CZASOPISMO BEZPŁATNE
ISSN: 1505-2419 DWUMIESIĘCZNIK NR 2(132)/2020

ZABEZPIECZENIA

Widok

każdego zakątka, nawet z dużej odległości.

AXIS P3719-PLE umożliwia pokrycie czterech różnych obszarów z wykorzystaniem tylko jednej kamery. Doskonały obraz 24h/dobę nawet przy niesprzyjających warunkach oświetlenia. Kamera dostarcza jednocześnie wysokiej jakości widok ogólny i wyraźne szczegóły dzięki innowacyjnym rozwiązaniom zastosowanym w tym efektywnym kosztowo urządzeniu. Kamera świetnie sprawdza się gdy potrzebny jest niezakłócony dozór wizyjny rozległych, zewnętrznych obszarów, skrzyżowań ulic i na narożnikach budynków.

Więcej na www.axis.com/products/axis-p3719-ple

AXIS COMMUNICATIONS

RACS 5

Polski system kontroli dostępu i automatyki budynkowej klasy *Enterprise*

Przewodowa kontrola dostępu

Bezprzewodowa kontrola dostępu

Rejestracja czasu pracy

Automatyka budynkowa

Zarządzanie kluczami

Identyfikacja mobilna BLE, NFC i QR

roger®

Intelligence for Building

WYRÓB POLSKI

SPIS TREŚCI

Nowości produktowe

Wydarzenia, informacje

Nowe technologie

Systemy zintegrowane

Telewizja dozorowa

Systemy sygnalizacji pożarowej

Ochrona perymetryczna

ZŁOTE MEDALE Targów Securex 2020

securex® POLAND
Międzynarodowe Targi Zabezpieczeń

27 lutego 2020 r. sąd konkursowy pod przewodnictwem prof. dr. hab. inż. Marka Domańskiego z Politechniki Poznańskiej przyznał Złote Medale Grupy MTP produktom zgłoszonym przez wystawców tegorocznych **Międzynarodowych Targów Zabezpieczeń Securex.**

W dniach **18-20 listopada** będzie można je bliżej poznać na Międzynarodowych Targach Poznańskich. Eksperci wskazali również najlepszy spośród nich, przyznając nagrodę Grand Prix, która ogłoszona zostanie podczas uroczystej ceremonii otwarcia imprezy.

Do 16 kwietnia można oddać głos na złotych medalistów w internetowej rywalizacji o Złoty Medal - Wybór Konsumentów.

CLAW
– Bariera Przeciwinwazyjna
SECUTEC Sp. z o.o. - zgłaszający
VOLKMANN & ROSSBACH GmbH & Co. KG - producent

CyberVigilant®
IndigoVision Ltd

Dysk twardy do systemów monitoringu wizyjnego Skyhawk 16TB AI
TOKANTIS Edyta Sokół - zgłaszający
Seagate Technology LLC - producent

Elektroniczna klamka blueSmart ETB-IM do drzwi wewnętrznych
WINKHAUS POLSKA BETEILIGUNGS Sp. z o.o. Sp. k.

GEMOS MOSAIC
ELA-COMPIL Sp. z o.o.

Hybrydowy system bezpieczeństwa SSWiN/SKD - Kontroler UDK-R
ELECTRONIC POWER AND MARKET Spółka z o.o.

Kamera FLIR Saros™ DH-390 Dome
LINC POLSKA Sp. z o.o. - zgłaszający
FLIR Systems, Inc. - producent

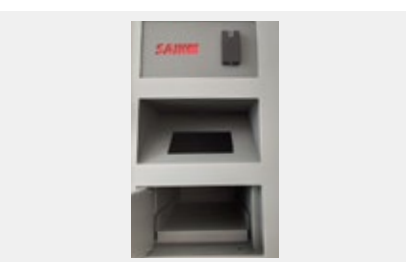
Liniowa Czujka Dymu FireBeam Xtra CR
CREATIO A. Waligóra - zgłaszający
The Fire Beam Company - producent

LivEye PRO 2.0
LivEye Gmbh

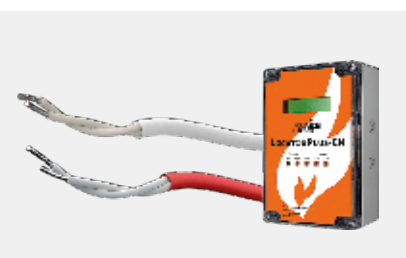
Multispektralna kamera IP MOBOTIX M73
LINC POLSKA Sp. z o.o. - zgłaszający
MOBOTIX AG - producent

Oprogramowanie do zarządzania wideo i systemami bezpieczeństwa średniej i dużej skali.
CBC (POLAND) Sp. z o.o. - zgłaszający
CBC Group - producent

Radar Magos Scepter-C
LINC POLSKA Sp. z o.o. - zgłaszający
Magos Systems - producent



SAIK GUN
BT ELECTRONICS Sp. z o.o.
- zgłaszający i producent



Signaline FT-EN
LGM Products Ltd.
- zgłaszający i producent

Zewnętrzny sygnalizator akustyczno-optyczny SAOZ-Pk2
W2 Włodzimierz Wyrzykowski

Złote Medale MTP są równoważne, kolejność alfabetyczna. **www.zlotymedal.com**

ZUP-230V – Zasilacz do systemów wentylacji pożarowej
MERAWEX Sp. z o. o.
- zgłaszający i producent

Aplikacja Traffic CaMMRa

do szybkiej analizy ruchu drogowego przeprowadzanej w kamerze

Rys. 1. Interfejs aplikacji TraFFic CaMMRa. Aplikacja jest obecnie testowana w trzech czeskich miastach, a także wykorzystywana w projekcie pilotażowym w dziewięciu innych krajach Europy i południowej Afryki

Dzięki nowej aplikacji **Traffic CaMMRa** oferowanej przez **Axis Communications** kamery AXIS można przekształcić w czujniki rozpoznające tablicę rejestracyjną, kierunek jazdy, kolor, markę, typ, a w niektórych przypadkach określony model pojazdu. Aplikacja działa bezpośrednio w kamerze. Została opracowana przez FF Group.

– *Możliwości zastosowania TraFFic CaMMRa są naprawdę duże – od monitorowania ruchu, liczenia pojazdów i gromadzenia danych aż po automatyczne pobieranie opłat. Aplikacja może identyfikować ciężarówki, wykrywać naruszenia przepisów ruchu drogowego, takie jak wyprzedzanie czy jazda po złym pasie, a nawet wyszukiwać skradzione samochody. Na kolejnym etapie chcemy umożliwić także pomiar prędkości pojazdu* – powiedział Jan Hazlbauer, manager projektu w FF Group.

Oprogramowanie działa bezpośrednio w kamerach sieciowych firmy Axis Communications. Wykorzystuje ich moc obliczeniową za sprawą przetwarzania brzegowego. W rezultacie nie jest wymagane użycie dodatkowego sprzętu ani serwera. Ponadto firma wprowadziła nową kamerę – AXIS Q1700-LE, która służy do rozpoznawania tablic rejestracyjnych i jest w pełni dostosowana do integracji z zewnętrznym oprogramowaniem, niezależnie od tego, czy są to systemy serwerowe czy aplikacje ACAP, takie jak TraFFic CaMMRa.

Połączenie specjalistycznej kamery AXIS Q1700-LE i aplikacji TraFFic CaMMRa daje wiele możliwości. Dzięki wysokiej wydajności obliczeniowej kamery, zoptymalizowanej pod kątem wykorzystania w systemach kontroli ruchu drogowego, wszystkie dane są natychmiast przetwarzane i analizowane w kamerze. System jest bardzo szybki. Aplikacja może „zauważyć" pojazd jadący z prędkością do 160 km/h w ciągu 120–250 milisekund, a zatem może analizować sytuację nawet na trzech pasach ruchu jednocześnie. Zakres analizy wynosi maksymalnie 240 metrów w ciągu dnia i około 40 metrów w nocy.

– *Kamery Axis Communications mogą wykorzystywać aplikacje innych firm, co pozwala nam współpracować z ekspertami branżowymi. W rezultacie wspólnie tworzymy rozwiązania dopasowane do konkretnych potrzeb klientów. TraFFic CaMMRa jest tego świetnym przykładem. Ponadto kamerę wraz z aplikacją można łatwo zintegrować z systemami zarządzania strumieniami wizyjnymi. Inteligentna analiza treści obrazu, która odbywa się bezpośrednio w kamerze, jest z pewnością przyszłościowym rozwiązaniem w sektorze transportowym – wszechstronnym, prostym i bardzo szybkim* – podsumował Dalibor Smažinka, Business Development Manager w Axis Communications.

Więcej informacji o aplikacji można znaleźć na stronie www.ff-group.org/axis.

Bezpośr. inf. Axis Communications

Nowe czytniki
w ofercie firmy AAT HOLDING

W związku z oczekiwaniami klientów i instalatorów firma **AAT HOLDING** wprowadziła do swojej oferty trzy nowe modele czytników – **KDH-C130M-7UID, KDH-CK130M-7UID** oraz **KDH-C150MQR.**

Dwa pierwsze modele są przeznaczone do odczytu siedmiobajtowego numeru UID z kart Mifare Plus i Mifare Desfire. Karty te charakteryzują się znacznie lepszymi zabezpieczeniami niż w kartach Mifare Classic. W wersji podstawowej karty w sektorze domyślnym zapisany jest unikatowy 56-bitowy numer. Taka liczba bitów jest wysyłana poprzez interfejs Wieganda do kontrolera. Czytniki są przeznaczone do współpracy z kontrolerami, które obsługują taki format. Czytnik KDH-CK130M-7UID jest wyposażony w klawiaturę, dzięki której umożliwia więcej sposobów potwierdzania uprawnień do dostępu (podanie przez użytkownika kodu dostępu; odczyt karty i podanie kodu dostępu; odczyt karty lub podanie kodu dostępu). W przypadku tego modelu możliwy jest również tryb pracy, w którym użytkownik jest identyfikowany na podstawie wprowadzonego na klawiaturze czytnika numeru wirtualnej karty. W obu czytnikach możliwa jest zmiana domyślnego formatu wyjściowego Wiegand z 56-bitowego na 34-bitowy. W modelu bez klawiatury format jest zmieniany poprzez dołączenie do masy dodatkowego przewodu, a w modelu z klawiaturą – poprzez wydanie specjalnej komendy w trybie programowania. Czytnik z klawiaturą umożliwia również ustawienie czterobitowego lub ośmiobitowego domyślnego formatu wyjściowego dla klawiatury.

Model KDH-C150MQR został wprowadzony z myślą o łatwej i taniej obsłudze gości przybywających na spotkanie do obiektu wyposażonego w system kontroli dostępu. Zaproszony na spotkanie gość może otrzymać przesłany do smartfonu kod QR wygenerowany w programie do obsługi recepcji. Po przybyciu do obiektu gość zbliża smartfon do czytnika kodów QR i uzyskuje zezwolenie na wejście. Ten model odczytuje również standardowe karty Mifare Classic.

Kody QR będzie można generować i wysyłać do użytkowników również z programu NMS AC w wersji 4.0 i wyższej. Innym sposobem jest użycie dowolnego generatora kodów QR. Kod musi zawierać same cyfry – nie więcej niż dziesięć.

Aby zwiększyć bezpieczeństwo w systemie kontroli dostępu czytnik kart KDH-C150MQR powinien być zainstalowany w przejściu przeznaczonym tylko dla gości. Standardowi użytkownicy systemu nie powinni mieć uprawnień do korzystania z tego przejścia. Pozwoli to zapobiec uzyskaniu dostępu do obiektu po wygenerowaniu przez osoby postronne kodu QR z numerem karty pracownika. Wygenerowany numer karty w postaci kodu QR powinien być odczytywany tylko ustaloną liczbę razy i umożliwiać dostęp tylko przez ograniczony czas (np. przez godzinę).

Bezpośr. inf. Ryszard Sobierski
AAT HOLDING

Integracja systemu RACS 5
z oprogramowaniem VMS XProtect firmy Milestone Systems

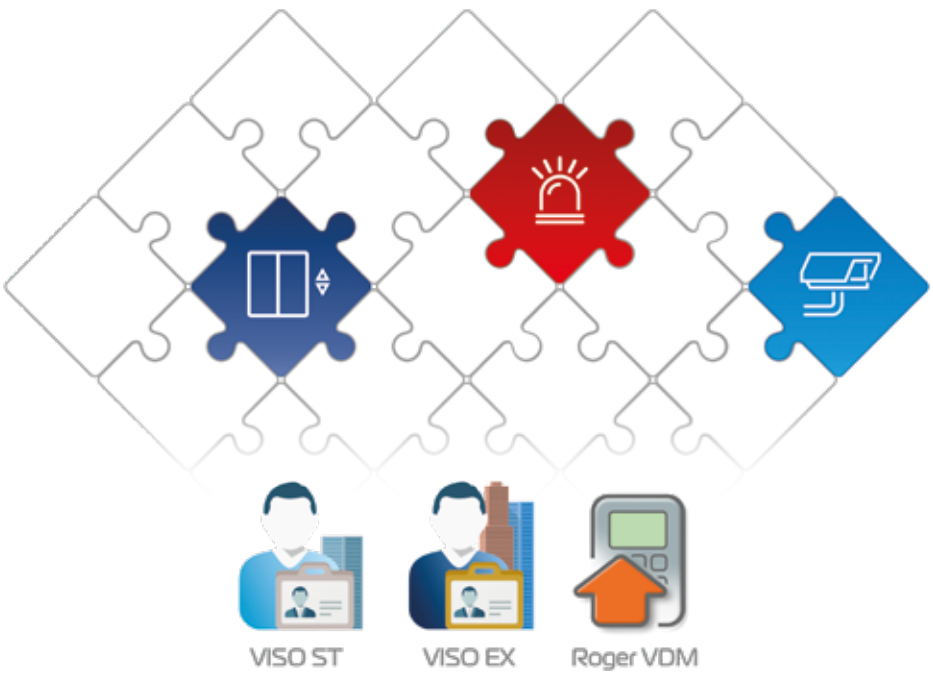
W kolejnej wersji systemu kontroli dostępu i automatyki budynkowej **RACS 5** (w wersji 5.6) umożliwiono integrację oprogramowania zarządzającego systemem kontroli dostępu z oprogramowaniem **VMS XProtect firmy Milestone Systems**.

Wdrożona koncepcja integracji umożliwia współpracę systemu kontroli dostępu z systemem VMS na dwa sposoby. W pierwszym z nich informacje dotyczące zdarzeń z systemu kontroli dostępu są przekazywane oprogramowaniu VMS, gdzie są prezentowane i przetwarzane na takich samych zasadach jak te, które pochodzą z innych systemów bezpieczeństwa budynku. W szczególności mogą być przedstawiane graficznie na mapach obiektu. Dodatkowo w tej formie współpracy możliwe jest wydawanie poleceń systemowi kontroli dostępu z poziomu oprogramowania VMS. W drugim ze sposobów oprogramowanie systemu kontroli dostępu może pobierać zdjęcia i filmy z systemu VMS podobnie jak z rejestratorów wizyjnych z systemu telewizji dozorowej. Dzięki integracji z oprogramowaniem VMS XProtect system RACS 5 może funkcjonować tam, gdzie wymagane są zaawansowane formy dozoru i monitorowania pracy systemu z udziałem pracowników ochrony prowadzących ciągły lub interwencyjny nadzór nad budynkiem, a także w miejscach, w których wymagana jest wizualizacja pracy całego systemu bezpieczeństwa w zintegrowanym środowisku wizyjnym.

Firma Milestone Systems jest czołowym producentem oprogramowania VMS, powszechnie rozpoznawalnym w branży wizyjnych systemów dozorowych i o rosnącej popularności na rynku polskim. Integracja oprogramowania VMS XProtect z systemem RACS 5 powiększa asortyment systemów bezpieczeństwa dostępnych na prężnie rozwijającym się rynku krajowych inwestycji biurowych.

Bezpośr. inf. ROGER

Oprogramowanie systemu RACS 5
w wersji 5.6



Dzięki najnowszej wersji oprogramowania system kontroli dostępu i automatyki budynkowej **RACS 5** ma nowe funkcje, z których najważniejsze to integracja programowa z systemem alarmowym **Galaxy firmy Honeywell** oraz integracja z oprogramowaniem zarządzającym systemem wizyjnym **VMS XProtect firmy Milestone Systems**. Dzięki integracji z systemem Galaxy użytkownicy systemu RACS 5 mogą sterować włączeniem w dozór stref alarmowych z poziomu czytników i klawiatur systemu kontroli dostępu, które podają jednocześnie aktualny stan powiązanych z nimi stref alarmowych. Informacje dotyczące zdarzeń z systemu alarmowego są wyświetlane w oknach służących do monitorowania pracy systemu kontroli dostępu i dopisywane do jego bazy danych. Połączenie z oprogramowaniem VMS XProtect jest dwukierunkowe i umożliwia zarówno pobieranie zdjęć i filmów z wizyjnego systemu dozorowego, jak i przesyłanie danych dotyczących zdarzeń z systemu kontroli dostępu do oprogramowania XProtect. Do innych nowych funkcji, jakie zyskujemy dzięki wersji 5.6, należy także czasowe nadawanie uprawnień użytkownikom systemu, automatyczne generowanie raportów z uwzględnieniem czasu przebywania użytkowników w poszczególnych częściach budynku oraz rozszerzona współpraca z Active Directory. Z jednej strony możliwe jest automatyczne blokowanie uprawnień nieaktywnych użytkowników usługi Active Directory do dostępu, a z drugiej przypisywanie użytkownikom uprawnień z poziomu Active Directory. W wersji 5.6 udostępniono również nową aplikację VISO Web, która umożliwia m.in. tworzenie raportów związanych z rejestracją czasu pracy.

Bezpośr. inf. ROGER

TL-SL1226P

przełącznik PoE+ do systemów dozoru wizyjnego

TL-SL1226P to niezarządzalny przełącznik IP zgodny ze standardem 802.3af/at PoE+. Są w nim 24 porty PoE o maksymalnej obciążalności równej 30 W i sumarycznym budżecie mocy równym 250 W. Jest wyposażony w dwa dodatkowe gniazda Combo SFP, każde o przepustowości 1 Gb/s.

