systemie kontroli dostępu RACS 5

Grzegorz Wensker

System RACS 5 oferuje wielopoziomowe zabezpieczenie, którego celem jest przeciwdziałanie próbom nieprzestrzegania zasad kontroli ruchu osób i wyposażenia w dozorowanym obiekcie

Na system zabezpieczeń składają się trzy główne elementy:
- identyfikatory zabezpieczone przed dupliko-waniem,
- szyfrowanie wszystkich rodzajów komunika-cji stosowanych w systemie,
- kontrolowany dostęp do oprogramowania zarządzającego.

Do systemu RACS 5 dostosowana jest duża grupa czytników serii MCTxxM obsługujących karty zbliżeniowe MIFARE, w tym karty typu DESFire oraz Plus oferujące wysoki stopień zabezpieczeń szyfrujących. Kod karty MIFARE może być przechowywany w szyfrowanych sektorach jej pamięci, przez co nie jest łatwe jego odczytanie i zduplikowanie nawet w przypadku uzyskania fizycznego dostępu do zasobów karty. Hasło szyfrujące, kod karty i miejsce jego przechowywania na karcie MIFARE podlegają indywidualnemu programowaniu, co powoduje, że karty z obcych systemów nie działają w danej instalacji kontroli dostępu. Opcjonalnie karty MIFARE można skonfigurować w taki sposób, że będzie możliwe ich wykorzystanie w wielu aplikacjach (systemach), ale tak długo, jak kod karty będzie przechowywany w osobnym sektorze danych i zabezpieczony tajnym hasłem, poziom bezpieczeństwa systemu kontroli dostępu nie będzie obniżony.

System RACS 5 umożliwia wykorzystanie smartfonu jako identyfikatora użytkownika. Również w tym przypadku komunikacja pomiędzy smartfonem a czytnikiem podlega szyfrowaniu, więc nie można przechwycić danych uwierzytelniających.

Kolejnym zabezpieczeniem są wieloetapowe tryby identyfikacji użytkowników, które wymuszają użycie więcej niż jednej formy identyfikacji. System umożliwia zarówno typowe tryby potwierdzania tożsamości, np. za pomocą karty i PIN-u czy karty i odcisku palca, jak i tworzenie własnych, bardziej złożonych trybów, np. trybu, w którym odczytywana jest karta, linie papilarne i wprowadzany PIN. Oferowany jest również czytnik linii papilarnych RFT1000, który przechowuje wzorce linii papilarnych w wewnętrznej pamięci lub na karcie zbliżeniowej MIFARE, którą posługuje się użytkownik.

Zastosowanie kart zbliżeniowych MIFARE w połączeniu z wielostopniowymi trybami identyfikacji tworzy bardzo skuteczną barierę, która może być dodatkowo wzmocniona funkcją „Dostęp z autoryzacją przez operatora" oraz funkcją „Wejście komisyjne". W przypadku pierwszej z nich na dostęp zezwala ostatecznie operator systemu, który powinien najpierw zidentyfikować osobę na podstawie obrazu z kamery i następnie potwierdzić dostęp. W przypadku drugiej z wymienionych funkcji dostęp jest możliwy dopiero po identyfikacji dwóch użytkowników uprawnionych do otwarcia danego przejścia.

Oprogramowanie zarządzające systemem i kontrolery dostępu komunikują się przez sieć komputerową. Połączenie jest szyfrowane metodą AES128 CBC. Metoda ta polega na szyfrowaniu za pomocą dynamicznie zmieniającego się hasła, co z jednej strony czyni przesyłane ramki nieczytelnymi, a z drugiej blokuje możliwość sterowania systemem przez ich replikację. Połączenie kontrolera dostępu z czytnikami i innymi modułami może być przewodowe (poprzez magistralę RS485, sieć komputerową), a także bezprzewodowe (radiowe). W każdym z tych przypadków jest szyfrowane i – podobnie jak połączenie z użyciem sieci LAN – zabezpieczone przed replikowaniem.

Dostęp do oprogramowania obsługującego system wymaga uwierzytelnienia hasłem. System dopuszcza obsługę przez wielu operatorów z różnymi uprawnieniami. Działania operatorów są rejestrowane w przeznaczonym do tego celu dzienniku zdarzeń, który może stanowić cenne źródło informacji w przypadku potrzeby odtworzenia przebiegu zdarzeń związanych z zarządzaniem, konfiguracją i obsługą systemu.

Uwaga!

W odróżnieniu od powszechnie spotykanych czytników kart standardu MIFARE czytniki serii PRTxxMF oraz MCTxxM (Roger) mogą odczytać zarówno nieszyfrowany kod karty (tzw. kod CSN), jak i kod szyfrowany (tzw. kod SSN). Jeżeli system kontroli dostępu wykorzystuje kod CSN karty MIFARE lub karty EM 125 KHz, istnieje ryzyko sklonowania kart, co stanowi bardzo istotne obniżenie poziomu bezpieczeństwa. W systemach, w przypadku których obniżenie poziomu bezpieczeństwa wynikające ze sklonowania kart jest zbyt duże, należy stosować czytniki odczytujące kod SSN (np. czytniki serii MCTxxM Roger)

Grzegorz Wensker
ROGER

Zabezpieczanie biura i domu wolnostojącego

Maciej Prelich

Budując dom wolnostojący, ludzie pragną przede wszystkim wolności, prywatności oraz większego komfortu niż w przypadku mieszkań, apartamentów czy nawet segmentów. Często jednak wszystkie środki przeznacza się na sam budynek i umeblowanie pomieszczeń, a całkowicie pomija się zabezpieczenia, od których może zależeć pożądany spokój. Może to wynikać z braku wiedzy o dostępnych możliwościach lub z błędnych założeń. Jednym z podstawowych zadań integratorów systemów alarmowych jest informowanie o tych możliwościach oraz pomoc w doborze odpowiedniego systemu

Niezależnie od typu posiadłości (dom letni, dom całoroczny, siedziba firmy itp.) jest wiele dostępnych rozwiązań składających się na efektywny system zabezpieczeń. Możemy je podzielić na dwie główne grupy – zabezpieczenia mechaniczne, które można nazwać systemem antywłamaniowym, takie jak ogrodzenie czy wzmocniony zamek szyfrowy, oraz zabezpieczenia elektroniczne, do których należą między innymi kamery CCTV, kamery termowizyjne oraz ochrona perymetryczna, które jedynie informują o wykryciu intruza oraz o czasie i miejscu takiego zdarzenia, ale same nie stanowią fizycznej bariery dla włamywaczy (chociaż mogą zniechęcić ich do wejścia na dany teren).

Sama wiedza o próbie wtargnięcia może wydawać się niepotrzebna, jednak wyobraźmy sobie sytuację, w której dochodzi do włamania na teren prywatnej posesji, gdzie przechowujemy nasze cenne rzeczy osobiste, biżuterię lub dokumenty, z których nie korzystamy codziennie. Jeśli znikną, dowiemy się o tym dopiero w momencie, gdy będziemy ich potrzebowali, a próba zlokalizowania lub odzyskania tych przedmiotów po dłuższym czasie będzie niemożliwa. Co więcej, jeśli nastąpi wykrycie włamania lub jego próby, będzie można wezwać pomoc, powiadomić policję lub ochronę, a dokładne określenie miejsca włamania znacznie przyspieszy neutralizację zagrożenia. Świadomość posiadania kontroli nad sytuacją, a także bycie przygotowanym na ewentualne zagrożenia daje ogromne poczucie bezpieczeństwa, tak trudno osiągalne w dzisiejszych czasach.

Aby zwiększyć bufor czasowy, np. aby dać odpowiednim służbom czas na dojazd, łączy się dwa typy systemów. Klasycznym przykładem będzie ogrodzenie, którego sforsowanie wymaga dłuższego czasu, oraz system napłotowy, który będzie informował o próbach sforsowania ogrodzenia. Fot. 1 przedstawia metalowe ogrodzenie

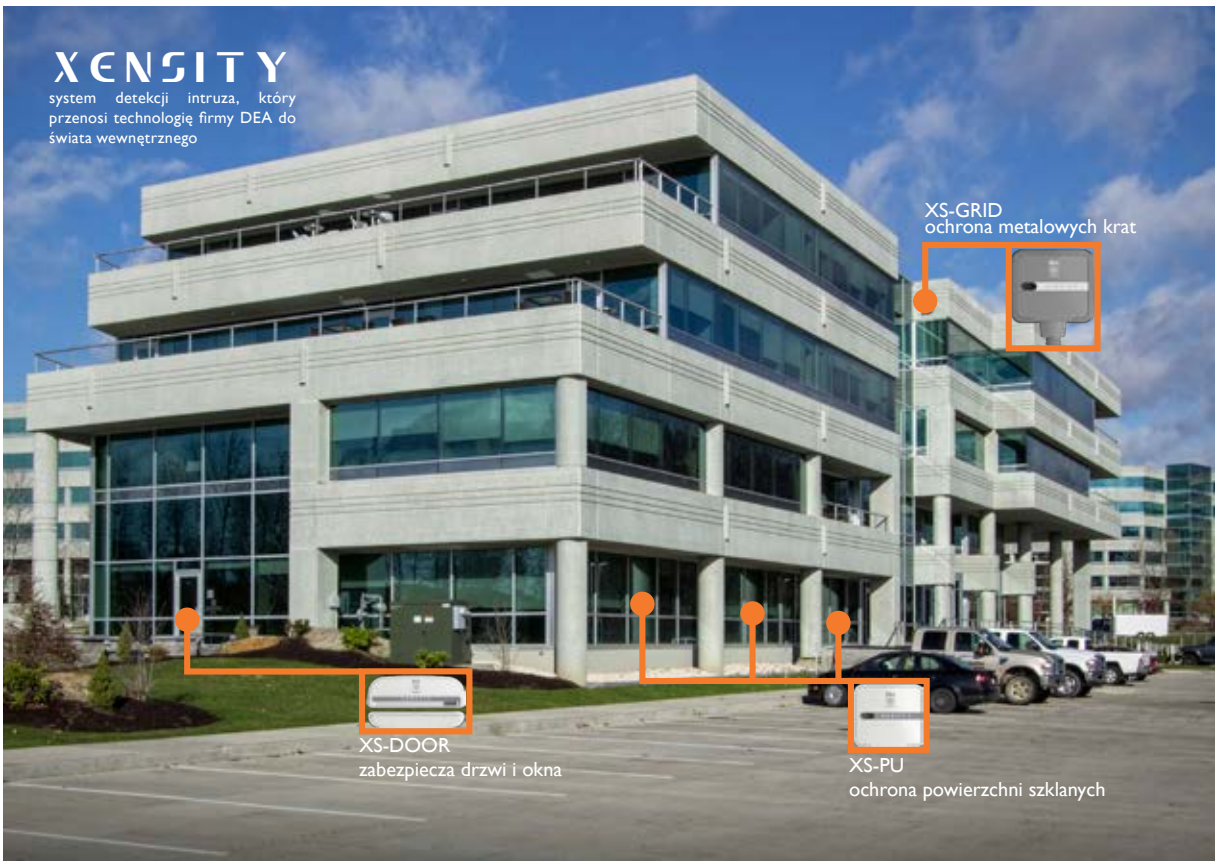
Fot. 1. System napłotowy DEA SERIR 50

wraz z kablem DEA SERIR 50. Systemy można łączyć, nawet jeśli początkowo wydają się one niepowiązane. Przykładem może być ogrodzenie oraz system zakopywanych sensorów, niewidoczny dla włamywacza. Takie rozwiązanie jest pokazane na fot. 2. Jest na nim system DEA SISMA CP.

Coraz popularniejszym rozwiązaniem dostosowanym do prywatnych posesji jest połączenie metalowego ogrodzenia, zamka szyfrowego oraz systemu elektronicznego zainstalowanego na terenie posesji, np. czujek wykrywających próbę włamania przez okno, wyłamania drzwi oraz naruszenia innych newralgicznych miejsc. Jest to rezultat zwiększającej się dostępności takich rozwiązań, jak również łatwości ich obsługi za pomocą komputera lub nawet smartfonu.

