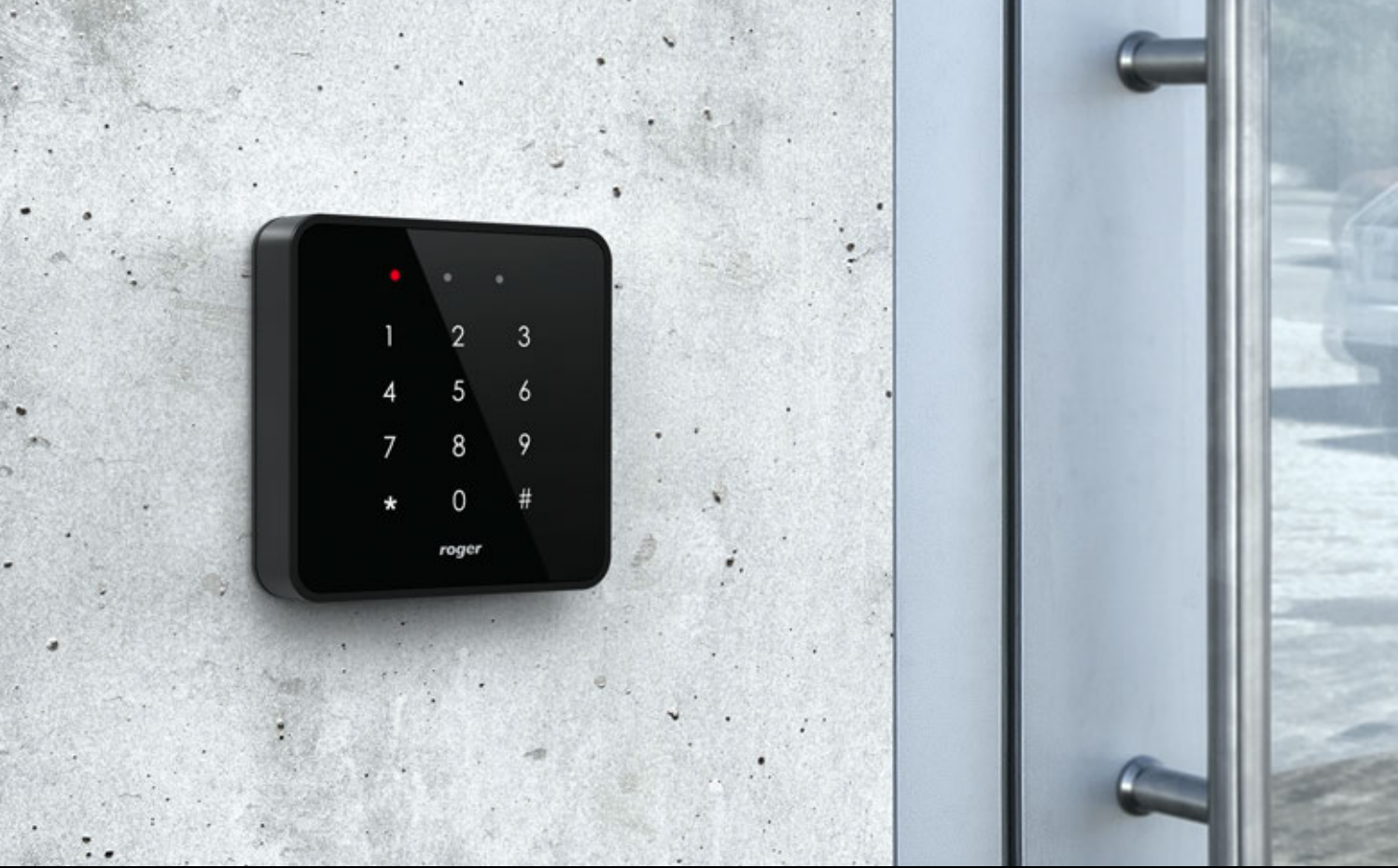
CZASOPISMO BEZPŁATNE
ISSN: 1505-2419 DWUMIESIĘCZNIK NR 1(125)/2019

ZABEZPIECZENIA



RACS 5

Skalowalny system bezpieczeństwa, automatyki i kontroli dostępu

Przewodowa kontrola dostępu

Bezprzewodowa kontrola dostępu

Rejestracja czasu pracy

Automatyka budynkowa

Zarządzanie kluczami

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

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

roger®

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

Kamery typu rybie oko

NVIP-5DN2008V/IR-1P oraz NVIP-9DN2018V/IR-1P w połączeniu z rejestratorami z serii 4000