Przełącznik TL-SL1226P został zaprojektowany specjalnie z myślą o cyfrowych systemach dozoru wizyjnego. Jego zastosowanie skraca czas instalacji kamer wchodzących w skład systemu i zmniejsza jej koszt. Można go wykorzystać do obsługi systemu dozorowego i innych aplikacji biurowych w małych i średnich firmach.

Praca wybranych portów w trybie *Extend* umożliwia transmisję danych oraz zasilanie metodą PoE kamer umieszczonych w dużych odległościach od przełącznika. Maksymalna długość kabla przy pracy w tym trybie wynosi 250 m. Tryb *Extend* jest przydatny w systemach służących do monitorowania rozległych obiektów.

Tryb *Priority* umożliwia przyznanie pierwszeństwa portom o numerach od 1 do 8. Gdy całkowity pobór mocy przekracza 250 W, funkcja inteligentnego zarządzania rozdziałem energii wyłącza zasilanie portów, które nie mają pierwszeństwa, tym samym chroniąc przełącznik przed przeciążeniem. Jednocześnie zachowana jest możliwość podglądu obrazów z wyznaczonych kamer i inne najważniejsze funkcje.

Z kolei tryb *Isolation* rozdziela ruch na wszystkich portach w celu eliminacji problemów związanych z podsłuchem i kopiowaniem danych oraz zapobieżenia powstawaniu burz broadcastowych.

Przełącznik TL-SL1226P nie wymaga konfiguracji czy instalacji oprogramowania. Wystarczy podłączyć go do systemu i podłączyć do niego urządzenia końcowe. Urządzenie jest gotowe do pracy zaraz po włączeniu zasilania.

Bezpośr. inf. TP-Link Polska

Większa wydajność rejestratorów NMS NVR

Dzięki zastosowaniu procesorów nowej generacji rejestratory **NMS NVR** oraz **stacje robocze NVSO** mają teraz większą wydajność. Rejestratory **NMS NVR 7-4U-II** (montowany w racku) i **NMS NVR 7-T-II** (wersja wolnostojąca, w obudowie typu *tower*) mogą nagrywać do 150 strumieni wizyjnych o rozdzielczości 1920 x 1080, wykorzystując kodek H.265. W przypadku korzystania z kodeka H.264 możliwy jest zapis do 120 strumieni przy równoczesnym wyświetlaniu maksymalnie 70 strumieni pomocniczych. Maksymalna rozdzielczość kamer to 4000 x 3000. Wszystkie jednostki umożliwiają podłączenie do trzech monitorów i równoczesną pracę wszystkich urządzeń z rozdzielczością 4K. Umożliwiają też podłączenie maksymalnie pięć dysków w celu zapisu materiału archiwalnego.

W przypadkach, w których wymagana jest instalacja dodatkowego oprogramowania, zaleca się stosowanie NVSO. Jest to platforma otwarta, która nie ma powłoki *shell* i ma wyłączoną część zabezpieczeń.

Rejestratory NMS NVR i stacje robocze NVSO są rekomendowane do systemów z dużą liczbą kamer oraz wieloma punktami nadzoru wymagającymi przesyłania strumieni wizyjnych do wielu użytkowników.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Nowe funkcje
rejestratorów NOVUS z serii 4000

W nowej wersji oprogramowania układowego **8- i 16-kanałowych rejestratorów NOVUS** z **serii 4000** dostępne są nowe funkcje powiązane z rozpoznawaniem twarzy. Funkcje te – *Repeat visitors* oraz *Face attendance* – zostały wyodrębnione w menu AI. Pierwsza z nich pozwala na ustalenie, czy w zdefiniowanym przedziale czasowym dana osoba pojawiła się na obrazach z wyselekcjonowanych kamer, a jeśli tak, to ile razy miało to miejsce. Punktem odniesienia może być wizerunek twarzy z bazy danych rejestratora, ale może to być również zdjęcie w formie pliku graficznego. Druga z funkcji – *Face attendance* – może działać w przypadku całego zbioru lub pojedynczo zdefiniowanych twarzy i umożliwia uzyskanie w graficznej formie informacji o tym, kiedy dana osoba pojawiała się w polu widzenia kamer i została rozpoznana. Tym samym, gdy podane są godziny aktywności, otrzymujemy informację o liczbie spóźnień oraz przedwczesnych wyjść w określonym przedziale czasowym, którego długość jest ograniczona jedynie wielkością archiwum. Bez dodatkowych urządzeń administrator systemu może np. szybko zweryfikować częstość i punktualność patroli, a także aktywność wybranych osób w miejscu widocznym na obrazach z kamer systemu wizyjnego. Wyselekcjonowane dane mogą być wyeksportowane do pliku CSV do dalszej obróbki.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Kamera PNM-9085RQZ firmy Hanwha Techwin
unowocześniania ciąg dalszy

Firma **Hanwha Techwin** dodała do asortymentu kamer z cieszącej się ogromną popularnością serii P nowy model – **PNM-9085RQZ**. To wielokierunkowa kamera o rozdzielczości 20 megapikseli, z wbudowanymi oświetlaczami IR o zasięgu 30 m dla każdego z układów optycznych. Jest wyposażona w cztery obiektywy o kącie widzenia regulowanym zdalnie w zakresie od 4,13 mm do 9,4 mm. Nowością jest obsługa sterowania PTRZ (*pan*, *tilt*, *rotate*, *zoom*). Litera *R* (od *rotate*) oznacza, że obiektywy w kamerze mogą poruszać się po okręgu i mogą być zmieniane w każdej chwili bez konieczności otwierania kamery. W kamerze umieszczono chipset Wisenet 5, znany wszystkim z serii X, który charakteryzuje się wysoką wydajnością pracy oraz umożliwia instalowanie dodatkowych aplikacji analitycznych, za co otrzymał nagrodę High-Tech Safety Industry Product and Technology Award.

Każdy z czterech sensorów może wytwarzać 30 albo 60 obrazów na sekundę. Funkcja WDR pozwala na rozszerzenie zakresu dynamiki obrazu do 120 dB. Dodatkowo jest możliwość ustawiania różnych funkcji do analizy treści obrazu dla każdego z sensorów z osobna, niezależnie od tego, co jest ustawione w innym sensorze. Można wybrać wiele funkcji analitycznych, w tym wykrywanie prób sabotowania pracy kamery, zbyt długiego przebywania osób w określonej strefie, przekroczenia wirtualnej linii, wejścia do wyznaczonej strefy i wyjścia z tej strefy, pozostawienia lub zabrania przedmiotu, poruszania się obiektów w niedozwolonym kierunku, a także rozpoznawanie twarzy.

Kamerę PNM-9085RQZ można łatwo i szybko zainstalować i nie ma potrzeby regulacji obiektywów podczas instalacji. Koszty zakupu są niższe dzięki zastosowaniu jednego urządzenia zamiast czterech oddzielnych i jednej licencji VMS. Kamera nadaje się do użytku na zewnątrz pomieszczeń, ponieważ jest wandaloodporna i przystosowana do pracy w trudnych warunkach pogodowych. Podczas instalacji kamer wieloczujnikowych zużywa się mniej przewodów i sprzętu montażowego oraz wymagana jest mniejsza liczba portów w przełączniku IP i licencji w aplikacji VMS ze względu na pojedynczy adres IP każdej z takich kamer.

Kamery PNM-9085RQZ znajdują zastosowanie w systemach monitoringu miejskiego lub komercyjnych. Nawet korzystając z tylko jednego takiego urządzenia, można monitorować obszar szerszy niż w przypadku zastosowania innej kamery.

Bezpośr. inf. Hanwha Techwin Europe
Diamond Business Park, budynek B
ul. Posag 7 Panien 1
02-495 Warszawa
www.hanwha-security.eu/pl
htesecurity@hanwha.com
+48 518 346 039

Dwudziesta międzynarodowa konferencja na temat gaszenia mgłą wodną – IWMC

Dwudziesta międzynarodowa konferencja na temat gaszenia mgłą wodną (**International Water Mist Conference – IWMC**) odbędzie się **7 i 8 października 2020 r**. w hotelu Regent w Warszawie.

Poświęcona temu wydarzeniu strona internetowa będzie funkcjonować od 15 maja. W celu ułatwienia dostępu będzie na nią prowadził link zamieszczony na stronie głównej IWMA (www.iwma.net). Od 15 maja prelegenci, inni uczestnicy i sponsorzy będą mogli zarejestrować się online.

Do 15 lipca IWMA będzie oferować zmniejszenie opłaty za uczestnictwo w konferencji. Będą też specjalne oferty dla studentów, organizacji wspierających, a także dla delegatów z Polski.

Uczestnicy, a wśród nich wystawcy, znajdą na stronie internetowej IWMC wszystkie informacje o tym, jak dojechać na miejsce, w którym odbędzie się konferencja, jak zarezerwować kwaterę i jak przetransportować towary. Będzie dostępny również ogólny opis z najważniejszymi informacjami dotyczącymi wydarzenia.

Program IWMC będzie na stronie poświęconej konferencji od 1 lipca.

Kontakt z prasą:
Bettina McDowell
tel.: +49 (0) 40 35085-215
faks: +49 (0) 40 35085-80
e-mail: mcdowell@iwma.net

Tłumaczenie: redakcja

POLON-ALFA

PROJEKTUJEMY zgodnie ze sztuką

SYSTEMY SYGNALIZACJI POŻAROWEJ

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

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

SYSTEM DETEKCJI GAZÓW SDG 6000

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

V edycja **Seminarium Branży Elektronicznych Systemów Bezpieczeństwa** i konkursu o tytuł **Mistrza Elektronicznych Systemów Bezpieczeństwa**

W dniu 04.02.2020 roku na terenie **Instytutu Systemów Elektronicznych (ISE) Wydziału Elektroniki (WEL) Wojskowej Akademii Technicznej (WAT)** odbyła się już **V edycja Seminarium Branży Elektronicznych Systemów Bezpieczeństwa (SBESB)** połączona z konkursem o miano **Mistrza Elektronicznych Systemów Bezpieczeństwa** dla studentów głównie specjalności Inżynieria Systemów Bezpieczeństwa (ISB) kierunku Elektronika i Telekomunikacja (EiT). Seminarium oraz konkurs dla studentów zostały zorganizowane przy znaczącym udziale firm, z którymi WAT współpracuje od wielu lat. W konkursie tej edycji, w którym startowało ponad 40 studentów, wyłoniono 10 laureatów. Zwycięzcą został inżynier Przemysław Bojaronus student V roku specjalności ISB na kierunku EiT, tytuł pierwszego i drugiego wicemistrza wywalczyli odpowiednio Rafał Kulik i Bartosz Plewko, a pozostałych 7 laureatów wyróżniono nagrodami rzeczowymi. W grupie tej znaleźli się: inż. Kamil Krzemiński, Krzysztof Świątkowski, Maciej Kalinowski, Hubert Skrucha, inż. Łukasz Grzegorczyk, inż. Mateusz Nadolny oraz inż. Karolina Skiba. Studenci mieli odpowiedzieć na 20 pytań testowych na temat elektronicznych systemów bezpieczeństwa. Pytania przygotowała kadra dydaktyczna ISE przy współudziale Polskiej Izby Systemów Alarmowych (PISA), głównie na podstawie treści kształcenia przekazywanych w przedmiotach specjalistycznych ujętych w planie studiów. Zwycięzcy i wyróżnieni otrzymali statuetkę, pamiątkowe dyplomy oraz upominki ufundowane przez firmy uczestniczące w seminarium. W tegorocznej V edycji udział wzięło 9 firm i organizacji: AAT HOLDING S.A., Bosch, ICS Polska, ID Electronics, Janex International, POLON-ALFA, Pulsar, Satel, Schrack Seconet, oraz reprezentant tej branży w Krajowej Izbie Gospodarczej jakim jest Polska Izba Systemów Alarmowych (PISA). W spotkaniu uczestniczyli dziekan prof. dr. hab. inż. Andrzej Dobrowolski oraz prodziekan ds. naukowych dr. hab. inż. Mateusz Pasternak. Seminarium rozpoczęła prezentacja działalności i osiągnięć Koła Naukowego Elektroników (KNE) WAT, a następnie swoje prezentacje przedstawili przedstawiciele zaproszonych firm. Podczas spotkania w uznaniu

za zaangażowanie w działalność KNE, na wniosek przewodniczącego sekcji Elektronicznych Systemów Bezpieczeństwa KNE WAT, dziekan WEL wyróżnił dyplomem Sebastiana Brodę, zastępcę dyrektora Działu Serwisu w firmie AAT HOLDING. Po zakończeniu seminarium na strzelnicy sportowej Studium Wychowania Fizycznego WAT odbył się turniej strzelecki dla pracowników firm biorących udział w seminarium o puchar Dziekana WEL. Najlepszym strzelcem wśród uczestników konkursu okazał się Pan Dariusz Okrasa dyrektor firmy ID Electronics. Współpraca WEL z firmami branżowymi przynosi wymierne korzyści obydwu stronom. Firmy od lat doposażają w sprzęt elektronicznych systemów bezpieczeństwa laboratoria ISE WEL i chętnie zatrudniają naszych absolwentów oraz organizują staże i praktyki dla naszych studentów.

Dr hab. inż. Jacek Paś, prof. WAT

Bezpieczna identyfikacja zbliżeniowa
dzięki usłudze LEGIC Connect

Dariusz Kafka

W dzisiejszych czasach, zarówno w działalności biznesowej, jak i w życiu prywatnym, często zachodzi potrzeba skorzystania z wirtualnych poświadczeń przeznaczonych do natychmiastowego użycia, tworzonych ad hoc na smartfonach lub innych urządzeniach mobilnych. LEGIC Connect jest usługą programową, która ma do tego służyć

Usługę LEGIC Connect można łatwo realizować w istniejącej infrastrukturze telekomunikacyjnej. Zapewnia ona identyfikację użytkowników podczas transakcji przeprowadzanych z użyciem urządzeń mobilnych, wymagających tworzenia doraźnych poświadczeń do natychmiastowego wykorzystania. Usługa jest dostępna na całym świecie i jest bezpieczna dzięki szyfrowaniu transmitowanych danych metodą *end-to-end*.

Dzięki usłudze LEGIC Connect oraz istniejącej infrastrukturze telekomunikacyjnej smartfon może pełnić wiele funkcji. Może służyć do otwierania drzwi w budynkach, uruchamiania samochodów, stanowić identyfikator personalny w systemach rejestracji czasu pracy, być elektronicznym biletem kolejowym etc. By zrealizować te i tym podobne funkcje, do komunikacji z urządzeniami brzegowymi wykorzystuje się łącza Bluetooth oraz NFC dostępne w każdym współczesnym smartfonie.

Dzięki rozwojowi IoT LEGIC Connect może znaleźć różne zastosowania. Elementem zapewniającym bezpieczne uwierzytelnienie jest moduł logiczny SE zainstalowany w każdym z terminali. LEGIC Connect może służyć na przykład do uwierzytelniania personelu szpitalnego w celu uzyskiwania przez pracowników dostępu do wydzielonych pomieszczeń, aparatury medycznej czy szafek z lekarstwami. Dane dostępowe mogą być przechowywane w chmurze i udostępniane urządzeniom brzegowym w razie potrzeby. Dalszą poprawę bezpieczeństwa można uzyskać za pomocą aplikacji służących do rozpoznawania twarzy i odcisków palców, dostępnych w smartfonach. Dodatkowym zabezpieczeniem może być żądanie wprowadzenia ważnego kodu PIN. Wszystkie te funkcje można zrealizować z użyciem klasycznego smartfonu z aplikacją LEGIC Connect.

Jak działa LEGIC Connect

Na poniższym rysunku przedstawiony jest schemat wyjaśniający zasadę działania systemu uwierzytelniającego wykorzystującego LEGIC Connect.

Rys. 1. Wyjaśnienie zasady działania usługi LEGIC Connect

Jak wynika ze schematu, jednostka nadrzędna systemu z usługą LEGIC Connect komunikuje się ze smartfonem poprzez szyfrowany kanał utworzony w istniejącej infrastrukturze telekomunikacyjnej. Odbiorcą danych jest aplikacja mobilna zainstalowana w smartfonie. Dane dla jednostki brzegowej są przekazywane za pośrednictwem łącza Bluetooth lub NFC w smartfonie. W celu ułatwienia pracy projektantów systemów uwierzytelniających i autorów aplikacji na urządzenia mobilne udostępniono specyfikację API i narzędzie aplikacyjne Mobile SDK.

Podstawą bezpieczeństwa w systemie z usługą LEGIC Connect jest szyfrowanie danych metodą *end-to-end* na trasie między jednostką nadrzędną a modułem logicznym zawartym w układzie scalonym LEGIC Reader zainstalowanym w urządzeniu brzegowym. Szyfrowanie połączenia telekomunikacyjnego jest pomocne, jednak ma drugorzędne znaczenie. Siła tego systemu bierze się z szyfrowania metodą *end-to-end*.

Łącze RFID, Bluetooth i moduł szyfrujący w jednym układzie scalonym

Układ SM-6300 jest wykorzystywany przy produkcji czytników RFID zgodnych ze światowymi standardami. Układ obsługuje karty zbliżeniowe w formatach LEGIC, NXP MIFARE i HID iCLASS, a także aplikacje wykorzystujące pliki LEGIC NEON. Szyfrowanie metodą *end-to-end* jest uzyskiwane dzięki modułowi logicznemu SE wbudowanemu w ten układ.

Układ SM-6300 zawiera łącza RFID, Bluetooth i NFC, które w połączeniu ze wspomnianym modułem SE zapewniają szyfrowanie komunikacji między smartfonem a urządzeniem IoT. Ze względu na wysoki poziom bezpieczeństwa układ może być stosowany m.in. w systemach kontroli dostępu, bankomatach, systemach do zarządzania pracą biur, wypożyczalniach samochodów. Ułatwieniem dla konstruktorów urządzeń zabezpieczających są jego małe rozmiary (8 mm x 8 mm x 1,1 mm). Układ nie wymaga stosowania elementów zewnętrznych, takich jak mikrokontroler czy rezonatory kwarcowe.