Do ochrony budynku można wykorzystać nowości zaprezentowane na tegorocznych targach SECUREX w Poznaniu, do których należą system DEA Xensity oraz czujki A03, A03 Pro i SPC/SPR. W czujkach piezodynamicznych firmy DEA zastosowano mechanizmy i algorytmy sprawdzone i przez lata wykorzystywane w systemach stosowanych przez jednostki militarne oraz przedsiębiorstwa na całym świecie (ich działanie zostało opisane w numerze 4/17 *Zabezpieczeń*). Czujki te ostrzegają o próbach sforsowania drzwi,

Fot. 2. System zakopywany DEA SISMA CP



Rys. 1. Schemat przykładowej instalacji DEA Xensity

okien, metalowych krat lub ścian wszędzie tam, gdzie zostały zainstalowane. Reagują one nawet na najmniejsze drgania, więc wykrywają nie tylko samo zbicie szyby lub wyłamanie ramy okiennej, lecz także ich nieudane próby. Wszystkie elementy są produkowane przez jedną firmę, więc wyeliminowane zostały problemy z kompatybilnością między czujkami, a dodatkowo system może być połączony z centralą alarmową obsługującą inne systemy ochrony obwodowej. Najnowsze czujki mogą również być kalibrowane i konfigurowane z poziomu smartfonu z zainstalowaną odpowiednią aplikacją. Rysunek 3 przedstawia schemat przykładowej instalacji systemu DEA Xensity.

Aby spełnić oczekiwania swoich klientów, Firma ATLine ma rozszerzony asortyment zamków szyfrowych o różnorodnych zastosowaniach, np. proste zamki mechaniczne do drzwi drewutni, małe zamki elektroniczne przeznaczone do szafek, np. w siłowniach lub w biurach, specjalne zamki przystosowane do drzwi szklanych i metalowych, specjalne, rozbudowane zamki do biur lub drzwi frontowych, które mogą być obsługiwane przez 350 użytkowników i umożliwiają dostęp za pomocą kodu, specjalnych kart, bransoletek zbliżeniowych lub telefonu. Dokładny opis zamków szyfrowych znajduje się w numerze 2/18 *Zabezpieczeń*.

Oferujemy wiele różnych rozwiązań, dlatego klienci mogą wybrać takie, które odpowiada im najbardziej, również ze względu na cenę. Systemy z naszej oferty ograniczają do minimum liczbę fałszywych alarmów. Od ponad 25 lat działalności Firma ATLine instaluje systemy zabezpieczeń w przeróżnych obiektach prywatnych, wojskowych oraz przemysłowych. Ciągle udoskonala oferowane zabezpieczenia i uwzględnia przy tym wymagania i preferencje użytkowników. Jej misją niezmiennie jest dbanie o pełną satysfakcję klientów. Każdy zainstalowany system ma zapewnić bezpieczeństwo i spokój.

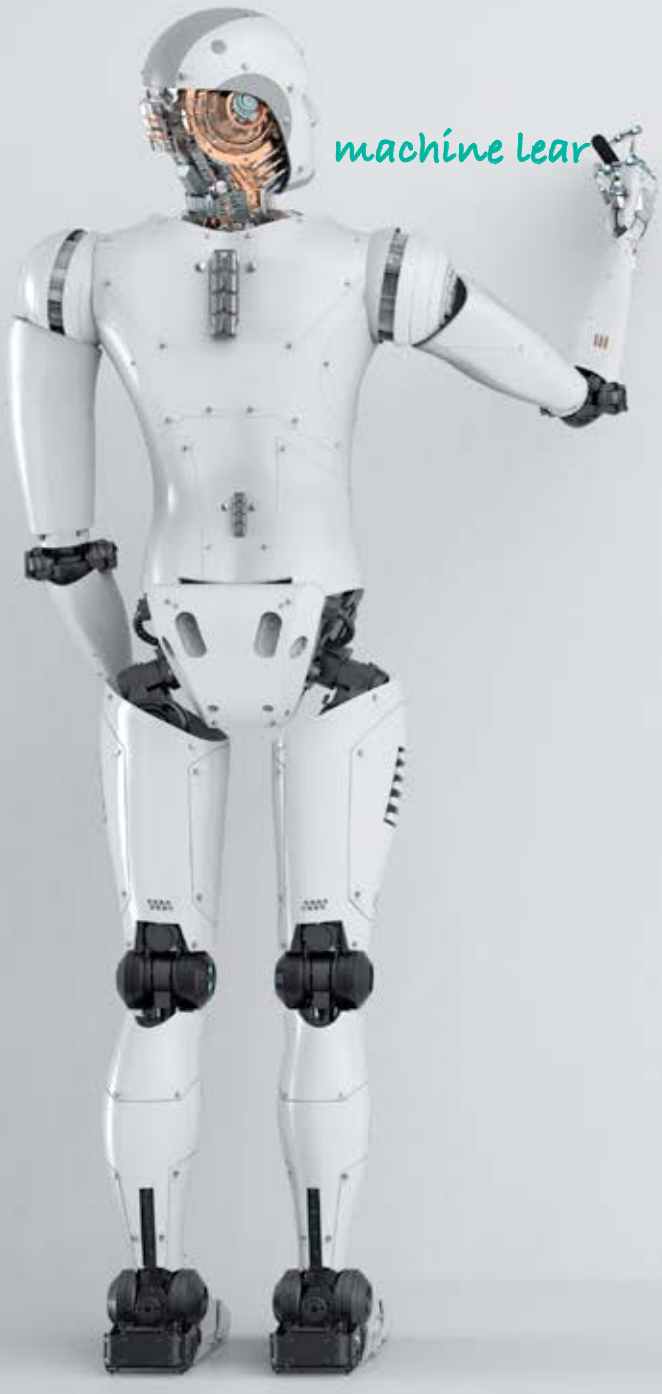
Maciej Prelich
Firma ATLine sp.j. Sławomir Pruski
mprelich@atline.pl

Nowe rozwiązania w ochronie ogrodzeń i granic

dzięki zaawansowanej analizie obrazu

John Merlino

Istotą ochrony ogrodzenia nie jest zastosowanie systemu dozoru wizyjnego, lecz dostarczenie obrazu, który umożliwi trafną ocenę sytuacji



Znaczna część obrazu zapisanego bądź obrazu transmitowanego na żywo nigdy nie zostanie obejrzana przez operatora. Dlaczego? Duża liczba kamer sieciowych – na przykład dla instalacji wykorzystywanych przez Ministerstwo Obrony czy agencje krajowe – wytwarza wiele obrazów w trybie ciągłym, dlatego prześledzenie całego zgromadzonego materiału wizyjnego jest praktycznie niewykonalne. Jest on po prostu zbyt obszerny.

Analiza obrazu, sztuczna inteligencja i uczenie się przez systemy (ang. *machine learning*) umożliwia wydobycie użytecznych informacji z ich ogromnego zasobu i podjęcie właściwych działań na ich podstawie.

W zapisie poddanym analizie zachowywane są jedynie odpowiednio przefiltrowane fragmenty nagrań. Aplikacje wykorzystujące sztuczną inteligencję i *machine learning* umożliwiają dodawanie do materiału wizyjnego metadanych i takie ich przetwarzanie, by stanowiły one funkcjonalne narzędzia w zastosowaniach publicznych i prywatnych. Każde z tych narzędzi przyczynia się do wykorzystania obrazu w ochronie obwodowej w sposób coraz bardziej zaawansowany.

Zdefiniujmy sztuczną inteligencję i uczenie się przez maszyny lub systemy. Sztuczna inteligencja to inteligentne wykonywanie przez komputery zadań, które z reguły są realizowane przez ludzi. Uczenie się przez maszynę lub system jest czymś jeszcze bardziej zaawansowanym. Jest ono związane z takim zastosowaniem sztucznej inteligencji, które umożliwia komputerom analizę danych oraz uczenie się w najlepszy możliwy sposób. Automatyzuje ono proces tworzenia modelu analitycznego – komputer ustala optymalne rozwiązanie bez potrzeby zmian w jego funkcjonowaniu. Wszystko to przekłada się na dozór wizyjny, w szczególności w przypadkach, w których ochroną obwodową objęte są rozległe obszary. Oprogramowanie nie tylko jest w stanie wyodrębnić różne rodzaje obrazu, ale także umożliwia przeglądanie wszystkich danych wizyjnych w celu dokonania wyboru materiału do dalszej analizy na podstawie danych fizycznych, detekcji ruchu, zachowania obiektów i innych kryteriów.

Do inteligentnej analizy obrazu zaliczamy analizę każdego z pikseli z osobna. Jest to podstawowa funkcja wykorzystywana w przypadku pogorszenia jakości obrazu, spowodowanego np. sabotażem sprzętowym. W przypadku wykrycia ruchu na obrazie wywoływany jest alarm. Inną funkcją jest rozpoznawanie obiektów (znacznie bardziej zaawansowana funkcja; możliwe jest rozpoznawanie określonych rodzajów obiektów, np. samochodów, ludzi, drzew czy budynków, a także śledzenie obiektów ruchomych), a także analiza obrazu i rozpoznawanie obiektów pod kątem specjalistycznych zastosowań (np. rozpoznawanie tablic rejestracyjnych, rozpoznawanie twarzy czy wykrywanie pożaru).

Omówione narzędzia analityczne mają szereg zastosowań w systemach ochrony obwodowej. Służą np. do wykrywania przekroczenia linii. Aplikacja może zasygnalizować przekroczenie umownej linii tworzącej wirtualne ogrodzenie. Możliwe jest określenie reakcji na jej przekroczenie. Reakcją może być alarm. Po wykryciu ruchu na określonym terenie może zostać włączona rejestracja obrazu. Możliwe jest też wykrycie porzuconego obiektu, czyli ruchomego obiektu, który pozostaje przez pewien czas w polu widzenia kamery i który może być niebezpieczny dla otoczenia lub zawierać informacje, które nie powinny zostać upublicznione. Czas przebywania osób na danym terenie może być rejestrowany. Po wykryciu podejrzanego zachowania na obrazie chronionego obszaru ukazuje się miejsce zaobserwowanego incydentu i podany jest jego dokładny czas. Ponadto zostaje podjęta próba identyfikacji osób.

Gdy personel uzyska informację o nietypowym zdarzeniu, inteligentna analiza treści obrazu umożliwi rozpoznanie potencjalnego zagrożenia, o ile nadal będzie ono występować, i szybką, adekwatną reakcję.

Innym zastosowaniem inteligentnej analizy treści obrazu jest zapobieganie nielegalnemu przekraczaniu granic. Możliwa jest detekcja intruzów na kilku poziomach. Powszechnie stosowane są kamery termowizyjne. Analiza obrazu termicznego uzupełniona danymi z radarów naziemnych i innych detektorów, a także informacjami uzyskanymi dzięki analizie treści obrazów z kamer pracujących w świetle widzialnym pozwala na określenie poziomu zagrożenia oraz podjęcie odpowiednich działań.

Dwa kolejne środki bezpieczeństwa, których znaczenie w ochronie obszarów i granic ciągle wzrasta, to funkcje rozpoznawanie twarzy oraz funkcje odczytu danych z tablic rejestracyjnych samochodów. Zastosowanie funkcji rozpoznawania twarzy ma duży potencjał mogący zrewolucjonizować wiele systemów ochrony granic i ochrony perymetrycznej. Możliwa staje się szybka identyfikacja podejrzanych osób, w tym osób objętych zakazem wstępu na określony teren. Oba rodzaje analizy będą niezwykle przydatne w przyszłych zastosowaniach sztucznej inteligencji, *machine learning* oraz *deep learning*, ponieważ dostarczają dokładnych metadanych.

