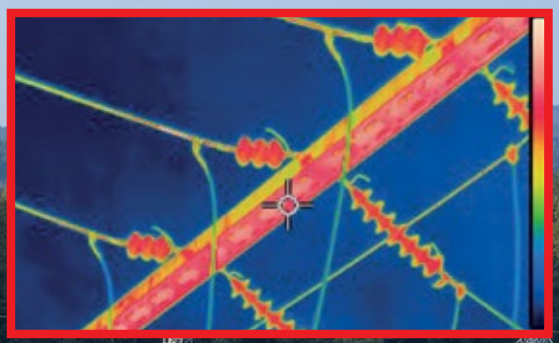
CZASOPISMO BEZPŁATNE
ISSN: 1505-2419 DWUMIESIĘCZNIK NR 5(129)/2019

ZABEZPIECZENIA

VIDEOTEC



Ulisse evo Thermal

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

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

ONVIF | S Q

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

VIDEOTEC

VIDEO SECURITY PRODUCTS

www.videotec.com

Made in Italy

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

SPIS TREŚCI

Nowości produktowe

6 Kamery kopułkowe Bosch FLEXIDOME IP starlight 8000i – czas uruchamiania i instalacji ograniczony nawet o 75% dzięki innowacyjnej koncepcji
– Bosch Security and Safety Systems

7 TL-SF1005P i TL-SG1005P – wydajne i kompaktowe przełączniki sieciowe przeznaczone do stosowania w domowych systemach nadzoru wizyjnego
– Iwo Ostalski, TP-Link Polska

8 64-kanałowy rejestrator NOVUS z serii 6000
– Patryk Gańko, AAT HOLDING

10 Identyfikacja mobilna w systemie RACS 5
– ROGER

11 System RACS 5 w wersjach LT, ST i EX
– ROGER

12 Seria 7 – sztuczna inteligencja dostępna dla każdego
– Grzegorz Długosz, Dahua Technology Poland

13 Autonomiczny rejestrator czasu pracy z funkcją kontroli dostępu
– Grzegorz Michalski, Dahua Technology Poland

14 PNM-9000VD z serii Wisenet P firmy Hanwha Technology – dwuobiektywowa kamera o rozdzielczości 5 Mpx
– Hanwha Techwin Europe

16 Kamera IP Starlight w jednej obudowie z obiektywem motor-zoom
– Patryk Gańko, AAT HOLDING

Wydarzenia, informacje

18 16 edycja Kongresu Pożarnictwa FIRE | SECURITY EXPO 2019 – podsumowanie
– Ela Końka

Telewizja dozorowa

20 Prognozowana wartość światowego rynku wizyjnych systemów dozorowych od trzech lat utrzymuje silną tendencję wzrostową
– Jon Cropley, IHS Markit

22 Nowy zintegrowany system dozorowy firmy Fujifilm do obserwacji rozległych obszarów. Sukces rynkowy systemu kamerowego Fujinon SX800
– Fujifilm Optical Devices Europe

24 Skuteczna ochrona prywatności w systemach dozoru wizyjnego
– Axis Communications

28 Łatwość obsługi ważną zaletą systemów dozoru wizyjnego
– Axis Communications

Radiokomunikacja

30 **Rola anten w systemach monitorowania alarmów na przykładzie produktów firmy Poynting. Część 2**
– Poynting

Kontrola dostępu

36 **NMS ACCESS CONTROL – czas na start**
– Ryszard Sobierski, AAT HOLDING

Systemy sygnalizacji pożarowej

42 **Nadzorowanie pomieszczenia z podestem**
– Jerzy Ciszewski, IBP NODEX

46 **Wydruki z centrali SAP**
– Jan Dziedzic

Nowe technologie

50 **Technologie jutra**
– Maciej Pietrzak, Dahua Technology Poland

54 **AI dla każdego. Część 5**
– Piotr Rogalewski

Porady prawne

60 **Nowe prawo zamówień publicznych**
– Joanna Filipiak

Case Study

62 **Bosch zabezpiecza Port Praski – miasto nowej generacji**
– Bosch Security and Safety Systems

66 **Spis teleadresowy**

70 **Spis reklam**

Kamery kopułkowe Bosch FLEXIDOME IP starlight 8000i

Czas uruchamiania i instalacji ograniczony nawet o 75% dzięki innowacyjnej koncepcji

Innowacyjna koncepcja upraszcza proces wstępnej konfiguracji, instalację oraz uruchamianie kamer FLEXIDOME. Dzięki temu czas instalacji i uruchamiania systemu jest nawet o 75% krótszy niż w przypadku tradycyjnych kamer sieciowych. Instalacja kamer **FLEXIDOME IP starlight 8000i** jest bardzo łatwa. Należy tylko zamontować uchwyt mocujący, podłączyć kable i zamocować moduł kamery. Dzięki funkcji zdalnego uruchamiania moduł kamery pozostaje w zamknięciu przez cały proces instalacji i konfiguracji, co zapewnia ochronę przed zanieczyszczeniami.

Wszystkie kamery FLEXIDOME IP starlight 8000i mają nową funkcję Camera Trainer, która jest kolejnym etapem rozwoju metod analizy treści obrazu i umożliwia wykorzystanie „uczenia maszynowego" w kamerach **Bosch**. Dzięki Camera Trainer integratorzy systemów mogą dostosować parametry inteligentnej analizy treści obrazu do wymagań danego klienta. Funkcja może mieć także inne zastosowania, takie jak np. identyfikacja poszczególnych pojazdów stojących jeden za drugim na światłach albo określenie czasu postoju samochodu zaparkowanego w zatoce.

We wszystkich kamerach serii FLEXIDOME IP starlight 8000i dostępna jest funkcja Starlight. Wszystkie modele kamer (o rozdzielczościach HD 1080p, 6 megapikseli i 4K ultra HD) zapewniają bardzo wysoki poziom szczegółowości obrazu, także przy słabym oświetleniu. Szybko poruszające się obiekty są w łatwy sposób rejestrowane z częstotliwością do 60 klatek na sekundę, a szeroki zakres dynamiki (do 134 dB) pozwala kompensować nierównomierność oświetlenia ciemnych i jasnych fragmentów obserwowanych scen.

Kamery są wodoodporne (IP66), mają wysokiej jakości podwójną powłokę, która dodatkowo chroni przed korozją, są odporne na akty wandalizmu (IK10+) i mogą być stosowane w temperaturach od -50 do +60°C. Można je zamontować zarówno w pomieszczeniach, jak i na zewnątrz.

Bezpośr. inf. Bosch Security and Safety Systems

TL-SF1005P i TL-SG1005P

wydajne i kompaktowe przełączniki sieciowe przeznaczone do stosowania w domowych systemach nadzoru wizyjnego

TL-SF1005P

TL-SG1005P

Przełączniki **TL-SF1005P** i **TL-SG1005P** zostały zaprojektowane specjalnie z myślą o nadzorowaniu obiektów z wykorzystaniem kamer sieciowych. Znajdujące się w nich porty uplink ułatwią połączenie z istniejącą siecią domową. Dzięki zasilaniu kamer metodą PoE instalacja systemu jest łatwa, bezpieczna i mniej kosztowna. Urządzenia nie wymagają żadnej konfiguracji.

Przełącznik TL-SG1005P ma pięć portów RJ45 10/100/1000 Mb/s, przy czym cztery z nich mogą być użyte do zasilania urządzeń peryferyjnych metodą PoE, zgodnie ze standardem IEEE 802.3af. Dopuszczalny pobór mocy z każdego z portów PoE jest równy 15,4 W, zaś łączny pobór mocy ze wszystkich portów PoE wynosi 56 W.

Przełącznik TL-SG1005P realizuje funkcję QoS zgodnie ze standardem 802.1p, klasyfikacją DSCP i z wykorzystaniem funkcji IGMP Snooping.

Przełącznik TL-SF1005P ma konstrukcję identyczną jak przełącznik TL-SG1005P. Jest wyposażony w pięć portów RJ45 10/100 Mb/s, przy czym cztery z nich mogą zasilać urządzenia zgodne ze standardem PoE IEEE802.3af. Maksymalny pobór mocy z każdego z portów PoE to 15,4 W, a ze wszystkich łącznie wynosi 58 W.

Ani jeden, ani drugi przełącznik nie wymaga wstępnej konfiguracji. Każdemu z czterech portów z funkcją PoE przypisany jest inny priorytet, dzięki czemu przełączniki mogą poprawnie pracować w warunkach przeciążenia spowodowanego nadmiernym poborem prądu. Urządzenia podłączone do portów o wyższym priorytecie są zasilane w pierwszej kolejności.

Bezpośr. inf. Iwo Ostalski
TP-Link Polska

64-kanałowy rejestrator NOVUS
z serii 6000

Do autonomicznych rejestratorów **NOVUS** z serii 6000 dołączony został model **NVR-6364-H8/R** obsługujący do 64 kamer. Strumienie wizyjne mogą być kodowane w formacie H.265 z rozdzielczością do 8 Mpx. W celu efektywnego obserwowania obrazów przez operatora urządzenie zostało wyposażone w wyjścia monitorowe trzech rodzajów – główne HDMI o rozdzielczości 4K i prędkości odświeżania 60 Hz, VGA oraz pomocnicze HDMI o rozdzielczości Full HD. Dla wyjścia głównego i wyjść pomocniczych operator może ustalić dowolne podziały ekranu i przyporządkować do nich strumienie wizyjne ze wszystkich 64 kamer.

W celu archiwizacji takiej ilości danych rejestrator został wyposażony w osiem złącz SATA oraz dwa niezależne złącza eSATA do podłączenia dysków o pojemności do 8 TB. Bezpieczeństwo danych jest zagwarantowane przez wbudowany, sprzętowy kontroler RAID obsługujący tryby RAID0, RAID1, RAID5, RAID6 i RAID10.

Rejestrator został wyposażony w dwa interfejsy sieciowe 1000 Mb umożliwiające równoczesny dostęp nawet 20 użytkowników. Dostęp jest możliwy z użyciem oprogramowania klienckiego oraz komputera z systemem operacyjnym Windows lub macOS, za pomocą urządzenia mobilnego z systemem operacyjnym Android lub iOS, a także z użyciem przeglądarki sieciowej.

Opisywany rejestrator, podobnie jak pozostałe rejestratory z serii 6000, ma inteligentne funkcje do analizy treści obrazu, w tym wykrywanie pojawienia się albo zniknięcia obiektu, przekroczenia linii, wejścia do zakazanej strefy oraz sabotażu.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

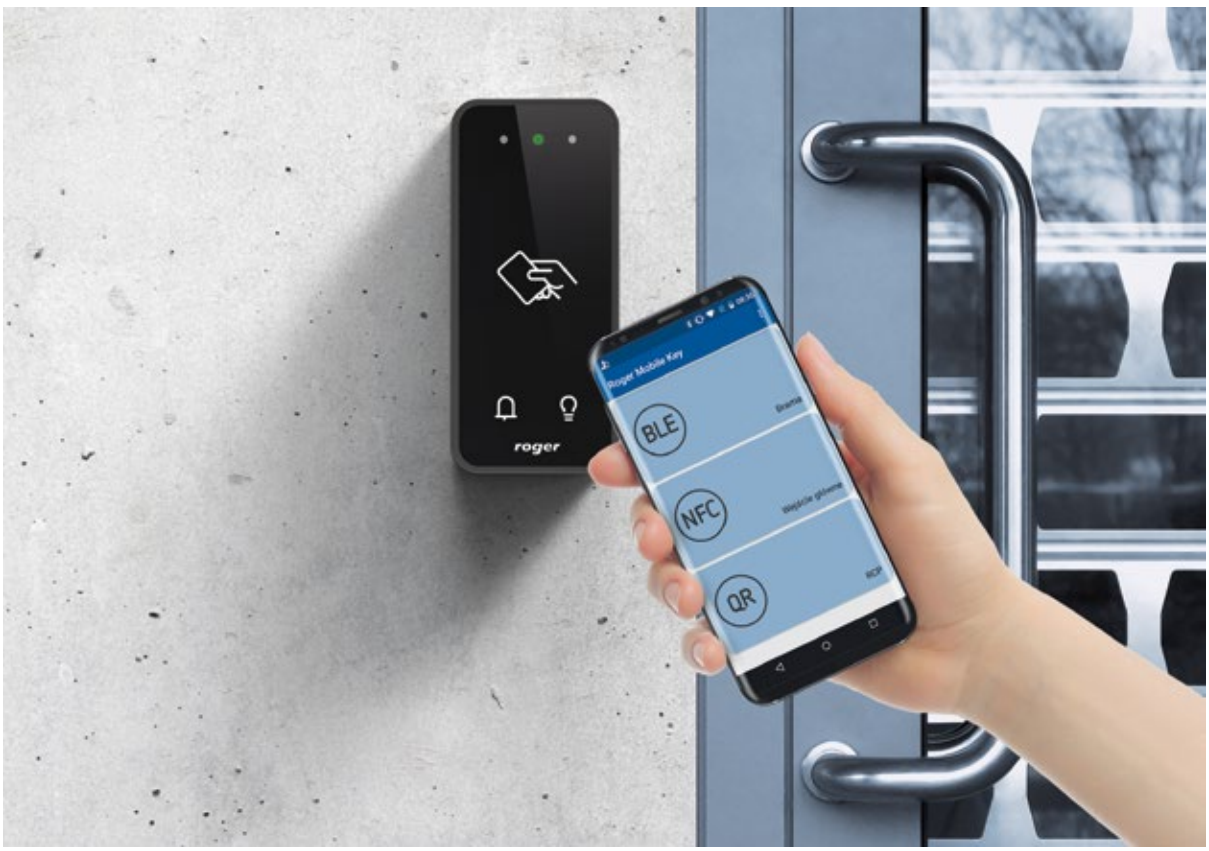
NOVUS®

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

Identyfikacja mobilna w systemie RACS 5



Oprócz standardowych metod potwierdzania tożsamości, np. za pomocą karty oraz kodu PIN, system **RACS 5** umożliwia użycie w tym celu urządzeń mobilnych – smartfonów i tabletów. W takim przypadku kod identyfikatora może być przekazany do czytnika za pomocą NFC, Bluetooth LE (BLE) lub na skutek wyświetlenia kodu kreskowego QR na ekranie urządzenia przenośnego.

Logowanie z wykorzystaniem NFC oraz kodu QR wymaga zbliżenia urządzenia mobilnego do czytnika na odległość kilku centymetrów. W przypadku wykorzystania BLE urządzenie mobilne może znajdować się w odległości kilku metrów od czytnika, co może ułatwić potwierdzanie tożsamości w miejscach wjazdu i bramach. Kod identyfikacyjny jest przechowywany w urządzeniu mobilnym w postaci tzw. klucza elektronicznego REK (Roger Electronic Key). Klucz REK to zaszyfrowany plik zawierający kod identyfikacyjny użytkownika, a także dodatkowe informacje określające warunki wykorzystania klucza. Taki klucz można utworzyć za pomocą aplikacji mobilnej RMK (Roger Mobile Key) lub otrzymać od administratora systemu RACS 5 (np. pocztą elektroniczną).

Użytkownik może posiadać wiele kluczy REK i używać ich w zależności od potrzeb na różnych przejściach lub w punktach rejestracyjnych systemu RCP. Potwierdzanie tożsamości za pomocą urządzeń mobilnych może zarówno być stosowane jako uzupełnienie tradycyjnych metod logowania z użyciem karty zbliżeniowej oraz PIN-u, jak i zastępować te metody.

Aplikacja RMK jest dostępna w wersjach dostosowanych do systemów Android oraz iOS. W chwili obecnej logowanie za pomocą urządzenia mobilnego jest możliwe w przypadku zastosowania terminali MCT88M-IO lub MCT80M-BLE (NFC, BLE).

Bezpośr. inf. ROGER

System RACS 5
w wersjach LT, ST i EX

W ramach dalszego rozwoju systemu kontroli dostępu, bezpieczeństwa i automatyki budynkowej RACS 5 system ten będzie dostępny w trzech wersjach – **RACS 5 LT, RACS 5 ST i RACS 5 EX**. Celem tego zabiegu jest lepsze dostosowanie oferty do potrzeb.

Wersja RACS 5 LT jest przeznaczona do wykorzystania w miejscach, w których wymagania dotyczące systemu kontroli dostępu są typowe i potrzebna jest standardowa integracja z systemem alarmowym, VSS oraz RCP. Do tej wersji systemu przeznaczony jest program zarządzający VISO LT oraz specjalna linia niedrogich kontrolerów dostępu z serii MC16-LT.

Program VISO LT charakteryzuje się uproszczonym interfejsem użytkownika, który przyśpiesza proces konfiguracji systemu oraz ułatwia jego późniejszą obsługę.

Wersja RACS 5 ST jest przeznaczona do obsługi średnich i dużych obiektów, w których wymagane są bardziej zaawansowane funkcje i możliwości integracji niż to miało miejsce w systemie RACS 5 LT.

Wersja RACS 5 EX jest przeznaczona do zastosowania w średnich i dużych obiektach, w których potrzebna jest integracja programowa z systemami inteligentnych wind, obsługa parkingów, obsługa szafek i schowków, monitorowanie obiegu wyposażenia, w tym kluczy, a także integracja z innymi systemami inteligentnego budynku, które wraz z systemem RACS 5 mają tworzyć jednolite środowisko sprzyjające komfortowemu i produktywnemu wykorzystaniu nowoczesnego biurowca. W przypadku wersji RACS 5 EX wymagane jest stosowanie kontrolerów dostępu z serii MC16-EX.

Niezależnie od wersji w systemie RACS 5 mogą być wykorzystane dowolne urządzenia peryferyjne (ekspandery, czytniki, interfejsy), które są do niego dostosowane.

Bezpośr. inf. ROGER

Seria 7
sztuczna inteligencja dostępna dla każdego

W dobie ukierunkowania świata na rozwój nowych technologii opartych na sztucznej inteligencji i algorytmach uczenia maszynowego **Dahua Technology** – jeden z liderów w branży zabezpieczeń – przenosi systemy nadzoru wizyjnego na nowy poziom rozwoju technologicznego. Dobrym przykładem jest kamera **DH-IPC-HFW7842H-Z** z serii Ultra-AI. Sercem tego urządzenia jest chipset HiSilicon realizujący zaawansowane algorytmy uczenia maszynowego, a obraz o bardzo wysokiej jakości jest dostarczany przez przetwornik CMOS Starlight o przekątnej 1/1,8" i rozdzielczości 8 megapikseli, odznaczający się wysoką czułością oraz szerokim zakresem dynamiki obrazu. Kamera sieciowa Ultra-AI ma nowe inteligentne funkcje, które sprawdzają się nawet w najtrudniejszych warunkach oświetleniowych, a dzięki algorytmom głębokiego uczenia się urządzenie lepiej niż dotychczas wykonuje kluczowe zadania, takie jak rozpoznawanie twarzy, liczenie osób, ochrona perymetryczna, strukturyzacja obrazu z podziałem na kategorie rozpoznanych obiektów oraz rozpoznawanie tablic rejestracyjnych pojazdów.

Zastosowanie algorytmów sztucznej inteligencji poprawia wydajność i precyzję analizy treści obrazu w porównaniu ze stosowanymi wcześniej funkcjami wykorzystywanymi w kamerach. Przykładem może być algorytm korzystający z wielu baz danych, umożliwiający szybką identyfikację osób na podstawie obrazu twarzy. Do liczenia ludzi wykorzystano algorytm głębokiego uczenia się w celu wykrywania cech ludzkiego ciała i śledzenia celu w czasie rzeczywistym. Na tej podstawie tworzone są statystyki liczby wejść i wyjść z dokładnością do 98%. Do ochrony perymetrycznej wykorzystuje się podział obiektów na typy oraz tworzenie niestandardowych granic. Umożliwia to automatyzację procesu identyfikacji intruzów w miejscach o ograniczonym dostępie, takich jak strefy przeznaczone wyłącznie dla pojazdów lub strefy tylko dla pieszych.

Dodatkowym atutem jest transmisja danych metodą ePoE z wykorzystaniem zaawansowanego kodowania 2D-PAM3 w warstwie fizycznej łącza sieciowego – obrazy mogą być przekazywane drogą kablową na odległość ponad 800 metrów przy prędkości 10 Mb/s lub 300 metrów przy prędkości 100 Mb/s. Przekłada się to na bardziej elastyczną konstrukcję systemu nadzoru, poprawia niezawodność oraz ogranicza koszty budowy i okablowania.

Bezpośr. inf. Grzegorz Długosz
Dahua Technology Poland

Autonomiczny rejestrator czasu pracy z funkcją kontroli dostępu

Firma **Dahua Technology** pracuje nad rozszerzeniem swojej oferty w zakresie systemów kontroli dostępu, czego efektem jest wprowadzenie do sprzedaży kontrolera **ASA1222G**. Terminal jest odpowiedzią na sugestie ze strony klientów poszukujących rozwiązań intuicyjnych i prostych w obsłudze, dla takich obiektów jak biura, punkty gastronomiczne, sklepy, oddziały banków, hotele, szkoły.

Po zainstalowaniu terminalu na ścianie trzeba tylko podłączyć go do źródła zasilania. Dodatkowo można podłączyć kontroler do sieci TCP/IP w celu zdalnego zarządzania poprzez aplikację Smart PSS. Oprócz funkcji związanej z rozliczaniem czasu pracy jest też możliwość kontroli dostępu do wybranego pomieszczenia.