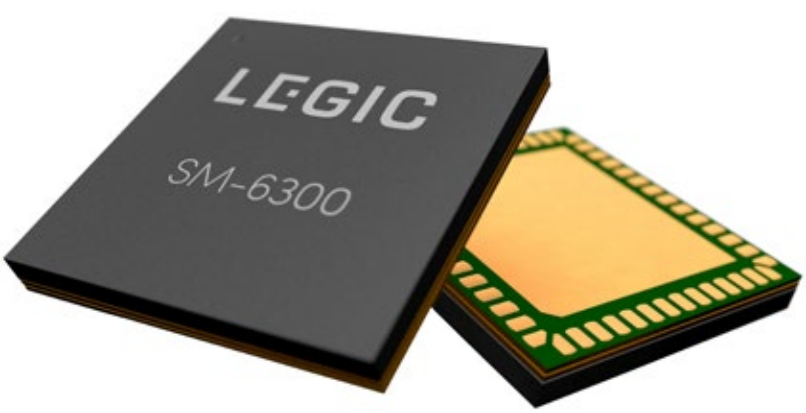
Dystrybucja kluczy szyfrujących

W układzie SM-6300 zastosowano sprzętową metodę przechowywania i dystrybucji danych specyficznych dla użytkowników systemu oraz kluczy szyfrujących. Do współpracy z aplikacją LEGIC ORBIT wstępnie zaprogramowany został bezpieczny klucz transportowy. Podczas transmisji danych szyfrowanej metodą *end-to-end* może być wykorzystana chmura LEGIC i protokół Trusted Service.

Platforma bezpieczeństwa LEGIC

Do tworzenia systemów uwierzytelniających wykorzystujących usługę LEGIC Connect służy platforma sprzętowa i programowa LEGIC, w skład której wchodzą układy scalone do budowy czytników i inteligentnych kart zbliżeniowych, narzędzia do zarządzania kluczami, a także usługa LEGIC Connect realizowana z użyciem protokołu Trusted Service i narzędzia aplikacyjnego Mobile SDK.

Dzięki wszechstronności i bezproblemowej współpracy tych komponentów można szybko i łatwo stworzyć wiele aplikacji wykorzystujących inteligentne karty zbliżeniowe i smartfony.



Fot. 1 . LEGIC chip SM-6300

Efekty i korzyści

W systemach uwierzytelniających, w których wykorzystywana jest usługa LEGIC Connect, można stosować karty zbliżeniowe w formatach LEGIC, NXP MIFARE i HID iCLASS. Niski pobór prądu przez układy SM-6300 umożliwia

Fot. 2. Zestaw ewaluacyjny LEGIC EK-6300

zastosowanie ich w systemach z zasilaniem bateryjnym. Jednoczesne przeszukiwanie kanałów radiowych Bluetooth, NFC i RFID zapewnia bardzo szybkie nawiązywanie połączenia z elementem uwierzytelniającym. Dzięki narzędziu Mobile SDK można tworzyć aplikacje do bezprzewodowej transmisji plików LEGIC NEON lub wysyłania poleceń do systemów klienckich z wykorzystaniem usług LEGIC Trusted Service. Specyficzne dane użytkowników oraz klucze szyfrujące są przechowywane w bezpiecznych modułach SE wchodzących w skład układu scalonego SM-6300.

Wszystkie wymienione powyżej właściwości i zalety systemów zbudowanych z wykorzystaniem usługi LEGIC Connect umożliwiają spełnienie wymagań dotyczących bezpieczeństwa Common Criteria na poziomie EAL5+.

Zestaw uruchomieniowy EK-6300

Dla ułatwienia pracy konstruktorów sprzętu i projektantów systemów bazujących na usłudze LEGIC Connect stworzono zestaw uruchomieniowy, w skład którego wchodzi płytka ewaluacyjna EVB-6300 z układem scalonym SM-6300 oraz zestaw programistyczny DKS-6000 z przykładami aplikacji wyjaśniającymi sposób wykorzystania oprogramowania układowego OS50.

Szczegółowe dane na temat zestawu uruchomieniowego można znaleźć na stronie firmy LEGIC (https://www.legic.com/security-platform/reader-ics/sm-6300/).

Dariusz Kafka
LEGIC Identsystems
e-mail: dariusz.kafka@legic.com

Unowocześnianie miast

dzięki postępowi w dziedzinie techniki

Axis Communications

Coraz więcej mówi się o rozwoju miasta w kontekście jego przemiany w tzw. inteligentne miasto (*smart city*). Najważniejszym motorem tej transformacji jest technika. To właśnie ona może sprawić, że aglomeracje staną się bezpieczniejsze. W 2020 roku najbardziej przyczyni się do tego analiza w urządzeniach brzegowych oraz wykorzystanie chmur prywatnych i hybrydowych

Spośród trendów rozwojowych, które mogą odegrać najważniejszą rolę w tym roku, oprócz techniki na pierwszy plan wysuwają się także kwestie regulacyjne związane z bezpieczeństwem oraz prywatnością. Istotne będą także możliwości samych urządzeń, w tym rosnąca moc obliczeniowa.

Przetwarzanie danych w urządzeniach brzegowych

Obecnie do sieci podłączone są już miliardy urządzeń, a liczba ta z roku na rok gwałtownie rośnie. Wraz z nią rośnie także dynamika obliczeń i analizy w urządzeniach brzegowych. Wynika to głównie z właściwości urządzeń i stawianych im wymagań. Aby spełniać swoje role, obecnie muszą one mieć możliwość natychmiastowej, samodzielnej reakcji. Doskonałym przykładem są autonomiczne auta – aby mogły

skutecznie zauważać potencjalne zagrożenie, np. obiekt znajdujący się na drodze, muszą podejmować decyzje w ułamku sekundy. Nie byłoby to możliwe, gdyby dane były wysyłane z samochodu do centrum przetwarzania danych. W takim przypadku proces przetwarzania i analizy byłby zbyt długi i uniemożliwiłby skuteczną reakcję w odpowiednim czasie.

Podobnie jest w przypadku innych urządzeń, np. kamer. – *Aby miasto mogło stać się prawdziwym* smart city, *systemy wizyjne powinny umożliwiać natychmiastowe reakcje, a nie być tylko wsparciem, np. w postępowaniu dowodowym. Przejście do skutecznego działania będzie możliwe tylko wówczas, gdy kamery będą samodzielnie dokonywały analizy potencjalnych zagrożeń i automatycznie informowały o nich odpowiednie służby* – podkreśla Konrad Badowski, Business Relationship Manager z Axis Communications.

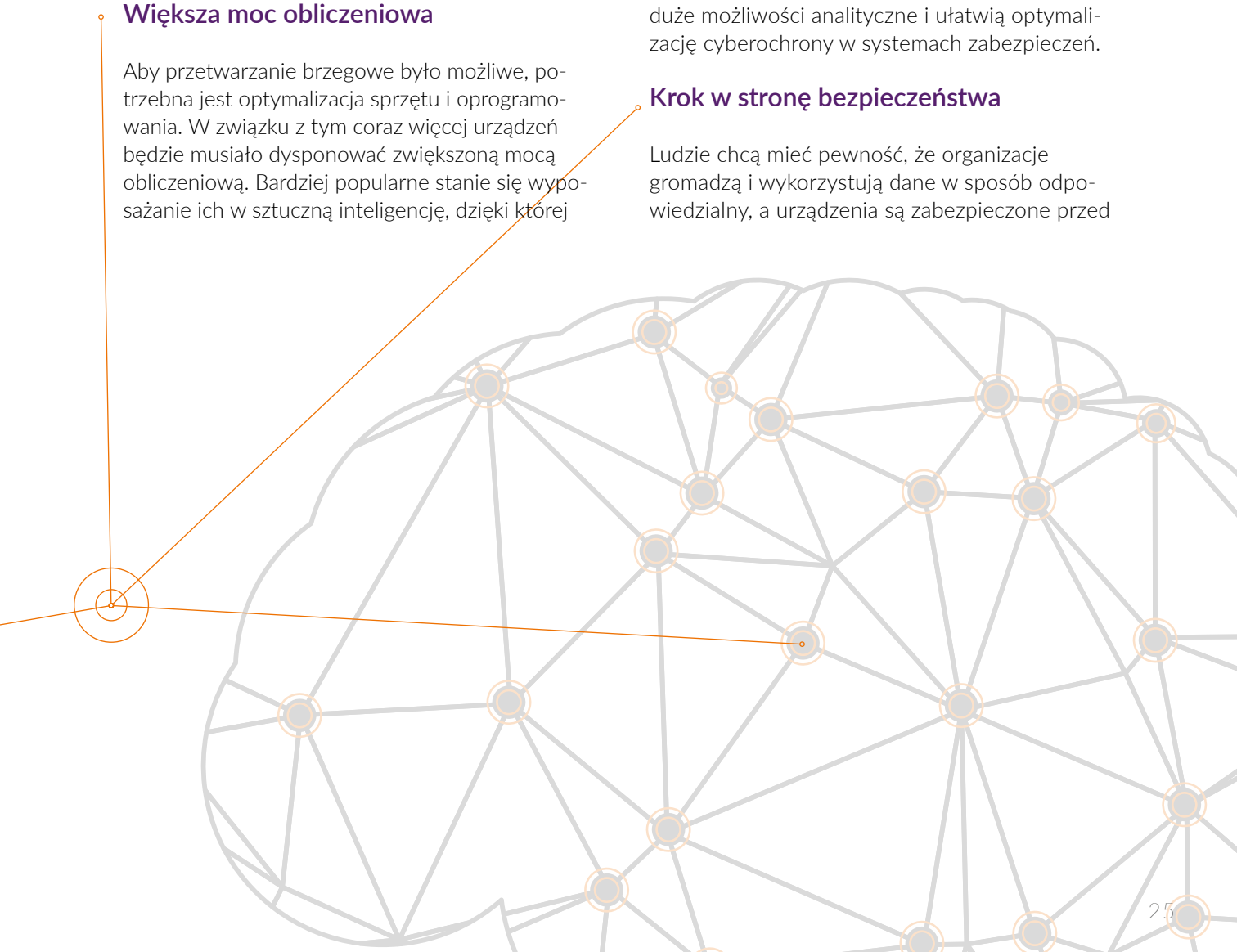
Większa moc obliczeniowa

Aby przetwarzanie brzegowe było możliwe, potrzebna jest optymalizacja sprzętu i oprogramowania. W związku z tym coraz więcej urządzeń będzie musiało dysponować zwiększoną mocą obliczeniową. Bardziej popularne stanie się wyposażanie ich w sztuczną inteligencję, dzięki której będą mogły się uczyć. Już w tej chwili coraz więcej firm zauważa, że jest to element niezbędny do ich rozwoju. Wyzwaniem może jednak okazać się stworzenie nowych, „lżejszych" modeli, które będą spełniać swą funkcję, wykorzystując mniej pamięci i mocy obliczeniowej.

Obecnie w transporcie publicznym kamery, które mają własne procesory i aplikacje, mogą analizować zachowanie kierowcy, np. prowadzącego autobus. Z kolei kamery zainstalowane na zewnątrz pojazdów komunikacji miejskiej mogą działać jak lusterka, pomagając prowadzącemu umiejętnie i bezpiecznie wykonywać skomplikowane manewry. W niedalekiej przyszłości kamery będą także samodzielnie ustalały, czy podnoszone ze sklepowych półek produkty nie są kradzione, oraz informowały o ewentualnych nieprawidłowościach w dostawie przesyłek. Umożliwiają to procesory nowej generacji, np. Artpec 7 firmy Axis Communications, które mają duże możliwości analityczne i ułatwią optymalizację cyberochrony w systemach zabezpieczeń.

Krok w stronę bezpieczeństwa

Ludzie chcą mieć pewność, że organizacje gromadzą i wykorzystują dane w sposób odpowiedzialny, a urządzenia są zabezpieczone przed



cyberprzestępcami. W celu ochrony danych potrzebne jest między innymi zabezpieczenie urządzeń brzegowych. Zasadnicze znaczenie ma w tym przypadku zabezpieczenie całego łańcucha dostaw. Chociaż umieszczanie chipów szpiegujących w sprzęcie na etapie produkcji już jest możliwe, lub będzie możliwe w przyszłości, o wiele łatwiej jest zainstalować oprogramowanie szpiegujące w urządzeniu poprzez jego aktualizację niż podczas produkcji. Przy zwiększonej ilości danych przetwarzanych w urządzeniach brzegowych cyberbezpieczeństwo stanie się szczególnie istotne. Podstawą bezpiecznego systemu jest zarządzanie poszczególnymi urządzeniami, całym „cyklem życia" tego systemu i jego wszystkimi elementami, tzn. sprzętem i oprogramowaniem, a także użytkownikami.

W inteligentnym mieście oprócz cyberbezpieczeństwa ważne będzie poszanowanie prywatności. – *Już teraz prężnie rozwija się technika, dzięki której możliwe jest respektowanie prawa do pozostania anonimowym, także w kontekście monitoringu miejskiego. Techniki korekcji obrazu pozwalają na poprawienie rejestrowanego materiału wizyjnego tak, aby np. sylwetki ludzi były maskowane, zapewniając tym samym zgodność z przepisami. Istnieje także możliwość udostępnienia takiego materiału wizyjnego – nagrań, które nie naruszają prywatności – podmiotowi zewnętrznemu* – podkreśla Konrad Badowski. Ze względu na wagę kwestii związanych z ochroną prywatności można spodziewać się, że tego typu rozwiązania techniczne będą rozwijane także w kolejnych latach.

Regulacje a technika

Prawne uregulowanie nowych technik jest często trudne, jeśli nie niemożliwe. Właściwie lepiej powiedzieć, że próbuje się uregulować ich użycie w konkretnych przypadkach. Na przykład rozpoznawanie twarzy w trakcie odprawy w porcie lotniczym może znacznie przyspieszyć tę czynność i być całkiem nieszkodliwym, a wręcz pożądanym ułatwieniem, jednak użycie tego samego narzędzia w celu śledzenia obywateli może budzić wątpliwości związane z ingerencją w prywatność. Choć technika jest dokładnie taka sama, przypadek użycia okazuje się zupełnie inny.

Rozporządzenie RODO, które weszło w życie w 2018 roku, w dużym stopniu zmieniło sposób rozumienia prywatności i uświadomiło wszystkim nieuchronność wprowadzenia regulacji związanych z ochroną danych osobowych. Regulacje powinny nadążyć za postępem technicznym, ale najważniejsza będzie ich analiza pod kątem konkretnych przypadków, tak aby móc tworzyć prawo uwzględniające określone zastosowania urządzeń z korzyścią dla obywateli.

Różnorodność sieci

Bezpośrednim skutkiem zawiłości związanych z regulacjami, prywatnością i bezpieczeństwem na przełomie ostatnich dwóch dekad jest zauważalne odchodzenie od całkowicie otwartej sieci. W pewnym zakresie analizowanie, przechowywanie i przesyłanie danych z wykorzystaniem Internetu, np. w usługach, w których wykorzystuje się chmury publiczne, nie zmieni się, jednak coraz bardziej popularne będą chmury hybrydowe i prywatne. Zauważalny jest wzrost liczby „inteligentnych wysp", gdzie systemy do konkretnych zastosowań mają bezpośrednie połączenia z innymi systemami współzależnymi.

Choć niektórzy zwracają uwagę na to, że odejście od otwartych modeli jest niepożądane, przekonujące mogą okazać się argumenty dotyczące bezpieczeństwa i ochrony danych. Ponadto jedną z wymienianych korzyści otwartości sieci jest uczenie się przez komputery – przy założeniu, że jest ono możliwe tylko dzięki korzystaniu przez nie z wielkich zbiorów danych. Obecnie modele sieciowe dostosowane do konkretnych aplikacji korzystają ze stosunkowo niewielkiej ilości danych. Na przykład model systemu stworzony przez firmę Axis Communications do monitorowania ruchu ulicznego zawierający 7000 przykładowych zdjęć umożliwił zmniejszenie liczby fałszywych alarmów podczas wykrywania wypadków przez kamery aż o 95 procent.

Axis Communications

KRAJOWE CENTRUM MONITORINGU

Dostawca rozwiązań dla Agencji Ochrony

Outsourcing - Pracujemy tylko dla branży ochrony.
Ograniczamy koszty i wspieramy rozwój nowych usług.

Dla Twojego klienta jesteśmy niewidoczni!

Outsourcing - gwarantujemy pełne bezpieczeństwo biznesowe

Korzystamy z nowoczesnych rozwiązań technologicznych. Dysponujemy wykwalifikowaną kadrą operatorów, handlowców, informatyków, techników oraz administratorów. Posiadamy status USI oraz specjalistyczną infrastrukturę. Zapewniamy wysoki poziom cyberbezpieczeństwa – mamy własną serwerownię, zapasowe centrum danych oraz niezależność energetyczną i teletechniczną.

Bierzemy na siebie największe biznesowe problemy branży ochrony.