Kamery typu rybie oko **NVIP-5DN2008V/IR-1P** oraz **NVIP-9DN2018V/IR-1P** są kompatybilne z aplikacją **NMS** i mogą współpracować z rejestratorami z serii 4000 z portami PoE – **NVR-4308P8-H1** oraz **NVR-4204P4-H1**. Dzięki temu kamery te można wykorzystać nawet w obiektach, w których liczba kamer ma być niewielka. Aby obraz był prawidłowo wyświetlany, po automatycznym wyszukaniu i dodaniu kamery do systemu należy wybrać sposób jej zamontowania – na suficie, biurku, ścianie lub na skośnym stropie. Dostępne tryby wyświetlania to m.in. *virtual reality*, który pozwala uzyskać podobne efekty jak w przypadku zastosowania kamer PTZ, dokonywać zbliżeń wybranych fragmentów obserwowanej sceny lub obserwować pełną scenę w postaci koła. Pełny obraz sytuacji pozwalają uzyskać tryby *cylinder* oraz *panorama 180* i *panorama 360*. Najbardziej efektywnymi trybami wyświetlania są tryby podziału z jednym ogólnym widokiem oraz trzema lub ośmioma oknami z niezależnymi widokami ustawianymi przez operatora systemu.
Zachęcamy do obejrzenia krótkiego filmu instruktażowego, znajdującego się pod adresem https://www.youtube.com/watch?v=TMJwZ0x1OfE, w celu zapoznania się ze sposobem sterowania kamerami typu rybie oko.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

ULISSE EVO

Następny etap ewolucji kamer PTZ firmy Videotec

Videotec zapowiada wprowadzenie kamery **ULISSE EVO**, której konstrukcja stanowi kolejny krok naprzód w dążeniu do tworzenia innowacyjnych, coraz skuteczniejszych i coraz bardziej niezawodnych składników wizyjnych systemów dozorowych. Ta nowa, wszechstronna kamera PTZ jest konkurencyjna cenowo i ma niespotykany dotychczas wygląd.

W kamerach ULISSE EVO połączono najnowsze osiągnięcia techniki z wyszukanym wzornictwem. Są to urządzenia gwarantujące najwyższy poziom bezpieczeństwa monitorowanych obszarów miejskich, obiektów infrastruktury krytycznej, środków transportu, infrastruktury drogowej i kolejowej.

Kamery ULISSE EVO mają rozdzielczość Full HD, wytwarzają 60 klatek wizyjnych na sekundę, odznaczają się dużą światłoczułością. Są wyposażone w obiektywy zmiennoogniskowe o krotności x30. Wykorzystanie funkcji Delux powoduje, że barwne obrazy z kamer ULISSE EVO są wyraźne i pełne szczegółów zarówno podczas obserwacji prowadzonych w dzień, jak i w nocy. Funkcje wykrywania ruchu i maskowania sektorów prywatnych umożliwiają inteligentne zarządzanie pracą systemów dozorowych i natychmiastowe zgłaszanie alarmów w przypadku wykrycia niepożądanego wtargnięcia.

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

Obudowa kamery jest wyposażona w wycieraczkę zapewniającą wyraźny obraz w niesprzyjających warunkach środowiskowych. Dostępny jest oświetlacz LED umożliwiający widoczność nawet w całkowitej ciemności. Jest to osobny element pracujący w świetle o długości fali 850 nm, 940 nm lub w świetle widzialnym. Kamera automatycznie rozpoznaje rodzaj zainstalowanego oświetlacza i odpowiednio kalibruje wiązkę światła.