Fot. Analiza obrazu odgrywa i będzie odgrywać kluczową rolę w ochronie granic i w ochronie obwodowej

John Merlino
Axis Communications
Opracowanie: Redakcja

NOVUS®

3000 SERIA IP • 6000 SERIA IP

IDEALNE DOPASOWANIE

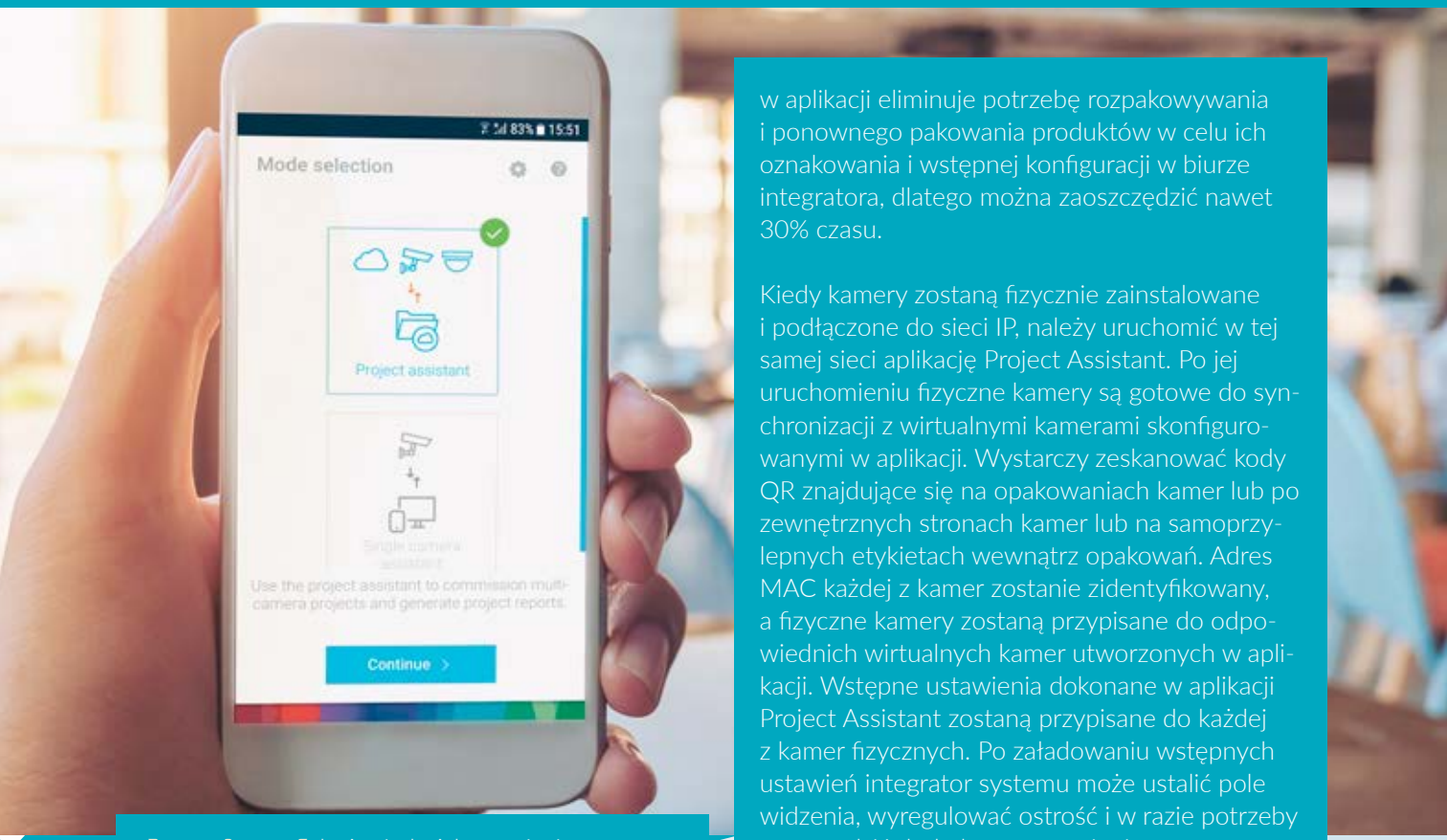
KAMERY IP SERII 3000 TYPU „RYBIE OKO” I REJESTRATORY SERII 6000

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

Nowy sposób inteligentnego planowania,
który zwiększa wydajność podczas realizacji projektów

Bosch Building Technologies

Bosch Building Technologies wprowadza na rynek aplikację Project Assistant – inteligentne rozwiązanie, które ma ułatwić pracę integratorom systemów i instalatorom. Dotychczas planowanie, konfiguracja, instalacja i raportowanie projektów systemów telewizji dozorowej wymagało zastosowania wielu różnych narzędzi oraz włożenia wielu godzin pracy w dokończenie i udokumentowanie procesu, przez co integratorom systemów było trudno zarządzać równocześnie kilkoma projektami, aż do stworzenia finalnego raportu. Dzięki aplikacji Project Assistant możliwe jest zapewnienie przejrzystości i wydajności kontroli na każdym etapie projektu systemu dozoru wizyjnego



Wdrażanie każdego wizyjnego systemu dozorowego obejmuje ustalanie haseł dla kamer, przydzielanie adresów IP, wstępne ustawianie kamer, instalację i konfigurację systemu oraz przedstawienie klientowi końcowemu dokumentacji powykonawczej. W związku z tak dużą liczbą zadań naturalne jest to, że – pomimo najlepszych intencji – mogą pojawić się błędy, wady czy utrudnienia w komunikacji, które wydłużają czas pracy i zwiększają koszty projektu.

Pojawienie się na rynku aplikacji Project Assistant ma zatem istotne znaczenie. Integrator może rozpocząć pracę nad projektem i wstępną konfigurację (uruchomienie) już w biurze. Będąc w posiadaniu jedynie planów, kompletu adresów IP i otrzymanych od klienta haseł, może stworzyć nowy projekt, wprowadzając wszystkie dane do aplikacji lub dodając je zbiorczo w postaci pliku programu Excel. Można wprowadzić hasło i adres IP osobno dla każdej z kamer lub – za pomocą aplikacji – ustawić hasło i zakres adresów IP dla całego systemu. Aplikacja Project Assistant automatycznie wprowadza informacje dla każdej z kamer, co pozwala zaoszczędzić czas. Pozostałe informacje także można dodać w aplikacji – nie jest potrzebna fizyczna obecność kamer (np. można podać nazwę kamery i określić jej lokalizację). Utworzenie zestawu wirtualnych kamer w aplikacji eliminuje potrzebę rozpakowywania i ponownego pakowania produktów w celu ich oznakowania i wstępnej konfiguracji w biurze integratora, dlatego można zaoszczędzić nawet 30% czasu.

Kiedy kamery zostaną fizycznie zainstalowane i podłączone do sieci IP, należy uruchomić w tej samej sieci aplikację Project Assistant. Po jej uruchomieniu fizyczne kamery są gotowe do synchronizacji z wirtualnymi kamerami skonfigurowanymi w aplikacji. Wystarczy zeskanować kody QR znajdujące się na opakowaniach kamer lub po zewnętrznych stronach kamer lub na samoprzylepnych etykietach wewnątrz opakowań. Adres MAC każdej z kamer zostanie zidentyfikowany, a fizyczne kamery zostaną przypisane do odpowiednich wirtualnych kamer utworzonych w aplikacji. Wstępne ustawienia dokonane w aplikacji Project Assistant zostaną przypisane do każdej z kamer fizycznych. Po załadowaniu wstępnych ustawień integrator systemu może ustalić pole widzenia, wyregulować ostrość i w razie potrzeby wprowadzić dodatkowe ustawienia.

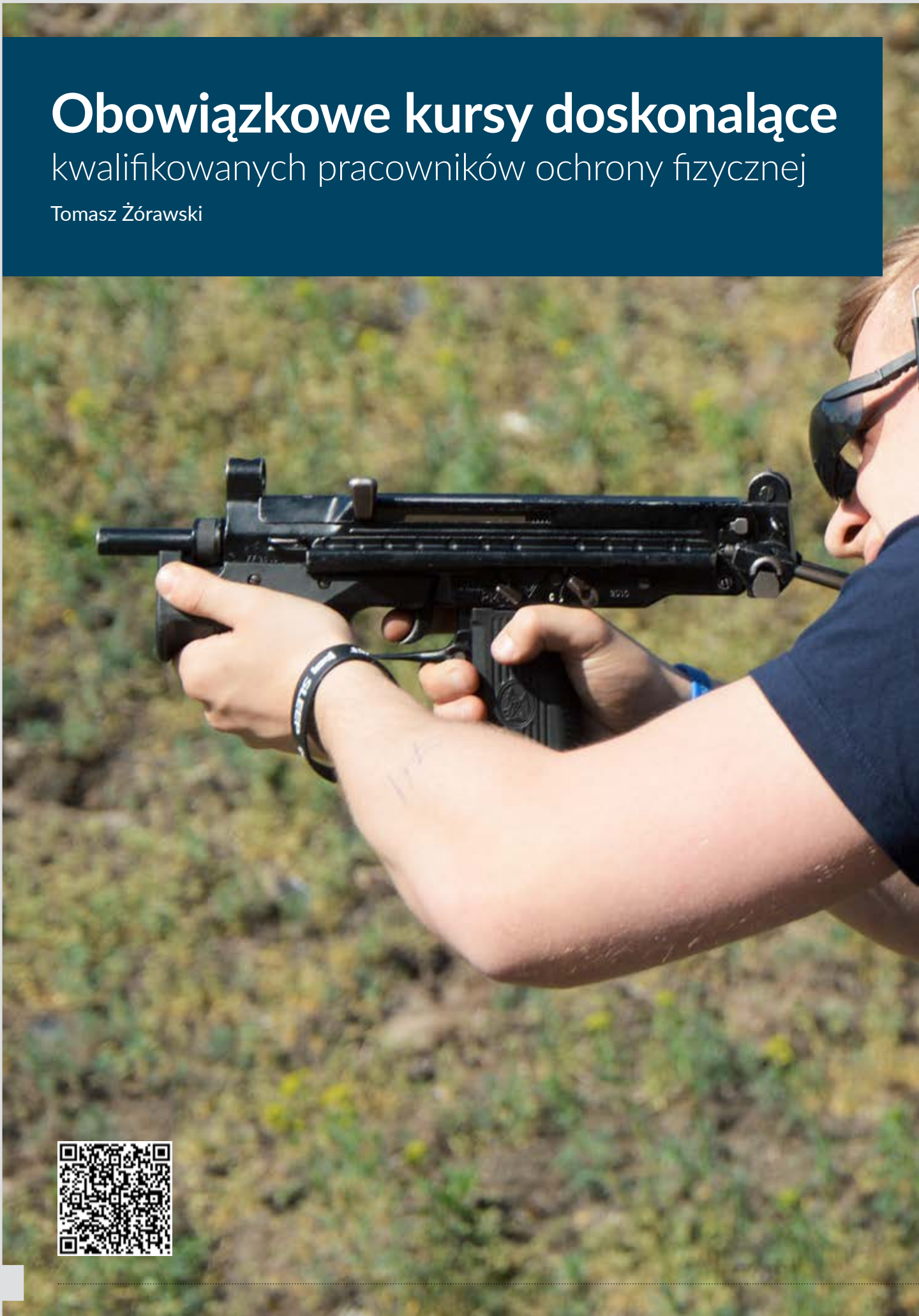
Aplikacja Project Assistant ma pomóc w zarządzaniu projektem systemu telewizji dozorowej na każdym etapie realizacji. Ułatwia ona także przygotowanie dokumentacji końcowej, ponieważ umożliwia sprawdzenie każdej z kamer z poziomu aplikacji, utworzenie dotyczącego jej raportu oraz sporządzenie dla klienta raportu całościowego, zawierającego zdjęcia, które pokazują, jakie jest pole widzenia kamer. Projekty utworzone w aplikacji Project Assistant można udostępniać zainteresowanym podmiotom za pośrednictwem chmury. Dzięki temu każdy z nich może sprawdzić, jaki jest etap realizacji projektu, co pozwala zachować przejrzystość prowadzonych działań.