Współpraca z nami to szereg wymiernych korzyści

- Zwiększenie rentowności – zyskanie nawet 80% oszczędności kosztów
- Zmniejszenie ryzyka biznesowego – przeniesienie odpowiedzialności za zlecone usługi
- Pozyskanie profesjonalnego wsparcia – eksperta w branży ochrony
- Szansa na poszerzenie zakresu swoich usług
- Dostęp do nowoczesnych technologii i skutecznego oprogramowania

01 Outsourcing Centrum Monitorowania Alarmów

02 Outsourcing video-ochrony

03 Outsourcing – nadzór nad ochroną fizyczną

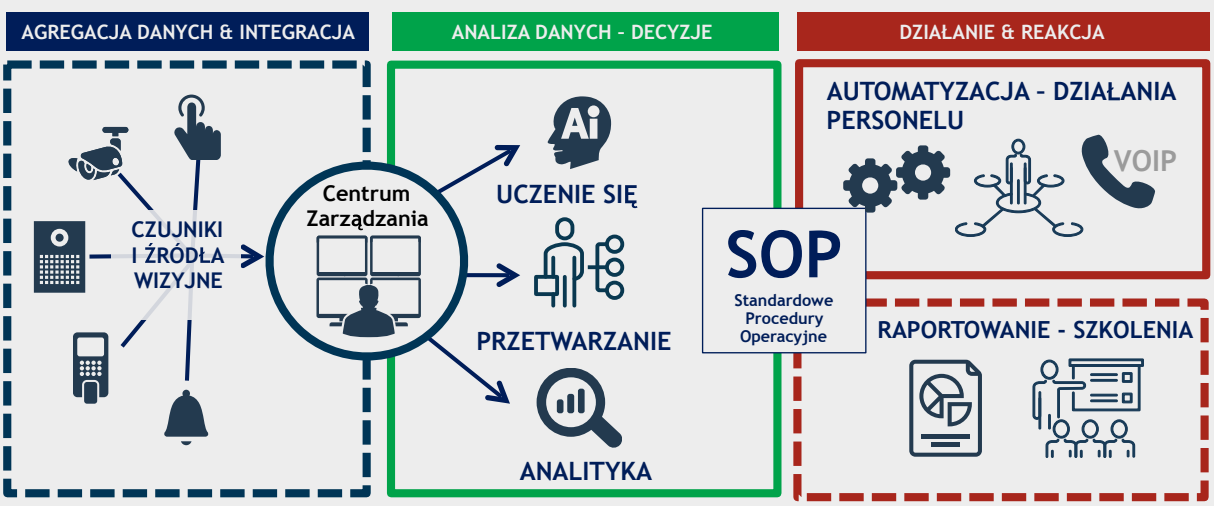
www.**krajowe**centrum**monitoringu**.pl +48 22 100 41 11 kontakt@kcm24.pl

Teleste S-AWARE
system świadomości sytuacyjnej

Dariusz Łabędzki

Żyjemy w czasach, w których informacje są na wagę złota. Jesteśmy otoczeni urządzeniami i systemami, które są coraz bardziej złożone i generują coraz więcej danych różnego typu. To powoduje, że efektywne zarządzanie nimi staje się coraz trudniejsze i coraz bardziej kosztowne. Podejmowanie właściwych decyzji w różnych sytuacjach jest uwarunkowane uświadomieniem sobie ich specyfiki

Innowacyjne rozwiązanie S-AWARE firmy Teleste umożliwia gromadzenie i analizowanie informacji na temat każdego niepokojącego zdarzenia, które pochodzą z różnych źródeł, oraz zarządzanie nimi. Dzięki temu właściwe identyfikowanie potencjalnych i zaistniałych zagrożeń jest szybsze i bardziej efektywne, co umożliwia kontrolę i zarządzanie, ułatwia pracę personelu i poprawia funkcjonowanie obiektu. Zastosowanie tzw. systemu świadomości sytuacyjnej S-AWARE firmy Teleste powoduje, że w przypadku zaistnienia sytuacji kryzysowej odpowiednie informacje docierają do odpowiednich osób lub jednostek we właściwej formie i właściwym czasie. S-AWARE umożliwia integrację i zarządzanie różnego typu systemami – bezpieczeństwa, informacyjnymi, a także niezwiązanymi z bezpieczeństwem obiektowym, np. produkcyjnymi. Zebrane dane są udostępniane z użyciem jednego graficznego interfejsu użytkownika, za którego pośrednictwem można także zarządzać incydentami i który można bardzo swobodnie konfigurować.



Rys. 1. S-AWARE – gromadzenie danych oraz zarządzanie incydentami

Gromadzenie danych

Platforma S-AWARE umożliwia pozyskiwanie różnego rodzaju danych z dowolnej liczby czujników, urządzeń, a także aplikacji działających w obiekcie. Do tych danych mogą należeć np. obrazy z kamer, informacje o alarmach, informacje o lokalizacji osób, informacje pochodzące z systemów kontroli dostępu, systemów wykrywania włamań, systemów analizy treści obrazu itp. Mogą one pochodzić także z systemów, które nie są związane z bezpieczeństwem obiektowym, np. z modułów automatyki przemysłowej bądź systemów trzecich przeznaczonych do przechowywania różnego typu danych.

Analiza danych, sztuczna inteligencja i rozpoznawanie zdarzeń

Dzięki S-AWARE możliwe jest automatyczne zbieranie i łączenie danych po to, by na ich podstawie, z wykorzystaniem między innymi sztucznej inteligencji, rozpoznawać zdarzenia i łańcuchy zdarzeń, a także określać ważność zdarzeń.

Automatyzacja pracy (organizacja zadań) z użyciem skryptów

Platforma S-AWARE pozwala wstępnie definiować procedury dotyczące przebiegu pracy (*workflow*) oraz standardowe procedury operacyjne (SOP), które powinny być realizowane przez personel operacyjny w przypadku wystąpienia konkretnych, określonych zdarzeń, a także zdarzeń niespodziewanych. Proces aktywowania procedur może być zautomatyzowany, co pozwala na znaczne skrócenie czasu reakcji personelu na konkretne zdarzenia i zwiększenie efektywności działania. Ponadto system umożliwia wyświetlanie informacji statusowych dotyczących poszczególnych spraw lub zdarzeń, które zostały wygenerowane automatycznie (np. zdarzeń alarmowych) lub przez obsługę systemu. Mogą one być przypisywane odpowiednim jednostkom, a ich przepływ może być monitorowany.

Komunikacja ze zdalnymi i mobilnymi systemami oraz interesariuszami

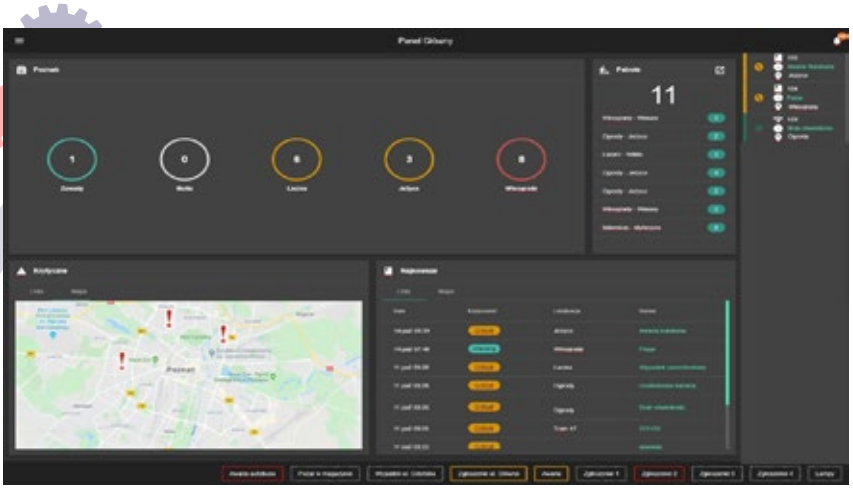
S-AWARE pozwala na niezakłócone komunikowanie się patroli, zdalnych systemów i centrów dowodzenia. Platforma udostępnia narzędzia (takie jak komunikator czy poczta elektroniczna), które umożliwiają niezawodną i bezpieczną wymianę informacji między interesariuszami w czasie rzeczywistym.

Zarządzanie dochodzeniami

S-AWARE może pomóc w prowadzeniu dochodzeń w związku z zaistniałymi zdarzeniami poprzez przechowywanie informacji dowodowych, jak również śledzenie ich przepływu. Platforma umożliwia także gromadzenie różnego rodzaju dowodów cyfrowych.

Raportowanie i szkolenie

Platforma S-AWARE przechowuje i rejestruje informacje ze wszystkich komponentów systemu, śledzi pojawianie się zdarzeń w systemie, ich przebieg oraz reakcje personelu, a także umożliwia swobodne wyszukiwanie zdarzeń i generowanie raportów, które mogą być tworzone ręcznie lub automatycznie, zgodnie z harmonogramem. Raporty te mogą być wykorzystywane podczas przeprowadzania standardowych analiz funkcjonowania systemu i działania personelu, a także podczas prowadzenia szkoleń. Do raportów można dołączać np. instrukcje, zdjęcia, filmy, linki do stron internetowych bądź e-maile. W swojej warstwie szkoleniowej system umożliwia również tworzenie scenariuszy działań na wypadek potencjalnych zdarzeń. Scenariusze te mogą być wykorzystywane podczas szkolenia personelu, dzięki czemu nabierze on umiejętności podejmowania szybkich i właściwych decyzji. System raportowania umożliwia także chronologiczne odtworzenie przebiegu zdarzeń oraz operacji wykonanych w ramach procedur w celu weryfikacji poprawności tych procedur.



Rys. 2. Widok interfejsu graficznego systemu S-AWARE

Obsługa systemu informacji geograficznej (GIS)

Bardzo pomocna dla personelu i poprawiająca funkcjonowanie systemu jest możliwość prezentacji i obsługi różnego rodzaju map, np. Google Maps, Microsoft Bing czy Open Street. Dotyczy to zarówno map geograficznych, jak i różnego rodzaju planów obiektów. Dostęp do map wraz z naniesionymi na nie obiektami umożliwia sprawną orientację w terenie, a także odnalezienie obiektu i miejsca zdarzenia. Do obiektów można zaliczyć nie tylko obiekty statyczne, takie jak budynki, kamery czy systemy, ale także urządzenia mobilne i przemieszczających się użytkowników.

S-AWARE jest dostępny jako samodzielny produkt lub może funkcjonować jako dodatkowa warstwa systemu S-VMX firmy Teleste, który służy do nadzoru i zarządzania i jest bardzo efektywny. S-AWARE jest platformą otwartą. Może zostać zintegrowany praktycznie z każdym innym technicznym systemem firm trzecich, co czyni go niezwykle elastycznym narzędziem do zarządzania. Już w chwili obecnej platforma S-AWARE zapewnia kompatybilność z produktami czołowych firm z branż zabezpieczeń i transportu publicznego.

Teleste Video Networks

Kontakt:
Dariusz Łabędzki, dariusz.labedzki@teleste.com
Adam Zajkowski, adam.zajkowski@teleste.com
www.telestevn.pl

Teleste Video Networks realizuje projekt nr POIR.01.01.01-00-0235/17 pod nazwą S-AWARE – zaawansowany inteligentny system zapewnienia bezpieczeństwa w ramach Programu Operacyjnego Inteligentny Rozwój 2014–2020 współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego (wartość projektu to 13611646,62 zł).

SMART,
SAFE
AND
SMOOTH

Teleste S-AWARE
Your key to sharper decision-making

www.teleste.com

TELESTE

2020 – rok pełen szans
dla naszych partnerów i ich klientów

Hanwha Techwin

Rozwój sztucznej inteligencji, Internetu rzeczy (IoT) i cyberbezpieczeństwa stwarza nowe szanse dla ludzi zajmujących się tworzeniem systemów nadzoru wizyjnego

W ostatnich latach za wzrost sprzedaży kamer do systemów nadzoru wizyjnego, urządzeń rejestrujących i oprogramowania do zarządzania systemami wizyjnymi odpowiadały firmy i organizacje świadome potrzeby poprawy bezpieczeństwa. Menedżerowie odpowiedzialni za bezpieczeństwo mają wspólny cel, jakim jest ochrona nowoczesnych systemów nadzoru wizyjnego, które są częścią IoT, przed coraz bardziej złożonymi cyberatakami. Nic więc dziwnego, że globalny rynek profesjonalnych urządzeń do nadzoru wizyjnego nadal dynamicznie rośnie, a osiągnięte w 2019 roku przychody wynosiły 19,9 mld USD, co stanowi wzrost w porównaniu z 18,2 mld w roku 2018 (dane z publikacji Video Surveillance Intelligence Service firmy IHS Markit). Nowe, bardziej zaawansowane kamery, które zostaną wprowadzone w 2020 roku, umożliwią użytkownikom (również tym dysponującym ograniczonym budżetem) unowocześnienie posiadanych systemów nadzoru wizyjnego i jeszcze większą poprawę bezpieczeństwa.

Innowacyjne rozwiązania na rok 2020 i kolejne lata

Oczekiwania użytkowników wobec systemów nadzoru wizyjnego rosną, więc można się spodziewać wielu nowych kamer, zaawansowanych funkcji analizy treści obrazu w urządzeniach brzegowych i w chmurze, a także rozwiązań bazujących na sztucznej inteligencji i *deep learning*. Poparcie dla tej prognozy można znaleźć w raporcie firmy Gartner zajmującej się badaniami i rozwojem, która sugeruje, że wykorzystanie sztucznej inteligencji i zaawansowanych metod analizy znacznie wzrośnie w ciągu kilku kolejnych lat, a do 2022 r. globalna wartość takich rozwiązań sięgnie 3,9 biliona USD. W ciągu następnych kilku lat mogą zostać wprowadzone apli-

Fot. 1. Bob (H.Y.) Hwang PhD – Managing Director Europe w firmie Hanwha Techwin

kacje wykorzystujące sztuczną inteligencję, które udoskonalą systemy nadzoru wizyjnego w sposób, jaki aktualnie może wydawać się niemożliwy.

Kamery Wisenet 7

W 2020 r. przedstawimy nowy asortyment kamer wyposażonych w chipset nowej generacji – Wisenet 7, który zapewnia jeszcze większą moc obliczeniową i wiele funkcji, m.in. wykorzystujących sztuczną inteligencję. Te nowe kamery zaprojektowano pod kątem wykrywania i klasyfikacji ludzi i pojazdów w czasie rzeczywistym, rejestrowania zróżnicowanych cech obiektów i osób, takich jak rysy twarzy czy znaki rejestracyjne. Oprócz tego, że zapewnią większą dokładność i mniej fałszywych alarmów użytkownikom, którzy chcą wykrywać działania przestępcze, będą również ułatwiać firmom opracowanie sposobów na podniesienie wydajności. Na przykład sprzedawcy detaliczni będą mieć dostęp do wyników analizy danych, takich jak informacje o wieku i płci poszczególnych klientów.

Zaawansowane zabezpieczenia cybernetyczne

Cyberataki są coraz bardziej złożone, więc stworzenie odpornego na nie systemu bezpieczeństwa jest już konieczne. Nasi projektanci ulokowali cyberbezpieczeństwo na pierwszym miejscu listy wymagań dotyczących nowych kamer Wisenet 7. Nowe kamery mają funkcję bezpiecznego startu, która uniemożliwia dostęp do oprogramowania sprzętowego kamer osobom nieupoważnionym już na etapie podłączenia do sieci i pierwszego uruchomienia urządzeń.

Nowe rozwiązania techniczne na 2020 r.

Oczekując na ekscytujące szanse i wyzwania biznesowe, których spodziewamy się w tym roku i kolejnych latach, zdajemy sobie jednocześnie sprawę, jaki wpływ na sektor nadzoru wizyjnego będzie mieć Internet rzeczy i 5G. Zachęcamy do śledzenia naszej oferty w nadchodzących miesiącach, ponieważ będziemy do niej wprowadzać nowe, przełomowe produkty i rozwiązania, które pomogą integratorom w pozyskiwaniu nowych klientów i jednocześnie zapewnią użytkownikom nową jakość i wartość dodaną. Wszystkie zostały zaprojektowane z myślą o ułatwieniu integratorom pracy i obniżeniu kosztów operacyjnych.

Dzięki nowym, mającym wiele przydatnych funkcji kamerom wielokierunkowym i panoramicznym użytkownik końcowy może uniknąć kosztów, z jakimi trzeba się liczyć w przypadku instalacji większej liczby standardowych kamer. Całkowity koszt posiadania systemu może być zatem mniejszy przy takiej samej wielkości nadzorowanej przestrzeni. Aby skrócić czas montażu kamer w obiekcie, wyposażyliśmy kamery w mechanizm PTZ, który umożliwia łatwą zmianę pozycji obiektywu w celu ustawienia odpowiedniego pola widzenia.

Z nowych funkcji skorzystają przede wszystkim branże niszowe, a także sektory transportu i handlu detalicznego, dla których przygotowaliśmy wiele nowych produktów i rozwiązań, np. kamery termowizyjne w wersji przeciwwybuchowej i z funkcją automatycznego rozpoznawania tablic rejestracyjnych pojazdów (ANPR).

Do wielu nowych kamer, które wprowadzimy w roku 2020, należy model o rozdzielczości 8K, który zapewnia doskonałą jakość obrazów. Operatorzy będą mogli przybliżyć mały fragment obrazu, który będzie wyraźny i wolny od zjawiska pikselizacji.

Całkowity koszt posiadania systemu zostanie zmniejszony dzięki naszemu ekonomicznemu rozwiązaniu wykorzystującemu oprogramowanie do zarządzania systemami nadzoru wizyjnego Wisenet WAVE, aby system był dostępny nawet dla użytkowników dysponujących ograniczonym budżetem.

Nowoczesne rozwiązania

Przy tworzeniu naszych produktów i rozwiązań uwzględniliśmy uwagi partnerów i sygnały przekazywane z łańcucha dostaw. Podczas projektowania stosowaliśmy nieszablonowe i innowacyjne podejście. Integratorzy systemów i ich klienci mogą mieć pewność, że z pomocą naszej spółki-matki Hanwha Group będziemy nadal sprawnie reagować na zmieniające się potrzeby rynku, rozwijając nowe, interesujące produkty i rozwiązania oparte na najnowszych zdobyczach techniki. W ten sposób pomożemy im w rozwoju i potwierdzimy, że ich zaufanie do marki Wisenet jest uzasadnione.

Generowanie popytu

W roku 2020 nadal będziemy powiększać zespoły architektoniczno-inżynieryjne, przedsprzedaży i rozwoju biznesu. W związku z tym będziemy poszukiwać najlepszych specjalistów podzielających naszą pasję do budowania partnerskich relacji z integratorami i innymi uczestnikami łańcucha dostaw. Dzięki temu nasz ogromny asortyment produktów dotrze do jeszcze większej liczby odbiorców i stanie się dla partnerów źródłem kolejnych szans biznesowych.