Kamera ULISSE EVO ma podłużny kształt. Jej konstrukcja jest maksymalnie wytrzymała i niezawodna, a jednocześnie ma bardzo ograniczoną wagę. Oznacza to łatwy i szybki montaż, a także niższe koszty instalacji i konserwacji.

Kamery ULISSE EVO mogą być instalowane na różne sposoby, nawet w pozycji odwróconej, typowej dla szybkoobrotowych kamer kopułowych, przy użyciu różnych dostępnych wysięgników i uchwytów aby spełnić wszystkie wymagania instalacyjne. Wysięgniki są wyposażone

w szybkozłączki do podłączania kabli ethernetowych, przez co prace instalacyjne są znacznie ułatwione. Kamery pracują bezobsługowo i nie wymagają konserwacji.

Kamery ULISSE EVO są produkowane w dwóch standardowych wersjach kolorystycznych – czarnej i szaro-białej. Nowe kamery ULISSE EVO będą dostępne na rynku w pierwszym kwartale 2019 roku.

Bezpośr. inf. Videotec
Tłumaczenie: Andrzej Walczyk

Nowe etui chroniące zbliżeniowe karty płatnicze

Firma ATLine wprowadza do swojej oferty **etui chroniące zbliżeniowe karty płatnicze**. Każde etui jest pokryte specjalną powłoką blokującą sygnał NFC odpowiedzialny za płatności bezdotykowe. NFC (ang. *near-field communication*) to standard radiowy umożliwiający bezprzewodową łączność między urządzeniami na odległość do dwudziestu centymetrów.

Płatności bezdotykowe są bardzo wygodne i już powszechnie się z nich korzysta, jednak ułatwiają one kradzieże. Większość urządzeń z chipem NFC, np. smartfonów, można bowiem przeprogramować, aby działały jak terminale do kart. Mimo że w większości przypadków, w których używa się karty bezdotykowo i bez podania PIN-u, limit wynosi 50 zł, zwykle nie ma ograniczenia liczby użyć karty w ten sposób. Złodzieje pojawiają się w miejscach publicznych, mocno zatłoczonych, takich jak galerie handlowe czy środki transportu miejskiego, i korzystają z nieuwagi lub nawet braku możliwości natychmiastowego wykrycia kradzieży. W momencie jej wykrycia złodzieje mogą być już daleko, a środki mogą zostać przelane na rachunki bankowe, których właścicieli nie będzie można pociągnąć do odpowiedzialności

Etui ochronne pozwala zabezpieczyć karty zbliżeniowe w wygodny sposób, bez konieczności rezygnowania z komfortu, jaki dają płatności zbliżone, a dzięki kompaktowym wymiarom bez problemu mieści się w każdym portfelu. Zamówienia będziemy przyjmować e-mailowo (info@atline.pl). Więcej informacji na ten temat znajduje się na naszej stronie internetowej.

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

Czytnik administratora
Elatec T4BTFB2BEL6PI

W ostatnim czasie ofertę firmy **AAT HOLDING** wzbogacił czytnik administratora **Elatec T4BTFB2BEL6PI**. Urządzenie to, skonfigurowane standardowo, ułatwia wprowadzanie numerów kart UNIQUE, MIFARE Classic, HID Prox oraz Kantech ioProx do systemów kontroli dostępu. Działając jako emulator klawiatury, umożliwia wprowadzenie numeru karty w pola tekstowe w najczęściej spotykanych formatach wyświetlania – zarówno decymalnych, heksadecymalnych, jak i mieszanych. Do podłączenia czytnika do stacji administratora wykorzystuje się interfejs USB. T4BTFB2BEL6PI jest urządzeniem *plug and play* i nie wymaga instalacji dodatkowych sterowników.