Kontroler występuje w dwóch wersjach. Model ASA1222G obsługuje identyfikatory Mifare Classic (13,56 MHz), a model ASA1222G-D identyfikatory Unique (125 kHz). Tożsamość użytkowników może być weryfikowana na podstawie kodu PIN, wzoru linii papilarnej lub użycia karty. Moduł biometryczny cechuje się krótkim czasem identyfikacji (poniżej 1,5 s), niskim współczynnikiem błędnych odrzuceń (FRR < 0,5%) i niskim współczynnikiem błędnych akceptacji (FAR < 0,00004%). Pamięć kontrolera umożliwia obsługę 1000 użytkowników i 100 000 zdarzeń. W przykładowym systemie obsługującym 100 pracowników i przy założeniu, że każdy z użytkowników generuje cztery zdarzenia dziennie, tj. wejście, rozpoczęcie przerwy, zakończenie przerwy, wyjście, urządzenie jest w stanie zgromadzić logi z 250 dni. Po tym czasie najstarsze zdarzenia zostaną nadpisane. W celu trwałego zarchiwizowania zdarzeń należy przenieść dane do bazy danych programu Smart PSS.

Pracownik ma możliwość korzystania z intuicyjnego interfejsu wyposażonego w wyświetlacz TFT 2,4", informującego o typie zdarzenia RCP. Dodatkowo na wyświetlaczu wyświetlana jest aktualna data i godzina. Do obsługi interfejsu służy klawiatura wyposażona w 16 mechanicznych przycisków. Każde zdarzenie jest dodatkowo potwierdzane komunikatem głosowym.

Do analizy zdarzeń związanych z rejestracją czasu pracy administrator może wykorzystać szablony najbardziej popularnych typów raportów lub – po wyeksportowaniu zdarzeń do pliku .xls – przygotować własny szablon.

Pomimo swoich kompaktowych rozmiarów terminal ma baterię o pojemności 2600 mAh umożliwiającą pracę urządzenia przez ok. dziesięciu godzin przy odłączonym zasilaniu sieciowym, wyjście przekaźnikowe do obsługi elementu ryglującego, np. zwory elektromagnetycznej lub elektrozaczepu, oraz wejście do podłączenia przycisku wyjścia.

W celu zapoznania się z pozostałymi produktami z oferty firmy Dahua Technology zapraszamy do obejrzenia strony https://www.dahuasecurity.com/ lub do odwiedzenia siedziby jednego z naszych partnerów.

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

PNM-9000VD z serii Wisenet P firmy Hanwha Technology

dwuobiektywowa kamera o rozdzielczości 5 Mpx

Najnowsza kamera z serii **Wisenet P** firmy **Hanwha Techwin** – **PNM-9000VD** – łączy w sobie funkcje dwóch kamer. Jest to kamera dwukierunkowa z funkcjami analizy treści obrazu. Jest wyposażona w dwa osobne obiektywy modułowe. Wytwarza doskonałej jakości obrazy przyległych obszarów. Obrazy te mają rozdzielczość 5 Mpx. W zależności od wymaganego pola widzenia w kamerze PNM-9000VD można zamontować moduły obiektywów o ogniskowych 3,7 mm, 4,6 mm lub 7 mm (dostępne osobno).

Ekonomiczność

Tak jak w przypadku wielokierunkowych kamer Wisenet PNM-7000VD o rozdzielczości 2 Mpx, które wprowadzono na rynek w 2018 r., również dzięki wielostrumieniowemu modelowi Wisenet PNM-9000VD można znacznie zmniejszyć koszty instalacji systemu (standardowo konieczne byłoby zainstalowanie dwóch osobnych kamer, np. w celu monitorowania dwóch odcinków korytarza w kształcie litery L lub dwóch stron budynku). W związku z tym PNM-9000VD można zastosować w miejscach, gdzie trzeba nadzorować dużą, otwartą przestrzeń, np. na parkingach, w centrach handlowych i w magazynach.

PNM-9000VD wymaga tylko jednego adresu IP, mimo że generuje dwa różne strumienie wizyjne. Potrzebna jest też tylko jedna licencja na oprogramowanie do zarządzania systemem wizyjnym (VMS), co jeszcze bardziej obniża koszt posiadania systemu, podobnie jak zasilanie metodą PoE, dzięki której nie trzeba kłaść okablowania zasilającego.

WiseStream II

PNM-9000VD obsługuje formaty kompresji H.264, H.265 i MJPEG. Przepływność strumienia wizyjnego można też zmniejszyć nawet o 99% w porównaniu z obrazem skompresowanym powszechnie stosowaną metodą H.264, jeśli zostanie zastosowane połączenie kompresji H.265 z funkcją WiseStream II, która dynamicznie steruje kodowaniem, równoważąc jakość i poziom kompresji zależnie od ruchu w kadrze.

Najważniejsze funkcje

Do najważniejszych funkcji kamery PNM-9000VD należy zaliczyć szeroki zakres dynamiczny (WDR) sięgający 120 dB. Umożliwia on uzyskiwanie wyraźnych obrazów nawet wówczas, gdy w kadrze jednocześnie znajdują się obszary bardzo jasne i bardzo ciemne. Na uwagę zasługuje też korekcja zniekształceń obrazu wprowadzanych przez obiektyw i cyfrowa stabilizacja obrazu. Funkcje analizy treści obrazu, o których należy wspomnieć, to detekcja twarzy, detekcja pojawienia się albo zniknięcia przedmiotów, wykrycie podejrzanego zachowania osób oraz wykrycie przekroczenia wirtualnej linii. Do funkcji poprawiających czytelność obrazu należy zaliczyć redukcję zamglenia i pracę w trybie korytarzowym. W kamerze znajdziemy miejsce na dwie karty pamięci SD/SDHC/SDXC. PNM-9000VD jest odporna na trudne warunki pogodowe i działania wandali, co potwierdzają klasy odporności IK10 i szczelności IP66.

Bezpośr. inf
Hanwha Techwin Europe

Kamera IP Starlight

w jednej obudowie z obiektywem motor-zoom

Seria kamer 4000 IP marki **NOVUS** została powiększona – dodano do niej model **NVIP-2H-4412M/F**. Kamera została wyposażona w gwarantującą wysoką czułość matrycę CMOS 1/2.8" Sony STARVIS, popularnie określaną mianem *Starlight*. Dzięki wysokiej czułości jest polecana zwłaszcza do obserwacji rozległych przestrzeni otwartych w trudnych warunkach oświetleniowych. Do takich zastosowań dodatkowo predestynuje ją zastosowany obiektyw typu motor-zoom o ogniskowej regulowanej w zakresie od 5 mm do 50 mm oraz o sile światła równej F/1.6, zapewniający możliwość dużych zbliżeń i rozpoznawania drobnych detali obserwowanej sceny. Dodatkowo została wyposażona w oświetlacz IR o zasięgu 80 m i szerokim kącie świecenia 130° składający się z ośmiu diod. Dzięki funkcji WDR z podwójnym skanowaniem przetwornika kamera bardzo dobrze sprawdza się przy nierównomiernym oświetleniu obserwowanej sceny i silnym wstecznym oświetleniu. Może bezpośrednio łączyć się z aplikacją mobilną RxCamView działającą pod systemem operacyjnym iOS lub Android i zapewniać jej użytkownikom podgląd obrazów na żywo kodów z użyciem protokołu P2P, przy czym nie ma konieczności przekierowywania portów lub zapewniania stałego adresu IP. Kamera ma interfejsy wejściowe i wyjściowe umożliwiające dwukierunkową transmisję dźwięku. Uzupełnieniem powyższych funkcji są dostępne w rejestratorach z serii 4000 oraz w aplikacji NMS funkcje analizy obrazu, w tym wykrywanie sabotażu, pojawienia się albo zniknięcia obiektu, przekroczenia wyznaczonej linii, wkroczenia do strefy, detekcja twarzy, osób, dźwięków i liczenie przekroczeń linii.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Zbyszku!
Będzie nam Ciebie bardzo brakowało...

Z żalem informujemy, że 27 sierpnia br., w wieku 64 lat, zmarł Zbigniew Osowicki – wieloletni pracownik firmy POLON-ALFA, wybitny specjalista z dziedziny ochrony przeciwpożarowej, współtwórca wytycznych dotyczących projektowania systemów sygnalizacji pożarowej, autor wielu artykułów i opracowań z zakresu bezpieczeństwa pożarowego, przez blisko dwadzieścia lat główny organizator Ogólnopolskich Warsztatów SAP – największych tego typu warsztatów w naszym kraju.

Odszedł wspaniały, mądry, a zarazem bardzo skromny i życzliwy wszystkim człowiek. Całe środowisko branżowe straciło niezwykle wartościowego specjalistę, a wielu z nas przyjaciela.

Zbyszku! Będzie nam Ciebie bardzo brakowało...

Bezpośr. inf. POLON-ALFA

Kongres Pożarnictwa FIRE SECURITY EXPO 2019

podsumowanie

25 lipca br. na **PGE Narodowym** odbyła się **16. edycja Kongresu Pożarnictwa FIRE SECURITY EXPO**. W kongresie wzięło udział ponad 70 wystawców i prawie 900 uczestników, m.in. instalatorzy, projektanci, architekci, integratorzy oraz rzeczoznawcy.

Tegoroczny kongres był podzielony na trzy panele tematyczne. Pierwszy z nich był poświęcony bezpieczeństwu pożarowemu budynków (od projektowania po wykonawstwo).

Zaprezentowano różne materiały budowlane, omówiono ich zastosowanie i wymagania w świetle przepisów pożarowych. Uczestnicy mieli okazję dowiedzieć się m.in., jak powinna wyglądać prawidłowa dokumentacja dotycząca wyrobu budowlanego, jak powinno oddzielać się strefy pożarowe od dróg ewakuacyjnych, jak powinien być zaprojektowany i wykonany system detekcji gazu. Omówiono również istotę technologii BIM.

W drugim panelu omówiono wymagania dotyczące instalacji i urządzeń przeciwpożarowych oraz okablowania w przestrzeni biurowej. Zaprezentowano przewody do instalacji przeciwpożarowych. Omówiono sterowanie stałymi automatycznymi urządzeniami gaśniczym i współdziałanie systemu oświetlenia awaryjnego z systemem sygnalizacji pożarowej w celu zapewnienia bezpiecznej ewakuacji z budynku. Zaprezentowano również najnowsze zasilacze do urządzeń przeciwpożarowych.

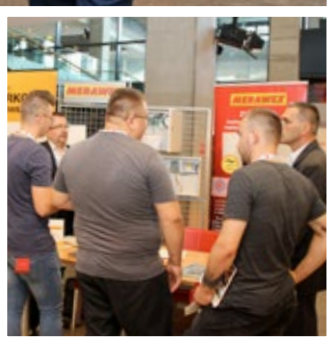
W trzecim panelu tematycznym podano wymagania i wytyczne dotyczące fazy projektu, budowy i użytkowania systemu pożarowego.

Kongresowi towarzyszyła debata ekspertów poświęcona konfrontacji przepisów ze stosowanymi praktykami w ochronie pożarowej obiektów. Uczestnicy kongresu mogli również skorzystać z konsultacji z prawnikami, ekspertami i rzeczoznawcami ds. zabezpieczeń przeciwpożarowych.

Podczas kongresu odbyły się warsztaty firmy POLON-ALFA poświęcone realizacji scenariuszy działań w czasie pożaru

z wykorzystaniem systemu POLON 6000 i warsztaty firmy Robert Bosch, na których przedstawiono metody rozmieszczania głośników pożarowych za pomocą narzędzia do symulacji akustycznych EASE Address.

Firma Ela-compil z Poznania, wystawca na kongresie, zorganizowała wycieczkę do centrum monitorowania stadionu. Na PGE Narodowym zainstalowany jest system integrujący GEMOS oraz centrala FPM+ służąca do sterowania urządzeniami przeciwpożarowymi. PGE Narodowy jest jednym z pierwszych obiektów, w których wdrożono moduł GEMOS MOSAIC (w 2018 r.). Jest to moduł systemu zarządzania bezpieczeństwem GEMOS 4.0 oferujący nowy, innowacyjny sposób wyświetlania, prezentowania i analizowania gromadzonych danych ze zintegrowanych systemów. GEMOS MOSAIC umożliwia obsługę zdarzeń niezwłocznie po ich wystąpieniu i konfigurowalne interakcje, które zwiększają szybkość oceny zagrożenia. Dzięki zastosowaniu nowych silników graficznych możliwe jest wprowadzenie łatwo definiowalnych stref bezpieczeństwa, a w związku z tym poprawienie funkcjonalności systemu.



Jak co roku przyznano nagrody za najlepszą prezentację, stoisko oraz innowacyjny produkt.

Organizatorowi Kongresu Pożarnictwa, firmie DND Project, bardzo dziękujemy za zaproszenie i życzymy powodzenia oraz kolejnych udanych branżowych spotkań.

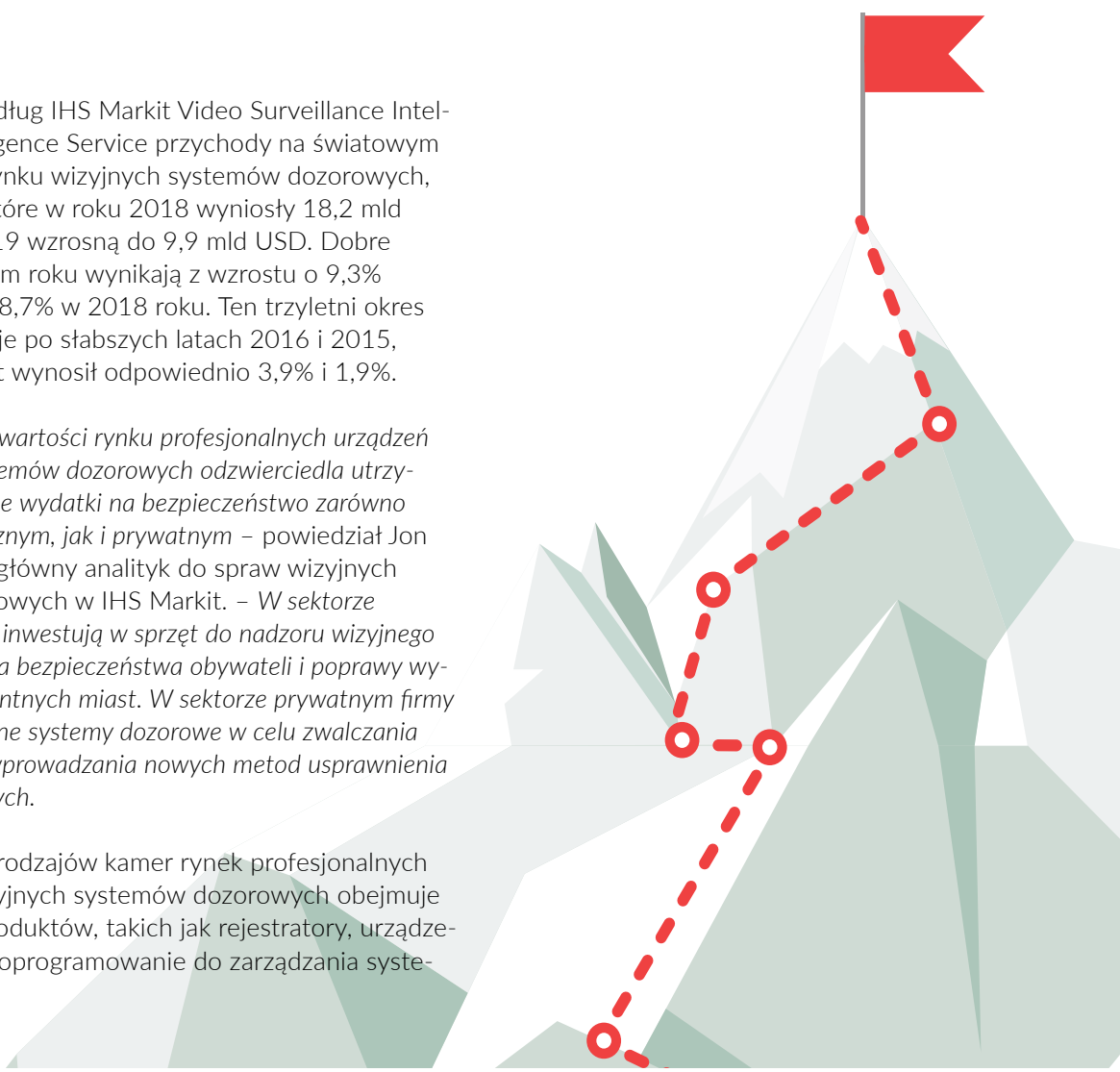
Bezpośr. inf. Ela Końka

Prognozowana wartość światowego rynku wizyjnych systemów dozorowych

od trzech lat utrzymuje silną tendencję wzrostową

Jon Cropley

Na światowym rynku profesjonalnego sprzętu do wizyjnych systemów dozorowych od trzech lat utrzymuje się silna tendencja wzrostowa. Wartość tego rynku ma wzrosnąć w roku 2019 o 9,3%. Tak silny wzrost jest napędzany silnym popytem na systemy zapewniające poprawę bezpieczeństwa publicznego i usprawnienie działań biznesowych



Według IHS Markit Video Surveillance Intelligence Service przychody na światowym rynku wizyjnych systemów dozorowych, które w roku 2018 wyniosły 18,2 mld USD, w roku 2019 wzrosną do 9,9 mld USD. Dobre wyniki w bieżącym roku wynikają z wzrostu o 9,3% w 2017 roku i o 8,7% w 2018 roku. Ten trzyletni okres wzrostu następuje po słabszych latach 2016 i 2015, w których wzrost wynosił odpowiednio 3,9% i 1,9%.

– *Obecny wzrost wartości rynku profesjonalnych urządzeń do wizyjnych systemów dozorowych odzwierciedla utrzymujące się wysokie wydatki na bezpieczeństwo zarówno w sektorze publicznym, jak i prywatnym* – powiedział Jon Cropley, starszy główny analityk do spraw wizyjnych systemów dozorowych w IHS Markit. – *W sektorze publicznym rządy inwestują w sprzęt do nadzoru wizyjnego w celu zwiększenia bezpieczeństwa obywateli i poprawy wyposażenia inteligentnych miast. W sektorze prywatnym firmy inwestują w wizyjne systemy dozorowe w celu zwalczania przestępczości i wprowadzania nowych metod usprawnienia działań biznesowych.*

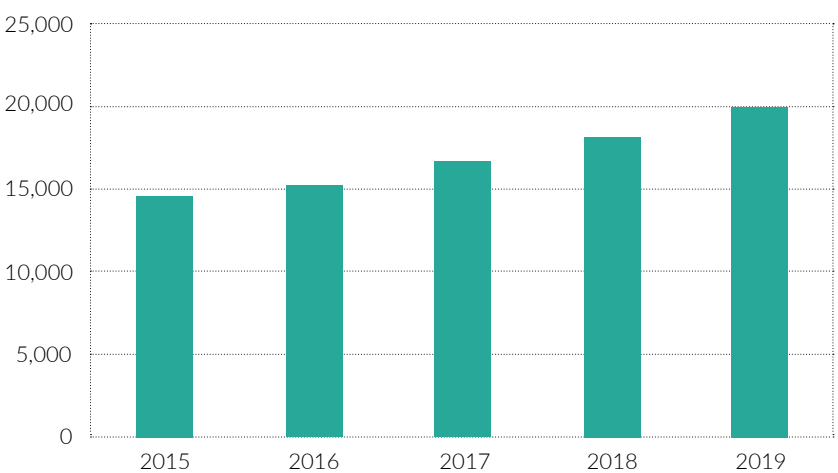
Oprócz różnych rodzajów kamer rynek profesjonalnych urządzeń do wizyjnych systemów dozorowych obejmuje szereg innych produktów, takich jak rejestratory, urządzenia analityczne i oprogramowanie do zarządzania systemami wizyjnymi.

Boom na chińskim rynku wizyjnych systemów dozorowych

Chiny napędzają globalny rynek profesjonalnych urządzeń do wizyjnych systemów dozorowych. W 2018 roku kraj ten stanowił prawie połowę globalnego biznesu – z 45% światowych przychodów. Chiński rynek powiększył się w zeszłym roku o imponujące 13,5%. Z wyłączeniem Chin światowy rynek wzrósł zaledwie o 5%.

– *Głównym czynnikiem powodującym wzrost wartości chińskiego rynku jest rządowy program Xue Liang, który promuje inwestowanie zarówno w projekty systemów monitoringu miejskiego, jak i w rozszerzenie tych systemów w celu objęcia nadzorem obszarów podmiejskich* – powiedział Cropley. – *Przewiduje się, że program Xue Liang zakończy się w 2020 roku, co spowoduje spowolnienie wzrostu wartości chińskiego rynku po upływie tego terminu. W międzyczasie Xue Liang będzie nadal generować silny wzrost wartości chińskiego oraz globalnego rynku sprzętu do wizyjnych systemów dozorowych.*

Globalna prognoza przychodów na rynku sprzętu do wizyjnych systemów dozorowych (w milionach USD)



Rynek wizyjnych systemów dozorowych się konsoliduje

Mimo że ten rynek jest bardzo rozdrobniony w porównaniu z wieloma innymi, baza dostawców profesjonalnych urządzeń do wizyjnych systemów dozorowych stopniowo staje się coraz bardziej skonsolidowana. Piętnastu najlepszych dostawców wygenerowało 65% globalnych przychodów w 2018 roku (dla porównania –52% w 2014 roku).