Opracowano na podstawie materiałów firmy Hanwha Techwin
Redakcja

BŁYSKAWICZNA DETEKCJA OSÓB Z PODWYŻSZONĄ TEMPERATURĄ

ZOBACZ JAK DZIAŁA SYSTEM W PRAKTYCE

YouTube

NOVUS® 8000 VSS IP THERMO VISION

PROFESJONALNY ZESTAW DO ZDALNEGO POMIARU TEMPERATURY CIAŁA NVIP-2H-8912M/TS SET

- MOŻLIWOŚĆ JEDNOCZESNEGO POMIARU **16 TWARZY W CZASIE KRÓTSZYM NIŻ 1 SEKUNDA**
- DOKŁADNOŚĆ **POMIARU +/- 0,3°C**
- ALGORYTM **WYKRYWANIA TWARZY**

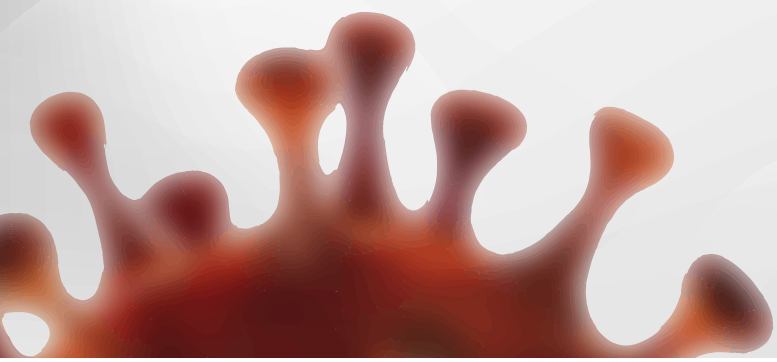
ZATWIERDZAMY DO WALKI Z PANDEMIĄ

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

Produkty NOVUS w walce z koronawirusem SARS-Cov-2

Profesjonalny zestaw do zdalnego pomiaru temperatury ciała

Patryk Gańko



Nowy koronawirus SARS-Cov-2 wywołuje chorobę o nazwie COVID-19. Choroba objawia się najczęściej gorączką, a także dodatkowymi symptomami, takimi jak duszności, kaszel, bóle mięśni oraz zmęczenie. Mierzenie temperatury ciała jest jednym z podstawowych sposobów wczesnego diagnozowania choroby. Gorączka może wskazywać na konieczność przeprowadzenia testów laboratoryjnych i kwarantanny. Stałe kontrolowanie temperatury, noszenie masek ochronnych i kwarantanna to podstawowe sposoby przeciwdziałania zagrożeniu, czego przykładem może być sytuacja na Tajwanie. Oczywiście uwaga społeczeństwa jest skupiona na walce z koronawirusem, ale według specjalistów do wczesnych objawów 28 spośród 39 rozpoznanych chorób zakaźnych należy podwyższona temperatura ciała, a zatem mierzenie temperatury jest szczególnie ważne

Fot. 1. Dualna kamera IP do pomiaru temperatury ciała

Fot. 2. Urządzenie kalibrujące NV-BBU do kamer termowizyjnych

Rozwiązanie, które przedstawiam w poniższym artykule, zostało stworzone między innymi do wczesnej, masowej diagnostyki, m.in. do diagnozowania grypy w szkołach. Jego przydatność została zweryfikowana w setkach przypadków. Pomogło w zapobieganiu przenoszeniu wirusa, a tym samym absencjom w szkołach, przedszkolach, zakładach produkcyjnych, biurowcach czy obiektach infrastruktury krytycznej, a może przede wszystkim wyłączeniom takich obiektów z eksploatacji. Rozwiązanie to ma charakter uniwersalny – nie tylko może być pomocne w związku z aktualnym zagrożeniem koronawirusem, lecz powinno być standardem w polityce bezpieczeństwa dotyczącej obiektów, w których przebywa wiele osób i dochodzi do interakcji między nimi.

Zestaw NVIP-2H-8912M/TS SET składa się z dualnej kamery IP NVIP-2H-8912M/TS służącej do pomiaru temperatury ciała, urządzenia kalibrującego NV-BBU oraz aplikacji CMS służącej do obsługi i analizy.

Najważniejsze cechy zestawu to:
- dokładność pomiaru temperatury (do +/- 0,3°C),
- jednoczesny pomiar u maksymalnie 16 osób w mniej niż sekundę,
- brak fałszywych alarmów (dzięki zastosowaniu zaawansowanych metod analizy treści obrazu pomiar jest dokonywany wyłącznie w obrębie górnej części twarzy),
- każdorazowe przypisywanie wyniku pomiaru do konkretnej osoby i przechowywanie go w bazie danych wraz z obrazem (ułatwia to późniejszą analizę).

Duża dokładność pomiaru (rzędu +/- 0,3°C) istotnie wpływa na przydatność zestawu w rzeczywistych warunkach i wynika z zastosowania dwóch unikatowych elementów – zestawu kalibrującego oraz dualnej kamery z funkcją rozpoznawania

twarzy. Urządzenie kalibrujące (fot. 2) jest niczym innym jak wzorcem temperatury o obszarze emisji 70 x 70 mm, stabilności +/- 0,1°C ~ 0,2°C / 30 min oraz emisyjności 0,97 +/- 0,02. Urządzenie kalibrujące powinno być zainstalowane w odległości trzech metrów od kamery – oczywiście w jej polu widzenia oraz na tej samej wysokości co kamera, czyli 2,2–2,3 m, jak na rys. 1.

w którym zainstalowany jest system pomiarowy, a temperaturą na zewnątrz. Dokładność pomiaru uzyskuje się także dzięki wysokiej rozdzielczości zastosowanego w kamerze termowizyjnej mikrobolometrycznego przetwornika obrazu FPA o liczbie efektywnych pikseli 400 (H) x 300 (V) oraz czułości termicznej 40 mK. W celu zapewnienia odpowiedniej rozdzielczości obrazu górnej części twarzoczaszki ważne jest zachowanie

Rys. 1. Zasady montażu zestawu NVIP-2H-8912M/TS SET

Temperatura w obrębie głowy człowieka nie wszędzie jest taka sama, co utrudnia pomiar. Różnica pomiędzy poszczególnymi częściami może wynosić nawet 3°C. Temperatura gałki ocznej jest niższa niż wewnętrzna temperatura ciała i wynosi 34°C, natomiast temperatura jamy ustnej to 37°C. Pomiar jest realizowany tylko w obrębie czoła i oczu. To właśnie w tym miejscu, a zwłaszcza w kącikach oka, gdzie powieka górna styka się z dolną, jego wynik jest najbardziej reprezentatywny. Sposobem uzyskania takiego wyniku jest rozpoznanie miejsca pomiaru za pomocą tradycyjnej kamery z funkcją rozpoznawania twarzy w połączeniu z dokonaniem pomiaru w wyznaczonym miejscu przez kamerę termowizyjną. Trzymanie w ręku naczynia z gorącym napojem lub pojawienie się innych obiektów o temperaturze ludzkiego ciała lub wyższej w polu widzenia kamery nie zaburza wyniku pomiaru. Algorytm minimalizuje wpływ różnicy pomiędzy temperaturą pomieszczenia, odległości pomiarowych przedstawionych na rys. 1. Zwiększenie odległości pomiędzy kamerą a obserwowaną osobą i urządzeniem kalibrującym zmniejsza dokładność.

Coraz bardziej powszechne, a w niektórych krajach, np. w Czechach, już obowiązkowe noszenie masek ochronnych zupełnie nie wpływa na wynik pomiaru temperatury, natomiast rekomendowane jest zdjęcie nakrycia głowy oraz okularów.

Zestaw umożliwia jednoczesny pomiar temperatur ciał szesnastu osób w czasie krótszym niż jedna sekunda. Dzięki temu możliwa jest bezinwazyjna, nie powodującą zatorów kontrola dużej liczby przemieszczających się ludzi, np. w zakładach pracy o systemie zmianowym, w dużych biurowcach czy w obiektach użyteczności publicznej – w szkołach, na uniwersytetach, na dworcach kolejowych, w portach lotniczych – gdzie ręczne, czasochłonne pomiary tempera-

tury mogą zakłócić harmonijne funkcjonowanie tych obiektów. W celu zwiększenia czytelności bazy danych pomiar temperatury każdej sprawdzanej osoby zostaje przeprowadzony tylko jednokrotnie.

Rys. 2. Równoczesny pomiar temperatur ciał wielu osób

Integralną częścią zestawu do natychmiastowego pomiaru temperatury jest aplikacja CMS. Jest to rozbudowane narzędzie. W tym miejscu opiszę tylko zarządzanie za jego pomocą informacjami związanymi z pomiarami temperatur. Aplikacja może obsłużyć wiele pojedynczych systemów służących do pomiaru temperatury. Jej podstawowy interfejs graficzny składa się z dwóch pól, na których wyświetlane są obrazy z kamery dualnej, pola z wynikami pomiarów temperatur ciał osób oraz bloku rozpoznań alarmowych.

Rys. 3. Podstawowy interfejs systemu CMS

Wszystkie zapisane wyniki są umieszczane w *Bazie pomiarów*, gdzie można ich szukać, kierując się określonymi kryteriami (urządzenie, czas, grupa, numer identyfikacyjny osoby i in.), i skąd można je następnie wyeksportować do pliku o rozszerzeniu .xls. Zapisane wyniki rozpoznań mogą być archiwizowane i analizowane w module statystycznym dla zdefiniowanych przedziałów czasowych.

Informacje o wszystkich przekroczeniach zdefiniowanego zakresu temperatur są wyświetlane w dodatkowym oknie. Możliwe jest także uruchamianie sygnalizatorów akustycznych.

Dwa strumienie RTSP z kamery, termalny i wizyjny, zawierają informacje o każdej z zaobserwowanych osób i zmierzonej temperaturze.

Rys. 4. Baza pomiarów

Dzięki temu system może współpracować z dowolnym rejestratorem sieciowym. Ponadto jest kompatybilny z systemem NMS (Novus Management System), który jest bardzo często użytkowany w dużych strategicznych obiektach o dużym ruchu pieszych i może być również zainstalowany na serwerze PC z aplikacją CMS.

Aby dowiedzieć się więcej na temat możliwości systemu, warto zapoznać się z materiałami zamieszczonymi na kanale YouTube firmy AAT HOLDING lub umówić się na indywidualny pokaz jego działania (adres kontaktowy: patryk.ganko@aat.pl).

Patryk Gańko
AAT HOLDING

VMS GANZ CORTROL
i kontrola dostępu

CBC Poland

W ciągu ostatnich kilku lat zainteresowanie inteligentnymi systemami bezpieczeństwa gwałtownie wzrosło. Autonomiczne systemy zarządzania strumieniami wizyjnymi nie wystarczają, dlatego my koncentrujemy się na dostosowaniu oprogramowania VMS GANZ CORTROL do interakcyjnej współpracy z innymi systemami

Wielozadaniowość i interakcja

Klienci chcą mieć możliwość kontrolowania całego systemu z jednego miejsca, a systemy są coraz większe i coraz bardziej złożone. Ze względu na rosnące wymagania dotyczące dostępności usług związanych z bezpieczeństwem potrzebny jest prosty i przyjazny dla użytkownika system zarządzający. Komponenty takiego systemu powinny być odpowiednio dobrane, a jego skomplikowane warstwy, wykonujące w tle całą pracę związaną z automatyzacją, powinny pozostać niewidoczne dla użytkownika końcowego. Nie istnieje uniwersalny system, który zadowoliłby wszystkich. Każde oprogramowanie jest tworzone według ściśle określonych założeń, a wyma-

gania są różne w zależności od miejsca zastosowania i oczekiwań klienta.

Współpraca na poziomie oprogramowania nie tylko zapewnia ujednolicony interfejs, dzięki któremu użytkownik końcowy może łatwiej sterować systemem i kontrolować go, ale także umożliwia skonfigurowanie interaktywnych scenariuszy używanych do automatyzacji działania całego systemu. Informacje o zdarzeniach generowane przez jeden komponent (np. czytnik ROGER) wyzwalają polecenia w innym miejscu w systemie. Dzieje się to automatycznie, bez udziału człowieka, ale w razie potrzeby może odbywać się pod nadzorem operatora. Ułatwia to użytkowanie całego systemu, minimalizuje skutki ludzkich błędów oraz zmniejsza poziom zagrożenia.

W świetle powyższych faktów wydaje się oczywiste, że współpraca oprogramowania VMS do zarządzania strumieniami wizyjnymi z systemem kontroli dostępu przynosi korzyści klientowi. Co oferuje w tym zakresie GANZ CORTROL?

Ujednolicony interfejs i dynamiczna reakcja

Oprogramowanie GANZ CORTROL pozwala na integrację z kilkoma systemami kontroli dostępu, m.in. firm ROGER, Keri Systems oraz Feenics. Dwie wersje – Premier oraz Global – umożliwiają tę integrację bez żadnych ograniczeń. Integracja

z systemem ROGER RACS5 jest możliwa od wersji 1.16.0 oprogramowania CORTROL.

Na etapie konfiguracji systemu tworzona jest lista czytników. Serwer CORTROL pobiera informacje o czytnikach z systemu kontroli dostępu, co w kolejnym etapie konfiguracji umożliwia powiązanie ich z określonymi drzwiami. Dane z systemu KD można wykorzystać do wygenerowania informacji o zdarzeniach w Konfiguratorze Zdarzeń i Akcji i powiązania ich z różnymi akcjami. Możliwy jest na przykład scenariusz, zgodnie z którym będziemy otrzymywać powiadomienia o osobach próbujących bez uprawnienia uzyskać dostęp do określonej lokalizacji. Dodatkowo, po odpowiednim zdefiniowaniu akcji, VMS CORTROL może również wysłać określone komendy zwrotne do systemu kontroli dostępu (np. wysłać komendę zmiany stanu drzwi na *zablokowane*).

Oprogramowanie CORTROL obsługuje interaktywne mapy synoptyczne bazujące na zaimportowanym obrazie lub na mapie świata on-line. Zmiany stanu drzwi są odzwierciedlane przez dynamiczne zmiany wyglądu map w aplikacji CORTROL Client, jeśli zostały odpowiednio skonfigurowane. W tym celu na mapie umieszcza się odpowiednie znaczniki drzwi (ikony), co pozwala natychmiast sprawdzić aktualny status drzwi, a także zmienić go ręcznie. Ponadto do zmiany stanu drzwi można użyć różnych funkcji i urządzeń systemowych, takich jak wejścia alarmowe, przyciski użytkownika, funkcje rozpoznania twarzy osób z tzw. białej listy itp. Zastosowanie automatyzacji zamiast sterowania ręcznego minimalizuje czas interakcji i pomaga w ten sposób zbudować wysoce wydajny system do rutynowej codziennej pracy, nawet jeśli przepływ osób jest duży.

Dzięki aplikacji CORTROL Client uzyskuje się zaawansowane raporty tworzone na podstawie informacji o zdarzeniach pochodzących z czytników, generowanych na podstawie danych odczytanych z kart użytkowników. Dane posiadaczy kart są wprowadzane w systemie kontroli dostępu, natomiast wyszukiwanie danych do raportu oraz ich filtrację można przeprowadzać w aplikacji CORTROL. Taki sposób wyszukiwania umożliwia przegląd zdarzeń z systemu KD wraz z powiązanym materiałem wizyjnym. Nie ma więc potrzeby posługiwania się w tym celu interfejsem systemu kontroli dostępu.

Nadzór, kontrola i weryfikacja

Gdy CORTROL Client jest podłączony do co najmniej jednego serwera CORTROL z dodanym systemem ROGER, na górnym pasku w aplikacji Client pojawia się dodatkowa zakładka mająca związek z kontrolą dostępu, umożliwiająca przeglądanie rejestrów w kilku trybach.

Można filtrować zdarzenia według zakresu czasowego, nazwy drzwi, konkretnej nazwy posiadacza karty, a także docelowej nazwy zdarzenia. Na przykład można:

- zobaczyć, które drzwi dany użytkownik otworzył w ciągu dnia,
- sprawdzić, czy dana osoba używa własnej karty dostępu, przez porównanie zdjęcia posiadacza karty z nagraniem z kamery,
- sprawdzić aktualny stan drzwi i w razie potrzeby ręcznie je zablokować albo odblokować.

Po kliknięciu dowolnego zdarzenia na liście można odtworzyć powiązany z nim materiał wizyjny. Odtwarzany obraz pojawia się po prawej stronie ekranu, w oknie podglądu, w którym dostępne są wszystkie przyciski sterujące odtwarzaniem.

Podczas pracy w trybie *Drzwi* kliknięcie na dowolnych drzwiach na liście umożliwia sprawdzenie statusu tych drzwi. W tym miejscu możliwe jest również ręczne zablokowanie albo odblokowanie drzwi.

W czasie pracy w trybie *Posiadacze kart* wyświetlona jest lista wszystkich posiadaczy (użytkowników) kart zarejestrowanych w bazie danych systemu kontroli dostępu. Jeśli osoba wprowadzająca do systemu ROGER nowych użytkowników kart zadba również o dodanie ich zdjęć, to zdjęcia będą widoczne również w systemie CORTROL. Dzięki temu operator będzie mógł łatwo sprawdzić, czy na zdjęciu i na obrazie z kamery widać tę samą osobę.

Wdrażanie środków zapobiegawczych

Niezależnie od tego, czy realizowany jest projekt obejmujący wiele budynków czy tylko instalację jednych drzwi, integracja z systemem kontroli dostępu umożliwia kontrolowanie całego obiek-

tu z jednego miejsca. Dzięki funkcji CORTROL *Zdarzenia i akcje* (Event & Action) można zautomatyzować znaczną część procedur sterowania. Oto kilka przykładowych scenariuszy (spośród wielu możliwych kombinacji):

1. Jeśli drzwi nr 1 zostaną otwarte po godzinach pracy (np. nocą), powiadom pracowników ochrony SMS-em i komunikatem dźwiękowym oraz wyślij powiadomienie e-mailem do osoby odpowiedzialnej za bezpieczeństwo.
2. Gdy nastąpi zanik strumienia wizyjnego z kamery, częściowo zablokuj możliwość poruszania się po obiekcie. Opcjonalnie można umożliwić operatorowi ręczne (nadrzędne) otwarcie przejść za pomocą przycisków użytkownika.
3. Podczas próby uzyskania dostępu przez nieuprawnioną osobę ustaw kamerę PTZ w określonej pozycji i wyświetl obraz na żywo na monitorze alarmowym.

Dostęp do obiektu może być ograniczony (np. możliwy tylko dla osób uprawnionych, w określonych godzinach). Ponieważ wszystkie informacje o zdarzeniach dotyczących drzwi są rejestrowane, można w każdej chwili skorzystać z rejestru zdarzeń, np. w celu sprawdzenia, czy do budynku wszedł tylko upoważniony personel, lub upewnienia się, że nikt nie używa kart dostępu przekazanych przez inne osoby.