Aplikację można pobrać bezpłatnie z oficjalnych sklepów – na komputer, tablet lub smartfon. Działa ona na platformach Apple, Windows i Google. Bosch Project Assistant ułatwia planowanie, wstępną konfigurację, rozruch i raportowanie, dzięki czemu każdy projekt systemu telewizji dozorowej można teraz zrealizować szybciej, zachowując większą kontrolę i przejrzystość prowadzonych prac. Krótko mówiąc, aplikacja umożliwia inteligentne projektowanie systemów telewizji dozorowej.

Bosch Building Technologies

Obowiązkowe kursy doskonalące
kwalifikowanych pracowników ochrony fizycznej

Tomasz Żórawski



Kwalifikowanych pracowników ochrony jest około stu tysięcy. W tym roku wielu z nich powinno zaliczyć kurs, który przedłuży ważność ich uprawnień o kolejne pięć lat. Dlaczego rok 2018 jest tak ważny dla ponad połowy pracowników naszej branży? Otóż w pierwszym kwartale 2014 roku, po deregulacji zawodu pracownika ochrony, wszyscy ówcześni posiadacze licencji pierwszego i drugiego stopnia zostali wpisani na listy kwalifikowanych pracowników ochrony (licencja została zniesiona i zastąpiona wpisem na listę). Ważność uprawnień tych osób skończy się na początku 2019 roku i do tego czasu powinni oni złożyć zaświadczenie o ukończeniu kursu doskonalącego właściwemu komendantowi wojewódzkiemu policji.

Zgodnie z art. 38b ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2017, poz. 2213 ze zm.) obowiązek odbycia kursu doskonalącego (wymaganego co pięć lat) dotyczy tylko kwalifikowanych pracowników ochrony. Ten obowiązek nie dotyczy osób pełniących funkcje członków organów zarządzających, prokurentów lub pełnomocników ustanowionych do kierowania działalnością określoną w koncesji lub prowadzących koncesjonowaną działalność gospodarczą jako przedsiębiorcy indywidualni lub wspólnicy osobowej spółki handlowej, jeżeli osobiście nie wykonują czynności związanych z bezpośrednią ochroną fizyczną. Omawiany przepis wskazuje również podmioty, które mogą prowadzić powyższe kursy, a są nimi m.in. publiczne i niepubliczne placówki i ośrodki kształcenia ustawicznego, działające na podstawie art. 117 ust. 5 ustawy z dnia 14 grudnia 2016 r. – *Prawo oświatowe*. W związku z tym warto sprawdzić, czy dany podmiot jest uprawniony do prowadzenia przedmiotowego kursu doskonalącego, gdyż, jak pokazuje rzeczywistość, bywa z tym różnie.

Zakres kursu jest uregulowany w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 21 stycznia 2016 r. w sprawie szczegółowej tematyki, formy oraz czasu trwania kursu doskonalącego umiejętności kwalifikowanych pracowników ochrony fizycznej (Dz. U. 2016, poz. 103). Kurs doskonalący trwa 40 godzin i jest prowadzony w formie wykładów i zajęć praktycznych. Jego tematyka obejmuje aktualny stan prawny i dotyczy ustawy o ochronie osób i mienia, ustawy o broni i amunicji oraz uprawnień kwalifikowanych pracowników ochrony fizycznej z uwzględnieniem wykorzystania przez nich środków przymusu bezpośredniego lub broni palnej, a także ich odpowiedzialności karnej i cywilnej (w sumie cztery godziny), zasady udzielania pomocy przedlekarskiej (osiem godzin), szkolenie strzeleckie, w tym strzelanie z kilku rodzajów broni palnej – pistoletu, rewolweru, pistoletu maszynowego, karabinku i strzelby gładkolufowej (w sumie 12 godzin), a także samoobronę i techniki interwencyjne (16 godzin).

Wejście w życie przepisów wprowadzających obowiązkowe kursy doskonalące spotkało się z olbrzymim oburzeniem zarówno pracodawców, jak i pracowników, głównie ze względu na zbyt dużą liczbę godzin na kursie, koszty i zamęt organizacyjny. Większość w naszym środowisku twierdziła, że ten pomysł pozbawiony jest sensu, gdyż, jak wiadomo, doskonalenie zawodowe powinno być procesem ciągłym, a prowadzenie zajęć raz na pięć lat całkowicie mija się z celem. Niektóre firmy zapewniają systematyczne doskonalenie zawodowe swoim pracownikom ochrony, szczególnie tym korzystającym z broni i środków przymusu bezpośredniego, ale w wielu agencjach ochrony doskonalenie zawodowe nie funkcjonuje. Przyjęliśmy do wiadomości, że kurs doskonalący jest obowiązkiem i nikt już tego nie kwestionuje. Po prostu trzeba go odbyć. Okazało się też, że – mimo początkowej niechęci – pracownicy przekonali się do kursów. Niektórzy z nich przyznali, że mają służbową broń (a więc także legitymacje uprawniające do posiadania broni), ale na zajęciach z pierwszej pomocy przedlekarskiej, samoobrony i na treningu strzeleckim byli pięć lat temu lub dawniej. Z tego wynika, że w niektórych przypadkach lepiej doskonalić raz na pięć lat niż wcale.

Obowiązkowe kursy doskonalące dla kwalifikowanych pracowników ochrony zaczęto organizować już w połowie 2017 roku, gdy kilka agencji ochrony zleciło przeprowadzenie kursów dla swoich pracowników właściwym placówkom szkoleniowym. Duża część pracowników z naszej branży jest zobowiązana do odbycia kursu do końca roku. Niektórzy zwlekają z pójściem na kurs do ostatniej chwili, aby mieć uprawnienia ważne do końca 2023 roku. Pomimo tego, że pracodawcy nie mają obowiązku pokrycia kosztów kursów doskonalących dla swoich pracowników, większość firm je pokrywa. Podkreślenia wymaga fakt, że taki kurs to spory wydatek dla pracodawców, szczególnie tych, którzy zatrudniają dużą liczbę osób. Średnie ceny kursu to 300–600 zł za osobę i często zależą od liczby uczestników. Są też oferty wystawienia zaświadczenia za 150 zł bez zorganizowania zajęć...

Skoro szkolenia są obowiązkowe, powinny być przeprowadzane fachowo, a uczestnicy powinni faktycznie z nich skorzystać, gdyż poprawi to jakość świadczonych usług ochrony fizycznej.

Tomasz Żórawski
rzeczoznawca i członek zarządu Polskiej Izby Ochrony
dyrektor-instruktor Centrum Szkoleniowego Służb Ochrony DELTA

RACS 5

Skalowalny system kontroli dostępu i automatyki budynkowej

Przewodowa kontrola dostępu

Bezprzewodowa kontrola dostępu

Rejestracja czasu pracy

Automatyka budynkowa

Zarządzanie kluczami

- Identyfikacja mobilna (Bluetooth, NFC, QR)
- Identyfikacja biometryczna za pośrednictwem linii papilarnych
- Identyfikacja za pośrednictwem tablic rejestracyjnych
- Integracja z systemem alarmowym
- Integracja CCTV (HIKVISION, DAHUA, ONVIF)
- Integracja z zamkami bezprzewodowymi APERIO (ASSA ABLOY)
- Integracja z zamkami bezprzewodowymi RWL (ROGER)
- Kontrola dostępu do parkingów
- Kontrola dostępu do pokoi hotelowych
- Kontrola dostępu do wind klasycznych
- Kontrola dostępu do wind KONE
- Kontrola dostępu do szafek
- Monitorowanie obiegu przedmiotów w tym kluczy
- Kontrola uprawnień do wypożyczenia przedmiotów
- Obsługa sprzedaży towarów i usług (PoS)
- Obsługa drukarek kart
- Zarządzanie i konfigurowanie z poziomu aplikacji Windows (VISO ST i EX)
- Zarządzanie z poziomu aplikacji webowej (VISO Web)
- Zarządzanie z poziomu aplikacji mobilnej (VISO Mobile)
- Serwer Integracji

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

roger®

Pomoc dla seniorów
jako usługa agencji ochrony

Andrzej Bochacz

W państwach rozwiniętych systematycznie wzrasta liczba obywateli w średnim wieku. Dotyczy to także Polski

Sytuacja demograficzna

Z danych statystycznych wynika, że z powodu różnych dolegliwości stałej pomocy oraz regularnej opieki wymaga obecnie w naszym kraju ponad 1,5 miliona osób w wieku 65 lat i starszych. Liczba Polaków, którzy przekroczyli wiek 75 lat aktualnie wynosi 2,4 mln. Z danych statystycznych wynika, że za 12 lat, w roku 2030, ta grupa populacyjna przekroczy 5 mln.

Nie każda starsza osoba cieszy się dobrym zdrowiem. Kiedy problem ten dotyczy osób bliskich, możemy zdecydować się na skorzystanie z oferty domów opieki. Oferta kosztowniejszych placówek może obejmować pełen zakres usług i udogodnień, jednak większość ludzi czuje się najlepiej we własnych domach, dlatego komfort psychiczny seniorów, którzy są objęci opieką i zarazem pozostają we własnych mieszkaniach, jest zdecydowanie wyższy.

Poczucie bezpieczeństwa seniora

W krajach wysokorozwiniętych przykłada się wagę do wspierania opieki domowej. Zaspokajanie potrzeb oraz spełnianie oczekiwań seniorów w ich naturalnym środowisku zwiększa komfort życia i może kosztować mniej niż stały pobyt w domu opieki. Rozwój techniki wpływa w naturalny sposób na możliwości współczesnych systemów opieki społecznej i medycyny.

W starzejącym się społeczeństwie zalety rozwiązań, które dają seniorom poczucie bezpieczeństwa i przyśpieszają udzielenie pomocy w przypadku zagrożenia zdrowia lub życia, zdecydowanie przeważają nad wadami. Te wyraźne korzyści zaczynają być dostrzegane również w polskim społeczeństwie.

Jak już wspomniano, alternatywą dla przeprowadzki do obcego miejsca jest opieka domowa. Osoba starsza preferuje takie rozwiązanie. Dzięki niemu przebywa ona w swoim własnym domu i jest otoczona bliskimi, co może pozytywnie wpływać na jej stan zdrowia, gdyż wciąż czuje się częścią rodziny i nie grozi jej samotność, która dla większości z nas jest nie do zniesienia.

Ograniczeniem, szczególnie dla osób samotnych, jest brak poczucia bezpieczeństwa. Boją się, że w trudnym momencie nie uzyskają pomocy. Takie zdarzenia jak upadek, zasłabnięcie, udar, wylew czy zawał przyczyniają się do znacznego ograniczenia aktywności seniorów.

Optymalnym rozwiązaniem jest świadczenie starszym ludziom usług opiekuńczo-ratunkowych. Możliwe jest wprowadzenie w otoczenie seniorów dyskretnych urządzeń monitorujących. Najprostszy identyfikator poinformuje o wyjściu z domu lub wstawaniu w nocy z łóżka. Bardziej zaawansowane urządzenia mogą rejestrować więcej.

Uzupełnienie klasycznego modelu opieki domowej o system monitorowania zachowań seniora połączony z sygnalizacją SOS i łącznością telefoniczną w trybie głośnomówiącym sprawia, że starszy człowiek czuje się bezpieczniej.

Możliwości agencji ochrony

Do standardowych zadań agencji ochrony należy nadzór nad mieniem oraz osobami przebywającymi na terenie objętym ochroną. Agencje mogą wysyłać patrole interwencyjne i dysponują specjalistycznym sprzętem, a także funkcjonującymi całodobowo centrami interwencyjno-alarmowymi. Wszystko to sprawia, że mogą one zajmować się pomaganiem starszym osobom.