Rynek wizyjnych systemów dozorowych przesuwa się również w kierunku kamer sieciowych, pracujących z wykorzystaniem protokołu IP, wyposażonych w mechanizmy umożliwiające pracę w sieciach przewodowych lub bezprzewodowych. 70% wszystkich kamer dozorowych sprzedanych w 2018 roku stanowiły kamery sieciowe. W tym samym okresie globalne dostawy kamer HD CCTV, znanych również jako analogowe kamery HD, zmniejszyły się.

Tekst opracowany przez Jona Cropleya, starszego głównego analityka w IHS Markit
Tłumaczenie: Andrzej Walczyk

Nowy zintegrowany system dozorowy firmy Fujifilm do obserwacji rozległych obszarów

Sukces rynkowy systemu kamerowego Fujinon SX800

Fujifilm Optical Devices Europe

Fujifilm oferuje nowy moduł kamerowy Fujinon SX800 przeznaczony do prowadzenia obserwacji na dużą odległość. Dzięki zastosowaniu kamery o rozdzielczości Full HD, z przetwornikiem o rozmiarach 1/1,8", i optycznie stabilizowanego obiektywu Fujinon z ogniskową regulowaną w zakresie od 20 mm do 800 mm uzyskano innowacyjny i funkcjonalny moduł kamerowy. Stworzenie takiego produktu jest wynikiem wieloletniego doświadczenia w tworzeniu cyfrowych aparatów fotograficznych i zwracania szczególnej uwagi na jakość elementów optycznych. Moduł jest szczególnie przydatny w zastosowaniach związanych z lotnictwem

We współczesnym społeczeństwie potrzeba zapewnienia bezpieczeństwa obywatelom nabiera coraz większego znaczenia. Kamery z obiektywami o długich ogniskowych są nie tylko wykorzystywane do rozwiązywania drażliwych problemów, takich jak bezpieczeństwo granic, ale także, coraz częściej, włączane do infrastruktury publicznej, takiej jak lotniska, porty morskie i autostrady.

Systemy przeznaczone do prowadzenia obserwacji na dużą odległość muszą radzić sobie ze szczególnymi wyzwaniami. W przypadku obiektywów o długich ogniskowych najmniejsze wibracje powodują rozmazanie obrazu. Termiczne drgania powietrza lub mgła również pogarszają jego jakość. Do utraty istotnych ze względu na bezpieczeństwo informacji może prowadzić zbyt wolna praca mechanizmu regulacji ostrości. Opracowując nowy moduł Fujinon SX800, firma Fujifilm znalazła jednak sposób na pozbycie się wpływu tych czynników na jakość obrazu. Zamiast prowadzić niezależne prace nad konstrukcją kamery i osobnego, dołączanego do niej obiektywu, zrealizowano koncepcję w pełni zintegrowanego systemu składającego się z kamery i obiektywu.

Oprócz wysokiej jakości obiektywu zmiennoogniskowego moduł Fujinon SX800 ma wbudowany bardzo skuteczny w działaniu układ mechaniczno-optyczny służący do stabilizacji obrazu. Umożliwia on wyeliminowanie negatywnego wpływu drgań kamery o amplitudzie kątowej dochodzącej do +/- 0,22 stopnia. Zintegrowany, szybki w działaniu układ automatycznego ogniskowania pozwala na uzyskanie ostrego obrazu w czasie krótszym niż sekunda. Filtr przeciwmgielny i układ redukcji zamglenia zapobiegają zakłóceniom pogodowym.

Moduł Fujinon SX800 umożliwia tworzenie bardzo ostrych obrazów obiektów oddalonych nawet o kilka kilometrów od kamery. Ponadto jego zintegrowana konstrukcja przyczynia się do skrócenia czasu instalacji i regulacji punktu obserwacyjnego.

W trzecim kwartale 2019 roku moduł Fujinon SX800 będzie dostępny w sprzedaży w dwóch wersjach – jako samodzielny, ruchomy punkt obserwacyjny oraz jako składnik systemu obserwacyjnego z głowicą uchylno-obrotową.

Informacje na temat produktu:
www.fujifilm.eu/sx800.

Fujifilm Optical Devices Europe
Fujistr. 1, 47533 Kleve
Niemcy
Tel.: +49 2821 7115 400
E-mail: cctv_eu@fujifilm.com
www.fujifilm.eu/fujinon

Tłumaczenie:
Andrzej Walczyk

Skuteczna ochrona prywatności

w systemach dozoru wizyjnego

Axis Communications

Na skutek obowiązywania RODO właściciele i operatorzy wizyjnych systemów dozorowych muszą przywiązywać wagę do ochrony prywatności w procesie pozyskiwania, przetwarzania i przechowywania danych. Można wykorzystać w tym celu AXIS Live Privacy Shield. To jedyne na rynku narzędzie wykorzystujące analizę brzegową (ang. *edge computing*) – inteligentnie maskujące obiekty w czasie rzeczywistym, z zachowaniem możliwie najlepszej jakości obrazu i wysokiej dynamiki sceny. Może ono działać na już istniejących urządzeniach firmy Axis Communications

Zasada działania

AXIS Live Privacy Shield porównuje obraz ruchomych obiektów wychwyconych przez kamerę z tłem z określonej sceny i generuje dynamiczną, przezroczystą maskę dla odróżniających się obszarów. Innymi słowy, osoby i przedmioty będące w ruchu są wyświetlane na danym planie jako przeźrocze. Cały proces maskowania przebiega szybciej niż mrugnięcie oka i skutecznie chroni prywatność obserwowanych osób, wykluczając niepotrzebną dla danego użytkownika systemu rejestrację danych osobowych i ujawnianie tożsamości przechodzących osób. Co istotne, proces przebiega w czasie rzeczywistym, przy pełnej szybkości przetwarzania klatek obrazu, z zachowaniem pełnej rozdzielczości kamery.

Łatwa konfiguracja i ekonomiczna obsługa

Domyślnie dynamiczne maskowanie jest stosowane w całym polu widzenia kamery, ale użytkownicy mogą określić miejsca, w których maskowanie ma być wyłączone – na przykład wówczas, gdy potrzebna jest obserwacja taśmy transportującej, którą należy widzieć w pełni, w zakładzie produkcyjnym lub przy kasie sklepowej. Można także skonfigurować system tak, aby bez maskowania dostarczał oddzielny strumień wizyjny do wybranych stanowisk obserwacyjnych, gdzie upoważnieni operatorzy mogą uzyskać dostęp do danych w celach dochodzeniowych w przypadku incydentu. Poniższa ilustracja pokazuje zdolność AXIS Live Privacy Shield do jednoczesnego przesyłania strumieni wizyjnych z dynamicznym maskowaniem (A) i bez (B).

Rys. 1. Obraz widoczny na lewym monitorze powstał z włączoną funkcją Live Privacy Shield. Obraz widoczny na prawym monitorze powstał z wyłączoną funkcją Live Privacy Shield

Rys. 2. Obraz powstały z włączoną funkcją Live Privacy Shield

W miejscach, w których maskowanie jest wymagane stale, można użyć funkcji maskowania statycznego. Dotyczy to zwłaszcza ukrywania obiektów o niezmiennym położeniu, takich jak ekrany komputerów lub terminali płatniczych, które mogą być źródłami danych wymagających ochrony. Na podkreślenie zasługuje również to, że AXIS Live Privacy Shield działa bezpośrednio w systemach kamer firmy Axis Communications pracujących w trybie analizy brzegowej. Nie trzeba więc dodatkowo inwestować w drogie serwery. Skalowanie i rozbudowa systemu również są ułatwione.

AXIS Live Privacy Shield jest doskonałym narzędziem do obserwacji prowadzonych zgodnie z wymaganiami RODO zabezpieczającymi użytkownika systemu przed naruszaniem czyjejkolwiek prywatności, które mogłoby być dla niego dość kosztowne.

Funkcjonalność

AXIS Live Privacy Shield jest przeznaczona do użytku w pomieszczeniach o dobrym, stabilnym oświetleniu. Sprawdza się podczas obserwacji zdalnych lub dyskretnych, prowadzonych w trybie ciągłym, gdy dozór wizyjny może nastręczać problemów natury prawnej ze względu na zasady i przepisy dotyczące prywatności. Nadaje się do obserwacji tam, gdzie odbywa się produkcja, sprzedaż, można ją wykorzystać w logistyce, transporcie, w placówkach edukacyjnych i obiektach administracji publicznej, gdy śledzenie przebiegu procesów, zdarzeń i przepływu osób ma istotny wpływ na wyniki finansowe, efektywność organizacji pracy, bezpieczeństwo pracowników lub jakość obsługi klienta.

Axis Communications

securex®
POLAND
Międzynarodowe Targi Zabezpieczeń

ZAPRASZA
mtp
GRUPA

21-23.04.2020
POZNAŃ

www.securex.pl

Międzynarodowe
Targi Poznańskie

OSTATNIA
SZANSA
NA NIŻSZĄ
CENĘ
JESZCZE
W 2019

ZABEZPIECZ SWÓJ SUKCES!

O wartości każdej z technik przesądza tylko możliwość jej wykorzystania przez użytkownika o określonych umiejętnościach. Analizując sposoby korzystania z oprogramowania biznesowego czy też biorąc pod uwagę fakt użytkowania jedynie niewielu funkcji naszych telefonów komórkowych, widzimy, jak rzadko w pełni wykorzystujemy możliwości, jakie daje technika. Ogólnie przyjęty i stosowany tzw. model akceptacji techniki (ang. *technology acceptance model*) pokazuje, że oprócz użyteczności również łatwość obsługi ma decydujący wpływ na to, w jakim stopniu da się z danej techniki czerpać

Łatwość obsługi
ważną zaletą systemów dozoru wizyjnego

Axis Communications

Dotyczy to zarówno dozoru wizyjnego, jak i wszystkich innych dziedzin. W pełni wykorzystuje się systemy, które charakteryzują się intuicyjną i łatwą obsługą. Chociaż w ostatnich latach jakość obrazu w systemach dozorowych znacznie się poprawiła, a wsparcie ze strony innych technik sieciowych i upowszechnienie funkcji analizy treści obrazu zwiększyło zakres zastosowań oraz dostarczyło cennych informacji biznesowych, niewiele się zmieni, jeżeli operator nie będzie mógł w pełni wykorzystać tych innowacji. Dotyczy to szczególnie zastosowań w handlu detalicznym, hotelarstwie, placówkach edukacyjnych czy zakładach produkcyjnych, gdzie rzadko zatrudniane są osoby specjalnie do obsługi i zarządzania wizyjnym systemem dozorowym.

Intuicyjny interfejs użytkownika ma kluczowe znaczenie dla osób, do których obowiązków należy konfigurowanie i obsługa kamer, a także zapewnienie związanych z tym korzyści w zakresie bezpieczeństwa i odpowiedniej obsługi. W tym kontekście najważniejsze zalety interfejsu to:

- automatyczne wykrywanie kamer i możliwość skorzystania z kreatorów konfiguracji w celu jak najszybszego przygotowania systemów do pracy,
- możliwość jednoczesnego podglądu obrazu na żywo i obrazu z nagrania,
- zakładki umożliwiające natychmiastowe obejrzenie wybranych obrazów,
- umieszczone na ekranie elementy sterujące, które są powiązane z typowymi i użytecznymi funkcjami kamer,
- zawsze aktywna oś czasu ułatwiająca dochodzenie po każdym incydencie,
- proste eksportowanie materiału wizyjnego do właściwych służb.

W wielu małych firmach operator systemu wizyjnego nie poświęca całego czasu pracy na jego obsługę ze stacjonarnego stanowiska dozorowego. Po otrzymaniu e-mailowego powiadomienia z załączonym obrazem jest on w stanie ocenić aktualną sytuację, wykorzystując mobilną aplikację służącą do podglądu obrazów. Może to zrobić w trakcie wykonywania innej pracy.

Każda jednostka organizacyjna ma własną specyfikę, dlatego najpierw należy określić wymagania dotyczące systemu dozorowego w danym miejscu. Przykładem może być społeczna szkoła średnia Washington Community High School. Po rozbudowie placówki dotychczasowy system bezpieczeństwa złożony z wielu kamer analogowych różnych producentów przestał spełniać wymagania. Sprawiał kłopoty w obsłudze i generował dużą liczbę fałszywych alarmów. Oprócz tego występowały luki w pokryciu monitorowanego obszaru. Szkoła zdecydowała się przejść na system oparty na sieci IP w celu uzyskania poprawy jakości, pokrycia i łatwości obsługi. Teraz zatrudniony w szkole pracownik ochrony jest w stanie sprawnie odnaleźć incydenty w zapisanym materiale, dokładnie ustalić, co się stało, i bezzwłocznie podjąć odpowiednie działania, zamiast spędzać godziny na przeglądaniu zapisu analogowego, aby znaleźć potrzebne pięć minut materiału. Korzystając z oprogramowania do zarządzania obrazem, personel zajmujący się ochroną może poświęcić więcej czasu na wykrywanie potencjalnych problemów w szkole. – *Nowy system działa znacznie lepiej niż poprzedni. Dzięki niemu każdego dnia oszczędzam mnóstwo czasu, prawdopodobnie kilka godzin. Nie da się nawet porównać jakości obrazu do jego jakości w poprzednim systemie. Teraz jestem w stanie widzieć to, co jest znacznie dalej i zobaczyć więcej detali, zatem nie ma już wątpliwości dotyczących tego, co faktycznie widać na obrazie* – powiedział Troi Westbrook, specjalista ds. bezpieczeństwa i prewencji pracujący w WCHS. Wygodny interfejs do obsługi systemu umożliwia szybkie wdrożenie nowych użytkowników, dzięki czemu można zaoszczędzić na szkoleniach i znacznie zredukować konsekwencje błędów podczas użytkowania.

Dzięki współczesnym intuicyjnym narzędziom do zarządzania systemami korzyści z nadzoru wizyjnego są większe niż kiedykolwiek i bardziej dostępne dla większej liczby organizacji.

Axis Communications

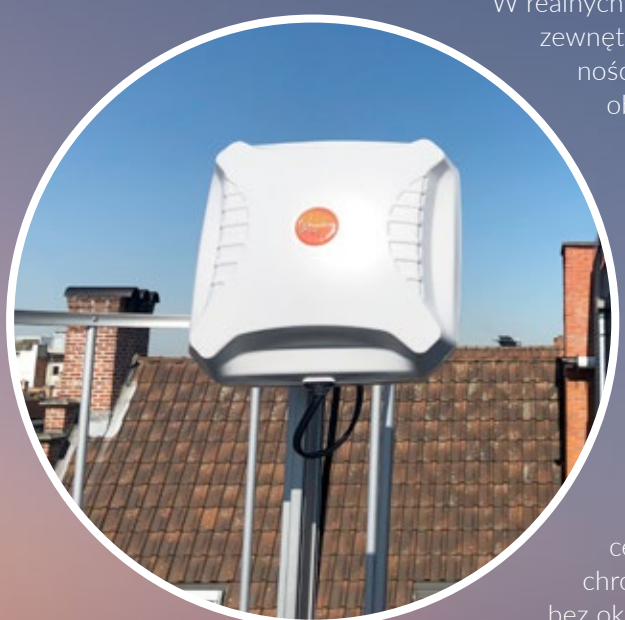
Rola anten w systemach monitorowania alarmów

na przykładzie produktów firmy Poynting. Część 2.

Poynting

Poprzednia część dotyczyła podstaw radiokomunikacji, a zwłaszcza zagadnień związanych z antenami i ich wpływem na eliminację szumów. Antena jest częścią bezprzewodowej instalacji zabezpieczającej i ma decydujący wpływ na działanie całego systemu. Dlaczego więc jej rola jest tak często lekceważona przez użytkowników?

Przyczyn jest kilka. Niewiele z powszechnie używanych urządzeń mobilnych ma widoczną antenę lub złącze do podłączenia anteny zewnętrznej. Przeważnie antena jest ukryta we wnętrzu obudowy i osobom niezorientowanym w temacie może się wydawać, że jej w ogóle nie ma. W dogodnych warunkach eksploatacyjnych, czyli tam, gdzie sygnał ze stacji bazowych sieci komorowej jest silny, na przykład w miastach i wzdłuż ważniejszych tras komunikacyjnych, urządzenia mobilne działają poprawnie, więc użytkownik nabiera przekonania, że żadna antena zewnętrzna nie jest konieczna. Po znacznym oddaleniu się od stacji bazowej okazuje się jednak, że bez dodatkowej anteny urządzenie przestaje poprawnie działać, połączenie nie jest stabilne i nie można na nim polegać.



Fot. 1. Antena Poynting XPOL-2 LTE MIMO zapewnia komunikację internetową LTE małym firmom i obiektom prywatnym (Autor: Frontier Computer Corp. b.v.).

W realnych warunkach eksploatacyjnych użycie anteny zewnętrznej radykalnie poprawia jakość i niezawodność działania łącza radiowego. Dotyczy to zarówno obszarów gęsto zabudowanych, gdzie na drodze od nadajnika do odbiornika jest wiele przeszkód materialnych, takich jak wysokie budynki czy urządzenia przemysłowe, jak i obszarów wiejskich, gdzie przeszkód nie ma, ale odległości między nadajnikiem a odbiornikiem są znaczne. Mimo że zastosowanie odpowiednich anten jest ze wszech miar zalecane, często inwestor bądź instalatorzy nie decydują się na nie. Jest wiele czynników wpływających na taką decyzję.

Jednym z nich jest czas i koszt instalacji. W systemach zabezpieczających dba się o to, by centrala alarmowa była zainstalowana w dobrze chronionym miejscu, w zamkniętym pomieszczeniu bez okien, za ciężkimi, metalowymi drzwiami, najlepiej gdzieś w piwnicy. Aby zaoszczędzić czas instalator montuje nadajnik systemu monitorowania w tym samym pomieszczeniu. Takie rozwiązanie można zastosować, gdy stacja monitorowaniu alarmów mieści się dwie ulice dalej i poziom sygnału jest bardzo wysoki, ale przy większych odległościach skuteczność działania takiego systemu będzie niewielka.

Często zdarza się, że instalatorzy nie mają wystarczającej wiedzy z dziedziny radiokomunikacji i zdają się na rozwiązania fabryczne. Tymczasem producenci sprzętu koncentrują się jedynie na dostawie dobrze działających urządzeń i nie wypowiadają się na temat doboru anten. Często do zestawu dołączana jest fabryczna antena, montowana wprost na złączu wyjściowym nadajnika, która powinna służyć jedynie do wstępnego uruchomienia systemu, a nie do jego eksploatacji.

Fot. 2. Kierunkowe anteny Poynting LDPA-92 zapewniają połączenie ze stacją BTS na odległość 15 km (Autor: Fergus, Ireland)

Fot. 3. Wielofunkcyjna antena Poynting MIMO-1 zamontowana na ciężarówce. We wspólnej obudowie znajdują się dwie anteny LTE, antena GPS/Glonass oraz dwie anteny Wi-Fi (na pasma 2.4 i 5GHz)

Często przy opracowywaniu projektu antena w ogóle nie zostaje uwzględniona. Nikt nie myśli o roli anteny w projekcie komunikacji bezprzewodowej. W rezultacie w kosztorysie nie ma przewidzianych kosztów instalacji dobrych anten.

Osobnym zagadnieniem jest właściwy dobór anten. W różnych warunkach eksploatacyjnych powinny być użyte różne anteny, tak jak w samochodzie opony powinny być dostosowane do warunków drogowych. Nie ma dwóch identycznych przypadków, można jedynie sformułować ogólne zalecenia. W aglomeracji miejskiej, gdzie odległości od stacji bazowych są niewielkie, a na swej drodze sygnał radiowy ulega wielokrotnym odbiciom, można stosować proste anteny dookolne. W terenie otwartym, na przedmieściach i na wsi, gdzie odległości od stacji bazowych są znacznie większe niż w mieście, zdecydowanie lepsze są anteny kierunkowe.

Kolejnym czynnikiem zniechęcającym jest niska trwałość anten dostępnych w handlu detalicznym. Często nie wiadomo, jaki producent wyprodukował dane anteny, nie przeszły one żadnych testów wytrzymałościowych. Ich odporność na niszczące czynniki środowiskowe jest niewielka. Instalator woli umieścić taką antenę w zamkniętym pomieszczeniu niż instalować ją na zewnątrz budynku, gdzie po kilku miesiącach ulegnie zniszczeniu przez wiatr.

Antena kierunkowa lub dookolna

Wiele osób zakłada, że antena kierunkowa o wysokim zysku energetycznym jest zawsze anteną najlepszą, jednak w praktyce nie zawsze tak jest. Antena powinna być dostosowana do warunków pracy.

Jeżeli użytkownik korzysta z więcej niż jednej stacji bazowej, najlepszym rozwiązaniem jest antena dookolna, np. Poynting XPOL-1 lub dwie anteny OMNI-292. Istnieje wiele powodów, dla których lepiej jest mieć dostęp do więcej niż jednej stacji bazowej.