Dwie przykładowe procedury realizowane przez system:

1. Jeśli drzwi prowadzące do miejsca o szczególnym znaczeniu (np. serwerowni) zostaną otwarte pod przymusem, natychmiast rozpocznij nagrywanie alarmowe kontynuowane przez określony czas lub do momentu, w którym operator zatrzyma je ręcznie.
2. Jeżeli drzwi są otwarte od ponad dziesięciu sekund, wyślij do kamery lub głośnika odpowiedni komunikat dźwiękowy (wykorzystując wstępnie skonfigurowany plik dźwiękowy).

Aby określić czynności wykonywane automatycznie w związku z zaistnieniem określonych zdarzeń, należy przeprowadzić konfigurację, korzystając z sekcji *Zdarzenia i akcje* w konsoli CORTROL Console (dostępnej w wersjach CORTROL Premier i CORTROL Global). W tej sekcji znajdują się osobne podsekcje. Następnie należy przejść do sekcji *Reguły* i utworzyć odpowiednie scenariusze.

Do każdego utworzonego scenariusza można dodać warunki i reguły – harmonogramy, czasy opóźnień reakcji itp. W harmonogramach mogą zostać podane dni i godziny, w których dana reguła obowiązuje (np. tylko w godzinach nocnych, tylko w weekendy). Możliwe jest rozpoczęcie jednej akcji na skutek spełnienia dwóch warunków jednocześnie, np. wysłanie powiadomienia, gdy dwoje drzwi ma jednocześnie status *otwarte*. Z kolei tzw. opóźniacze zawieszają na określony czas obowiązywanie reguły i ich efekt.

Podsumowanie

Konfiguracja oprogramowania systemu kontroli dostępu zajmuje tyle samo czasu co zwykle. Dodatkowe 15 minut zajmuje konfigurowanie systemu CORTROL związane z komunikacją z systemem ROGER. W zamian operatorzy systemu CORTROL otrzymują jeden spójny i przyjazny dla użytkownika interfejs. Nigdy więcej nie zajdzie konieczność korzystania z osobnych okien. Nie ma potrzeby stosowania dodatkowych monitorów do każdej aplikacji klienckiej.

W przypadku typowych czynności związanych z rutynową kontrolą dostępu nie ma potrzeby korzystania z innego interfejsu użytkownika, ponieważ cały system można obsłużyć za pomocą aplikacji CORTROL Client. Pojedyncza czynność związana z ręczną obsługą systemu kontroli dostępu może zająć zaledwie sekundę albo dwie, ale w ciągu dnia można zaoszczędzić dużo czasu ze względu na liczbę takich czynności. Realizacja nawet najbardziej złożonych scenariuszy jest w pełni zautomatyzowana. Układa się je tylko raz, a potem wielokrotnie z nich korzysta. Unika się przy tym błędów spowodowanych przez człowieka (operatora).

Nie ma znaczenia to, czy drzwi (czytniki) są sterowane za pomocą interfejsu natywnego czy zintegrowanego oprogramowania. Oczywiście integracja nie obejmuje wszystkiego. Zintegrowany system jest w pełni użyteczny i spełnia typowe wymagania.

CBC Poland

Klasyfikacja obiektów

w wizyjnych systemach dozorowych marki NOVUS

Daniel Xaysomvang

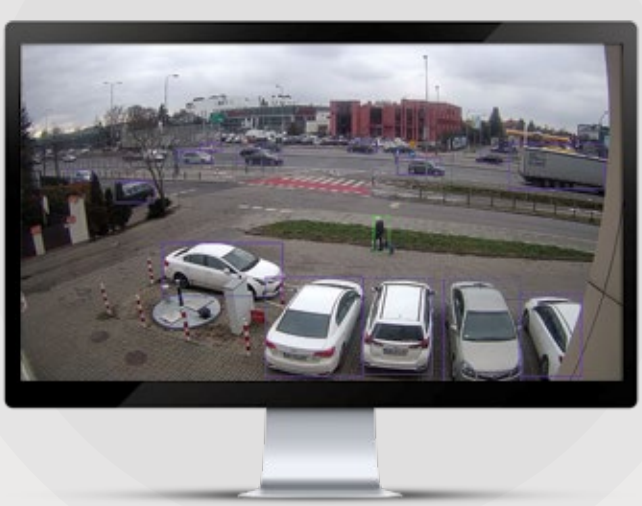
Pierwotna funkcja wizyjnych systemów dozorowych, czyli obserwacja i zapis obrazów z kamer, jest systematycznie wzbogacana w coraz nowsze zaawansowane algorytmy analizy treści obrazu. Mają one za zadanie zwiększyć skuteczność działania systemu poprzez automatyzację procesów decyzyjnych, zaś nowe funkcje zapewniają przyjazny dla operatora interfejs komunikacji

W ramach niniejszego artykułu chciałbym przedstawić rozwiązanie z dziedziny zaawansowanej analizy treści obrazu, które zastosowano w nowej serii kamer marki NOVUS, a mianowicie funkcję klasyfikacji obiektów pod względem typu. Funkcje wykrywania przekroczenia wirtualnej linii lub naruszenia wyznaczonego obszaru, a także wykrywania sabotażu kamery są już standardem w wizyjnych systemach dozorowych. Wymagania wobec nowych systemów są jednak coraz wyższe i wymienione wyżej funkcje analityczne w standardowej formie mogą w niektórych przypadkach nie wystarczyć.

Funkcję klasyfikacji obiektów wprowadzono w odpowiedzi na wzrost wymagań i w celu umożliwienia niestandardowych zastosowań. Zastosowany algorytm umożliwia rozpoznanie człowieka, samochodu, a także roweru lub motocykla w polu widzenia kamery. Rys. 1 ukazuje jeden z obszarów testowych – ruchliwą ulicę – i ciągłe, dynamiczne zmiany obserwowanej sceny. W takich warunkach użycie algorytmu umożliwiło bezbłędną klasyfikację obiektów, których rozmiary były nie mniejsze niż 1% obserwowanej sceny. Obiekty mniejsze mogą zostać wykryte w odpowiednich warunkach, takich jak dobrze doświetlona scena oraz duży kontrast pomiędzy obiektem a tłem, na jakim obiekt się porusza.

Opisywana funkcja klasyfikacji obiektów odznacza się wysoką skutecznością w trudnych warunkach atmosferycznych, między innymi podczas opadów deszczu i śniegu, a także w przypadku niekorzystnego oświetlenia sceny o zmierzchu albo o świcie.

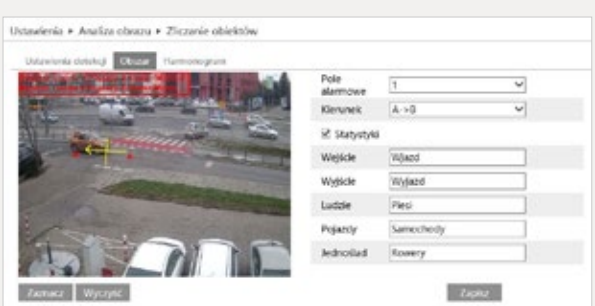
Dzięki możliwości rozróżnienia typu obiektu, który wtargnął w wyznaczony obszar lub przekroczył wirtualną linię, uzyskuje się znaczne zmniejszenie liczby niechcianych i zakłócających prawidłową pracę systemu fałszywych alarmów. Operator może zatem skoncentrować się na sytuacjach, które bezsprzecznie wymagają szybkiej i sprawnej interwencji. Konfiguracja opisywanej funkcji umożliwia ustawienie



Rys. 1. Klasyfikacja obiektów

czułości wykrywania, która określa, przy jakiej minimalnej odległości od wyznaczonej linii lub strefy obecność obiektu wywoła alarm. Ponadto konfiguracji podlegają także informacje wyświetlane przy licznikach kamery (o których mowa w dalszej części artykułu) – można dowolnie nazwać każdą kategorię (przykład podano na rys. 2). Informacja o zdarzeniu może być przekazana do oprogramowania NMS. Na podstawie odpowiednio zdefiniowanych scenariuszy system jest w stanie zareagować autonomicznie lub poinformować obsługę o konieczności podjęcia określonych działań.

Przykładem zastosowania opisywanej techniki jest monitorowanie miejsc pracy maszyn wielkogabarytowych z elementami ruchomymi, w pobliżu których w czasie działania nie może



Rys. 2. Okno dialogowe ustawień detekcji

przebywać człowiek. Skutkiem wykrycia człowieka w strefie zagrożenia będzie alarm w formie ostrzegającego przed niebezpieczeństwem sygnału akustycznego lub optycznego, a informacja o zaistniałej sytuacji zostanie zapisana w rejestratorze jako zdarzenie alarmowe, które będzie można łatwo odnaleźć. Inne przykładowe

Rys. 3. Zliczanie przekroczeń wyznaczonej linii

lokalizacje, w których wykrycie postaci ludzkiej może okazać się pomocne, to przejazdy kolejowe, wjazdy na parkingi podziemne i wyjazdy z tych parkingów, miejsca niedozwolonego przechodzenia pieszych przez jezdnię.

Kolejną dostępną w kamerach marki NOVUS funkcją rozszerzającą zakres analizy treści obrazu jest zliczanie przekroczeń wyznaczonej linii (rys. 3) przez obiekty różnych typów. Kamera ma sześć niezależnych liczników podających liczbę samochodów, ludzi i rowerów (albo motocykli), które zostały sklasyfikowane, zliczone i których kierunek przemieszczania się został ustalony. Liczniki mogą być resetowane automatycznie, po wyznaczonym czasie – po godzinie, dniu albo tygodniu, lub ręcznie, poprzez interfejs sieciowy kamery. Na podstawie zebranych w ten sposób danych możliwe jest utworzenie statystyk, które w przyszłości będą mogły posłużyć do optymalizacji ruchu pojazdów, pieszych i rowerów w danym obszarze. Korzystając z funkcji wykrywania kierunku przecinania wirtualnej linii przez wybrany obiekt, można także alarmować o nielegalnym przemieszczaniu się pojazdu w monitorowanych strefach, np. na drogach jednokierunkowych lub na wjeździe na parking.

Dzięki temu, że to kamera korzysta z algorytmu klasyfikacji, istniejące urządzenia rejestrujące nie wymagają rozbudowy lub wymiany. Rozproszenie elementów analizujących obraz zapewnia wysoką skalowalność oraz odporność na awarię całego systemu (w przeciwieństwie do rozwiązań bazujących na centralnych jednostkach analizujących).

W przeciwieństwie do rozwiązań, w których wykorzystuje się serwer przeprowadzający analizę treści obrazów, możliwa jest bezobsługowa, automatyczna kalibracja, która odbywa się przy każdym uruchomieniu funkcji lub restarcie kamery, co daje pewność, że algorytm zawsze działa z najwyższą wydajnością. Automatyczna kalibracja znacznie skraca czas konfiguracji, więc od instalatora wymaga się jedynie montażu kamery zgodnie z zaleceniami producenta.

Wydajność zastosowanych urządzeń oraz metod analizy pozwala na jednoczesne monitorowanie do 32 obiektów różnego rodzaju. Jeżeli na obrazie pojawi się większa liczba obiektów, to najpierw rozpoznane będą sylwetki ludzkie, następnie samochody, a na końcu jednoślady. Gwarantuje to niezawodną pracę systemu nawet w wyjątkowo dynamicznych miejskich sceneriach.

Zapraszam do zapoznania z filmem prezentacyjnym, który jest dostępny na naszym kanale YouTube. Link w postaci kodu QR znajduje się poniżej.

Daniel Xaysomvang
AAT HOLDING

NOVUS®

NIEZAWODNE PRZEŁĄCZNIKI – ZASILANIE PoE DO 250 m

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

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

Certyfikowane zasilacze do urządzeń zasilanych trójfazowo

Wojciech Rytlewski

Urządzenia przeciwpożarowe w większości przypadków są wyposażone w trójfazowe silniki elektryczne. W związku z tym, że są one elementami instalacji odpowiedzialnej za bezpieczeństwo w obiekcie, powinny być zasilane za pomocą odpowiednio certyfikowanej jednostki zasilająco-sterującej

Zasilacze używane do zasilania urządzeń przeciwpożarowych powinny spełniać wymagania normy zharmonizowanej EN 12101-10 *Systemy kontroli rozprzestrzeniania dymu i ciepła – Część 10: Zasilacze*. Wymienia ona m.in. wymagania dotyczące poprawnego zasilania z podstawowego źródła lub – w przypadku zaniku napięcia – z baterii czy prądnic. Certyfikowane urządzenia powinny również rozpoznawać i sygnalizować uszkodzenia. Zgodnie z normą producent zasilaczy musi spełniać odpowiednie wymagania dotyczące zakładowej kontroli produkcji.

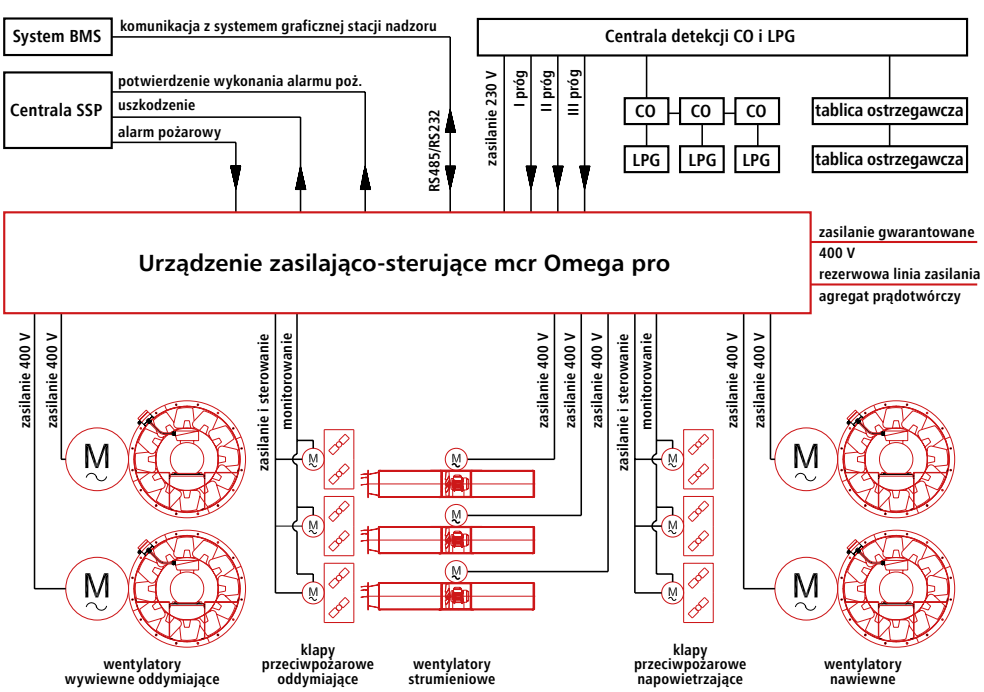
Dodatkowo, przed wprowadzeniem zasilacza do sprzedaży na rynku polskim, należy uzyskać odpowiednie świadectwo dopuszczenia potwierdzające zgodność z podpunktem 12.2 *Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2010 r. zmieniającego rozporządzenie w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania* (Dz. U. Nr 85, poz. 553).

Firma Mercor ma w swojej ofercie dwa typy urządzeń dostosowanych do zasilania elementów systemu kontroli rozprzestrzeniania się dymu i ciepła. Zasilacz mcr Omega proF 230 jest dostosowany do urządzeń zasilanych napięciem 230 V lub 24 V, m.in. doków i bram napowietrzających, do których, w przypadku zaniku napięcia podstawowego, dostarczana jest energia 230 V z akumulatorów. Zasilacz mcr Omega pro jest przeznaczony do zasilania, sterowania oraz kontroli pracy wszystkich urządzeń wchodzących w skład systemu kontroli rozprzestrzeniania się dymu i ciepła. Może również zapewnić gwarantowane napięcie i moc z sieci energetycznej lub – po zaniku tego napięcia – energię z wewnętrznego akumulatora dla urządzeń trójfazowych. Jest to wykorzystywane przede wszystkim przy zasilaniu wentylatorów napowietrzających na klatkach schodowych, gdzie nie ma drugiej linii zasilającej lub agregatu prądotwórczego. Przykładowe zastosowanie pokazano na rysunku 1.

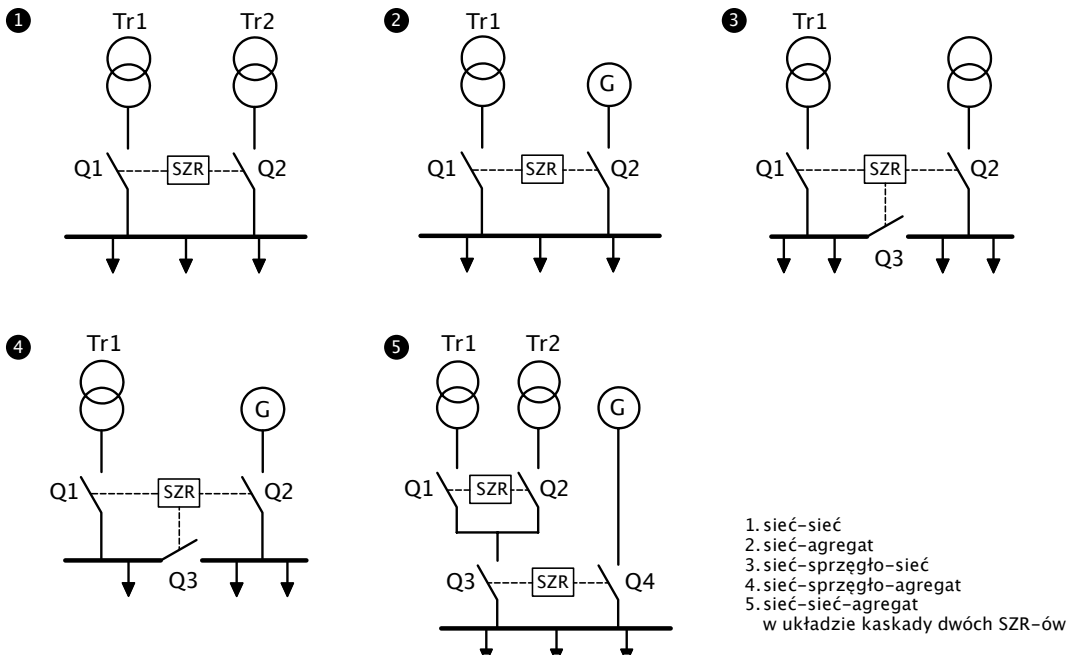
Zasilacz mcr Omega pro ma kompaktową, skalowalną obudowę o wymiarach od 200x200x150 mm do 220x1200x800 mm (w zależności od potrzebnej mocy oraz stopnia skomplikowania wykonywanych operacji). Urządzenie może mieć formę pojedynczej szafy lub trwale połączonych ze sobą nierozproszonych modułów. Konstrukcja obudowy zapewnia stopień ochrony IP54 lub IP55, wymagany w przypadku zastosowań przemysłowych. Jest to obudowa spełniająca kryteria III klasy środowiskowej, co gwarantuje poprawną pracę urządzenia w temperaturach od -25°C do +75°C. Produkowana jest w dwóch wersjach – do zastosowania wewnętrznego oraz zewnętrznego.