Podobnie jak w przypadku sygnału z instalacji alarmowej, w przypadku alarmu związanego z zachowaniem osób starszych podejmowane są interwencje. Odpowiednie procedury można zastosować w różnych sytuacjach, które są dla seniorów kryzysowe. Są one inne niż standardowe przyczyny interwencji, ale metody obsługi są podobne.

Od personelu agencji ochrony nie wymaga się umiejętności ratowniczych. Gdy tylko sygnał od osoby starszej dotrze do centrali interwencyjno-alarmowej, od razu zostanie zweryfikowany przez operatora, który zastosuje adekwatną do rodzaju zgłoszenia formę wsparcia. Najczęściej wystarczy rozmowa telefoniczna. Czasami należy wezwać pogotowie ratunkowe lub lekarza. Agencja ochrony dysponuje patrolami interwencyjnymi, więc możliwe jest dotarcie do podopiecznego i kierowanie akcją ratunkową na miejscu. To wszystko sprawia, że agencje ochrony nie tylko mogą, ale powinny zainteresować się wsparciem osób starszych jako dodatkową możliwą formą swojej działalności.

Ocena zgłoszenia alarmowego

Podstawowe sygnały są jednoznaczne i łatwo jest opracować właściwe procedury na wypadek wciśnięcia przycisku SOS, zgłoszenia zalania czy zadymienia pomieszczenia. Jak jednak zareagować, kiedy podopieczny zemdleje? Na pewno nie naciśnie on przycisku SOS, a trzeba działać natychmiast i ważna jest każda minuta.

Polska firma NaszSenior.pl, podobnie jak kilka innych na całym świecie, od kilku lat rozwija projekt wykorzystujący mechanizmy sztucznej inteligencji, który rozwiązuje podobne niedogodności. Osoba starsza jest dyskretnie monito-

rowana w celu umożliwienia ewentualnej interwencji. W razie potrzeby wysyłany jest sygnał do centrum interwencyjno-alarmowego lub SMS czy e-mail do opiekuna.

NaszSenior.pl wdraża system opiekuńczo-ratunkowy SilverCRS. Jest to bardzo zaawansowane rozwiązanie, którego zadaniem jest uczenie się zachowań podopiecznych. Znaczące odstępstwa od typowego schematu zachowań skutkują wszczęciem odpowiednich procedur alarmowych lub informacyjnych.

zdrowia, pory roku, warunków pogodowych, pory dnia, od tego, jaki jest miesiąc i dzień tygodnia. Można zgromadzić wiele informacji, które umożliwią ustalenie schematu zachowania starszej osoby. Im bardziej ustabilizowane jest jej życie, tym bardziej powtarzalne są jej zachowania.

To wszystko można pokazać na przykładach. Powiedzmy, że w dni powszednie senior wstaje między 7:00 a 7:45, a w soboty i niedziele między 8:00 a 8:30. Jest środa, godzina 8:30. Senior jeszcze nie wstał. System może automatycznie

Każdy z nas ma swój specyficzny, w dużym stopniu powtarzalny schemat codziennej aktywności. O podobnych porach zasypiamy i budzimy się, spożywamy posiłki, wychodzimy na spacer itd. Dotyczy to również, a może tym bardziej, osób starszych. Powtarzanie pewnych czynności może zależeć od wielu różnych czynników, np. od stanu

poinformować centrum interwencyjno-alarmowe. Operator w centrum będzie próbował skontaktować się z tą osobą telefonicznie. Już po godzinie może nadejść pomoc.

Senior wychodzi na spacer z psem dwa razy dziennie – o 8:00 i o 19:00. Nie ma go wówczas

w domu przez godzinę. System zarejestrował wyjście podopiecznego i psa o 8:15. Do godziny 10:00 nie wrócili do domu. W takiej sytuacji zostaje wysłana informacja do centrum interwencyjno-alarmowego, które sprawdzi, gdzie dana osoba się znajduje. Po kwadransie patrol interwencyjny będzie przy niej.

Jeżeli przebywający w domu senior przewróci się, a system wykryje zagrożenie dla zdrowia, do centrum-interwencyjno-alarmowego może zostać wysłana stosowna informacja. Operator spróbuje dodzwonić się do podopiecznego. Jeżeli nie uda mu się, na miejscu zdarzenia pojawi się posiadający klucze do mieszkania patrol interwencyjny.

Senior je obiad codziennie między 15:00 a 16:00. System jest w stanie wykryć, że pomimo obecności podopiecznego w domu nie rozpoczęły się przygotowania do posiłku. Operator może zadzwonić, żeby sprawdzić, czy wszystko w porządku.

Systematyczne zbieranie informacji z dyskretnych identyfikatorów umożliwia ustalenie schematu zachowań seniora. System informuje o odstępstwach. Podopieczny może korzystać z opasek telemedycznych, lokalizatorów, przycisków SOS, urządzeń głośnomówiących, czujników wykrywających dym, czad, zalanie wodą i wielu innych.

Wiele różnych elementów, których zadaniem jest sygnalizowanie stanów alarmowych lub zbieranie danych o zachowaniach i stanie zdrowia, błyskawicznie przesyła informacje do systemu, gdzie są one analizowane i podejmowane są decyzje dotyczące rodzaju reakcji.

Dzięki systemom sztucznej inteligencji można stworzyć skuteczne i sprawne modele zachowań, które zawierają historię czynności, stanu zdrowia i reakcji podopiecznych. Takie rozwiązania mają dodatkowy walor, jakim jest możliwość uczenia się i doskonalenia systemu wnioskowania.

Zakres usług świadczonych seniorom:
- poprawa bezpieczeństwa osób starszych, chorych i niepełnosprawnych, przebywających stale lub czasowo w domu;
- objęcie teleopieką osób potrzebujących wsparcia;
- rozszerzenie zakresu pomocy oferowanej przez domy pomocy społecznej;
- zaspokajanie potrzeb lokalnych społeczności;
- wprowadzenie nowoczesnych form wsparcia dla seniorów i osób niepełnosprawnych;
- wykonywanie regionalnych zadań społecznych;
- udzielanie wsparcia w warunkach domowych.

Korzyści z wprowadzenia systemu teleopieki:
- możliwość udzielenia pomocy w razie upadku, nagłego pogorszenia zdrowia itp., a także wsparcia w przypadku depresji czy osamotnienia;
- koszty teleopieki mogą być zrekompensowane obniżeniem kosztów rehabilitacji, pomocy społecznej oraz ochrony zdrowia;
- możliwość skrócenia okresu hospitalizacji pacjentów;
- mniejsze zapotrzebowanie na miejsca w domach opieki;
- większa mobilność pacjentów i opiekunów (korzystanie z teleopieki może być niezależne od miejsca ich pobytu);
- możliwość znalezienia osoby, która się zgubiła lub oddaliła od domu (dzięki systemowi GPS, opasce SiDLY i smartfonowi);
- opiekunowie mogą zdalnie kontrolować stan zdrowia podopiecznego;
- członkowie rodziny seniora mogą przebywać w pracy i być pewni jego bezpieczeństwa;
- konieczność obsługi tego typu systemów powoduje, że mogą powstać nowe miejsca pracy;
- pojawienie się nowych możliwości prowadzenia naukowych badań medycznych i socjologicznych na wielkich populacjach;
- możliwość współpracy z jednostkami samorządu terytorialnego, które odpowiadają za lokalną politykę społeczną i cały czas szukają rozwiązań dostosowanych do ich budżetów;
- możliwość skorzystania z unijnego dofinansowania w ramach Regionalnych Programów Operacyjnych (poziom dofinansowania przekracza 90%).

Andrzej Bochacz

NASZSENIOR.PL

NaszSenior.pl
ul. Modlińska 190
03-119 Warszawa
tel.: 22 510 36 35
e-mail: biuro@naszsenior.pl

IVSS Dahua - rejestrator NVR

Rozpoznawanie i zaawansowana analiza twarzy w czasie rzeczywistym

Cechy:

- **Analiza wideo w czasie rzeczywistym:** algorytm głębokiego uczenia umożliwia wykrywanie obiektu i przewidywanie potencjalnego zagrożenia.
- **Wyszukiwanie wideo według obrazu:** jednocześnie wyszukuje do 10 twarzy. Szybka analiza twarzy z informacją, gdzie i kiedy się pojawiły.
- **Urządzenie wielofunkcyjne:** zarządzanie wideo, przechowywanie, analiza z wykorzystaniem interfejsów AI.

Polecane modele

IVSS7008-1T

IVSS7016-4T

ISO 9001:2000

www.dahuasecurity.com/pl

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

Oprogramowanie AxxonSoft

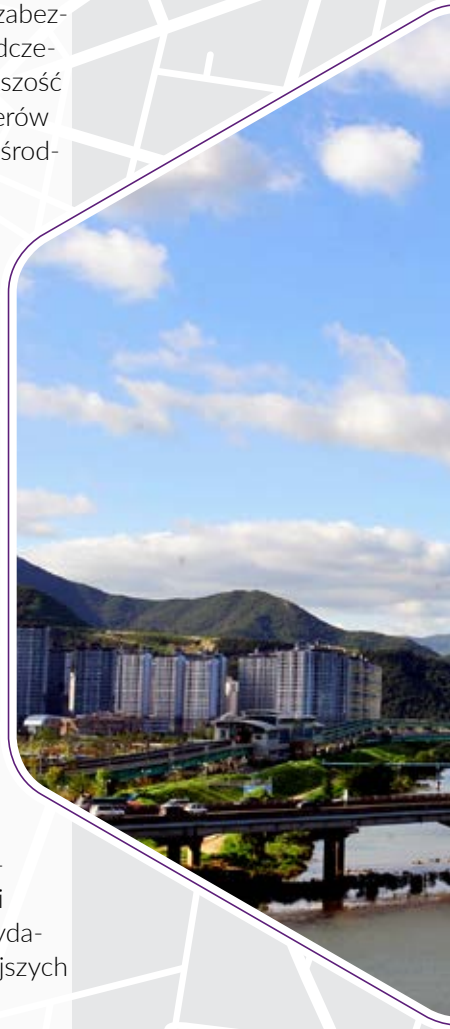
zapewnia bezpieczeństwo miastu Yangsan w Korei Południowej

AxxonSoft

Yangsan jest dużym miastem o powierzchni 485 kilometrów kwadratowych, liczącym około 300 tys. ludności. Wcześniejsze próby stworzenia jednolitego systemu wizyjnego w celu podniesienia poziomu bezpieczeństwa w przestrzeni miejskiej napotkały na znaczne trudności

W rozległym systemie dozorowym występowały zakłócenia, pojawiały się problemy z połączeniem nowych kamer, w szczególności kamer o wysokiej rozdzielczości. Rosnąca liczba kamer i lokalnych serwerów wizyjnych stała się przyczyną problemów z archiwizacją obrazów i z implementacją inteligentnych funkcji analizy treści materiału wizyjnego.

Wobec tych problemów władze miasta Yangsan zdecydowały, że system zabezpieczeń musi zostać zmodernizowany. Bazując na wcześniejszych doświadczeniach, sprecyzowano odpowiednie kryteria modernizacji. Uznano, że większość dotychczasowych problemów wynika ze zbyt dużej liczby lokalnych serwerów i rejestratorów wizyjnych oraz że konieczne jest stworzenie centralnego ośrodka kontrolującego wszystkie urządzenia wizyjne i powiązanie go z innymi systemami bezpieczeństwa w mieście. Uznano również, że w zmodernizowanym systemie należy zastosować kamery o odpowiednich parametrach użytkowych, w szczególności o wysokiej rozdzielczości. Pracami projektowymi i wdrożeniowymi miała się zająć firma GBU Data Links.



Rozwiązanie

By sprostać powyższym wymaganiom, firma GBU Data Links zaoferowała rozwiązanie najnowszej generacji, dostosowane do potrzeb miasta Yangsan, bazujące na oprogramowaniu Axxon Next VMS. Jakość uzyskiwanych w systemie obrazów jest na tyle wysoka, że można wykorzystać je w sądzie jako materiał dowodowy.