Gdy użytkownik znajduje się na obszarze zabudowanym, sygnał radiowy ulega wielokrotnym odbiciom, a stacje bazowe są rozmieszczone w małych odległościach od siebie, co oznacza, że użytkownik ma dostęp do więcej niż jednej stacji bazowej. Może wtedy wybrać antenę kierunkową, np. Poynting XPOL-2.

Do komunikacji z tylko jedną stacją bazową na obszarze niezurbanizowanym najlepiej wybrać antenę kierunkową o wysokim zysku energetycznym, co poprawi budżet energetyczny łącza

radiowego. Jeżeli stacja bazowa znajdująca się najbliżej użytkownika jest mocno obciążona, to zachodzi potrzeba skomunikowania się z dalszą stacją o mniejszej liczbie użytkowników. Najlepszym rozwiązaniem jest zastosowanie anteny kierunkowej.

Operatorzy sieci komórkowych zaczynają dostrzegać potrzeby społeczności z obszarów niezurbanizowanych, tzn. terenów wiejskich czy przedmieść, wymagające inwestowania celem poprawienia jakości mobilnych usług szerokopasmowych. W niektórych krajach europejskich lokalni operatorzy gwarantują swoim abonentom indywidualnym lub biznesowym pewien minimalny poziom usług. Anteny Poynting są wyselekcjonowane przez największego operatora w Norwegii oraz w Danii. Dokładne testy wykazały, że anteny XPOL-2 oraz XPOL-1 oferowane przez firmę Poynting są najbardziej niezawodne i skuteczne.

Fot. 4. Kierunkowe anteny Poynting LDPA-92 umożliwiają połączenie ze stacją BTS na odległość 15 km (Autor: Poynting Europe GmbH)

Postępy w technice antenowej mogą w krótkim czasie i przy stosunkowo niskich kosztach znacznie poprawić łączność i działanie sieci komórkowej. Dzięki zastosowaniu odpowiednio dobranych anten Poynting wzrośnie szybkość pobierania danych.

Podsumowując – aby zapewnić niezawodne działanie systemu, w tym skuteczne monitorowanie alarmów i przekazywanie obrazów z wizyjnego systemu dozorowego z wykorzystaniem łącz 3G/4G bądź – w niedalekiej przyszłości – 5G (np. transmisja obrazów z kamer montowanych na samochodach, autobusach, czy na placach budów), należy zastosować starannie dobrane anteny o jak najwyższej jakości wykonania. Dobrze jest skoncentrować się na wyrobach jednego, renomowanego producenta, gdyż wtedy można liczyć na usługi serwisowe i wsparcie techniczne. Takie warunki są spełnione przez wyroby firmy Poynting z RPA.

Co wyróżnia anteny firmy Poynting?

Asortyment produktów firmy Poynting jest na tyle szeroki, że praktycznie do każdego z chronionych obiektów da się dobrać właściwą antenę. Dotyczy to zarówno anten do sieci komórkowych, jak i anten służących do radiowej transmisji danych związanych z monitoringiem alarmów, a także typowych anten radiokomunikacyjnych. Są to setki wyrobów różniących się zakresami częstotliwości[1], charakterystykami promieniowania[2], zyskiem energetycznym[3], polaryzacją[4]. Projektantowi czy instalatorowi systemu umożliwia to swobodne dobranie właściwej anteny do warunków pracy.

Jak już wspomniano, wiedza na temat doboru profesjonalnych anten radiokomunikacyjnych nie jest powszechna, jednak firma Poynting wychodzi naprzeciw projektantom i instalatorom, dostarczając dokumentację techniczną oraz służąc poradami w każdym z indywidualnych przypadków.

Problemy z trwałością anten Poynting praktycznie nie istnieją. Technologia produkcji jest na najwyższym światowym poziomie, zaś jakość materiałów nie budzi najmniejszych zastrzeżeń. Złącza antenowe spełniają najwyższe wymagania środowiskowe. Produkty firmy Poynting znajdują zastosowanie zarówno w warunkach lądowych, w instalacjach stacjonarnych i ruchomych (np. XPOL-2, XPOL-1, OMNI-280, PUCK, MIMO-1, MIMO-3), jak i morskich

(np. OMNI-291 lub OMNI-402), gdzie niszczący wpływ słonej wody i silnego wiatru nie może być pominięty.

Tyle o jakości produktów firmy Poynting. Wróćmy do zagadnień technicznych. Dlaczego anteny firmy Poynting zapewniają lepszą jakość połączeń radiowych niż inne?

Istotnym, nie omówionym dotychczas zagadnieniem jest szerokopasmowość anten. Monitorowanie alarmów nie ogranicza się do przekazywania sygnałów z centrali alarmowej do stacji bazowej (o czym była mowa w pierwszej części artykułu. Często przekazywane są również obrazy z kamer i sygnały telemetryczne z urządzeń automatyki budynkowej. Taka transmisja odbywa się w szerokim zakresie częstotliwości, często nawet w różnych pasmach[5].

Innym przykładem transmisji szerokopasmowej jest telefonia komórkowa, w której różne rodzaje modulacji są stosowane w różnych pasmach. Antena, która ma zapewniać jednoczesną transmisję w systemach GSM900, GSM1800, LTE 4G, LTE 5G i Wi-Fi musi zapewniać wymagane parametry robocze w zakresach od 690 MHz do 960 MHz, od 1710 MHz do 2170 MHz, od 2300 MHz do 2700 MHz, od 3400 MHz do 3800 MHz (5G) i od 5000 MHz do 6000 MHz.

Konstrukcja anten spełniających tak wysokie wymagania jest bardzo skomplikowana. W celu osiągnięcia dobrych efektów konieczne jest zaangażowanie wysoko wykwalifikowanego personelu oraz wykorzystanie skomplikowanego wyposażenia. Do testowania profesjonalnych anten konieczne jest używanie tak zwanych komór bezechowych, czyli specjalnych pomieszczeń, w których wytłumione są wszelkie odbicia fal radiowych. Żaden przypadkowy producent anten nie dysponuje takim potencjałem ludzkim ani wyposażeniem.

Parametry anten Poynting podawane w kartach katalogowych dotyczą pełnych zakresów częstotliwości, w jakich mają one pracować, oraz najtrudniejszych warunków eksploatacyjnych. To odróżnia je od tanich wyrobów przypadkowych firm – w materiałach reklamowych podawane są ich najlepsze parametry (często bez charakterystyki promieniowania dla istotnych częstotliwości), osiągane jedynie w wycinkach zakresów częstotliwości, zaś anteny ulegają rozstrojeniu w ekstremalnych warunkach środowiskowych.

Ostatnim z omawianych zagadnień jest odbiór przestrzennie zbiorczy, czyli sposób na poprawę jakości połączeń radiowych z obiektami ruchomymi. Problem polega na tym, że fale radiowe emitowane przez antenę nadawczą docierają do anteny odbiorczej nie w linii prostej, lecz wieloma przypadkowymi drogami. Jest to szczególnie odczuwalne w terenie zurbanizowanym, gdzie fale ulegają wielokrotnym odbiciom od budynków. Rozpatrzmy przypadek dwóch fal poruszających się dwiema różnymi drogami. Gdy różnica długości tych dróg wyniesie dokładnie połowę długości fali, obie te fale zniosą się wzajemnie, czyli wyzerują, w punkcie odbioru. Innymi słowy wystąpi zanik odbioru. Wystarczy jednak nieznacznie przesunąć jedną z anten, by przywrócić odbiór.

Fot. 5. Antena kierunkowa Poynting XPOL-2 LTE MIMO zamontowana w Tunelu Gotthard w Szwajcarii. Antena zapewnia komunikację z naziemną siecią telekomunikacyjną, dzięki czemu w tunelu można wyświetlać reklamy (Autor: Movinglight-design.ch).

Jeśli odbiornik będzie umieszczony na ruchomym obiekcie, zaniki będą występowały okresowo, w krótkich odstępach czasu. To zjawisko, zwane sztachetowaniem, jest bardzo uciążliwe dla użytkowników systemów radiowych. By mu zapobiec, po stronie odbiorczej można zastosować dwie anteny i dwa niezależne odbiorniki. Prawdopodobieństwo, że zanik fal radiowych nastąpi jednocześnie w obu odbiornikach, jest znikome. Jakość odbioru bardzo się poprawia. Stosowanie dwóch oddzielnych anten nie jest wygodne z przyczyn instalacyjnych. Dogodniejszym rozwiązaniem jest zastosowanie anten dwusystemowych. W takim przypadku we wspólnej obudowie znajdują się dwie anteny.

Firma Poynting ma w swojej ofercie wiele takich anten, dostosowane do różnych zakresów częstotliwości. Każda z nich zawiera dwa układy dipoli różniące się polaryzacją o 90 stopni. W ten sposób ustawione dipole przypominają literę X, dlatego takie anteny są nazywane X-polami. Dipole ustawione prostopadle nie zakłócają się wzajemnie i można je traktować jak układ dwóch niezależnych anten. W przypadku anten kierunkowych o dużym zysku energetycznym stosuje się piętrowe ustawienie wielu zespołów X-poli. Wszystkie te elementy są zamknięte w jednej, wspólnej obudowie chroniącej X-pole przed zniszczeniem przez czynniki środowiskowe. To wyjaśnia, dlaczego anteny firmy Poynting zapewniają lepszą pracę systemów radiokomunikacyjnych niż tanie wyroby przypadkowych producentów.

Jak widać, firma Poynting zadbała o użytkowników bezprzewodowych systemów monitorowania alarmów, a jej asortyment jest bardzo różnorodny. Zainteresowanych szczegółowymi danymi technicznymi odsyłamy do strony https://poynting.tech/ lub prosimy o wysłanie emaila (może być w języku polskim) na adres sales-europe@poynting.tech.

Opracował na podstawie materiałów firmy Poynting
Andrzej Walczyk

Przypisy:

1. Przez zakres częstotliwości rozumie się przedział między górną a dolną częstotliwością graniczną, w którym parametry użytkowe anteny są zachowane.
2. Przez charakterystykę promieniowania rozumie się trójwymiarową bryłę obrazującą, w jakich kierunkach antena promieniuje silniej, a w jakich słabiej. Często operuje się przekrojami takiej bryły określającymi charakterystykę promieniowania w pionie i w poziomie.
3. Przez zysk energetyczny rozumie się proporcję między promieniowaniem danej anteny a promieniowaniem umownej anteny izotropowej (czyli anteny promieniującej jednakowo we wszystkich kierunkach). Przeważnie zysk energetyczny anteny wyraża się w decybelach i definiuje dla kierunku najsilniejszego promieniowania.
4. Przez polaryzację anteny rozumie się położenie wektora pola elektrycznego promieniowanej fali radiowej. Istnieją anteny o polaryzacji pionowej, poziomej, skośnej, eliptycznej.
5. Przez pasmo rozumie się umowny zakres częstotliwości, opisywany w pewien konkretny sposób, np. pasmo VHF mieści się w zakresie od 30 MHz do 300 MHz.

NMS ACCESS CONTROL

czas na start

Ryszard Sobierski

Jaki jest przepis na funkcjonalny, łatwy w obsłudze i spełniający oczekiwania klientów program do obsługi systemu kontroli dostępu i telewizji dozorowej? Program taki powinien realizować podstawowe i zaawansowane funkcje typowe dla aktualnie dostępnych programów nadzorczych, funkcje, których poszukują i oczekują instalatorzy i użytkownicy końcowi, a które nie są jeszcze dostępne, oraz wprowadzać opcje, których przydatności w takich systemach klienci jeszcze nawet nie brali pod uwagę. Właśnie taki będzie program nadzorczy NMS ACCESS CONTROL. Wersja, która aktualnie jest już dostępna, to początek rozwoju tego oprogramowania, jednak i tak jest bardzo zaawansowana i oferuje wiele funkcji

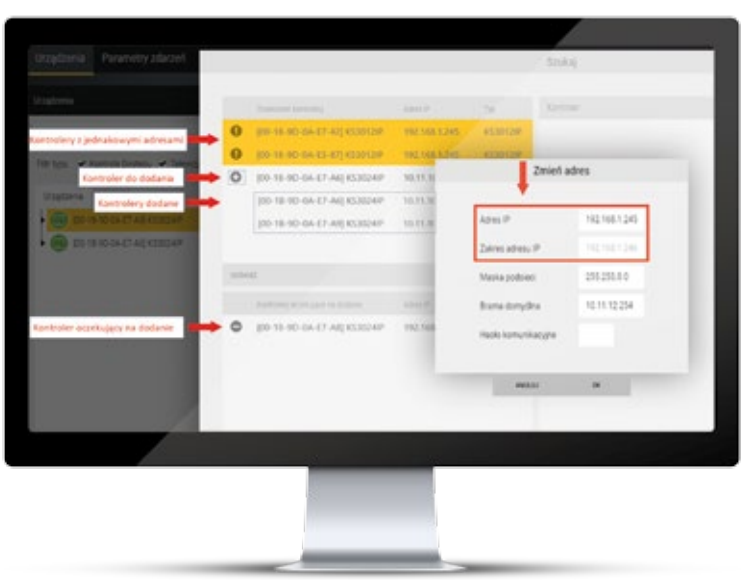
NMS ACCESS CONTROL to nowy program nadzorczy, który w obecnie dostępnej wersji jest przeznaczony do obsługi małych i średnich systemów kontroli dostępu. Współpracuje ze standardowymi kontrolerami typu KDH-KS3012-IP, KDH-KS3024-IP i KDH-KS2000-IP-ELV. Dzięki strukturze typu klient – serwer możliwa jest obsługa systemu na wielu stanowiskach (na dwóch stacjach klienckich w ramach licencji bezpłatnej i na dodatkowych po zakupie licencji rozszerzających). System jest prosty w instalacji i ma wygodny dla operatora interfejs graficzny. W obecnej wersji jest to program przeznaczony głównie do obsługi systemów kontroli dostępu, ale zawiera już pewne elementy systemu telewizji dozorowej i umożliwia rozbudowaną wizualizację stanów elementów systemu. Kolejne funkcje systemu nadzoru wizyjnego będą dodawane w następnych wersjach programu. Schemat blokowy systemu przestawia rys. 2.

Przystępując do opisu programu NMS ACCESS CONTROL, postanowiłem skupić się na korzyściach jakie uzyskają instalatorzy, administratorzy, operatorzy oraz pracownicy ochrony, czyli osoby, które będą miały z nim styczność w różnego rodzaju obiektach. To dla nich go stworzyliśmy. Zależy nam na tym, żeby każda z tych grup była zadowolona, gdy będzie tego programu używać w przeznaczonym dla niej zakresie.

Korzyści dla instalatorów

Z licznych rozmów, jakie przeprowadziłem z instalatorami, wynika, że najważniejsza jest dla nich łatwość obsługi programu, czas potrzebny na zaprogramowanie systemu, zwłaszcza wówczas, gdy obejmuje on bardzo wiele kontrolowanych przejść, oraz możliwość szybkiego sprawdzenia poprawności działania jego poszczególnych elementów. NMS ACCESS CONTROL spełnia te oczekiwania.

Jedną z ważniejszych czynności, jakie wykonuje instalator w obiekcie, jest montaż elementów systemu kontroli dostępu, czyli kontrolerów oraz kamer. Zainstalowane kontrolery i kamery są podłączane są do sieci Ethernet i do obwodów zasilania. Następnie należy je wprowadzić do bazy danych programu nadzorczego. NMS ACCESS CONTROL oferuje do tego celu znakomite narzędzie, jakim jest wyszukiwarka kontrolerów i kamer (rys. 1).

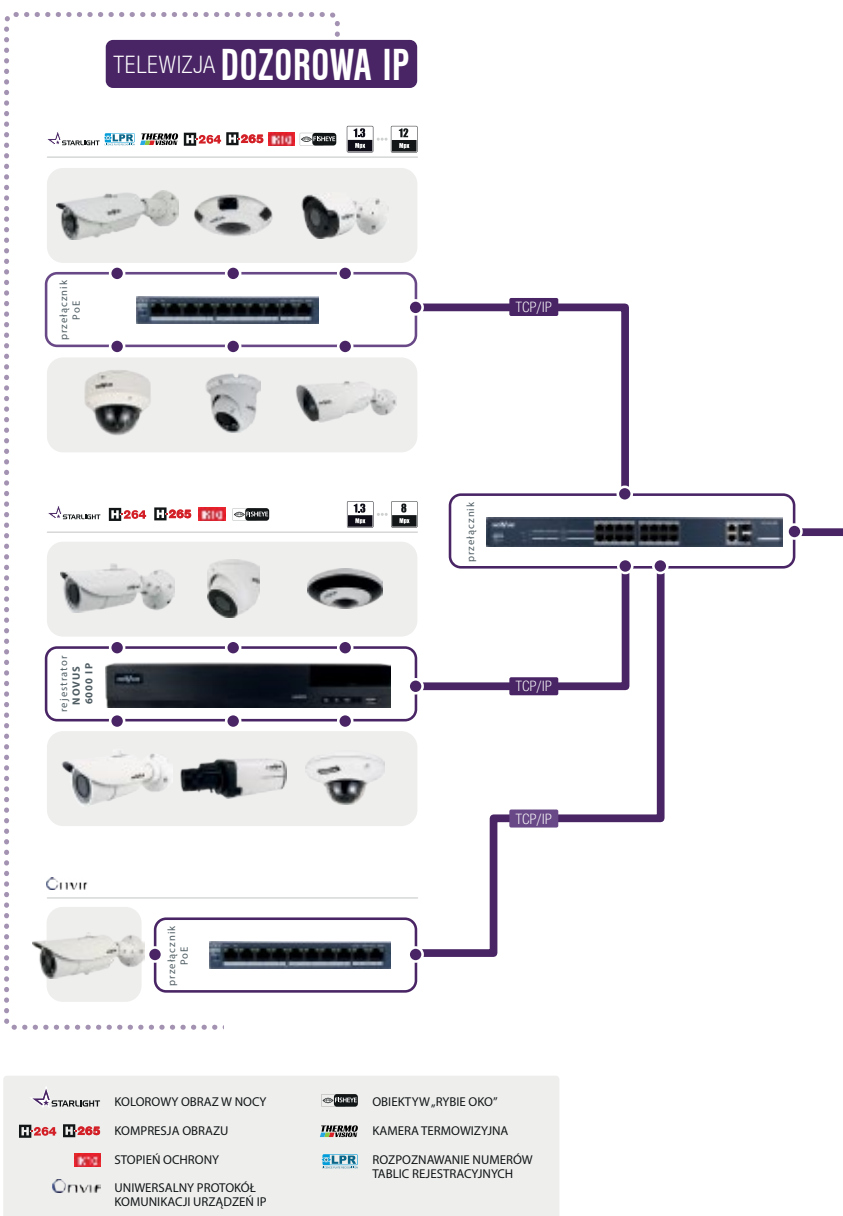


Rys. 1. Okno wyszukiwarki urządzeń

Wyszukując te urządzenia, program wykorzystuje ich adresy MAC. Dzięki temu na wyświetlanej liście są tylko te spośród nich, które współpracują z NMS ACCESS CONTROL. W pierwszej lewej kolumnie listy znajdują się ikony określające ich status sieciowy. Znalezione urządzenia są na liście automatycznie sortowane według tego statusu. Na pierwszym miejscu wyświetlane są urządzenia, które mają powtarzające się adresy IP (ikona wykrzyknika). Taka sytuacja ma miejsce, gdy zamontowane zostały nowe kontrolery z fabrycznym adresem 192.168.0.245. Po zaznaczeniu tej grupy kontrolerów (jednym kliknięciem wskazującym właściwą opcję) można automatycznie przypisać kolejne adresy, wpisując tylko pierwszy z nich z przydzielonej przez administratora puli. Po zmianie adresów kontrolery te pojawią się na liście z ikoną „+". Teraz można łatwo zaznaczyć wszystkie takie kontrolery na liście i jednym kliknięciem przenieść je do dolnego okna wyszukiwarki jako oczekujące na wprowadzenie. Kliknięcie przycisku *OK* zamyka okno wyszukiwarki, a nowe kontrolery pojawiają się na liście urządzeń systemu. Jeżeli jest taka potrzeba, to można na tym etapie zmienić ustawienia wybranych kontrolerów. Następnie, po kliknięciu przycisku *Zapisz*, następuje wprowadzenie kontrolerów do bazy danych systemu, nawiązanie z nimi komunikacji i przesłanie ustawień. Zmiana stanu ikon urządzeń na tej liście oraz seria komunikatów w oknie konsoli sygnalizuje pozytywne zakończenie tego procesu. Taka sama procedura obowiązuje w przypadku urządzeń systemu VSS.

Jak wynika z opisanej procedury, wprowadzenie i skomunikowanie z programem NMS ACCESS CONTROL nawet dużej liczby urządzeń to kwestia kilku minut. Nie ma żmudnego wypełniana licznych pól adresów IP. To z pewnością dobra wiadomość dla instalatorów, ponieważ pozwoli to zaoszczędzić mnóstwo czasu. W przypadku innych dostępnych na rynku programów do obsługi systemów kontroli dostępu czynności te są czasochłonne.