Elementem składowym mcr Omega pro jest moduł samoczynnego załączania rezerwy (SZR) umożliwiający zasilanie urządzeń z dwóch nieza-

leżnych źródeł. W przypadku zaniku lub nadmiernego obciążenia w torze zasilania podstawowego SZR przełącza zasilanie na rezerwowe. Moduł realizuje funkcje przełączania *sieć-sieć*, *sieć-sprzęgło-sieć lub sieć-agregat*. Przełączenia między liniami dokonuje się manualnie lub zdalnie i trwa ono kilka sekund. W czasie przełączenia urządzenia wykonawcze nie tracą swojej funkcjonalności. Ich działanie jest podtrzymywane przez zasilacz buforowy. mcr Omega pro może być również zasilany za pomocą agregatu prądotwórczego. Podczas zaniku napięcia wysyła sygnał startu do agregatu oraz sprawdza poprawność wykonania tej operacji.



Rys. 1. Przykładowe zastosowanie urządzenia zasilająco-sterującego mcr Omega pro



Rys. 2. Schemat układu samoczynnego załączania rezerwy dla urządzeń trójfazowych

W myśl obowiązujących przepisów czas rozruchu agregatu - do momentu osiągnięcia znamionowej wartości napięcia - nie może być dłuższy niż 15 sekund. Po wykryciu napięcia z agregatu, zasilanie zostaje przełączone na rezerwowe. Schemat takiego układu został pokazany na rysunku 2.

Do rozruchu wentylatorów i silników można stosować klasyczne układy styczników:

- załączenie bezpośrednie – polega na bezpośrednim włączeniu silnika elektrycznego (np. wentylatora) do sieci poprzez zasilenie cewki stycznika, przełączenie jego styków i podanie napięcia znamionowego na zaciski silnika;
- gwiazda-trójkąt – układ rozruchu umożliwiający znaczne ograniczenie prądów rozruchowych urządzenia (do 3xIn) oraz zmniejszenie przekrojów przewodów. W początkowej fazie rozruchu uzwojenia silnika są połączone w układ gwiazdy, a w momencie osiągnięcia prędkości znamionowej wirnika układ automatyki w układ trójkąta, co zmniejsza pobór prądu z sieci;
- układ Dahlandera – układ odpowiednio połączonych styczników umożliwiający automatyczne sterowanie prędkością obrotową silników poprzez zmianę liczby par ich biegunów;
- niezależne uzwojenia – regulacja prędkości obrotowej silników z dwoma niezależnymi uzwojeniami;
- rewersyjny – umożliwiający zmianę kierunku obrotów wentylatora poprzez zamianę kolejności faz. Możliwe jest zastosowanie pracy rewersyjnej we wszystkich ww. układach rozruchu, także w przypadku pracy dwubiegowej.

Zgodnie z obowiązującymi przepisami zasilanie urządzeń systemu kontroli rozprzestrzeniania się dymu i ciepła powinno być gwarantowane dzięki stosowaniu certyfikowanych zasilaczy. Urządzenia zasilające powinny zostać zbadane na zgodność z normą PN-EN 12101-10 oraz spełniać wymagania zawarte w podpunkcie 12.2 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 27 kwietnia 2010 r. Tylko urządzenia, których zgodność z wymienionymi normami została potwierdzona, mogą być stosowane do zasilania urządzeń przeciwpożarowych w budynkach. Zasilacze mcr Omega pro oraz mcr Omega proF uzyskały Certyfikat Stałości Właściwości Użytkowych 1438-CPR-0523 oraz Świadectwo Dopuszczenia nr 2904/2017 wydane przez Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej.

Wojciech Rytlewski
MERCOR S.A.
www.mercor.com.pl

Optymalizacja wizyjnego systemu wykrywania pożaru Aviotec firmy Bosch

pod kątem działania w tunelach

Bosch Security and Safety Systems

Szybkie i niezawodne wykrywanie dymu i płomieni

Wykorzystujący technikę wizyjną system wykrywania pożaru Aviotec IP Starlight 8000 może być teraz używany do niezawodnego i wczesnego wykrywania dymu i płomieni także w tunelach. Uzupełnia on powszechnie stosowane liniowe czujki termiczne, które reagują tylko na wyraźny wzrost temperatury i nie są w stanie wykrywać dymu. Jest niedrogi i można go szybko zainstalować. Możliwość przeglądania pamięci zdarzeń umożliwia błyskawiczną weryfikację alarmów i stanowi cenną pomoc dla służb ratowniczych.

Niezawodne wykrywanie pożaru także w trudnych warunkach oświetleniowych

Nowa wersja systemu Aviotec wykorzystuje algorytmy wykrywania dymu i płomieni, które zostały opracowane specjalnie z myślą o zastosowaniu systemu w tunelach i zoptymalizowane podczas kompleksowych testów przeprowadzonych w rzeczywistych warunkach. Do niezawodnego wykrywania dymu i płomieni kamery potrzebują światła z otoczenia o natężeniu zaledwie 7 luksów i wykorzystują funkcję inteligentnej analizy wideo. W celu umożliwienia zastosowania systemu w tunelach ponad dwukrotnie zwiększono zasięg detekcji (z 50 do ponad 100 metrów) dzięki użyciu nowych obiektywów. Zwiększony zasięg odpowiada standardowej odległości pomiędzy kamerami dozorowymi stosowanymi w podobnych warunkach. Dzięki takiemu rozwiązaniu system Aviotec umożliwia wykorzystanie tych samych kamer do dozoru wizyjnego oraz do wykrywania pożaru, co pozwala obniżyć nakłady inwestycyjne i koszty operacyjne.

Minimalizacja ryzyka wypadków dzięki dozorowi wizyjnemu

Do zminimalizowania ryzyka wypadków przyczynia się funkcja inteligentnej analizy wideo. Dzięki ciągłemu śledzeniu trajektorii ruchu kamery mogą automatycznie wykrywać pojazdy, które się zatrzymały, kierowców jadących pod prąd, a także ludzi znajdujących się na drodze. Podobnie jak w przypadku wykrycia dymu lub płomieni, system generuje powiadomienia, aby personel zajmujący się ochroną mógł natychmiast podjąć odpowiednie działania w celu zmniejszenia ryzyka wypadku. Inteligentna analiza wideo jest funkcją kamer, dlatego nie wymaga centralnego serwera, który mógłby ulec awarii. System Aviotec zapisuje także metadane wyszukiwane maszynowo, co umożliwia szybkie znajdowanie scen, gdy badane są przyczyny pożaru lub wypadku i zbierany jest materiał dowodowy.

Fot. 1. Szybkie i niezawodne wykrywanie dymu i płomieni

Jeszcze przed obecną aktualizacją system Aviotec był pierwszym wykorzystującym technikę wizyjną systemem wykrywania pożaru, który przeszedł wymagający test niemieckiej organizacji VdS Schadenverhütung GmbH. Procedura testowa VdS została przeprowadzona zgodnie z dyrektywami VdS 2203 *Requirements for fire protection software* oraz *Specifications for testing flame detectors*. System Aviotec IP Starlight otrzymał także certyfikat zgodności z australijską normą CSIRO TS010 dotyczącą systemów wykrywania pożaru stosujących technikę wizyjną.

W związku z tym, że Aviotec posiada certyfikaty VdS i CSIRO, może być wykorzystywany do poprawy wczesnego wykrywania pożaru i płomieni także w prawie każdym budynku o dużej kubaturze, ponieważ nie wymaga, aby w pobliżu czujki panowała wysoka temperatura lub docierał tam dym. Z tego powodu Aviotec sprawdzi się w dużych magazynach, hangarach, wielkopowierzchniowych centrach handlowych, pomieszczeniach z generatorami i w innych podobnych obiektach.

Operatorzy, którzy już używają systemu Aviotec, mogą skorzystać z bezpłatnej aktualizacji jego oprogramowania w celu uzyskania nowej wersji. Jeżeli wymagane jest zwiększenie zasięgu, po aktualizacji oprogramowania systemu może być potrzebny nowy obiektyw.

Opracowano na podstawie materiałów firmy Bosch Security and Safety Systems
Redakcja

Przydatność hydrantów wewnętrznych

Jan Dziedzic

Jeden z najlepszych opisów hydrantów wewnętrznych znajduje się na stronie internetowej czasopisma *Przegląd Pożarniczy* (w artykule Pawła Rochali pt. *Hydranty wewnętrzne*[1]). Nic dziwnego, ponieważ czasopismo jest wydawane przez Komendanta Głównego Państwowej Straży Pożarnej

Opis jest bardzo przejrzysty i dotyczy:
- rodzajów hydrantów wewnętrznych,
- zakresu stosowania hydrantów 25,
- zakresu stosowania hydrantów 33,
- zakresu stosowania hydrantów 52,
- zaworów hydrantowych,
- przeznaczenia hydrantów,
- hydrantów domowych.

Najciekawszy jest fragment dotyczący przeznaczenia hydrantów. Autor tekstu zastanawia się, dlaczego hydranty wewnętrzne są tak rzadko używane? Wyjaśnienie jest następujące:

1. Użycie gaśnicy (w początkowej fazie rozwoju pożaru) jest szybsze, bezpieczniejsze i przynosi znacznie mniej szkód.
2. Użycie hydrantu jest wolniejsze, mniej bezpieczne i może spowodować więcej szkód niż użycie gaśnicy.
3. Do użycia hydrantu potrzeba co najmniej dwóch osób, a w przypadku hydrantu 52 trzech, a czasem czterech osób.
4. Użycie hydrantu powinno nastąpić po wyłączeniu dopływu prądu do budynku. Należy użyć w tym celu przeciwpożarowego wyłącznika prądu. Do tego potrzebna jest ta czwarta osoba.
5. Bardzo niewiele osób, które nie są strażakami, jest przeszkolonych (z uwzględnieniem ćwiczeń praktycznych) w zakresie obsługi hydrantów, więc lepiej nie używać hydrantów wewnętrznych ze względu na wyżej wymienione problemy.
6. Nie ma jakichkolwiek danych, statystyk związanych z użyciem hydrantów wewnętrznych albo nie są one dostępne. Nie wiadomo, ile razy w ciągu roku użyto hydrantów wewnętrznych, czy kiedykolwiek ich użyto i jaki był skutek ich użycia (ugaszenie albo nieugaszenie pożaru, powiększenie albo niepowiększenie strat pożarowych itp.).

Zanim wypowiem się na temat przydatności hydrantów, opiszę przykładową instalację hydrantów wewnętrznych w budynku wysokim (trzy kondygnacje garażu podziemnego, wysoki parter z lokalami usługowymi i 14 pięter biurowych).

W jednym z istniejących budynków wysokich instalacja składa się z systemu rur o odpowiedniej średnicy, a także z:
- pompowni hydrantowej (dwie pompy oraz szafa zasilająca z falownikami, sygnalizacją, przełącznikami itp.);
- zaworu odcinającego zasilanie pompowni z sieci miejskiej (monitorowanego przez system sygnalizacji pożarowej);
- zestawu dwóch zaworów odcinających (monitorowanych przez system sygnalizacji pożarowej) zainstalowanych na wyjściu z pomp;
- zestawu dwóch zaworów zwrotnych, stosowanych przy pompach zasilających;
- zestawu sześciu hydrantów wewnętrznych 52 – po dwa hydranty na każdej kondygnacji (sześć szafek hydrantowych wyposażonych w zawór odcinający, zwijadło z jednym odcinkiem węża W-52 o długości 20 m, dodatkowy odcinek węża W-52 o długości 20 m, zwinięty w krąg lub ułożony w „harmonijkę", oraz prądownicę wodną dołączoną do odcinka węża na zwijadle);
- zestawu sześciu hydrantów wewnętrznych 25 – na parterze, w związku z liczbą lokali usługowych/najemców (sześć szafek hydrantowych wyposażonych w zawór odcinający, zwijadło z jednym odcinkiem węża W-25 o długości 30 m oraz prądownicę wodną);
- zestawu 39 hydrantów wewnętrznych 25 – po trzy na każdej z 13 kondygnacji biurowych (trzy szafki hydrantowe wyposażone w zawór odcinający, zwijadło z jednym odcinkiem węża W-25 o długości 30 m oraz prądownicę wodną dołączoną do węża na zwijadle[2]);
- zestawu czterech hydrantów wewnętrznych 52 na kondygnacji technicznej, umieszczonych ze względu na podział na strefy pożarowe w dwóch wentylatorniach, w kotłowni i w magazynach (cztery szafki hydrantowe

wyposażone w zawór odcinający, zwijadło z jednym odcinkiem węża W-52 o długości 20 m oraz prądownicę wodną dołączoną do odcinka węża na zwijadle);

Liczba poszczególnych elementów instalacji hydrantowej (oprócz rur i wyposażenia pompowni) w przykładowym budynku jest podana w tabeli.

Element	hydrant 52 (kompletny)	hydrant 25 (kompletny)	zawór hydrantowy 52	zawór odcinający	zawór redukujący ciśnienie	manometr
Ilość	16	39	62	38	21	80

- zestawu 16 zaworów hydrantowych (do dyspozycji straży pożarnej) zainstalowanych w przedsionkach przeciwpożarowych obu ewakuacyjnych klatek schodowych (na kondygnacjach od -3 do parteru) – po dwa zawory w każdym przedsionku ppoż.;
- zestawu dziesięciu zaworów hydrantowych (do dyspozycji straży pożarnej) zainstalowanych w przedsionkach przeciwpożarowych obu ewakuacyjnych klatek schodowych (na kondygnacjach od 1 do 5) – po jednym zaworze w każdym przedsionku;
- zestawu 36 zaworów hydrantowych (do dyspozycji straży pożarnej) zainstalowanych w przedsionkach przeciwpożarowych obu ewakuacyjnych klatek schodowych (na kondygnacjach od 6 do 14) – po dwa zawory w każdym przedsionku;
- zestawu 38 zaworów odcinających (stan zaworu jest monitorowany przez system SAP) do wykorzystania podczas awarii instalacji hydrantowej lub podczas remontu lub modyfikacji instalacji – po dwa zawory odcinające na każdej kondygnacji;
- zestawu 21 zaworów redukujących ciśnienie w instalacji hydrantowej (zmniejszających ciśnienie w instalacji do dopuszczalnej/maksymalnej wartości 0,7 b – zainstalowanych na wszystkich kondygnacjach garażowych, na parterze oraz na kondygnacjach biurowych (od 1 do 3);
- zestawu 38 manometrów zainstalowanych przy zaworach odcinających (za zaworami odcinającymi, jeśli patrzy się od strony zasilania);
- zestawu 42 manometrów zainstalowanych po obu stronach reduktorów ciśnienia (do nastaw i regulacji parametrów pracy zaworów redukcyjnych).

Koszt wykonania instalacji hydrantowej opisanej powyżej może wynieść ponad 200 000 zł. Koszty dodatkowe, ponoszone corocznie (przeglądy i pomiary pompowni i hydrantów oraz zaworów hydrantowych, badanie węży raz na pięć lat, ewentualne awarie, naprawy itp., koszt przeglądu instalacji sygnalizacji pożarowej w części monitorującej stan instalacji hydrantowej) mogą wynieść od kilku do kilkunastu tysięcy złotych. Od momentu rozpoczęcia użytkowania budynku przez kolejne dziesięć lat właściciel może wydać na instalację hydrantową nawet 500 000 zł. Czy musi? Musi! Czy warto? To pytanie należy zadać twórcom przepisów dotyczących ochrony przeciwpożarowej, w tym wyposażenia budynków w instalacje przeciwpożarowe.

Należy zastanowić się nad zasadnością stosowania szafek hydrantowych z wyposażeniem w instalacjach hydrantowych w budynkach wysokich (nie dotyczy to zaworów hydrantowych do dyspozycji straży pożarnej) ze względu na:

- brak statystyk dotyczących użycia hydrantów wewnętrznych, a tym bardziej informacji o skutkach ewentualnego użycia hydrantu,
- brak możliwości użycia hydrantu wewnętrznego bez wyłączenia prądu w budynku – przeciwpożarowy wyłącznik prądu może zostać użyty jedynie po decyzji kierującego działaniami ratowniczymi (dowódcy strażaków),
- brak umiejętności użycia hydrantu w przypadku użytkowników budynku (nieumiejętne użycie grozi utratą zdrowia, a nawet życia, ewentualnie powiększeniem strat pożarowych),

– krótki czas dojazdu samochodów gaśniczych Państwowej Straży Pożarnej.

Ponadto do przemyślenia jest fakt istnienia budynków wysokich (i nie tylko) wyposażonych w instalację tryskaczową (oczywiście taki budynek ma również system sygnalizacji pożarowej, dźwiękowy system ostrzegawczy, wentylację pożarową, jest wyposażony w gaśnice, jest podzielony na strefy pożarowe itp.). Czy wyposażenie budynku w instalację tryskaczową nie powinno zwalniać z obowiązku stosowania instalacji hydrantowej?