System Axxon Next VMS ma funkcje służące do analizy treści obrazu, które ułatwiają pracę służbom odpowiedzialnym za bezpieczeństwo publiczne. Do znanych rozwiązań należy funkcja wykrywania i odczytu danych znajdujących się na tablicach rejestracyjnych samochodów oraz funkcja identyfikacji osób na podstawie analizy obrazu twarzy. Unikatowym rozwiązaniem jest tak zwana kompresja czasowa, czyli narzędzie umożliwiające szybki przegląd zarejestrowanych wydarzeń bez konieczności wielokrotnego cofania się do wcześniejszych fragmentów materiału wizyjnego.

Wdrożenie systemu

Na terenie miasta Yangsan zainstalowano około 2500 kamer różnych producentów, w tym Arecont Vision, Samsung, Hikvision, Cellings, Flexwatch, Probe Digital. Około 900 takich kamer zostało zainstalowanych na peryferiach miasta. Bieżące strumienie wizyjne są kierowane do centralnej stacji monitorującej za pośrednictwem sieci światłowodowej. Materiał wizyjny jest przekazywany do jednostek pamięciowych o pojemności zapewniającej zapis obrazów przez 30 dni. W pomieszczeniu kontrolnym znajduje się trzynaście serwerów wizyjnych i piętnaście stacji roboczych, dzięki czemu możliwa jest całodobowa obserwacja obrazów z kamer.

Oprogramowanie Axxon Next VMS ma budowę modułową. Podczas rutynowej pracy system dozorowy wymaga jedynie licencji Axxon Next Professional. Wykorzystanie zaawansowanych funkcji wymaga dodatkowych licencji. Na przykład dodatkowa licencja Axxon Next Universe umożliwia korzystanie z analitycznych funkcji jednej ze wspomnianych klienckich stacji roboczych.

Zarówno bieżące obrazy z kamer, jak i wszystkie materiały wizyjne pochodzące z wcześniej wykorzystywanych systemów mogą być importowane do systemu Axxon Next VMS i poddane inteligentnej obróbce z użyciem najnowszych narzędzi.

Osiągnięte wyniki

Zastosowanie oprogramowania Axxon Next VMS umożliwiło spełnienie wymagań służb bezpieczeństwa publicznego miasta Yangsan. Pojawiły się zupełnie nowe możliwości. Zastosowanie pakietów programowych Greek Stream i Quick Sync Video radykalnie zmniejsza obciążenie głównego serwera wizyjnego. W związku z tym dotychczasowe problemy z odtwarzaniem bieżących lub archiwalnych obrazów z kamer przechodzą do historii. Dzięki ergonomicznemu interfejsowi Axxon Next GUI wyszukiwanie wydarzeń zarejestrowanych w systemie jest bardzo łatwe.

Dzięki optymalnemu wykorzystaniu dostępnych zasobów każdy z serwerów Axxon Next może obsłużyć maksymalnie 200 kamer. Wcześniejsze rozwiązania były ograniczone do 70 kamer. Specyfikacja SDK opublikowana przez firmę Axxon umożliwia łatwą integrację tego systemu z innymi rozwiązaniami innych producentów.

Rozwiązanie zaproponowane przez firmę Axxon spełniło oczekiwania władz miasta Yangsan i okazało się odpowiedniejsze od systemów sieciowych stosowanych dotychczas.

AxxonSoft
www.axxonsoft.com/pl
Tłumaczenie: Andrzej Walczyk

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

PROJEKTUJEMY
zgodnie ze sztuką

SYSTEMY SYGNALIZACJI POŻAROWEJ

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

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

SYSTEM DETEKCJI GAZÓW SDG 6000

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

Firma AxxonSoft

czuwała nad bezpieczeństwem podczas najlepszych piłkarskich mistrzostw świata

AxxonSoft

W dniach 14–15 czerwca 2018 r. w Rosji odbyły się finały dwudziestych pierwszych Mistrzostw Świata w Piłce Nożnej. Po raz pierwszy w historii Rosja była gospodarzem tych mistrzostw i poczyniła wielkie wysiłki, żeby wspaniale przygotować turniej, biorąc pod uwagę każdy aspekt, w tym bezpieczeństwo.

Trzydzieści dwa zespoły z całego świata rozegrały sześćdziesiąt cztery mecze na dwunastu stadionach zlokalizowanych w jedenastu rosyjskich miastach. Ponad trzy miliony kibiców zapełniły stadiony, a kolejne dziesiątki milionów śledziły przebieg rozgrywek w strefach dla kibiców i w innych miejscach wyznaczonych w celu oglądania meczów.

Członkowie międzynarodowej sportowej społeczności wielokrotnie zwracali uwagę na wzorowy poziom organizacji i zarządzania. Przewodniczący organizacji FIFA Gianni Infantino nazwał tegoroczny turniej najlepszym w historii. Zawodów nie zakłóciły żadne incydenty. Rosja zadbała o pozytywne wrażenia przybyłych kibiców.

Firma AxxonSoft miała swój istotny techniczny wkład w zapewnienie bezpieczeństwa zawodnikom i kibicom. Oprogramowanie AxxonSoft było szeroko wykorzystywane na stadionach, w ośrodkach treningowych, w strefach przeznaczonych dla kibiców, w infrastrukturze transportowej i w innych miejscach na terenie kraju, w których przebywali lub przemieszczali się członkowie zespołów i kibice. Ponadto oprogramowanie to zostało wybrane w celu utworzenia sieci centrów operacyjnych dla Ministerstwa Spraw Wewnętrznych Federacji Rosyjskiej, utworzonych specjalnie z powodu mistrzostw.

Oprogramowanie Intellect firmy AxxonSoft zastosowano w różnych miejscach na dziesięciu spośród dwunastu stadionów, na których rozegrano mecze mistrzostw. Platforma programowa Intellect służyła do zarządzania ponad 9000 kamer do nadzoru wizyjnego wykorzystanych do ochrony ponad dwóch milionów kibiców, którzy przyjechali na mecze.

Oprócz nadzoru wizyjnego zastosowano moduły programowe Auto Intellect i Face Intellect, aby umożliwić automatyczne rozpoznawanie tablic rejestracyjnych i rozpoznawanie twarzy przy bramkach stadionowych. Rozwiązania techniczne umożliwiające rozpoznawanie twarzy dowiodły swojej efektywności i są stosowane na arenach sportowych na całym świecie. Andrey Khristoforov, dyrektor handlowy w rosyjskim oddziale firmy AxxonSoft, wierzy, że ta technika ma dobrze zapowiadającą się przyszłość w branży sportowej.

– *Rozpoznawanie twarzy może być stosowane w ochronie antyterrorystycznej na imprezach masowych, w celu uniemożliwienia wstępu do obiektów sportowych kibicom, którym sądowo tego zakazano, i do powiązania danych biometrycznych kibiców z ich miejscami na stadionie (na podstawie biletów) w celu umożliwienia przeprowadzania dochodzeń w przypadkach incydentów lub wybryków* – powiedział Khristoforov.

Oprogramowanie Intellect wykorzystano jako podstawę zintegrowanego systemu nadzoru wizyjnego zaprojektowanego w taki sposób, by spełniał wymagania rosyjskiego ministerstwa spraw wewnętrznych dotyczące obiektów sportowych, na których odbywały się rozgrywki w ramach Mistrzostw Świata w Piłce Nożnej.

Na każdym z dwunastu stadionów oprogramowanie Intellect zostało połączone z istniejącymi systemami nadzoru wizyjnego poprzez specjalny zestaw interfejsów. Strumienie wizyjne były transmitowane do centrów operacyjnych Ministerstwa Spraw Wewnętrznych Federacji Rosyjskiej utworzonych w każdym rosyjskim mieście, w którym miały miejsce rozgrywki. Centra operacyjne otrzymywały materiał wizyjny również z miejskich stref dla kibiców. Z kolei dane wizyjne z regionalnych centrów operacyjnych były przesyłane do głównego centrum analiz sytuacji w Moskwie i Policyjnego Centrum Współpracy Międzynarodowej w Domodiedowie oraz wyświetlane tam na ścianach wizyjnych.

Produkty firmy AxxonSoft są wykorzystywane w całej Rosji również w infrastrukturze energetycznej, w transporcie publicznym, w rozwiązaniach na podstawie projektów tzw. bezpiecznego miasta, w międzynarodowych portach lotniczych i na trasach szybkiej kolei. Firma AxxonSoft jest bardzo dumna z tego, że w czasie jej warty na mistrzostwach w Rosji nie było żadnego poważnego incydentu.

AxxonSoft
www.axxonsoft.com/pl
Tłumaczenie: Paweł Karczmarzyk

Przeprowadzanie audytu

zarządzania bezpieczeństwem organizacyjno-technicznym obiektów. Część 5

Sprawdzenie sposobu i efektywności monitorowania poziomu bezpieczeństwa oraz weryfikacja skuteczności zarządzania incydentami w obiekcie

dr inż. Andrzej Wójcik

Do kluczowych elementów sprawdzanych podczas audytu bezpieczeństwa należy sposób i efektywność monitorowania poziomu bezpieczeństwa oraz skuteczność zarządzania incydentami w obiekcie. Na początek zajmiemy się skutecznością zarządzania zaistniałymi lub możliwymi zdarzeniami stwarzającymi zagrożenie, czyli incydentami mającymi wpływ na poziom bezpieczeństwa. Co rozumiemy przez incydent mający negatywny wpływ na bezpieczeństwo? Definicje zdarzenia mającego wpływ na bezpieczeństwo obiektu oraz incydentu mającego wpływ na bezpieczeństwo obiektu możemy zaczerpnąć z normy PN-ISO/IEC-27000 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Przegląd i terminologia*. Wcześniej należy jednak wyjaśnić, czym jest zdarzenie mające wpływ na bezpieczeństwo obiektu. Definicja zdarzenia określonego wyżej rodzaju jest następująca: „Zdarzenie związane z bezpieczeństwem obiektu to stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa, planu ochrony obiektu lub innych procedur bezpieczeństwa albo błąd zabezpieczenia lub nieznaną sytuację, która może być związana z bezpieczeństwem obiektu". A oto zawarta we wspomnianej normie definicja incydentu bezpieczeństwa mającego wpływ na bezpieczeństwo obiektu: „Incydent związany z bezpieczeństwem obiektu to pojedyncze niepożądane lub niespodziewane zdarzenie związane

z bezpieczeństwem obiektu lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu obiektu". Wynika z tego jednoznacznie, że skutki tak rozumianego incydentu są dla obiektu o wiele poważniejsze niż skutki zdarzenia (rozumianego w specyficzny, opisany wyżej sposób) i mogą mieć dużo większy wpływ na funkcjonowanie obiektu i procesy biznesowe, które są w nim realizowane.