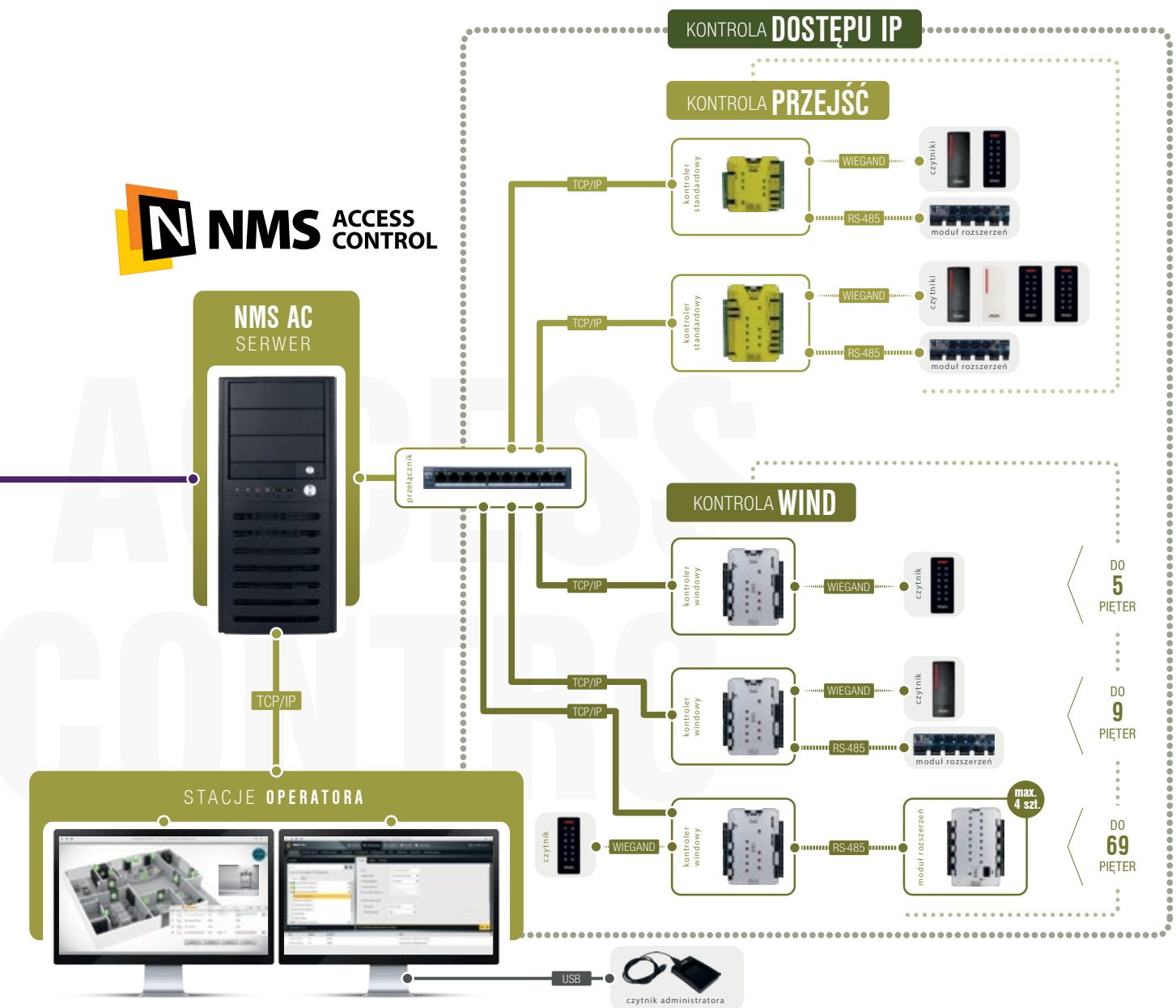
Kolejną korzyścią dla instalatorów jest możliwość szybkiego przetestowania zainstalowanego systemu pod kątem poprawności działania. Umożliwiają to dwa domyślnie skonfigurowane panele. Pierwszy z nich zawiera *STOS ZDARZEŃ* bieżących – umożliwia obserwację zdarzeń i alarmów, jakie są przesyłane z kontrolerów w procesie testowania systemu. Drugi panel zawiera tablicę synoptyczną, na której za pomocą animowanych ikon pokazane są stany wszystkich najważniejszych elementów systemu (kontrolerów, czujników otwarcia drzwi, linii dozorowych, wyjść sterujących oraz urządzeń VSS, czyli rejestratorów NVR i kamer IP). Dzięki dostępnym fil-



trom można sprawdzić stany wszystkich urządzeń równocześnie lub tylko urządzeń danego typu (np. tylko drzwi). To też skraca czas potrzebny na testowanie systemu.

Korzyści dla administratorów

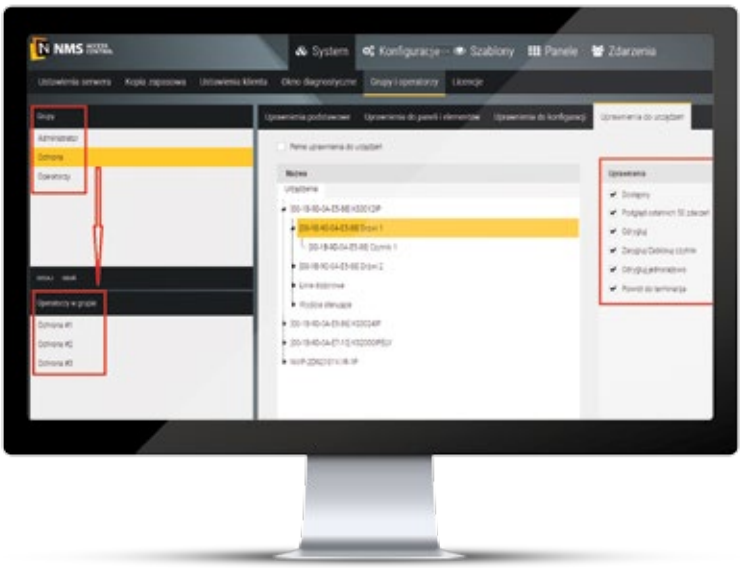
Rolą administratora systemów zabezpieczeń elektronicznych w obiekcie jest przejęcie ich od instalatora oraz sprawowanie kontroli nad pracą tych systemów w celu zapewnienia ich sprawnego codziennego funkcjonowania. W przypadku systemu kontroli dostępu pracującego pod nadzorem programu NMS ACCESS CONTROL administrator ma ułatwione zadanie, ponieważ dzięki możliwości obsługi systemu na wielu stacjach klienckich może rozdzielić zadania związane z tą obsługą między kilka stanowisk. Grupy operatorów wykonujące określone zadania powinny mieć dostęp tylko do niezbędnych pozycji menu programu. Chodzi o bezpieczeństwo systemu i obiektu. Administrator może skorzystać w tym



Rys. 2. Schemat blokowy systemu NMS ACCESS CONTROL

celu z możliwości definiowania uprawnień dla grup operatorów (rys. 3).

Administrator określa najpierw grupy operatorów (np. osoby zajmujące się operacjami dotyczącymi użytkowników kart (dodawanie, edycja, usuwanie), czynnościami służby ochrony itp.). Następnie określa, do których pozycji menu programu lub operacji dana grupa może mieć dostęp (tylko odczyt, pełny dostęp lub brak dostępu). Do tak utworzonych grup przydzielani są operatorzy (każdy ma własny login). Jeżeli trzeba zwiększyć liczbę operatorów, to wprowadza się ich do jednej z grup, a system automatycznie przydziela im uprawnienia, jakie posiada ta grupa. Domyślnie zdefiniowana jest grupa *Administratorzy* i jest jeden administrator z pełnymi uprawnieniami. Do grupy tej można dodawać kolejnych administratorów. Każdy z nich ma własny login.



Rys. 3. Okno definiowania uprawnień dla grup operatorów

W oknie diagnostycznym programu (zakładka *SYSTEM*) administrator ma wgląd do całego systemu i widzi listę operatorów aktualnie zalogowanych na stacjach klienckich. Mając pełny dostęp, administrator może sprawdzać, co dzieje się w systemie, i w pełni nim zarządzać.

Korzyści dla operatorów

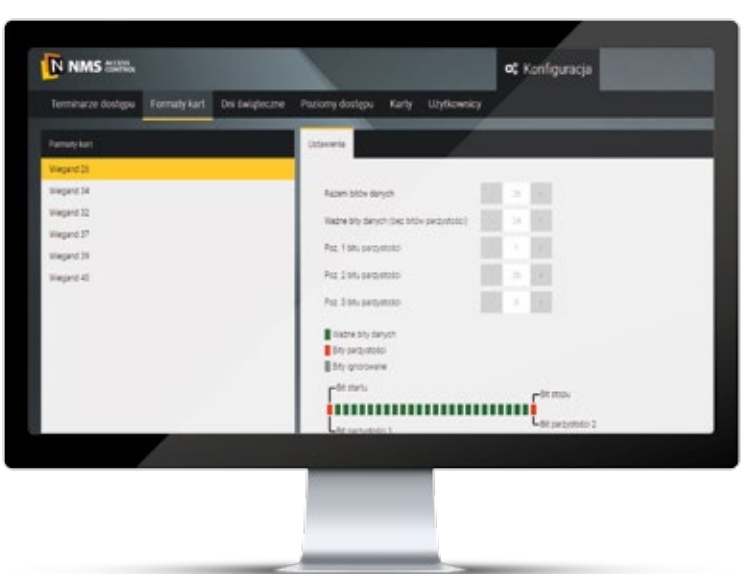
Operatorzy systemu zwykle mają ograniczony dostęp do programu. Zakres dostępu do niego oraz do fizycznych i logicznych elementów systemu przydziela im administrator. Operator ustala tylko swój login. Taki ograniczony dostęp znacznie ułatwia poruszanie się po programie. Przykładowo – operator zajmujący się tylko użytkownikami kart po zalogowaniu się widzi tylko kilka pozycji z menu (rys. 4).

W systemie zainstalowanym w kilku obiektach możliwe jest również ograniczenie dostępu tylko do fragmentu systemu w danej lokalizacji. Dzięki temu operator na stacji klienckiej widzi tylko zdarzenia/alarmy z jednego obiektu, a także ma dostęp tylko do ograniczonej liczby użytkowników kart i niektórych terminarzy. To znacznie ułatwia mu pracę.

Kolejną zasługującą na podkreślenie korzyścią dla operatorów systemu NMS ACCESS CONTROL jest możliwość importu z pliku danych użytkowników wraz numerami kart. W przypadku znacznej liczby użytkowników kart, sięgającej setek, a nawet tysięcy, jest to bardzo istotna opcja, dzięki której mogą oni zaoszczędzić czas. Plik z danymi użytkowników, przygotowany z wykorzystaniem dostępnego w programie szablonu w formacie CSV, w ciągu bardzo krótkiego czasu po wybraniu opcji importu utworzy bazę danych użytkowników. Trudno sobie wyobrazić, jak długo trwałoby ręczne wprowadzanie wszystkich danych i ile pomyłek mogłoby w jego trakcie zajść.

Korzyści dla służb ochrony

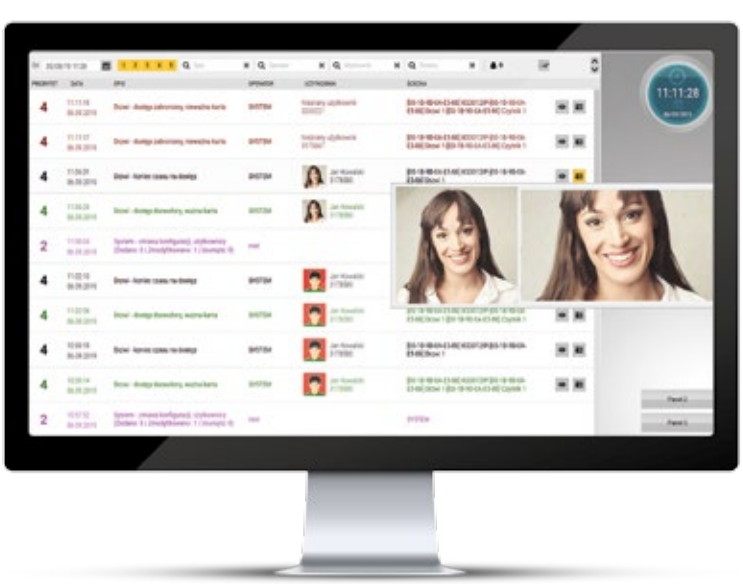
Program NMS ACCESS CONTROL sprawdzi się znakomicie w obiektach, w których pracują ochroniarze. Oferuje bardzo rozbudowane funkcje monitorowania i wizualizacji stanu systemu



Rys. 4. Menu programu dla operatora z ograniczonym dostępem

Rys. 5. Wizualizacja stanu systemu na panelach z hierarchiczną strukturą

na panelach. Instalatorzy i klienci końcowi, którzy użytkują naszą platformę integracyjną VENO, znajdą w programie NMS ACCESS CONTROL znajome elementy i funkcje na panelach do wizualizacji. Najważniejszą korzyścią dla pracowników ochrony mających dostęp do stacji klienckiej programu NMS ACCESS CONTROL będzie łatwość i szybkość uzyskania wiarygodnej informacji o stanie obiektu i systemu. Jest to możliwe dzięki analizie komunikatów wyświetlanych na *STOSIE ZDARZEŃ*, animowanych ikon wyświetlanych na mapie obiektu i tablicy synoptycznej oraz bieżących obrazów z kamer. W połączeniu z hierarchiczną strukturą paneli z mapami obiektu elementy te tworzą bardzo zaawansowane narzędzie, które gwarantuje wysoki poziom zabezpieczenia obiektu i stwarza możliwość szybkiego reagowania w sytuacjach kryzysowych. Bez opuszczania swojego stanowiska pracownik ochrony na bieżąco otrzymuje pełną informację o tym, co się dzieje lub czy wydarzyło się coś nieprawidłowego. Przykładowo – po sforsowaniu kontrolowanego przejścia na stacji klienckiej zostanie wygenerowany alarm (komunikat oraz sygnał akustyczny) i zostanie automatycznie



Rys. 6. Dostęp po weryfikacji wizyjnej

wyświetlone okno wizyjne z obrazem pokazującym to przejście. Dzięki temu możliwe będzie szybkie podjęcie stosownych działań.

Kolejna ciekawa opcja to możliwość weryfikacji dostępu – sprawdzenia, czy użytkownik użył swojej karty na czytniku, przechodząc przez kontrolowane przejście. Jeżeli umieścimy nad czytnikiem kamerę (lub zainstalujemy czytnik z wbudowaną kamerą), to możliwe będzie wyświetlenie na STOSIE ZDARZEŃ zdarzeń okna zawierającego zdjęcie użytkownika z bazy danych systemu oraz – obok – pojedynczej klatki obrazu z tej kamery. Po najechaniu wskaźnikiem myszy na odpowiednią ikonę możliwe jest porównanie obu tych zdjęć. W wersji bardziej zaawansowanej możliwe jest wprowadzenie konieczności potwierdzenia przez operatora uprawnień danej osoby do dostępu do pomieszczenia wymagającego specjalnej kontroli. Wówczas, po odczycie ważnej karty, do stacji klienckiej wysyłane jest żądanie potwierdzenia możliwości dostępu i dopiero po porównaniu obrazów następuje zgoda na dostęp.

Podsumowanie

Polecam NMS ACCESS CONTROL wszystkim instalatorom, ponieważ jest bardzo łatwy w instalacji, konfiguracji i użytkowaniu. Oszczędza czas potrzebny na wdrożenie i gwarantuje stabilne działanie. Informacje dotyczące tego systemu i oprogramowania znajdziecie Państwo na stronie www.nmsac.aat.pl lub otrzymacie, kontaktując się z działem kontroli dostępu firmy AAT HOLDING.

Ryszard Sobierski
AAT HOLDING

Nadzorowanie pomieszczenia z podestem

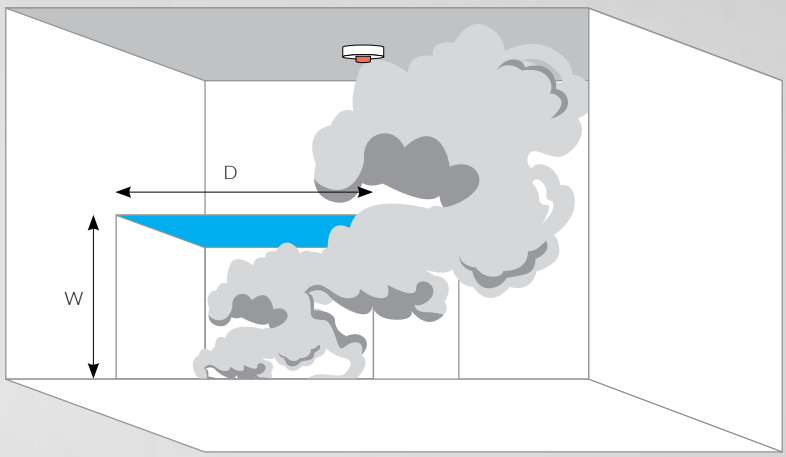
Jerzy Ciszewski

Zajmiemy się problemem, z którym projektant instalacji sygnalizacji pożarowej z pozoru rzadko się spotyka. Mowa o tak zwanych podestach. Istnieje wiele synonimów słowa *podest*. Podestem jest np. estrada, platforma, podium, podwyższenie, rampa, scena, podłoga itp. Nas będzie interesował przypadek, w którym na pewnej wysokości wewnątrz pomieszczenia znajduje się płaszczyzna nieprzepuszczająca dymu ani ciepłego powietrza

Należy zastanowić się, jak można skutecznie nadzorować takie pomieszczenie za pomocą czujek. Oczywiste jest zainstalowanie ich na stropie. Użycie odpowiedniej liczby czujek o odpowiednich zasięgach lub powierzchni dozorowej umożliwi nadzorowanie całej przestrzeni pomieszczenia. Czy na pewno?

Zakładam, że płaszczyzna podestu jest odsunięta od ściany. Ognisko pożaru znajduje się pod podestem, w centrum jego rzutu na podłogę. Jeżeli podest będzie miał dostatecznie dużą powierzchnię, wytwarzany dym nie będzie miał szans na dotarcie (w dostatecznym stężeniu) do czujki zainstalowanej na stropie. Z tego wynika, że pożar na określonym stopniu rozwoju nie będzie mógł być wykryty. Oczywiście, jeśli pozwolimy na większy rozwój pożaru, to w końcu wzrost stężenia dymu w pobliżu czujki na stropie umożliwi jego wykrycie, ale wtedy pożar może już być niebezpieczny dla ludzi, konstrukcji i samej instalacji automatyki pożarowej.

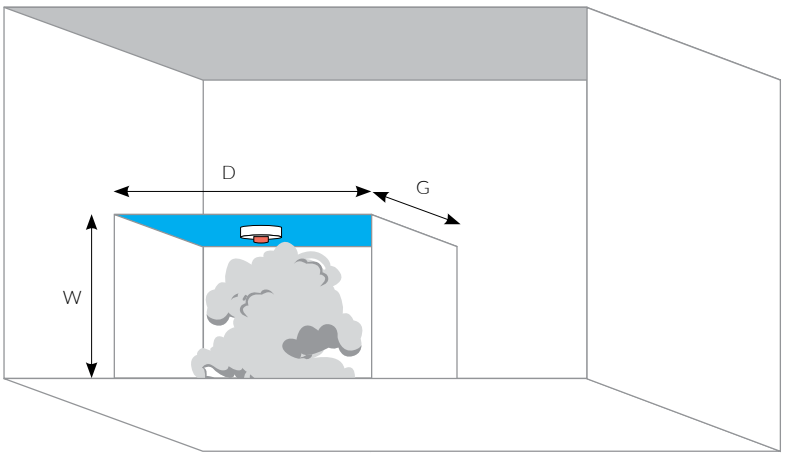
Z tego należy wysnuć wniosek, że jeżeli wymiary podestu będą dostatecznie duże, należy pod podestem zainstalować czujkę (dymu lub ciepła, w zależności od przyjętej koncepcji ochrony obiektu).



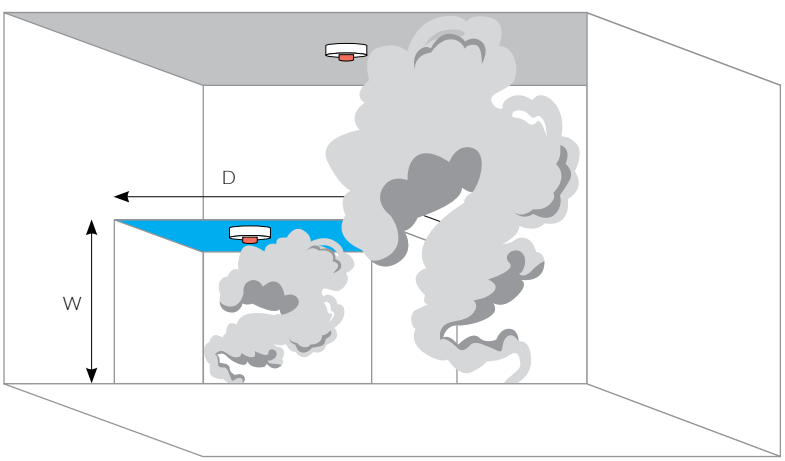
Rys. 1. Nadzorowanie przestrzeni pod podestem za pomocą czujki zainstalowanej na stropie pomieszczenia. Na rysunku pokazano dla uproszczenia wypływ dymu spod podestu tylko z jednej strony

Rodzaj czujki	Wysokość W [m]	Długość D [m]	Głębokość G [m]	Powierzchnia A [m²]
czujka ciepła (wg EN 54-5, EN 54-22)	≤ 7,5	≥ 2	≥ 2	≥ 9
czujka dymu (wg EN 54-7, EN 54-20)	≤ 6	≥ 2	≥ 2	≥ 16
	od 6 do 12	≥ 3,5	≥ 3,5	≥ 31,5

Zwykle przyjmuje się (wszelkie wytyczne należy traktować jako wiedzę techniczną – nie są one umocowane w żadnym przepisie prawnym), że wymiary podestu są takie, jakie podano w tabeli (zgodnie z wytycznymi SITP WP-02-2010 pkt 4.5.8 i VdS 2095:2010-05(07) pkt 6.2.7.10).