Na tym nie kończy się jednak zakres możliwości urządzenia. Czytnik T4BTFB2BEL6PI to bardzo pożyteczne narzędzie współpracujące z transponderami LF (125 kHz; 134,2 kHz) oraz HF (13,56 MHz) w większości znanych na świecie standardów, np. MIFARE DESFire EV1, MIFARE Plus X, HID iClass SE, AWID, IDTECK, Keri i w wielu innych. Urządzenie wykorzystuje też NFC. Można je skonfigurować na wiele sposobów – zakres możliwości konfiguracji jest szeroki. Dla każdego z odczytywanych przez czytnik standardów kart możliwe jest określenie danych wyjściowych, na przykład dotyczących sektora pamięci, w którym zapisany jest numer karty, kolejność odczytu bitów i bajtów oraz sposobu ich prezentacji (liczby znaków, formatu itd.). W związku z tym opisywany czytnik może być zastosowany praktycznie w każdym dostępnym systemie kontroli dostępu.

Dodatkowo czytnik firmy Elatec T4BTFB2BEL6PI może zostać skonfigurowany tak, aby identyfikował prezentowane transpondery. Po przyłożeniu nieznanej karty możemy uzyskać informacje o jej rodzaju, pamięci oraz numerze UID. Przykład danych odczytanych z karty i wyświetlanych jako ciąg znaków w dowolnym edytorze tekstu – „ISO14443A/MIFARE Plus X | UID Length 56 Bits | UID HEX 043A5E32175180". Rozwiązuje to problem niezidentyfikowanego „białego plastikowego prostokąta", czyli określenia używanego często przez instalatorów lub klientów do opisania posiadanej karty.

W celu uzyskania dodatkowych informacji prosimy o kontakt z działem kontroli dostępu firmy AAT HOLDING.

Bezpośr inf. Damian Sobczak
AAT HOLDING

Kamera DHI-ITC314-PH2A-TF
do systemu parkingowego

Nieustanny rozwój aglomeracji miejskich sprzyja powstawaniu coraz większej liczby centrów handlowych. W niektórych mniejszych miastach należą one do najatrakcyjniejszych miejsc publicznych. Ma to bezpośredni wpływ na rozwój handlu w regionie. Centra handlowe są jak magnes dla mieszkańców miast i okolic. Niestety w wielu takich obiektach nie ma wystarczającej liczby miejsc parkingowych i sprawnego przepływu informacji, który jest potrzebny do skutecznego zarządzania parkingiem.

Firma **Dahua Technology** – czołowy światowy dostawca wizyjnych systemów dozorowych – może pomóc rozwiązać ten problem. Oferuje ona kompletny system zarządzania parkingiem. Kluczowym elementem systemu są kamery **DHI-ITC314-PH2A-TF**. Dzięki ich zastosowaniu oprócz obrazów napływają do systemu informacje o liczbie zajętych miejsc parkingowych, a nawet dane z tablic rejestracyjnych zaparkowanych pojazdów.

Wszystkie te informacje są przetwarzane przez specjalistyczne oprogramowanie Parking Managment System. Informacja dotycząca liczby wolnych miejsc jest wyświetlana zarówno w centrum zarządzania obiektem, jak i na elektronicznych tablicach informacyjnych przy wjeździe do parkingu.

Bezpośr. inf. Maciej Pietrzak
Dahua Technology Poland

Czytniki firmy Dahua Technology

przeznaczone do systemu kontroli dostępu

ASR1101M

ASI1212D

ASI1201E

ASR1102A(V2)

Dahua Technology oferuje system kontroli dostępu, z którym mogą współpracować różnego rodzaju czytniki. Spełnią one wymagania nawet najbardziej wymagających klientów. Do dyspozycji mamy **serię ASIXXX**, do której należą czytniki autonomiczne z wbudowanymi kontrolerami, oraz **serię ASRXXX**, do której należą czytniki wymagające podłączenia do kontrolera.