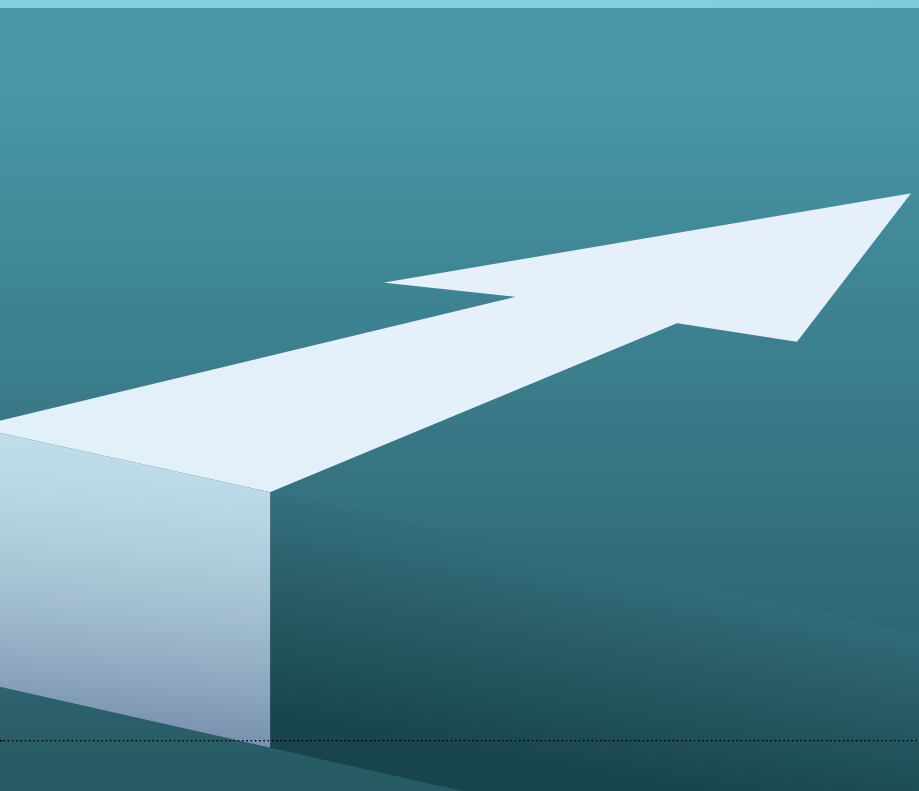
Zarządzanie incydentami mającymi wpływ na bezpieczeństwo obiektu powinno uwzględniać konkretne uwarunkowania. Jak w każdej tego typu działalności, należy zacząć od zebrania niezbędnych informacji, a potem odpowiednio je przetwarzać, by uzyskać wskazówki dotyczące skutecznego działania. W PN-ISO/IEC-27000 znajduje się następująca definicja systemu zarządzania incydentami mającymi wpływ na bezpieczeństwo w obiekcie: „system zarządzania incydentami w obiekcie to są procesy wykrywania, raportowania, szacowania, reagowania, podejmowania akcji i wyciągania wniosków z incydentów związanych z bezpieczeństwem obiektu."

Zarządzanie bezpieczeństwem obiektu wymaga podejścia systemowego, dlatego niezbędne jest przygotowanie odpowiedniej procedury. Procedura powinna wskazywać zakres obowiązków i odpowiedzialności poszczególnych osób – zarówno na poziomie kierowniczym, jak i na poziomie wykonawczym. Ważny jest przepływ informacji pomiędzy odpowiedzialnymi komórkami i podejmowanie decyzji w celu zapewnienia szybkiej, skutecznej i zaplanowanej reakcji na incydenty mające wpływ na bezpieczeństwo obiektu, informacji itd. Skuteczne zarządzanie incydentami powinno uwzględniać sposób zgłaszania zdarzeń z wykorzystaniem odpowiednich, sprawdzonych kanałów informacyjnych, aby podjęte działania były jak najszybsze.

Ważna jest także klasyfikacja incydentów i powiązany z nią sposób postępowania. Zgłaszający incydent powinien dokonać wstępnej klasyfikacji zdarzenia na podstawie dostępnych informacji oraz analizy okoliczności. Incydent może podlegać kwalifikacji z uwzględnieniem jego konsekwencji, np. kar finansowych, konsekwencji prawnych lub wizerunkowych, strat materialnych, strat w ludziach.

Przykłady kwalifikacji incydentów:

1. Incydent o stosunkowo małej ważności – działanie niezgodne z procedurą i naruszające bezpieczeństwo informacji. Taki incydent nie skutkuje karami pieniężnymi, konsekwencjami prawnymi i utratą wizerunku.
2. Incydent o średniej ważności. Jego skutkiem mogą być straty finansowe lub konsekwencje prawne, lub utrata wizerunku (występuje co najmniej jedna konsekwencja spośród wymienionych).



3. Incydent o dużej ważności. Jego skutkiem jest destrukcja (zniszczenie, utrata) kluczowych zasobów. Powoduje duże straty finansowe, konsekwencje prawne oraz utratę wizerunku.

Ocena zdarzeń mających wpływ na bezpieczeństwo i podejmowanie decyzji w ich sprawie to jedna z kluczowych faz zarządzania incydentami, która powinna być zgodna z udokumentowaną, zatwierdzoną i przyjętą procedurą w organizacji.

Zgłaszanie słabości mających wpływ na bezpieczeństwo (nie tylko słabości obiektu) jest związane z przygotowaniem pracowników, dostawców usług korzystających z obiektu, a także systemów technicznej infrastruktury do odnotowywania i zgłaszania wszelkich stwierdzonych zmian lub słabości mających wpływ na bezpieczeństwo obiektu, informacji, usług itd.

Skuteczność zgłaszania incydentów jest uzależniona od poinformowania pracowników i współpracowników i innych zainteresowanych stron, jak mają postępować w przypadku zaistnienia (powstania) incydentu. Oczywiście zapoznanie ich z procedurami i szkolenia są niezbędne. Bardzo pomocny może być także przygotowany katalog niepożądanych incydentów lub zdarzeń, które mogą być przyczyną incydentów.

Przykładowy katalog niepożądanych zdarzeń:
- naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych na terenie i w pomieszczeniach obiektu (uszkodzone zamki, okna, drzwi, naruszone plomby itp.);
- uruchomienie alarmu wynikające z zaniedbania lub z nieprzestrzegania procedur;
- przebywanie na terenie obiektu osób nieupoważnionych, które nie posiadają ważnego identyfikatora umieszczonego w widocznym miejscu;
- nietypowe zachowania użytkowników systemu (np. korzystanie z zasobów systemu w nietypowych godzinach, wysoka aktywność kont długo niewykorzystywanych, duża liczba nieudanych prób logowania w krótkim

Rys. Wybrane elementy systemu zarządzania incydentami

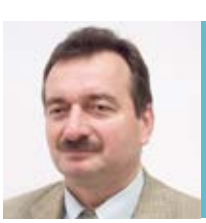
czasie, niewłaściwe wykorzystywanie lub nadużywanie zasobów informacyjnych);
- niedostępność systemów informatycznych oraz działania niezgodne ze specyfikacją (błędne) systemów informatycznych, zwłaszcza podstawowych lub najważniejszych systemów i aplikacji (z wyłączeniem kontrolowanych i zaplanowanych prac oraz dysfunkcji, które nie mają wpływu na bezpieczeństwo informacji);
- zdarzenia mające wpływ na cyberbezpieczeństwo (np. złośliwy program) ataki DDoS, próby omijania systemów zabezpieczeń, nieuprawniony dostęp do aplikacji i systemów, eskalacja poziomu uprawnień w systemach, ataki socjotechniczne, ataki z wykorzystaniem phishingu i skimmingu);
- wyciek istotnych danych biznesowych z firmy (który może być spowodowany również nieświadomym działaniem pracownika);
- kradzież lub zniszczenie urządzeń przetwarzających lub przechowujących informacje, a także nośników danych;
- wyłudzenia (lub próby wyłudzenia) informacji o szczególnym znaczeniu, takich jak hasła dostępowe czy tajemnice przedsiębiorstwa;
- nieprzestrzeganie zawartych w regulaminie wewnętrznym reguł dotyczących bezpieczeństwa informacji lub wynikających z nich zapisów w umowach z kontrahentami, lub przepisów prawa powszechnego dotyczących bezpieczeństwa informacji prawnie chronionych;
- incydenty wielokomponentowe (złożone incydenty dotyczące wielu systemów, podczas których mogą być przeprowadzane ataki z wielu stron).

Incydent powinien zostać poddany analizie przez wskazaną osobę (lub grupę osób), która staje się odpowiedzialna za adekwatne i skuteczne działania neutralizujące skutki incydentu.

Analiza incydentu powinna uwzględniać:
- charakter incydentu i jego znaczenie związane z naruszeniem bezpieczeństwa fizycznego lub teleinformatycznego;
- miejsce wystąpienia incydentu – wskazanie miejsca, w którym nastąpiło zdarzenie (np. serwera lub stacji roboczej;
- liczbę miejsc i zakres zasobów dotkniętych incydentem;
- określenie zasobów potrzebnych do dalszych działań w ramach postępowania stanowiącego reakcję na incydent związany z bezpieczeństwem informacji;
- sposoby ograniczenia skutków incydentu;
- oszacowanie szkód finansowych;
- określenie rodzaju ujawnionych informacji (jeśli ma to zastosowanie; mogą to być na przykład dane osobowe);
- określenie w przybliżeniu, kiedy skutki incydentu zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego ich usunięcia;
- wstępne oszacowanie skutków organizacyjnych i prawnych;
- proponowane działania korygujące lub naprawcze.

Osoba odpowiedzialna za bezpieczeństwo obiektu, w którym zaistniał incydent (właściciel, administrator, kierownik ochrony itp.), może skorzystać z pomocy innych osób, które są uprawnione i zobowiązane do udzielenia pomocy. Jeśli incydent jest związany z bezpieczeństwem danych osobowych, osoby odpowiedzialne za zarządzanie incydentami powinny niezwłocznie poinformować o tym kierownictwo jednostki organizacyjnej oraz właściciela obiektu. Ważne jest gromadzenie materiału dowodowego. Organizacja powinna określić i stosować procedury gromadzenia, pozyskiwania i utrwalania informacji, które mogą stanowić materiał dowodowy podczas postępowania organów administracji czy służb porządkowych.

System zarządzania incydentami może być źródłem wielu informacji dla audytora – informacji dotyczących m.in. skuteczności zastosowanych zabezpieczeń czy sposobu, w jaki korzystają z nich pracownicy i użytkownicy obiektu. Uzyskane informacje umożliwiają udoskonalenie systemu zarządzania bezpieczeństwem.



Andrzej Wójcik

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

NVIP-3DN3630SD/IRH-2

Kamera IP szybkoobrotowa STARLIGHT marki NOVUS

Matryca **CMOS Sony STARLIGHT** o rozdzielczości **3 Mpx** w połączeniu z obiektywem o zmiennej ogniskowej regulowanej w zakresie od 4.5 mm do 135 mm i promiennikiem podczerwieni o zasięgu 180 m, pozwala na efektywną obserwację rozległych obszarów i rozpoznawanie drobnych detali nawet w trudnych warunkach oświetleniowych

Obraz	
Przetwornik obrazu	3 Mpx, matryca CMOS, 1/2.8", SONY Exmor R STARVIS
Czułość	0,03 lx/F1.6 - tryb kolorowy 0,01 lx/F1.6 - tryb czarno-biały 0 lx (IR wł.) - tryb czarno-biały
WDR/DNR/F-DNR/HLC/BLC	tak/3D/tak/tak/tak
Obiektyw	
Zoom optyczny	30x
Typ obiektywu	motor-zoom z automatyczną przysłoną, f=4.5 ~ 135 mm/F1.6 ~ F4.4
Sieć	
Rozdzielczość strumienia wizyjnego	2048 x 1536 (QXGA), 1920 x 1080 (Full HD), 1280 x 720 (HD), 640 x 480 (VGA), 320 x 240 (QVGA)
Prędkość przetwarzania	25 kl./s dla 2048 x 1536 (QXGA)
Kompresja wizji/dźwięku	H.264, H.265, MJPEG/G.711
Liczba jednoczesnych połączeń/Przepustowość	maks. 6/łącznie 70 Mb/s
Zgodność z protokołem ONVIF	Profile S/G
Pozostałe funkcje	
Reakcja na zdarzenia alarmowe	e-mail z załącznikiem, zapis na kartę SD, aktywacja wyjścia alarmowego, powiadomienie HTTP, zmiana ustawienia PTZ
Oświetlacz IR	
Zasięg/Kąt świecenia	do 180 m (zależny od aktualnej ogniskowej)
Interfejsy	
Gniazdo kart pamięci	microSD - pojemność do 128 GB
Parametry instalacyjne	
Klasa szczelności	IP 66 (szczegóły w instrukcji obsługi)
Zasilanie	24 V_{DC}/24 V_{AC}
Obudowa	aluminiowa, w kolorze białym, stopień ochrony IK10, w zestawie: obudowa zewnętrzna (zintegrowana z kamerą), uchwyt ścienny

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

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

NVR-6332-H8/F

Rejestrator IP marki NOVUS z funkcją rozpoznawania twarzy

Rejestrator **32-kanałowy** do rejestracji strumieni wizyjnych z kamer o rozdzielczości do **8 Mpx** (3840 x 2160) i kompresji metodą H.264, H.264+ oraz H.265. W urządzeniu można zamontować do 8 dysków twardych o pojemności 6 TB każdy. Rejestrator we współpracy z kamerami serii 3000 obsługuje funkcje inteligentnej analizy obrazu m.in. **identyfikacji twarzy**.