Rys. 2. W przypadku przekroczenia wymiarów zawartych w tabeli należy zainstalować czujkę nadzorującą przestrzeń pod podestem



Rys. 3. Ostatecznie ustalony sposób nadzorowania pomieszczenia

Jeżeli poszczególne parametry podestu (W, D, G, A) przekroczą wartości podane w tabeli, to przestrzeń pod podestem powinna być nadzorowana przez odrębną czujkę.

Jeśli natomiast którykolwiek z parametrów nie przekroczy wartości podanych w tabeli, to dodatkowe nadzorowanie przestrzeni pod podestem nie jest konieczne.

Jak pokazano na rysunku numer 3, zainstalowana na stropie czujka (albo więcej czujek) nadzoruje przestrzeń całego pomieszczenia, a więc również powierzchnię podestu. Z kolei przestrzeń pod podestem jest nadzorowana przez czujkę zainstalowaną na stropie podestu.

Zagadnienia związane z nachylonymi strukturami zainstalowanymi w nadzorowanej przestrzeni, stanowiące rozwinięcie artykułu, są omawiane w trakcie organizowanych przez IBP NODEX kursów dla projektantów instalacji sygnalizacji pożarowej.

Jerzy Ciszewski
IBP NODEX

Literatura

1. Wytyczne SITP WP-02:2010 *Instalacje sygnalizacji pożarowej. Projektowanie.*
2. *VdS-Richtlinien für automatische Brandmeldeanlagen. Planung und Einbau. VdS 2095:2010-05(07).*

Instytut Bezpieczeństwa Pożarowego

NODEX

www.IBPNODEX.pl

Niezależny Ośrodek Doradców i Ekspertów

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

Atrakcyjne zniżki dla Członków Wspierających Rozwój Instytutu!

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

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

www.IBPNODEX.pl

Wydruki z centrali SAP

Jan Dziedzic

Każdy system sygnalizacji pożarowej (centrala systemu) jest (a przynajmniej powinien być) wyposażony w drukarkę. Drukarka pełni bardzo ważną rolę – trwale zapisuje na papierze informacje dotyczące wydarzeń zarejestrowanych przez centralę. Obsługa systemu może odczytać z wydruku (nie tylko na wyświetlaczu centrali) informacje o alarmach, awariach, odłączeniach i wysterowaniach poszczególnych urządzeń. Na wydrukach dokumentowane są również działania obsługi – odłączenia pojedynczych urządzeń lub ich grup, potwierdzenia przyjęcia alarmów, potwierdzenia kasowania alarmów itp.

W tym miejscu należy nadmienić, iż każda centrala SAP ma pamięć o pojemności od kilku tysięcy do nawet kilkudziesięciu tysięcy zdarzeń. Serwis systemu SAP, a czasem nawet personel obsługujący centralę zainstalowaną w budynku, może przeglądać rejestr zdarzeń, a nawet drukować wszystkie informacje dotyczące zdarzeń z określonego przedziału czasowego lub informacje dotyczące zdarzeń wybranych typów (np. awarii).

Producenci central systemów sygnalizacji pożarowej oferują wraz z centralą tzw. drukarkę systemową, najczęściej montowaną w obudowie centrali lub w dodatkowym module pod centralą. Jako systemowe stosowane są drukarki igłowe albo termiczne. Prawie każdy producent umieszcza w centrali gniazdo (RS, USB itp.), do którego można podłączyć drukarkę zewnętrzną praktycznie dowolnego typu.

Jednym z najważniejszych jest wydruk dotyczący alarmu pożarowego, zawierający informację o lokalizacji urządzenia zgłaszającego alarm – czujki, ROP-u, modułu nadzorującego np. stałe urządzenie gaśnicze. Niektórzy producenci central umożliwiają (w przypadku zastosowania drukarki systemowej) łatwe oddarcie zadrukowanej taśmy z informacją dotyczącą alarmu pożarowego pierwszego stopnia, aby pracownik ochrony lub strażak budynkowy nie musiał zapamiętywać danych potrzebnych do weryfikacji alarmu.

W przypadku alarmu drugiego stopnia drukarka najczęściej (prawie zawsze) drukuje informacje dotyczące wszystkich skutków wykonania zadań przewidzianych w scenariuszu pożaru. W ramach tych zadań nadawane są określone komunikaty przez dźwiękowy system ostrzegawczy, następuje odblokowanie drzwi na drogach ewakuacyjnych, włączane jest oddymianie i napowietrzanie (uruchamiana jest wentylacja pożarowa), następuje wysterowanie klap pożarowo-dymowych i pożarowych, zamykane są drzwi i bramy, które są otwarte, gdy nie ma zagrożenia, następuje wymuszenie zjazdu wind na poziom parteru, powiadamiana jest Państwowa Straż Pożarna (następuje wysłanie sygnału o pożarze przez system monitorowania), wykonywane są inne niezbędne w konkretnym obiekcie czynności (np. zamknięcie wjazdu do garażu podziemnego).

W wyposażonych w systemy przeciwpożarowe, wentylacji/klimatyzacji, bezpieczeństwa i inne systemy biurowych budynkach wysokich liczba sterowań zapisanych w scenariuszu pożaru, wykonywanych przez centralę SAP, waha się średnio od ok. 80 do nawet 200. Informacje dotyczące wszystkich sterowań są drukowane przez drukarki systemowe lub zewnętrzne. Na podaną liczbę sterowań składają się sterowania DSO (od kilku do kilkunastu urządzeń), KD (od kilku do kilkudziesięciu urządzeń), wentylacją pożarową (kilkadziesiąt urządzeń), drzwiami i bramami pożarowymi (od kilku do kilkudziesięciu urządzeń), windami (kilka urządzeń) i pozostałe sterowania (od kilku do kilkunastu).

W zależności od typu drukarki i szerokości arkuszy papieru wydruk w przypadku alarmu pożarowego może mieć długość od kilkudziesięciu centymetrów do nawet kilku metrów (albo od kilku do kilkunastu stron w formacie A4). W przypadku końcówki rolki lub niewielkiej ilości papieru w podajniku drukarki nie wszystkie informacje zostaną wydrukowane.

Przykładowe informacje wydrukowane przez drukarkę systemową podczas pożaru (dla poszczególnych grup sterowań):

1. „ALARM II STOPNIA, Czujki automatyczne, Grupa 1014/21, Piętro 10, 10.18 Archiwum, 15.08.19, 11:59:38, xxxxxxx (numer zdarzenia)".
2. „AKTYWACJA, Wyjście 888, Otwarcie klapy, FSD/10/2/NC, 15.08.19, 11:59:39, xxxxxxx (numer zdarzenia)". Takich sterowań jest kilkadziesiąt.
3. „AKTYWACJA, Wyjście 2200, Sterowanie, Zjazd windy A, 15.08.19, 11:59:39, xxxxxxx (numer zdarzenia)". Takich sterowań jest kilka.
4. „AKTYWACJA, Wyjście 991, Sterowanie, Napowietrzanie, Szyb windy C, 15.08.19, 11:59:39, xxxxxxx (numer zdarzenia)". Jest jedno takie sterowanie.
5. „AKTYWACJA, Wyjście 19, Sygnał do DSO, Ewakuacja +10, 15.08.19, 11:59:39, xxxxxxx (numer zdarzenia)". Takich sterowań jest kilka (oprócz zagrożonej kondygnacji +10: klatki schodowe, poziomy garażowe, kondygnacja techniczna).
6. „AKTYWACJA, Wyjście 1311, Sterowanie, Wyłączenie nagłośnienia lokalnego +10, 15.08.19, 11:59:39, xxxxxxx (numer zdarzenia)". Takich sterowań jest od kilku do kilkudziesięciu.

7. „AKTYWACJA, Wyjście 817, Sterowanie, Kontrola dostępu +10 odłączenie, 15.08.19, 11:59:39, xxxxxxx (numer zdarzenia)". Takich sterowań w budynku jest kilkadziesiąt.
8. „AKTYWACJA, Wyjście 1234, Sterowanie, Wentylacja bytowa STOP, 15.08.19, 11:59:39, xxxxxxx (numer zdarzenia)". Takich sterowań jest kilka – zależnie od systemu wentylacji/klimatyzacji zastosowanego w budynku.
9. „AKTYWACJA, Wyjście 445, Sterowanie, Zamknięcie bramy ppoż. -3, 15.08.19, 11:59:39, xxxxxxx (numer zdarzenia)". Takich sterowań jest kilka.
10. „AKTYWACJA, Wyjście 1017, Sterowanie, Wentylator oddymiający Nr 1 START, 15.08.19, 11:59:39, xxxxxxx (numer zdarzenia)". Są dwa takie sterowania.
11. „AKTYWACJA, Wyjście 1049, Sterowanie, Napowietrzanie klatki schodowej START, 15.08.19, 11:59:39, xxxxxxx (numer zdarzenia)". Są dwa takie sterowania.
12. „AKTYWACJA, Wyjście 1290, Sterowanie, Napowietrzanie przedsionka ppoż. START, 15.08.19, 11:59:39, xxxxxxx (numer zdarzenia)". Są dwa takie sterowania.
13. „AKTYWACJA, ..." (od kilku do kilkudziesięciu innych sterowań).

Należy zadać sobie pytania:
- czy wydruk wszystkich informacji w trakcie alarmu pożarowego jest potrzebny?
- kto czyta/sprawdza te wydruki?
- czy wydruk komunikat o awarii urządzenia zostanie natychmiast zauważony?
- czy można będzie szybko przejrzeć wydruk, aby znaleźć informacje o ewentualnych awariach?

Pełne, szczegółowe wydruki są potrzebne do ewentualnej późniejszej analizy zdarzenia. Niestety, ani ochrona obiektu, ani strażacy z PSP nie są w stanie na bieżąco analizować drukowanych informacji. Nie jest łatwo zauważyć (rozpoznać) lub odnaleźć informację dotyczącą awarii urządzenia, gdyż jest podobna do innych – może być np. taka: „AKTYWACJA, Wejście 889 Awaria, Klapa FSD/10/2/NC, 15.08.19, 11:59:39, xxxxxxx (numer zdarzenia)".

Wydruk z drukarki systemowej podczas alarmu pożarowego powinien zawierać (oprócz informacji dotyczących aktywności obsługi centrali, np. potwierdzenia rozpoznania) informacje o pożarze (adres, informację o tym, które urządzenie zgłosiło alarm, i dane systemowe) oraz informacje o awariach urządzeń uwzględnionych w scenariuszu pożarowym dla danej lokalizacji. Taki wydruk – oprócz informacji o pożarze – dostarczy informacji o urządzeniach, które nie wykonały powierzonego im zadania. Wykorzystanie tych danych zależy od tego, jakie urządzenie uległo awarii i jaki jest jej wpływ na bezpieczeństwo osób przebywających w budynku (ewakuujących się z budynku) oraz na ewentualną możliwość przeniesienia się pożaru do innej strefy pożarowej lub na drogi ewakuacyjne (klatki schodowe).

Aby ochrona faktycznie skorzystała z informacji zawartych na wydruku, a firmy serwisujące mogły mieć wydruk wszystkich potrzebnych danych (np. podczas przeglądów kwartalnych czy rocznych testów współpracy systemów przeciwpożarowych), oprogramowanie centrali SAP powinno mieć dwa tryby pracy – standardowy i pożarowy. Ciekawe, czy istniejące na polskim rynku systemy mają takie możliwości.

Jan Dziedzic

ARVINGE

OCHRONA PRZECIWPOŻAROWA

Praca na rzecz Właścicieli lub Zarządców Nieruchomości:

- Jednorazowe lub okresowe przeglądy budynków w zakresie bezpieczeństwa pożarowego i przestrzegania przepisów ppoż.
- Wstępne opiniowanie projektów modernizacji części budynku w zakresie zmian aranżacyjnych i instalacyjnych.
- Nadzór nad przebiegiem prac oraz uczestnictwo w odbiorach prac i testach funkcjonalnych instalacji ppoż.
- Szkolenie służb ochrony obiektu, służb sprzątających, służb technicznych, a także najemców (zwłaszcza Zespołów Ewakuacyjnych).
- Opracowywanie procedur dla służb budynkowych na wypadek ewakuacji (alarm pożarowy, inne zdarzenie).
- Opracowywanie procedur dla służb budynkowych, w zakresie prac pożarowo niebezpiecznych, czasowych odłączeń systemów ppoż. itp.
- Organizacja i realizacja ćwiczeń ewakuacyjnych.
- Opracowania i aktualizacja Instrukcji Bezpieczeństwa Pożarowego obiektu.
- Prowadzenie rocznych testów współpracy systemów ppoż. budynku.
- Prowadzenie testów funkcjonalnych pompowni pożarowych, bram i drzwi pożarowych, windy pozarowej.
- Przeglądy budynków w zakresie dostępu do pomieszczeń na wypadek alarmu pożarowego lub awarii technicznej.

Realizowanie prac zleconych:

- Realizacja prac jak dla Właścicieli lub Zarządców Nieruchomości.
- Ocena stanu ochrony ppoż. obiektu ze wskazaniem występujących nieprawidłowości.
- Ocena zagrożeń pożarem w procesach produkcyjnych i magazynowych.
- Ocena zagrożenia wybuchem w procesach produkcyjnych i magazynowych.
- Badanie przyczyn pożaru.
- Opracowywanie ekspertyz technicznych stanu ochrony ppoż. obiektu (w zespole rozszerzonym o rzeczoznawcę ds. zabezpieczeń ppoż. i rzeczoznawcę budowlanego).
- Realizacja innych prac zleconych we współpracy z biurami projektów, a także firmami instalatorskimi - w zakresie instalacji ppoż. w budynkach.

PHU ARVINGE
email: jan@arvinge.pl, tel: 504 85 83 85

Technologie jutra

Maciej Pietrzak

Stan branży zabezpieczeń zależy od rozwoju techniki i technologii. Dzięki postępowi można usprawnić istniejące rozwiązania, a także uzyskuje się coraz nowsze narzędzia i zupełnie nowe możliwości

Przykładem innowacji jest niewątpliwie coraz szersze wykorzystanie algorytmów sztucznej inteligencji. Rozpoznawanie twarzy lub detekcja intruzów wraz z rozpoznaniem typu obiektu umożliwiającym odróżnienie człowieka od pojazdu to tylko początek możliwości. Oczywiście to bardzo korzystnie wpływa na marketing, ale czy faktycznie przynosi wymierne korzyści w praktyce?

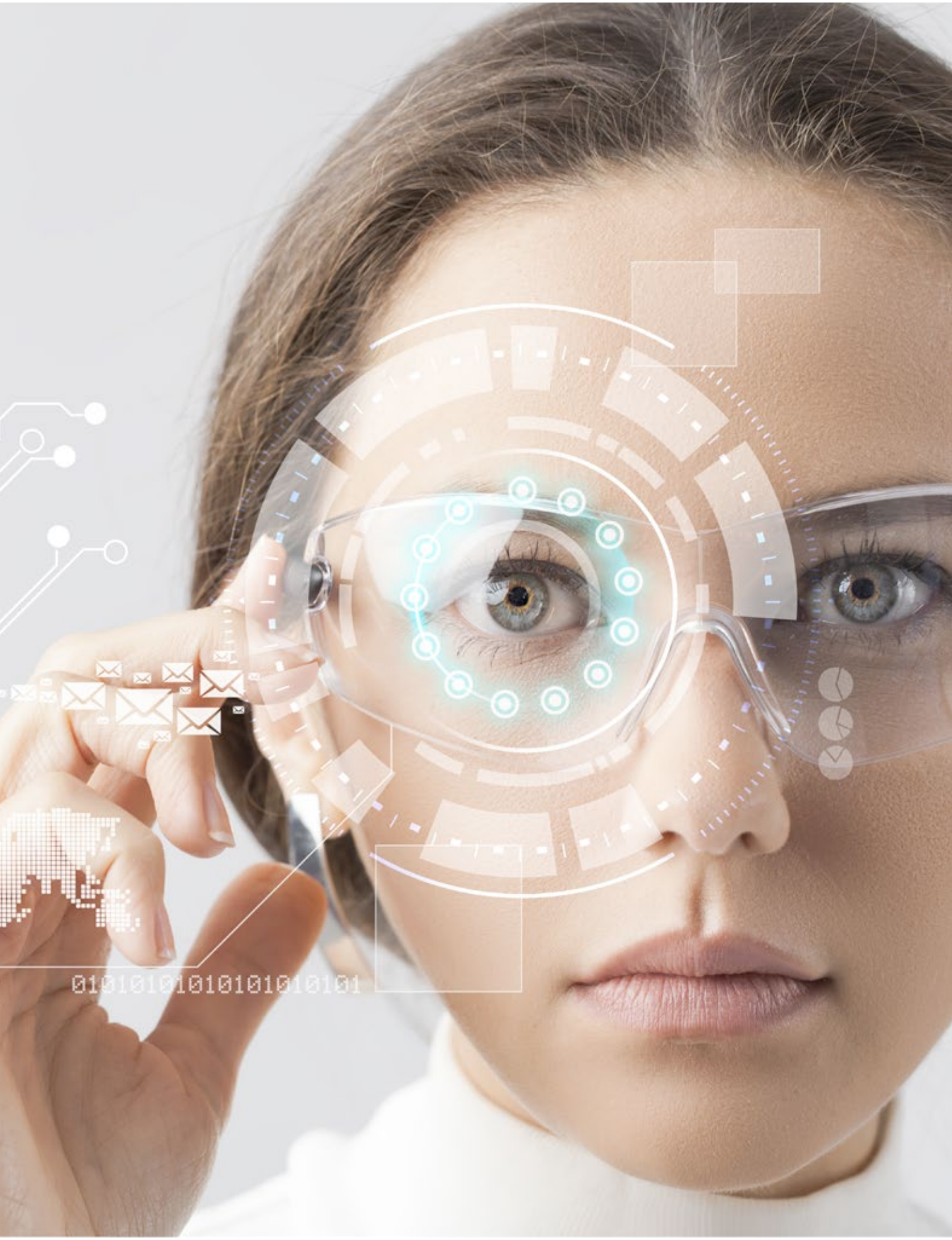
Rolą producentów jest nie tylko wykazanie, że dane rozwiązanie działa, ale przede wszystkim wskazanie, gdzie i jak użytkownik może je wykorzystać. Dużo mówi się ostatnio o 5G. Wprowadzenie telefonów piątej generacji ma przyczynić się do rozwoju Internetu rzeczy, a w konsekwencji także tzw. inteligentnych miast. Możliwe jest inteligentne sterowanie nie tylko jednym budynkiem, lecz całą aglomeracją, w tym zarządzanie ruchem drogowym, sterowanie oświetleniem ulicznym, a nawet kontrola czystości powietrza.

Jak zawsze przy wprowadzaniu innowacji oprócz entuzjazmu pojawia się obawa o bezpieczeństwo. Niejednokrotnie obawy są bezpodstawne, a ich przyczyną jest brak dostatecznej informacji, co dowodzi, że oprócz rozwijania techniki i technologii równie istotne jest uświadamianie społeczeństwu możliwości oraz zagrożeń związanych z tym rozwojem.

W przypadku wykorzystywania funkcji rozpoznawania twarzy, na przykład w systemach kontroli dostępu, użytkownicy obawiają się konfliktu z prawem, co ma związek z przetwarzaniem danych osobowych i ewentualnym naruszeniem prywatności. Ogólne rozporządzenie o ochronie danych z roku 2018 zakwalifikowało dane biometryczne jako dane osobowe, które powinny być szczególnie chronione. Chociaż przepisy dosyć klarownie opisują, w jakich przypadkach można wykorzystywać na przykład odcisk palca, nadal dla wielu osób jest to niejasne i nieustannie powtarza się pytanie „Co na to RODO?". Brak wiedzy na temat możliwości, jakie oferują aktualnie producenci systemów bezpieczeństwa, oraz wątpliwości powodują, że pomimo coraz większego wyboru nowoczesnych rozwiązań nadal tkwimy w rzeczywistości sprzed kilkunastu lat.

Doskonałym przykładem są nowo powstające wizyjne systemy dozorowe. Ogromna poprawa rozdzielczości przetworników wykorzystywanych w kamerach oraz ich wysoka czułość umożliwia skuteczną obserwację sceny nie tylko w dzień, ale i w nocy – coraz częściej bez korzystania z dodatkowego doświetlenia IR. Mimo to wymagania dotyczące kamer są często formułowane lakonicznie, a wśród parametrów pojawia się zaledwie rozdzielczość oraz czułość. Równie ważne właściwości stanowiące o jakości, takie jak apertura obiektywu, prędkość migawki przy jakiej czułość kamery jest określona, czy stosunek sygnału do szumu, nie są uwzględniane.