Do pierwszej z tych grup należą czytniki umożliwiające identyfikację użytkownika na podstawie wprowadzonego na klawiaturze kodu dostępu, poprzez odczyt karty (w standardzie Mifare lub Unique, w zależności od modelu) lub poprzez zeskanowanie linii papilarnych palca. Możliwa jest zaawansowana kontrola dostępu do pomieszczeń z zastosowaniem każdego ze sposobów identyfikacji. Dostępne są czytniki o różnych klasach szczelności – np. typowe czytniki wewnętrzne o klasie szczelności IP55 i zewnętrzne o klasie szczelności IP67, pracujące w temperaturach powyżej -30°C.

Czytniki linii papilarnych mogą przechowywać w swojej pamięci do 3000 odcisków palca w wersji podstawowej, maksymalnie do 30 000 w wersji z rozszerzoną pamięcią. Czas odczytu linii papilarnych wynosi poniżej 1,5 s.

W zależności od modelu czytniki wymagające podłączenia do kontrolera mają różne metody identyfikacji – tylko zeskanowanie odcisku palca, tylko odczyt karty lub weryfikacja na podstawie kodu dostępu wpisanego na klawiaturze i odczyt karty. Podobnie jak w przypadku autonomicznych czytników zintegrowanych z kontrolerami, mamy różne klasy szczelności urządzeń.

Na uwagę zasługuje również czytnik ASR1101M ze wzmocnioną konstrukcją, o klasie odporności mechanicznej IK08. Metalowe przyciski, solidna, wandaloodporna konstrukcja oraz możliwość pracy w niskich temperaturach sprawiają, że może on cieszyć się dużą popularnością.

Każdy z czytników posiada dwa interfejsy służące do podłączenia go do kontrolera – RS485 oraz Wiegand 34. Zwłaszcza to pierwsze rozwiązanie jest interesujące, gdyż umożliwia zainstalowanie czytnika w odległości do 1000 metrów od kontrolera.

Bezpośr. inf. Wojciech Pawlica
Dahua Technology Poland

Bezpieczna podróż
dzięki rejestratorowi TRM-1610M

Pociągi szybkiej kolei, metro, tramwaje i autobusy są niezbędne do życia w mieście. Korzystają z nich miliony osób, aby szybko i bezpiecznie dotrzeć do celu. Jednak wzrost ich popularności powoduje, że coraz częściej dochodzi w nich różnego rodzaju incydentów, np. do wypadków drogowych, napadów, kradzieży kieszonkowych. Aby zapobiec tego typu zdarzeniom lub zniwelować ich skutki, Hanwha proponuje zastosowanie w pojazdach komunikacji miejskiej rejestratorów mobilnych, które są wyposażone m.in. w GPS oraz przycisk alarmowy, za pomocą którego kierowca może szybko powiadomić o zaistniałym incydencie centrum monitorowania.

Rejestrator TRM-1610M to profesjonalne urządzenie, które jest w stanie pracować nawet w najtrudniejszych warunkach. Potwierdzają to certyfikaty EN-50155 (zastosowania kolejowe, odporność na uderzenia i wibracje) i EN-50121-4 (zastosowania kolejowe, zgodność elektromagnetyczna).

Połączenie 16-kanałowego rejestratora TRM-1610M z kamerami **XNF-8010R** umożliwia obserwację w pełnym polu widzenia równym 360 stopni, eliminując martwe pola i zastępując kilka kamer tylko jednym urządzeniem. Wbudowany mikrofon w połączeniu z funkcją analizy dźwięku umożliwia wykrywanie i klasyfikację nietypowych dźwięków, takich jak krzyki lub dźwięki tłuczonego szkła. Kamery XNF-8010R mogą być instalowane w różnych środowiskach, np. na zewnątrz budynków i pojazdów, wewnątrz nich, na sufitach lub na ścianach. Dostępna jest również mobilna wersja przeznaczona do instalacji w pojazdach, wykorzystująca złącza M12.

Sylwester Krupa
Hanwha Techwin Europe

Smart Monitoring
oferuje usługi monitorowania

Firma **Smart Monitoring** oferuje monitorowanie alarmów w niezależnym centrum monitorowania, które współpracuje z agencjami ochrony w całej Polsce. Podpisane umowy o gotowość patroli oraz grup interwencyjnych umożliwiają świadczenie usług wraz z przyjazdami interwencyjnymi do chronionych obiektów. Każdy z klientów centrum może mieć własnego operatora, co ułatwia kontakt.