Wizja	
Kamery IP	do 32 kanałów w rozdzielczości 3840 x 2160 (obraz + dźwięk)
Obsługiwana rozdzielczość	maks. 3840 x 2160
Kompresja	H.264, H.264+, H.265
Wyjścia monitorowe	główne (podział, pełny ekran, sekwencja): 1 x VGA, 1 x HDMI (4K UltraHD) spot: 1 x HDMI (FullHD)
Obsługa dwustrumieniowości	tak*
Obsługa dla kamer fisheye	tak, kamery IP serii 3000
Nagrywanie	
Prędkość nagrywania	960 kl./s (32 x 30 kl./s dla 1280 x 720), 960 kl./s (32 x 30 kl./s dla 1920 x 1080), 960 kl./s (32 x 30 kl./s dla 2048 x 1536), 960 kl./s (32 x 30 kl./s dla 2560 x 1440), 960 kl./s (32 x 30 kl./s dla 3840 x 2160)
Wielkość strumienia	256 Mb/s łącznie ze wszystkich kamer
Dyski	
Wewnętrzne	możliwość montażu: 8 x HDD 3.5" 6 TB SATA, do 48 TB
Alarmy	
Wejścia/wyjścia alarmowe lokalne	8/4 typu przekaźnikowego
Wejścia/wyjścia alarmowe w kamerach	obsługa wejść/wyjść dostępnych w kamerach*
Reakcja na zdarzenia alarmowe	sygnał dźwiękowy, e-mail, aktywacja wyjścia alarmowego, aktywacja nagrywania, zmiana ustawień PTZ
Inteligentna analiza obrazu	
Obsługiwane funkcje	wykrywanie obiektów, sabotaż, zmiana sceny, utrata ostrości, zmiana kolorystyki, przekroczenie linii, naruszenie strefy, identyfikacja twarzy
Sieć	
Interfejs sieciowy	2 x Ethernet - złącze RJ-45, 10/100/1000 Mbit/s
Zgodność z ONVIF	Profile S (ONVIF 2.2 lub wyższy)
Programy na PC/MAC	NMS, Internet Explorer, NVR-6000 Viewer/Safari
Programy na Smartphone	SuperLive Plus (iPhone, Android)
Maks. liczba połączeń z rejestratorem	4
Dodatkowe interfejsy	
Porty USB	2 x USB 2.0, 1 x USB 3.0
Parametry instalacyjne	
Mocowanie RACK 19"	2U

Inteligentna analiza obrazu działa tylko z kamerami NOVUS IP serii 3000
* Funkcja uzależniona od protokołu komunikacji, szczegółowe dane znajdują się w tabeli kompatybilności dostępnej w zakładce PLIKI DO POBRANIA.

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

MCT80M-BLE
Terminal dostępu do systemu RACS 5

MCT80M-BLE jest miniaturowym terminalem identyfikacji przeznaczonym do wykorzystania w systemie kontroli dostępu i automatyki budynkowej RACS 5. Terminal umożliwia rozpoznawanie użytkowników za pomocą kart zbliżeniowych standardu 13,56 MHz MIFARE Ultralight/Classic/DESFire/PLUS, a także za pomocą urządzenia mobilnego (telefonu) wyposażonego w technologię NFC lub Bluetooth. W przypadku identyfikacji przez Bluetooth zasięg odczytu może sięgać do kilku metrów. Pozostałe metody identyfikacji wymagają zbliżenia identyfikatora do czytnika na odległość kilku centymetrów. Identyfikacja mobilna wymaga zainstalowania w telefonie aplikacji Roger Mobile Key dostępnej dla systemu iOS oraz Android. Czytnik wyposażony jest w dwa przyciski funkcyjne oznaczone symbolami dzwonek i światło, które alternatywnie mogą być wykorzystane do innych celów niż wskazują powiązane z nimi symbole. MCT80M-BLE posiada interfejs RS485, za pośrednictwem którego jest podłączany do magistrali komunikacyjnej kontrolera. Urządzenie może być instalowane na zewnątrz budynków bez konieczności stosowania dodatkowych zabezpieczeń. Ze względu na relatywnie małe wymiary czytnik może być montowany na drzwiczkach do różnego rodzaju szafek i schowków. Terminal jest zaprojektowany zgodnie z linią wzorniczą QUADRUS.

Charakterystyka

- Terminal dostępu do systemu RACS 5
- Odczyt kart 13,56 MHz MIFARE Ultralight/ Classic/DESFire/PLUS
- Identyfikacja mobilna za pośrednictwem telefonu z NFC lub Bluetooth
- Przyciski funkcyjne: dzwonek i światło
- 3 LED-y sygnalizacyjne
- Buzzer
- RS485
- Tamper
- Praca na zewnątrz
- Wymiary: 100,0 x 45,0 x 16,0 mm (wys. x szer. x grub.)
- Linia wzornicza QUADRUS
- Znak CE

ROGER Sp. z o.o. Sp. k.
Gościszewo 59
82-400 Sztum, woj. Pomorskie
tel. 55 272 0132, faks 55 272 0133
e-mail: roger@roger.pl
http://www.roger.pl

MCT86M-IO-CH-HR

Terminal dostępu do systemu RACS 5

MCT86M-IO-CH-HR jest terminalem systemu RACS 5 przeznaczonym do wykorzystania w obiektach hotelowych. Główną funkcją terminala jest wyłączanie zasilania elektrycznego w czasie nieobecności gościa hotelowego w pokoju oraz sygnalizowanie życzeń gości: nie przeszkadzać, posprzątać, wezwanie pomocy oraz wezwanie obsługi. Terminal wyposażony jest w kieszeń na kartę zbliżeniową, której stan monitoruje w sposób ciągły. Reakcja kontrolera na włożenie i wyjęcie karty podlega konfigurowaniu i może być uzależniona od przypisanych do niej uprawnień. Sygnalizowanie życzeń gości odbywa się za pomocą dotykowych przycisków funkcyjnych, a ich aktualny stan jest prezentowany na wskaźnikach LED terminala, w oprogramowaniu zarządzającym systemem oraz na czytniku wejściowym do pokoju (MCT82M-IO-HR). Terminal MCT86M-IO-CH-HR udostępnia zestaw programowalnych linii wej./wyj. w tym jedno wyjście przekaźnikowe. Zwykle linie te są wykorzystywane do sterowania zasilaniem elektrycznym pokoju, klimatyzacją, oświetleniem oraz do podłączenia różnego rodzaju przycisków, przełączników i czujników. Wykorzystując terminal MCT86M-IO-CH-HR w komplecie z terminalem MCT82M-IO-HR można w ramach systemu RACS 5 uzyskać podstawowy zestaw realizujący typowe wymagania w zakresie kontroli dostępu i automatyki w pokojach hotelowych. Za pomocą Serwera integracji możliwe jest zintegrowanie systemu RACS 5 z programami innych producentów, a nawet realizowanie dodatkowych funkcji niedostępnych w systemie RACS 5. Terminal obsługuje szyfrowane sektory kart MIFARE, co zabezpiecza system przed użyciem nieautoryzowanych kart oraz duplikowaniem kart oryginalnych. Terminal wymaga podłączenia do kontrolera dostępu, który steruje działaniem systemu. Połączenie z kontrolerem jest realizowane za pośrednictwem magistrali RS485.

Charakterystyka

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

roger®

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

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

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

D PROD S

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

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

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

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

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

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

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

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

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

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

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

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

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

D I

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

I D PROD PROJ S

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

D PROD PROJ S

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

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

D PROD S

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

D I PROJ S

ROBERT BOSCH Sp. z o.o.
ul. Jutrzenki 105
02-231 Warszawa
tel. 22 715 41 00, faks 22 715 41 05
e-mail: securitysystems@pl.bosch.pl
www.boschsecurity.pl

D

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

I PROJ

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

D I PROD PROJ S

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

D PROD PROJ S

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

D I PROD PROJ S

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

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

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

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

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

eltrox.pl

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B C D PROD S

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

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: janex@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

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

D PROD PROJ S

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

PROD

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

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

D I PROD PROJ S

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

D PROJ S

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

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
faks 22 625 26 75
e-mail: techom@techom.com
www.techom.com

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

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

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

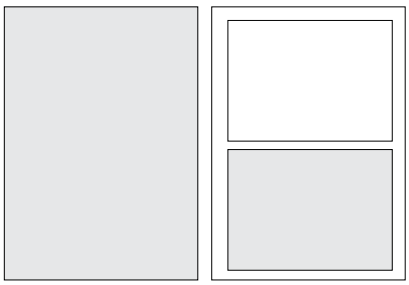
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie

Spis teleadresowy
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

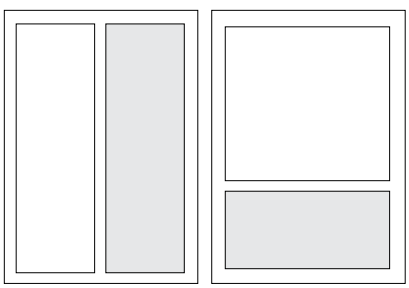
Ceny negocjujemy indywidualnie

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

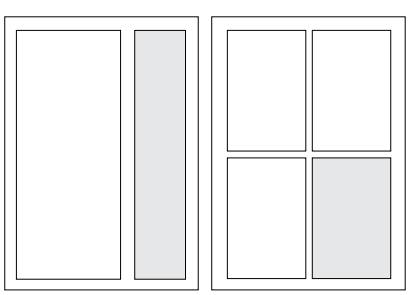
Udostępniamy również powierzchnię reklamową na naszej stronie internetowej http://www.zabezpieczenia.com.pl


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

Redakcja nie zwraca materiałów nie zamówionych oraz zastrzega sobie prawo do skrótu i redakcyjnego opracowania tekstów przyjętych do druku. Za treść reklam, ogłoszeń, tekstów sponsorowanych oraz kart katalogowych redakcja nie odpowiada. Wszelkie prawa zastrzeżone. Przedruk tekstów, zdjęć i grafiki bez zgody redakcji zabroniony.

NOVUS®

2000 SERIA IP • 4000 SERIA IP

IDEALNE DOPASOWANIE

KAMERY IP SERII 2000 TYPU „RYBIE OKO” I REJESTRATORY SERII 4000

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

FUJIFILM
Value from Innovation

W
yobraź
sobie nowy
teleobiektyw zoom
32x o rozdzielczości 2 megapikseli
dla doskonałej jakości Full HD w całym zakresie

ogniskowej i wyobraź sobie, że jest on coraz mniejszy i mniejszy i mniejszy

Obiektyw 32x Fujinon Zoom od 1/1.8" do 2/3"

Day Night Full HD 2MP

Dzięki kompaktowej konstrukcji, obrazom Full HD, przetwornikom o dużych formatach, zintegrowanym filtrem przeciwmgielnym oraz analogowym i szeregowym sterowaniu, oba teleobiektywy 32x zoom pasują do uniwersalnych obudów i znajdują idealne zastosowanie w monitoringu na dużych dystansach - nawet w warunkach słabego oświetlenia i złej pogody. Więcej informacji na stronie www.fujifilm.eu/fujinon lub zeskanuj kod **Fujinon. Widzisz więcej. Wiesz więcej.**

kremer agency

FUJINON