Zanim zaczniemy myśleć o wprowadzaniu nowoczesnych technik przetwarzania metadanych generowanych na podstawie analizy treści obrazu, musimy najpierw skupić uwagę na jego jakości, gdyż to on najczęściej jest słabym ogniwem w całym systemie. Podobnie jest


01010101010101010101

w przypadku wyboru formy rejestracji obrazu. Wymagania dotyczące rejestracji obrazu bardzo często ograniczają się do podania liczby kanałów i czasu, przez jaki dane mają być przechowywane. Brak określonej przepustowości na wejściu rejestratora czy brak wytycznych dotyczących dekodowania obrazu prowadzi do problemów ze spełnieniem wymagań dla systemu, na przykład na skutek niemożności wyświetlenia w tym samym czasie większej liczby obrazów.

Infrastruktura kablowa oraz aktywne urządzenia odpowiedzialne za transmisję również powinny wzbudzać większe zainteresowanie projektantów, a także instytucji odpowiedzialnych za certyfikację oraz formułowanie norm. Już nikogo nie dziwi wykorzystanie metody PoE umożliwiającej zasilanie urządzeń oraz transmisję danych tym samym przewodem, ale nadal borykamy się z ograniczeniem w postaci odległości między kamerami a przełącznikami sieciowymi. Na rynku dostępnych jest wiele rozwiązań pozwalających wyeliminować częsty problem, jakim jest dystans między urządzeniami w sieci IP. W przypadku okablowania UTP maksymalny dystans wynosi 100 metrów, a w przypadku STP – do 250 metrów. Coraz więcej producentów oferuje funkcje umożliwiające transmisję na nawet dwukrotnie większe odległości. Firma Dahua Technology będąca liderem branży zabezpieczeń opatentowała w ubiegłym roku metodę ePoE (enhanced Power over Ethernet). To innowacyjne rozwiązanie zapowiada rewolucję w systemach dozoru wizyjnego, w których wykorzystywane są kamery IP. Zaadaptowanie kodowania 2D-PAM3 i sposobów transmisji stosowanych dotychczas w kopalniach (standardy YD/T z lat 1947–2009) daje nowe możliwości zasilania urządzeń oraz transmisji obrazów. Metoda zastosowana w kamerach IP oraz przełącznikach sieciowych pozwala na transmisję danych i zasilanie kamer na odległość 800 m w przypadku wykorzystania zwykłego przewodu UTP. Możliwe stało się również wykorzystanie okablowania koncentrycznego i uzyskanie równie imponującego dystansu wynoszącego 1000 m. Brak wyraźnego zaaprobowania takich rozwiązań przez organizacje zajmujące się certyfikacją sprawia, że tego typu nowości nie są stosowane na większą skalę.

Nadal powinno się umacniać współpracę między producentami a firmami odpowiedzialnymi za projektowanie. Oczywiście nie może zabraknąć udziału organizacji standaryzujących systemy bezpieczeństwa. Na to, jakie systemy bezpieczeństwa będą stosowane, ma wpływ również wiedza użytkowników końcowych. Należy brać pod uwagę różne czynniki, które mają wpływ na możliwość stosowania nowoczesnych rozwiązań technicznych, na postęp w branży zabezpieczeń i na urzeczywistnianie śmiałych wizji.

Maciej Pietrzak
Dahua Technology Poland

RACS 5

Skalowalny system kontroli dostępu, bezpieczeństwa i automatyki

Przewodowa kontrola dostępu

Bezprzewodowa kontrola dostępu

Rejestracja czasu pracy

Automatyka budynkowa

Zarządzanie kluczami

Identyfikacja mobilna

roger®

Intelligence for Building

dla każdego

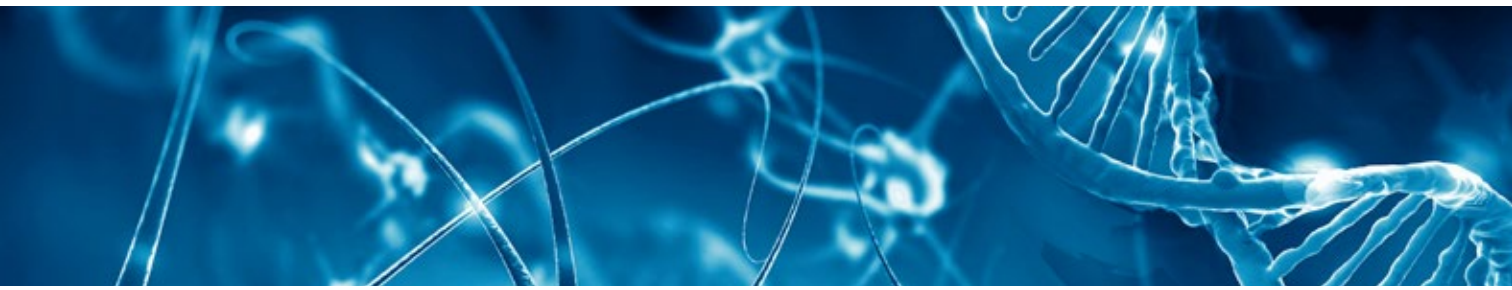
Część 5

Piotr Rogalewski

Z poprzednich części cyklu *AI dla każdego* można było dowiedzieć się, co to jest sztuczna inteligencja i jak przebiegał jej rozwój w ciągu ostatnich kilkudziesięciu lat. Opisałem także tzw. uczenie maszynowe, sztuczny neuron, sieć neuronową oraz jeden ze sposobów uczenia sieci neuronowych. Pora na podanie kilku przykładów wykorzystania sztucznej inteligencji ze szczególnym uwzględnieniem wizyjnych systemów dozorowych

Rozpoznawanie twarzy

Rozpoznawanie twarzy z wykorzystaniem sztucznej inteligencji to obecnie jedna z najbardziej dynamicznie rozwijających się dziedzin nadzoru wizyjnego i kontroli dostępu. Proces rozpoznawania podzielony jest na kilka etapów. Na początku twarz jest wykrywana, czyli określane jest miejsce na obrazie, gdzie twarz się znajduje. Następnie wyodrębniony fragment jest poddawany analizie zawartości. W rozpoznawaniu twarzy najczęściej stosuje się jedną z dwóch metod – globalną lub ekstrakcję cech (ang. *feature based*). W metodzie globalnej obraz twarzy jest traktowany jako całość, natomiast w przypadku ekstrakcji cech brane są pod uwagę geometryczne relacje pomiędzy wyodrębnionymi wcześniej składowymi twarzy (np. oczami i nosem). Ze względu na to, że pełna analiza treści obrazu jako graficznej mapy rastrowej powoduje konieczność generowania bardzo złożonych sieci neuronowych i spowalnia działanie systemu, najczęściej w procesie tym wprowadzany jest etap pośredni, polegający na utworzeniu biometrycznej siatki charakterystycznych punktów twarzy. Taki układ jest indywidualny dla każdego człowieka i nie zmienia się z wiekiem (długości odcinków mogą się zmieniać, ale proporcje między nimi pozostają te same). Dopasowanie obserwowanej twarzy do wzorca w bazie danych na podstawie porównania siatek biometrycznych trwa znacznie krócej niż w przypadku pełnego porównania obrazów w postaci map bitowych. W systemach rozpoznawania twarzy wykorzystuje się najczęściej uczenie nienadzorowane, np. metodą Hebba[i]. Jeżeli rozpoznawanie twarzy jest elementem systemu kontroli dostępu, to sam proces rozpoznawania nie jest wystarczający ze względu



na bezpieczeństwo takiego systemu. Istnieje ryzyko, że osoba nieuprawniona spróbuje oszukać system, prezentując kamerze wydrukowany obraz twarzy osoby uprawnionej lub nawet trójwymiarowy model takiej twarzy, np. wydrukowany za pomocą drukarki 3D.

Aby temu zapobiec, nowoczesne systemy rozpoznawania twarzy są wyposażone w mechanizmy wykrywania cech życia. Dwie kamery zapewniają obserwację stereoskopową, wykluczając próbę oszukania systemu za pomocą wydrukowanego obrazu twarzy. Algorytmy analizy ruchu gałek ocznych, mrugania i ruchu mięśni twarzy stanowią dodatkowe zabezpieczenia. W ofercie czołowych producentów systemów zabezpieczeń można znaleźć terminale kontroli dostępu umożliwiające rozpoznanie twarzy w czasie kilkuset milisekund.

ANPR (LPR)

Rozpoznawanie numerów tablic rejestracyjnych jest już bardzo powszechnym zastosowaniem analizy treści obrazu i jest często stosowane w systemach parkingowych. Aktualnie systemy te szeroko wykorzystują sztuczną inteligencję. Proces wyodrębnienia numeru tablicy rejestracyjnej jest podzielony na kilka etapów, z których najtrudniejszym jest wyodrębnienie obszaru, w którym znajduje się ta tablica. Nowoczesne systemy ANPR potrafią odfiltrować niewłaściwe dane w postaci napisów umieszczonych na pojazdach, a nie będących oznaczeniami rejestracyjnymi (np. reklamy na burtach ciężarówek, napisy „Taxi", „POLICJA" itp.). Po wyodrębnieniu miejsca z numerem tablicy rejestracyjnej następuje jej właściwe rozpoznanie, do czego wykorzystuje się techniki OCR (ang. *optical character recognition* – optyczne rozpoznawanie znaków). Ich działanie opiera się na zastosowaniu sieci neuronowych i uczenia nadzorowanego (model sieci został nauczony kształtów cyfr i liter widzianych pod różnymi kątami, o różnych krojach czcionki itp.). Częścią oprogramowania systemu ANPR jest wytrenowany model sieci potrafiący rozpoznawać litery i cyfry tablicy rejestracyjnej.

Klasyfikacja obiektów i filtrowanie fałszywych alarmów

Do niedawna kamery do nadzoru wizyjnego stosowane w ochronie obwodowej były tylko urządzeniami wspomagającymi. Głównym powodem była niedoskonałość algorytmów detekcji ruchu i analizy treści obrazu w warunkach terenowych. Ruchome gałęzie i liście drzew, przebiegające zwierzęta, falowanie gorącego powietrza, dynamiczne zmiany kontrastu i jasności na skutek przejściowego zachmurzenia i inne czynniki powodowały, że liczba fałszywych alarmów generowanych przez wizyjne systemy dozorowe starszej generacji była zbyt duża. Sztuczna inteligencja pozwala uporać się z tymi problemami. Zasada działania jest prosta. Proces analizy przebiega dwuetapowo. Na pierwszym etapie ruchome obiekty widoczne na obrazie są klasyfikowane według typu i tylko jeśli obiekt spełnia kryterium danego typu (np. jest to pojazd albo człowiek), uruchamiana jest dalsza analiza. Pozostałe ruchome obiekty, które nie spełniają kryteriów, zostają zignorowane. Na drugim etapie tylko aktywność obiektów odpowiadających kryteriom jest analizowana zgodnie z ustalonym scenariuszem. Tą aktywnością może być np. przekroczenie linii i wejście na dany teren. Dzięki takiej procedurze liczba fałszywych alarmów zostaje bardzo znacznie zredukowana, a efektywność systemu wydatnie wzrasta. Ponadto możliwe jest zastosowanie tych samych kryteriów i filtrów klasyfikacyjnych do wyszukiwania określonych scen w zarejestrowanym materiale wizyjnym. Wystarczy poinformować system, czego ma szukać (np. sylwetek osób). Opisana wyżej technika to doskonały przykład zastosowania uczenia nadzorowanego. Częścią oprogramowania układowego (firmware'u) kamery lub rejestratora, który realizuje

funkcję filtrowania fałszywych alarmów, jest wytrenowany model sieci neuronowej, nauczony rozpoznawania sylwetek osób i pojazdów lub innych obiektów.

Klasyfikacja cech

Rozwinięciem opisanej wyżej klasyfikacji obiektów jest klasyfikacja cech. Polega ona na tym, że po wyodrębnieniu z obrazu pożądanych obiektów algorytm analizy „przygląda się" dokładniej samym obiektom, szukając ich cech szczególnych. W przypadku analizy sylwetki ludzkiej można określić takie cechy jak płeć, wiek, dominujący kolor ubioru i wzrost, a także to, czy dana osoba nosi okulary, czy ma plecak, czy jedzie na rowerze itp. W przypadku pojazdów możliwe jest określenie np. marki, modelu, koloru i wielkości. Wizyjne systemy dozorowe mające takie możliwości klasyfikacji obiektów są już dostępne w ofercie czołowych producentów.

Co jeszcze?

Wykrycie paniki w tłumie ludzi, podejrzanego zachowania lub zgubienia transportowanego przez samochód ciężarowy ładunku, analiza prędkości ruchu czy automatyczne śledzenie obiektów przez kamery PTZ to kilka kolejnych przykładów wykorzystania sztucznej inteligencji w dziedzinie nadzoru wizyjnego. Dzięki zastosowaniu sieci neuronowych i głębokiego uczenia analiza treści obrazu w takich przypadkach jest nieporównywalnie lepsza niż bez użycia sztucznej inteligencji. Podane w tym artykule przykłady to oczywiście bardzo niewielki fragment tego, co już dziś ona potrafi. Wykorzystywana jest także w rozpoznawaniu mowy, systemach finansowych na giełdach (tzw. *fast trading*), diagnostyce medycznej, obserwacjach astronomicznych (w śledzeniu i wyszukiwaniu ciał niebieskich), symulacjach obciążeniowych w projektowaniu konstrukcji, w tzw. wirtualnych asystentach obecnych w portalach pomocy technicznej czy w modelach meteorologicznych i zaawansowanym prognozowaniu pogody. Bardzo ciekawym zastosowaniem sztucznej inteligencji jest też wykorzystywanie jej w nowoczesnych systemach antywirusowych. Przez ostatnich kilkanaście lat powstała tak duża liczba wirusów i innego szkodliwego oprogramowania, że skanowanie i wyszukiwanie złośliwego kodu tradycyjnymi metodami heurystycznymi w rozsądnym czasie staje się niemal niemożliwe. Sztuczna inteligencja radzi sobie z tym doskonale.

Co jest „pod spodem"?

Sztuczna inteligencja nabiera coraz większego znaczenia, ale tworzenie od podstaw dostosowanych do niej silników programowych i sprzętowych jest bardzo trudne i kosztowne, więc nie jest dla producentów priorytetem. W związku z tym praktycznie wszystkie stosowane obecnie w branży zabezpieczeń techniki związane ze sztuczną inteligencją bazują na gotowych rozwiązaniach lub ich rozmaitych modyfikacjach. Przyjrzymy się trzem najbardziej rozpowszechnionym.

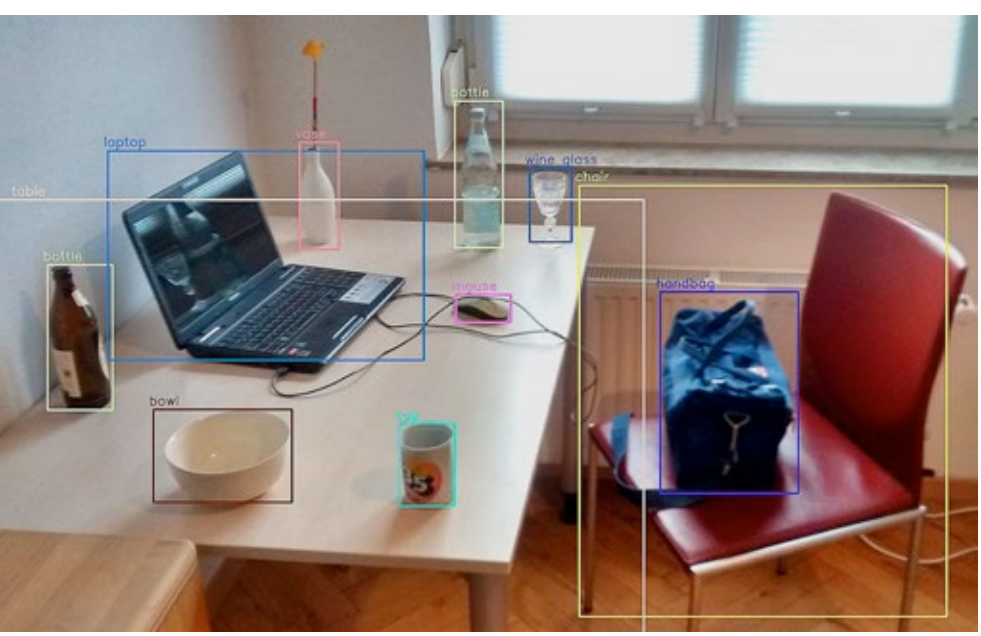
Movidius

Jednym z podstawowych problemów utrudniających korzystanie z modeli sieci neuronowych jest ich wielkość. Model sieci neuronowej w pełni wytrenowany dużym zbiorem danych

Fot. 1. NCS2 – „Domowy" sprzętowy akcelerator sztucznej inteligencji

testowych jest często zbyt „ciężki", by sprawnie przetwarzać te dane, szczególnie w czasie rzeczywistym. Dotyczy to na przykład systemów analizujących treść obrazu, w których kamery IP nie dysponują adekwatną mocą obliczeniową. Pomocne są specjalistyczne procesory nazywane akceleratorami sztucznej inteligencji. Jak wskazuje nazwa, przyspieszają one działanie modelu sieci dzięki temu, że działają tylko te jej fragmenty, które odpowiadają za osiągnięcie wyniku pożądanego w danym momencie. U podstaw tego procesu leży inferencja, czyli wnioskowanie i przewidywanie przez model sieci neuronowej nowych wyników na podstawie poprzednich zachowań. Movidius jest właśnie takim akceleratorem i jest obecnie stosowany przez kilku czołowych producentów wizyjnych systemów dozorowych.

Dla tych, którzy chcą spróbować własnych sił w kreowaniu i rozwijaniu systemów sztucznej inteligencji, twórca Movidiusa, firma Intel, oferuje miniaturowy moduł akceleratora Neural Compute Stick 2 (NCS2), podobny z wyglądu do popularnych pamięci USB. NCS2 można połączyć np. z popularnym miniaturowym komputerem modułowym Raspberry Pi, by rozpocząć własną przygodę ze sztuczną inteligencją za zaledwie kilkaset złotych.



Fot. 2. Rozpoznawanie obiektów dzięki wykorzystaniu biblioteki TensorFlow. Źródło: https://it.wikipedia.org/wiki/Object_recognition, autor: M. Theiler

TensorFlow

Tensor Flow jest stworzoną przez firmę Google biblioteką programistyczną typu *open source*. Można ją uruchomić na komputerach klasy PC, urządzeniach mobilnych, w systemach wbudowanych (ang. *embedded*), a także za pomocą kart graficznych i specjalistycznych procesorów wspierających (akceleratorów sztucznej inteligencji). Dużą popularność zawdzięcza łatwym w obsłudze interfejsom, z którymi radzą sobie nawet niezbyt zaawansowani programiści, a także gotowym, przykładowym modelom sieci neuronowych przygotowanym przez twórców biblioteki. TensorFlow obsługuje bezpośrednio model interfejsu CUDA firmy NVIDIA.

OpenCV

OpenCV to bazująca na koncepcji kodu otwartego biblioteka programistyczna opracowana przez firmę Intel. Biblioteka ta jest wieloplatformowa, więc można z niej swobodnie korzystać w systemie operacyjnym Windows, Linux i Mac OS. Pakiet zawiera wiele gotowych funkcji wykorzystywanych w procesie obróbki obrazu ze szczególnym uwzględnieniem analizy w czasie rzeczywistym. OpenCV jest szeroko wykorzystywana przy tworzeniu pojazdów autonomicznych, w systemach rozpoznawania znaków drogowych i dynamicznej korekcji toru jazdy.

W kolejnej, ostatniej już części cyklu *AI dla każdego* przyjrzymy się wyzwaniom i zagrożeniom, jakie może ze sobą nieść rozwój sztucznej inteligencji.

Piotr Rogalewski

Przypisy:
i: D. O. Hebb, *Distinctive features of learning in the higher animal*, Oxford University Press, Londyn 1961;
C. M. Bishop, *Neural Networks for Pattern Recognition*, Oxford University Press, Londyn 1995.

NOVUS®

6000 VSS IP

NOVUS IP NMS Compatible ONVIF

SKUTECZNE ROZPOZNAWANIE TWARZY

W REJESTRATORACH SERII 6000
W POŁĄCZENIU Z KAMERAMI SERII 6000

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

Nowe prawo zamówień publicznych

Joanna Filipiak

We wrześniu br. uchwalono nowe prawo zamówień publicznych.

Według Ministerstwa Przedsiębiorczości i Technologii oraz Urzędu Zamówień Publicznych głównymi problemami, jakie ma rozwiązać nowa ustawa, są:

- zbyt mały udział przedsiębiorców z sektora małych i średnich przedsiębiorstw w rynku zamówień publicznych (sztywne i rygorystyczne procedury zniechęcają małe i średnie przedsiębiorstwa do ubiegania się o zamówienia publiczne);
- niska konkurencyjność i malejące zainteresowanie wykonawców rynkiem zamówień publicznych (w 2017 r. w przetargu startowało średnio ok. 2,5 firmy, w 2018 r. już tylko 2,19, zaś w ok. 43% postępowań złożona została tylko jedna oferta);
- nierównowaga pozycji zamawiającego i wykonawcy;
- koncentracja zamawiających na spełnieniu wymogów formalnych, a nie na uzyskaniu najlepszego jakościowo przedmiotu zamówienia;
- nieefektywne udzielanie zamówień, tj. wybieranie przez zamawiających rozwiązań najtańszych, a nie najbardziej efektywnych w dłuższym okresie;
- brak powiązania wydatków na zamówienia publiczne z realizacją polityki oraz celów strategicznych państwa, m.in. wzrostu innowacyjności;
- ograniczona możliwość odwołania się od decyzji zamawiającego do Krajowej Izby Odwoławczej (KIO) oraz składania w sądach powszechnych skarg na wyroki KIO, niejednolitość orzecznictwa KIO i sądów powszechnych;
- nieefektywny system kontroli zamówień publicznych.