A może rozwiązaniem pośrednim byłoby zatrudnienie w budynku wysokim strażaka z doświadczeniem w gaszeniu pożarów (np. w systemie zmianowym w ramach ochrony)? Gdyby taki strażak miał przy sobie (np. w plecaku) odcinek węża W-52 z prądownicą (a dodatkowe odcinki byłyby w monitorowanym pomieszczeniu), po komunikacie o alarmie pożarowym z centrali SAP mógłby udać się we wskazane miejsce i ewentualnie (po uruchomieniu alarmu pożarowego drugiego stopnia skutkującego m.in. ewakuacją zagrożonej kondygnacji i wezwaniem PSP) podjąć próbę gaszenia pożaru, przyłączając wąż do zaworu hydrantowego w przedsionku przeciwpożarowym (przy założeniu, że budynek nie jest wyposażony w typowe szafki hydrantowe). Oczywiście do ugaszenia ewentualnego pożaru (zarzewia ognia) może wystarczyć gaśnica (strażak umie gasić gaśnicą skuteczniej niż przeciętny użytkownik budynku bez odpowiedniego przeszkolenia i doświadczenia).

Ponieważ koszt wykonania instalacji z zaworami hydrantowymi jest znacznie niższy niż koszt kompletnej instalacji (z szafkami, hydrantami oraz całą wymaganą aparaturą), właściciel lub zarządca budynku może mieć znacznie więcej pieniędzy na zatrudnienie strażaków. Zatrudnienie strażaków przyniosłoby dalsze spodziewane korzyści, np.: uniknięcie niepotrzebnej ewakuacji z budynku albo kondygnacji (strażak weryfikowałby alarmy z systemu SAP), nadzorowanie przez strażaka prac niebezpiecznych pożarowo (na etapie wydawania zgody, sprawdzenia miejsca prac, sprawdzenia przygotowania wykonawcy prac, odbioru prac i dodatkowej kontroli miejsca prac, np. w godzinę po ich zakończeniu w celu zmniejszenia ryzyka powstania pożaru), zgłaszanie przez strażaka wszelkich zagrożeń – zwłaszcza w związku z ewakuacją (zawężanie dróg ewakuacji) itp. Należy zauważyć, że strażak bez typowego wyposażenia, takiego jak w jednostkach PSP, podejmuje działania gaśnicze na podstawie własnej oceny sytuacji, bazując na swej wiedzy i doświadczeniu. W skrajnym przypadku odstępuje od działań gaśniczych i wprowadza do budynku (na zagrożoną kondygnację) strażaków PSP, opisując miejsce zagrożone (typowy pokój biurowy, archiwum, serwerownię itp.) i ewentualne zagrożenia.

W omawianym przykładowym obiekcie w ciągu ostatnich dziesięciu lat hydrant został użyty raz – pracownik ekipy sprzątającej użył hydrantu do umycia podłogi tarasu na jednej z najwyższych kondygnacji. Spowodowało to alarm pożarowy, ewakuację kondygnacji i przyjazd straży pożarnej. Po takich doświadczeniach podczas pożaru kontenera z odpadami ustawionego na dziedzińcu wewnętrznym (trwała przebudowa jednej z kondygnacji biurowych) strażak pracujący w ochronie obiektu użył węża ogrodowego służącego do czyszczenia tegoż dziedzińca, aby uniknąć alarmu pożarowego, ewakuacji z parteru i przyjazdu straży pożarnej (tak byłoby po użyciu hydrantu). Jak widać, zasadność stosowania instalacji hydrantowej w niektórych (a nawet w wielu) obiektach – zwłaszcza w budynkach wysokich, w obiektach wyposażonych w instalację tryskaczową, tam, gdzie zatrudnieni są strażacy – wydaje się wątpliwa.

Jan Dziedzic

Przypisy

1. https://www.ppoz.pl/index.php/rozpoznawanie-zagrozen/1895-hydranty-wewnetrzne (data dostępu: 12.03.2020).
2. W przypadku zastosowania hydrantów 33 – ze względu na ich zasięg – konieczne byłoby zainstalowanie trzech kompletnych szafek hydrantowych.

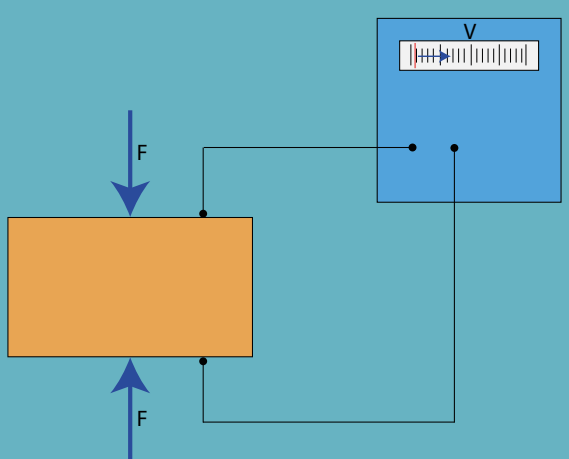
Czujniki piezoelektryczne
w systemach detekcji intruzów

Maciej Prelich

Sposoby włamań są coraz bardziej finezyjne, dlatego normy dotyczące systemów zabezpieczeń są coraz bardziej restrykcyjne, a wymagania użytkowników coraz większe. Nie wystarczy już, jak kiedyś, jeden prosty system. Obecnie klienci powinni decydować się na droższe, bardziej zaawansowane technicznie rozwiązania lub na połączenie kilku technik detekcji, np. kabel napłotowy lub zakopywany oraz kamery, jeśli naprawdę zależy im na skuteczności

Wielokrotnie na łamach magazynu *Zabezpieczenia* opisywaliśmy systemy DEA Security z unikatowym przetwornikiem piezoelektrycznym. Oferta bazująca na tym rozwiązaniu to system do ochrony wnętrz, systemy napłotowe na ogrodzenia sztywne, kable zakopywane, a nawet czujniki umieszczane pod posadzkami i podłogami technicznymi. Dla przypomnienia – detekcja za pomocą czujników piezoelektrycznych polega na przetworzeniu sił działających na sensor na napięcie elektryczne, co jest zobrazowane na rys. 1.

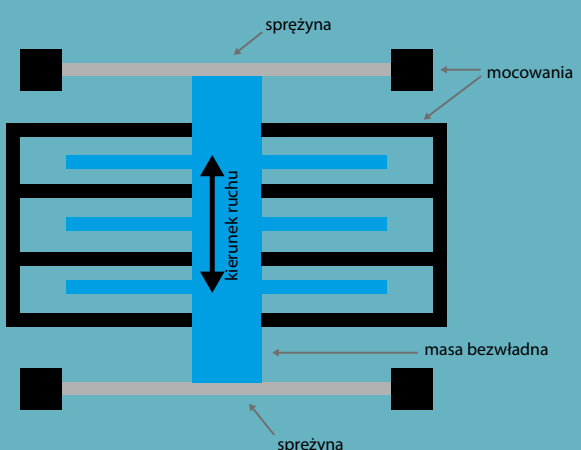
Opisana oferta została doceniona przez wojsko, służby specjalne, straż graniczną i w przemyśle petrochemicznym, a więc przez najbardziej wymagających klientów. Na szczególną uwagę zasługuje DEA Serir P2P. Jest to system montowany na ogrodzeniach, umożliwiający bardzo precyzyjną lokalizację intruza (z dokładnością do pojedynczego czujnika), a jednocześnie odporny na działanie czynników atmosferycznych oraz potencjalne próby sabotażu termicznego, mechanicznego lub magnetycznego. Systemowi zarzucano jednak zbyt wysoką cenę utrudniającą sprzedaż w krajach rozwijających się.



Rys. 1. Schemat działania przetwornika piezoelektrycznego

Producent stworzył nowy system – DEA Fusion P2P, który wykorzystuje do detekcji przetworniki piezoelektryczne oraz akcelerometry. Rozwiązanie to nosi nazwę DEA Sensor Fusion (DSF) i zapewnia niespotykaną do tej pory skuteczność detekcji oraz wielość zastosowań. Akcelerometry to czujniki reagujące na przyspieszenia w ruchu liniowym oraz kątowym. Uproszczony schemat wyjaśniający zasadę ich działania jest przedstawiony na rys. 2. Na skutek zetknięcia się masy

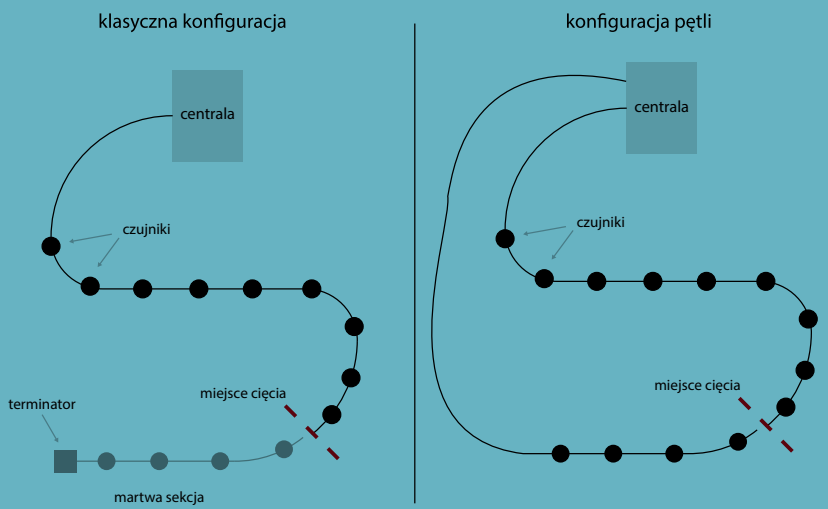
Fot. 1. Nowy czujnik DEA Fusion P2P



Rys. 2. Uproszczony schemat wyjaśniający zasadę działania akcelerometru

bezwładnej z mocowaniem wytwarzane jest napięcie elektryczne, a na podstawie jego wartości ustalane jest przyspieszenie. Akcelerometry dokonują pomiarów własnego ruchu względem ustalonej płaszczyzny.

System DEA Fusion P2P może być zainstalowany na ogrodzeniu każdego rodzaju (miękkim, panelowym i sztywnym), a nawet na ścianach, a dzięki zastosowaniu dwóch technik detekcji alarm jest wyzwalany tylko w momencie odebrania sygnałów z dwóch źródeł. Stale usprawniane algorytmy detekcji, rozwijane od ponad 20 lat, umożliwiają skuteczną detekcję intruzów, ustalenie przyczyny alarmu (przecięcie, przebicie, próba wspinaczki, próba sabotażu), a także



Rys. 3. Następstwo przecięcia kabla w zależności od typu połączenia

wyeliminowanie fałszywych alarmów powodowanych przez zakłócenia. Dzięki dokładnemu przeanalizowaniu, jak system pracuje na różnych ogrodzeniach i ścianach, możliwe było przygotowanie siedmiu inteligentnych algorytmów przeznaczonych do obróbki sygnałów z czujników pracujących na różnych rodzajach ogrodzeń. Dodatkowo, dzięki technice Point ID, która polega na pojedynczym indeksowaniu każdego sensora, możliwe jest ustawienie odpowiedniego algorytmu dla każdego czujnika z osobna.

Kolejną nową cechą systemu jest konfiguracja pętli, dzięki której może on nadal działać nawet w razie przecięcia kabla, ponieważ czujniki znajdujące się za miejscem przecięcia są połączone z centralą z drugiej strony pętli. W przypadku tradycyjnego połączenia wszystkie czujniki znajdujące się za miejscem przecięcia tracą połączenie z centralą. Oba scenariusze są zobrazowane na rys. 3.

Pomimo istotnych usprawnień, nowych funkcji i zwiększenia skuteczności i elastyczności udało się znacznie obniżyć cenę systemu – w zależności od zastosowania nawet do 30–40% w porównaniu z Serirem P2P. Powinno to mieć odzwierciedlenie w pozytywnej ocenie i zainteresowaniu potencjalnych użytkowników.

Nowe rozwiązania techniczne znajdują zastosowanie również w systemie DEA Xensity przeznaczonym do ochrony wnętrz (asortyment oferowanych czujników powiększono, a detektory przeznaczone do ochrony drzwi oraz ścian wykorzystują DEA Sensor Fusion) oraz w zupełnie nowym systemie SPC Pro, który omówimy szczegółowo w przyszłości.

Tworzenie nowych systemów oraz wprowadzanie nowych technik detekcji zawsze jest krokiem naprzód. Z jednej strony wydajność i skuteczność detekcji intruzów w systemach ochrony obwodowej jest stale poprawiana, z drugiej, dzięki licznym optymalizacjom, nawet najlepsze systemy mogą być wykorzystywane nie tylko przez służby specjalne i wojsko, lecz także w przemyśle, centrach logistycznych oraz obiektach infrastruktury krytycznej – tam, gdzie potrzebne są coraz lepsze zabezpieczenia. Skuteczne systemy detekcji intruzów pozwalają nie tylko zabezpieczyć sam obiekt, lecz często także obniżyć koszty związane z jego ubezpieczeniem. Czekamy z niecierpliwością na kolejne zabezpieczenia firmy DEA Security.

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

NODEX

www.IBPNODEX.pl

Niezależny Ośrodek Doradców i Ekspertów

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

Atrakcyjne zniżki dla Członków Wspierających Rozwój Instytutu!

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

Instytut Bezpieczeństwa Pożarowego NODEX Sp. z o.o.
ul. Pola Karolińskie 4, 02-401 Warszawa
tel.: +48 22 203 59 21, fax: +48 22 203 58 31

www.IBPNODEX.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. 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
e-mail: biuro@acss.com.pl
www.acss.com.pl

D S

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

D 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. Iłżecka 24 bud. F
02-135 Warszawa
tel. 22 751 53 54; faks 22 751 53 56
e-mail: biuro@assaabloy.com
www.assaabloy.com.pl

D I PROD PROJ S

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

C D PROJ S

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

I PROJ

BT Electronics Sp. z o.o.
ul. Rybitwy 22
30-722 Kraków
tel. 12 410 20 33, faks 12 410 85 11
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
e-mail: info@cbcpoland.pl
www.cbcpoland.pl

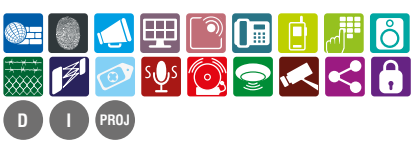
D PROD S

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

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@dahuatech.com
www.dahuasecurity.com/pl

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



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

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

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

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

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

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

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

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

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

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

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

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

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

ES-INSTAL Andrzej Wójcik
Al. gen. W. Sikorskiego 9 A/72 A
02-758 Warszawa
tel. kom. +48 501 277 513
e-mail: andrzejw@esinstal.pl
https://esinstal.pl/

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

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

GDE POLSKA
Leszek Mitusiński
Włosań, ul. Świątnicka 88
32-031 Mogilany
tel. 12 256 50 25, 12 256 50 35;
faks 12 270 56 96
e-mail: biuro@gde.pl
www.gde.pl

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

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

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

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

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

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

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

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

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

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

ROPAM Elektronik s.c.
Polanka 301
32-400 Myślenice
tel. 12 341 04 07
e-mail: biuro@ropam.com.pl
www.ropam.com.pl

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

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

smart-technologie
SYSTEMY OGNIOCHRONNE
TECHNIKA MONTAŻU BEZPOŚREDNIEGO

SMART-EKO Jarosław Szkaradek
(SMART-TECHNOLOGIE.PL)
ul. Domagały 1
30-741 Kraków
tel. kom. +48 791 061 485, 793 061 485
e-mail: biuro@smart-eko.pl
www.smart-technologie.pl

TAP

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

TECHOM

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

W2

W2 Włodzimierz Wyrzykowski
ul. Ceramiczna 1A
86-005 Kruszyn Krajeński
tel. 52 522 32 38
e-mail: biuro@w2.com.pl
www.w2.com.pl

Always precise WINKHAUS

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

Legenda

Kategorie*

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

Działalność*

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

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

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Paweł Karczmarzyk
Andrzej Walczyk

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

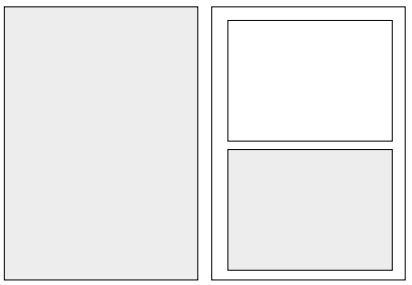
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie

Spis teleadresowy
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Ceny negocjujemy indywidualnie

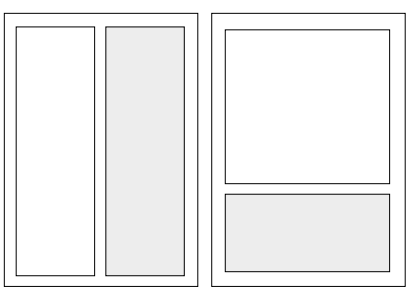
Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej http://www.zabezpieczenia.com.pl w dziale Reklama

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



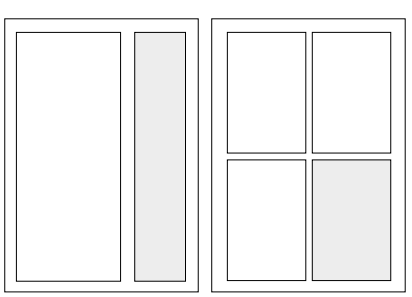
cała strona
(200 x 282 mm + 3mm spad)

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

NMS ACCESS CONTROL

PROFESJONALNE ROZWIĄZANIE
DO SYSTEMÓW KONTROLI DOSTĘPU
I NADZORU WIZYJNEGO

POZNAJ
NAJNOWSZE
OPROGRAMOWANIE

ODWIEDŹ NASZ ODDZIAŁ
JUŻ DZIŚ!

www.nmsac.aat.pl

Wielostanowiskowa obsługa systemu, struktura typu SERWER – KLIENT
Współpraca z nowymi kontrolerami serii KS3000
Bezpieczna baza typu MS SQL dla danych i zdarzeń
Integracja z rejestratorami NVR i kamerami IP marki NOVUS

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

FUJIFILM
Value from Innovation

HIGH-END CAMERA X TOP PERFORMANCE LENS

THE NEW FUJINON SX800. THE BEST OF BOTH.

With the new SX800, Fujinon combines both in one for the first time: camera and lens. For long range surveillance at the highest level with 40x optical magnification and constantly sharp images. **www.fujifilm.eu/sx800. Fujinon. To see more is to know more.**

FUJINON