Analiza rynku zamówień publicznych w branży zabezpieczeń potwierdza nadmiernie sformalizowany proces składania zamówień (w szczególności w procedurze krajowej) oraz przewagę pozycji zamawiającego, który narzuca wykonawcy trudne do spełnienia warunki kontraktowe i niewspółmiernie wysokie kary, co często prowadzi do przedwczesnego rozwiązywania umów.

Nowa ustawa jest więc aktem bardzo wyczekiwanym przez przedsiębiorców, choć już jej wstępna ocena pozwala przypuszczać, że nie rozwiąże ona wszystkich bolączek systemu.

Kluczowe zmiany, które niesie za sobą procedowana obecnie ustawa, to:

- zwiększenie roli konsultacji z przedsiębiorcami przed ogłoszeniem zamówienia (konsultacje mają zastąpić obecny dialog techniczny);
- wprowadzenie zasady efektywności składanych zamówień (uzyskanie jak najlepszego stosunku poniesionych kosztów do uzyskanych efektów – obniżenie kosztów nie poprzez poszukiwanie jak najniższej ceny, ale sprawnie prowadzoną procedurę wykorzystującą wszystkie dostępne zgodnie z ustawą narzędzia);
- nałożenie na zamawiających obowiązku dokonywania analizy potrzeb i wymagań (ma ona obejmować sprawdzenie, jakie są możliwości zaspokojenia potrzeb zasobami własnymi oraz zbadanie rynku pod kątem alternatywnych sposobów zaspokojenia tych potrzeb i możliwych wariantów realizacji zamówienia; należy też podać orientacyjną

wartość każdego ze wskazanych powyżej wariantów zamówienia, a także określić możliwość podziału zamówienia na części i przewidywany tryb złożenia zamówienia; analiza może też uwzględnić społeczne, środowiskowe lub innowacyjne aspekty zamówienia oraz rodzaje ryzyka związane z postępowaniem mającym na celu złożenie zamówienia i realizację umowy);
- ustalenie nowego sposobu określania wartości zamówienia na usługi o charakterze ciągłym w branży ochrony – wartość będzie ustalana na podstawie ceny wynikającej z umowy z ostatnich 12 miesięcy lub ostatniego roku budżetowego/obrotowego – z uwzględnieniem zmian wolumenu i wskaźnika inflacji (zmianę należy uznać za niekorzystną, gdyż w usługach tych często decydującym czynnikiem kosztotwórczym są koszty pracy podlegające dynamicznej zmianie ze względu na regulacje prawne oraz uwarunkowania rynku lokalnego);
- zmniejszenie obciążeń po stronie wykonawców oraz ujednolicenie i uproszczenie zasad udzielania zamówień poniżej progów UE (dla zamówień społecznych, w tym z branży zabezpieczeń, o wartości równej lub przekraczającej 130 000 zł obowiązywać będą takie same zasady jak dla innych zamówień podprogowych; zniesiony zostanie obowiązek składania podpisu elektronicznego w zamówieniach podprogowych oraz żądania wadium w postępowaniach unijnych);
- współdziałanie stron umowy o zamówienie publiczne w trakcie jej realizacji – możliwość mediacji i koncyliacyjnego rozwiązywania sporów (przy zamówieniach o znacznych wartościach, gdy przedmiot sporu ma wartość ponad 100 000 zł, strony umowy będą mogły zwrócić się do Sądu Polubownego przy Prokuratorii Generalnej Rzeczypospolitej Polskiej o szybkie rozstrzygnięcie sporu, zanim trafi on na drogę sądową);
- poszerzenie możliwości waloryzacji wynagrodzenia umownego na podstawie dodatkowych przesłanek (np. w związku ze zmianami cen materiałów lub kosztów) oraz w umowach innych niż zawierane na okres ponad 12 miesięcy (zatem możliwe w umowach trwających do 12 miesięcy);
- wprowadzenie klauzul abuzywnych w umowach o zamówienie publiczne (ograniczenie możliwości wprowadzania przez zamawiających jednostronnych postanowień, w tym dotyczących kar umownych);
- zabezpieczenie interesów podwykonawców (postanowienia zawarte w umowach z podwykonawcami, dotyczące kar umownych, płatności, nie będą mniej korzystne niż postanowienia zawarte w umowach z wykonawcami);
- obowiązek sporządzenia przez zamawiającego raportu dotyczącego realizacji zamówienia, gdy na tę realizację wydał on o co najmniej 10% więcej niż wynosiła przedstawiona w ofercie cena lub na wykonawcę zostały nałożone kary umowne większe o min. 10 % od ceny ofertowej, lub wystąpiły ponad 30-dniowe opóźnienia w realizacji umowy, lub jedna ze stron odstąpiła od umowy/wypowiedziała umowę w całości lub w części;
- wprowadzenie nowych zasad w procedurach odwoławczych, tj. wprowadzenie środków ochrony prawnej w pełnym zakresie w zamówieniach podprogowych, rozpoznawanie spraw przez KIO w składach trzyosobowych w przypadku zamówień unijnych, które umożliwi szerszą wymianę poglądów pomiędzy członkami Izby (jednoosobowo będą rozstrzygane odwołania w postępowaniach dotyczących zamówień o wartościach, które nie przekraczają progów unijnych), wyznaczenie jednego sądu zajmującego się zamówieniami publicznymi (Sądu Okręgowego w Warszawie), wydłużenie czasu na wniesienie do sądu skargi na orzeczenie KIO (do 14 dni) oraz obniżenie kwoty wpisu sądowego od skarg.

Ustawa ma wejść w życie 1 stycznia 2021 r. Powodem tak długiego *vacatio legis* ma być właściwe przygotowanie rynku do nowych regulacji. Trudno się z tym zgodzić zwłaszcza małym i średnim firmom, które od dawna oczekują uproszczenia procedur oraz bardziej otwartego i elastycznego podejścia zamawiających przy składaniu i realizacji zamówień publicznych.

Joanna Filipiak

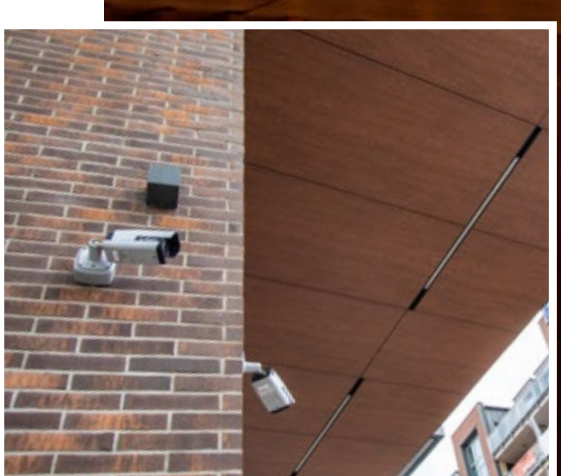
Bosch zabezpiecza Port Praski

Bosch Security and Safety Systems

W najstarszej dzielnicy prawobrzeżnej Warszawy, w pobliżu starówki i Stadionu Narodowego, powstaje miasto nowej generacji – Port Praski. Na terenie o powierzchni około 40 hektarów realizowane jest jedno z największych przedsięwzięć architektonicznych w Europie, a historia łączy się z nowoczesnością

Na Port Praski składają się Stara Praga, Doki, City i Park Mediów. Każda z tych części będzie pełnić różne funkcje – od mieszkalnej i biurowej aż po rekreacyjną i naukową. Stara Praga to mieszkalno-usługowa część całego kompleksu. Doki to część luksusowa, zlokalizowana tuż nad wodą, gdzie powstaną ekskluzywne butiki i restauracje z ogródkami, przystań oraz bulwary ciągnące się wzdłuż portu. Tuż przy stacji metra Stadion Narodowy powstanie City z czterema biurowcami. Z kolei Park Mediów będzie nowoczesnym kompleksem z forum technologicznym, fitness parkiem, centrum edukacji, centrum nowych technologii i centrum konferencyjno-widowiskowym. – *Te cztery części będą tworzyć jedną, spójną całość, która będzie zaspokajać wszystkie potrzeby mieszkańców oraz stanie się samowystarczalnym miastem w mieście* – powiedział Maciej Sulej, dyrektor ds. realizacji w Porcie Praskim.

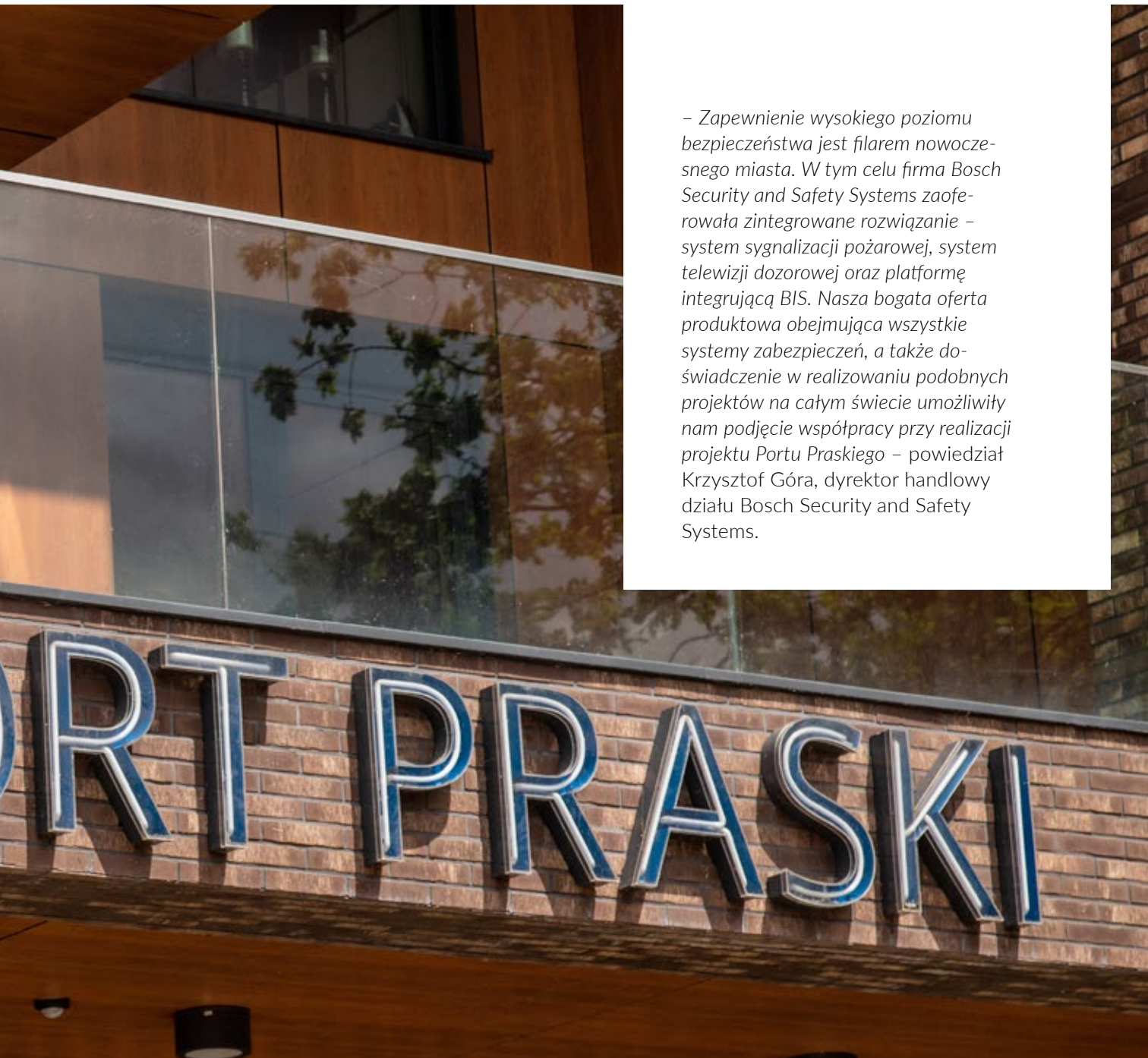
Na niezwykły charakter przedsięwzięcia duży wpływ ma bliskie sąsiedztwo rzeki. Port Praski powstaje przy dawnych dokach portowych nad Wisłą, a to wymaga zabezpieczenia przeciwpowodziowego, aby możliwa była realizacja całej inwestycji. Zabezpieczenie przeciwpowodziowe będzie chronić przed zalaniem także Pragę Północ – od ulicy Ratuszowej, przy której znajduje się zoo, po część Pragi Południe, aż do Gocławia. To nie jedyna forma ochrony życia i mienia na terenie Portu Praskiego.

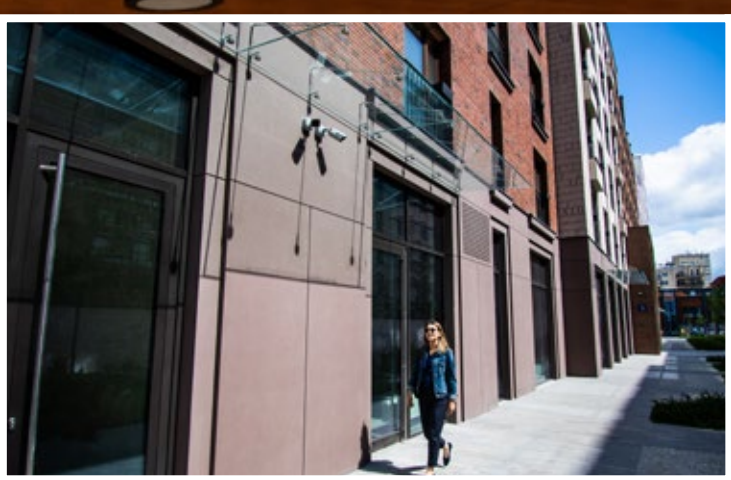


Fot. Bosch

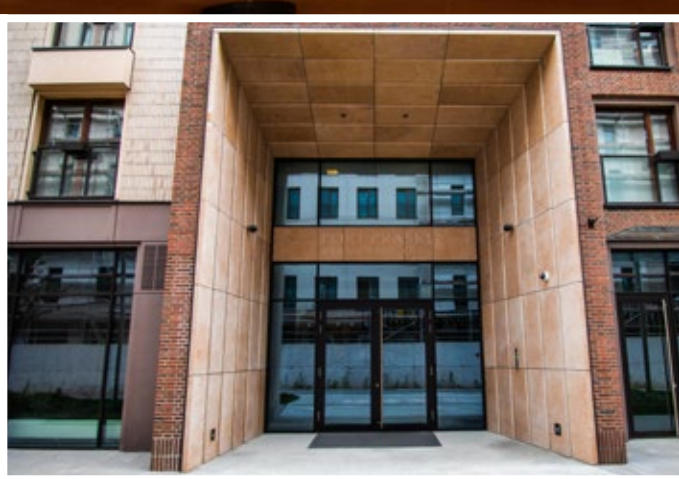
Fot. Bosch

– Zapewnienie wysokiego poziomu bezpieczeństwa jest filarem nowoczesnego miasta. W tym celu firma Bosch Security and Safety Systems zaoferowała zintegrowane rozwiązanie – system sygnalizacji pożarowej, system telewizji dozorowej oraz platformę integrującą BIS. Nasza bogata oferta produktowa obejmująca wszystkie systemy zabezpieczeń, a także doświadczenie w realizowaniu podobnych projektów na całym świecie umożliwiły nam podjęcie współpracy przy realizacji projektu Portu Praskiego – powiedział Krzysztof Góra, dyrektor handlowy działu Bosch Security and Safety Systems.





Fot. Bosch



Fot. Bosch

W przypadku systemu zabezpieczeń istotna była możliwość utworzenia wielu stacji operatorskich oraz rozproszenia elementów systemu na całym obszarze inwestycji, a jednocześnie globalnego zarządzania. Instalacja systemu na tak dużym obszarze nie stanowi problemu, gdyż rozwiązania sieciowe Bosch zostały stworzone z myślą o takich inwestycjach. Na przykład poszczególne centrale systemu sygnalizacji pożarowej typu FPA-5000 mogą być rozmieszczone w odległości nawet kilkudziesięciu kilometrów od siebie, a zarazem wszystkie centrale systemu są połączone zgodnie z koncepcją węzłów równoważnych, więc nie ma pojedynczego miejsca którego uszkodzenie doprowadziłoby do awarii systemu.

Całość inwestycji jest wyposażona również w system dozoru wizyjnego marki Bosch. Kamery zainstalowano na elewacjach, przy wejściach do budynków, w ciągach komunikacyjnych, windach oraz w garażach. Całość jest zintegrowana przez system BVMS (Bosch Video Management System) wizualizowany w rozproszonych stacjach operatorskich.

Ze względu na stały rozwój inwestycji realizowanej etapowo od poszczególnych systemów wymaga się elastycznej architektury oraz co najmniej pięcioletniej kompatybilności wstecznej urządzeń. Powinny one także być gotowe na przyszłe wyzwania. Intensywnie rozwijane rozwiązania przeznaczone do systemów zabezpieczeń w chmurze Bosch, integrowane bezpośrednio z kontrolerami poszczególnych systemów, dają wiele możliwości.

Całość dopełnia platforma integrująca BIS, która umożliwia centralne zarządzanie i obsługę systemów zabezpieczeń rozproszonych w poszczególnych obiektach.

Bosch Security and Safety Systems

AST DO BRAM DRZWI OKIEN

2 GRADE

CZUJKI MAGNETYCZNE DO BRAM, DRZWI i OKIEN

TERAZ ZE STOPNIEM ZABEZPIECZENIA GRADE 2

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

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

D PROD S

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

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

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

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

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

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

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

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

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

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

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

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

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

D I PROJ S

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

D PROD PROJ S

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

D PROD PROJ S

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

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

D PROD S

ASSA ABLOY POLAND Sp. z o.o.
ul. 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. kom. 604 569 775
e-mail: brabork@braborklab.pl
www.braborklab.pl

D I PROD PROJ

BT Electronics Sp. z o.o.
ul. Rybitwy 22
30-722 Kraków
tel. 12 410 20 33, faks 12 410 85 10
e-mail: bte@bte.pl
www.bte.pl

D I PROD PROJ S

CBC (Poland) Sp. z o.o.
ul. Anny German 15
01-794 Warszawa
tel. 22 633 90 90
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 Sp. J.
ul. Bonarka 21
30-415 Kraków
tel. 12 263 93 85; faks 12 263 93 86
email: biuro@dgelpro.pl
www.dgelpro.pl

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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. 12 272 39 71, 341 04 07; faks 12 379 34 10
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

D I S

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

D PROJ S

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

C S PROJ

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

B D PROD PROJ

Always precise WINKHAUS

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

D I PROD PROJ

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

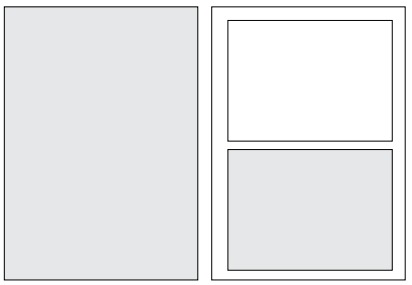
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie

Spis teleadresowy
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Ceny negocjujemy indywidualnie

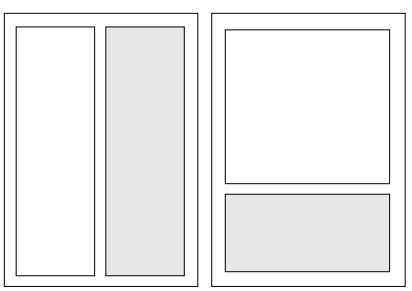
Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej http://www.zabezpieczenia.com.pl w dziale Reklama

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



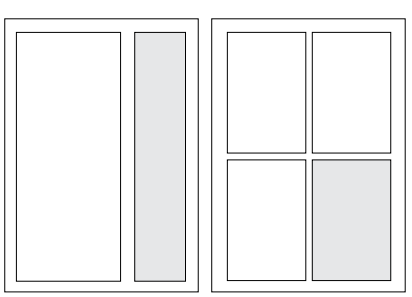
cała strona
(200 x 282 mm + 3mm spad)

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

AAT HOLDING	9, 59, 65, 71	MTP	27
Axis Communications Poland	1	PHU Arvinge	49
Firma ATline	15	POLON-ALFA	3
FUJIFILM	72	ROGER	53
IBP NODEX	45	SRGS	15
Lockus	64	Videotec	2

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

STABLE IMAGES X HIGH-SPEED AF

THE NEW FUJINON SX800. THE BEST OF BOTH.

The perfect combination of camera and lens. With optical and electronic image stabilization, fast autofocus under one second and 40x zoom. For maximum reliability in long range surveillance. **www.fujifilm.eu/sx800. Fujinon. To see more is to know more.**

FUJINON