Usługi firmy Smart Monitoring są przeznaczone w szczególności dla firm, które nie mają własnej stacji monitorowania i nie chcą inwestować we własną infrastrukturę. Smart Monitoring może również świadczyć usługę dublowania już istniejącej stacji monitorowania klienta.

Dzięki zaawansowanej infrastrukturze IT, zgodności z obowiązującą normą PN-EN 50518, niezależności energetycznej i teletechnicznej, nowoczesnemu oprogramowaniu, a także możliwości podpisania umowy SLA Smart Monitoring zapewnia wysoką jakość realizowanych usług.

Centrum monitorowania odbiera sygnały z systemów sygnalizacji włamania i napadu, mobilnych systemów GPS, systemów kontroli dostępu i wizyjnych systemów dozorowych. Podejmuje działania zgodnie z ustalonymi wcześniej procedurami. W razie incydentu patrole lub grupy interwencyjne mogą zostać wysłane do obiektów na terenie całej Polski.

Rozliczenie za każdy z obiektów z osobna zapewnia pełną elastyczność i brak stałych kosztów.

Bezpośr. inf. Kamil Fadrowski
kamil.fadrowski@smart-monitoring.pl
www.smart-monitoring.pl

smart monitoring

Nowość w ofercie firmy POLON-ALFA

czujki pożarowe z sygnalizatorem akustycznym

Dwusensorowa czujka dymu z sygnalizatorem akustycznym **DUO-6046AD** oraz wielosensorowa czujka dymu i ciepła z sygnalizatorem akustycznym **DUT-6046AD** to elementy adresowalne, które powiększają asortyment oferowanych czujek **serii 6000**. Czujki wraz z gniazdem **G-40S** są wykonane z niepalnego tworzywa i stanowią komplet.

Czujka DUO-6046AD jest przeznaczona do wykrywania widzialnego dymu powstającego w początkowym stadium rozwoju pożaru – wtedy, gdy materiał jeszcze się tli, a więc na ogół długo przed pojawieniem się otwartego płomienia i zauważalnym wzrostem temperatury. Ruch powietrza i zmiany ciśnienia mają niewielki wpływ na charakterystyki detekcyjne czujki. W czujkach zastosowano podwójny układ detekcji dymu w pasmach UV i IR.

Czujka DUT-6046AD jest przeznaczona do wykrywania początkowego stadium rozwoju pożaru, w którym pojawia się dym i następuje wzrost temperatury. Ruch powietrza i zmiany ciśnienia mają niewielki wpływ na charakterystyki detekcyjne czujki. Zastosowanie podwójnego układu detekcji dymu oraz podwójnego układu detekcji ciepła zapewnia zwiększoną odporność na fałszywe alarmy, wywoływane na przykład przez parę wodną i pył, przy zachowaniu niewielkich rozmiarów i estetycznego wyglądu czujki.

Czujki z sygnalizatorem akustycznym – DUO-6046AD i DUT-6046AD – są przeznaczone do pracy w adresowalnych liniach dozorowych central sygnalizacji pożarowej systemów POLON 4000 i POLON 6000. Załączenie sygnalizatora akustycznego w czujce następuje na polecenie wysłane ze współpracującej centrali. Zarówno w systemie 4000, jak i 6000 możliwe jest wysterowanie sygnalizatora akustycznego niezależnie od stanu czujki. Maksymalny poziom sygnału akustycznego z jednego kierunku przekracza 85 dB/m, a z pozostałych 70 dB/m.

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

Na czujki wydane zostały przez CNBOP-PIB (jednostkę notyfikowaną nr 1438) certyfikaty stałości właściwości użytkowych potwierdzające posiadanie cech/parametrów technicznych, które są narzucone przez normy EN 54-3, EN 54-7, EN 54-17, a w przypadku czujki DUT-6046AD dodatkowo przez normę EN 54-5.

Wyrób posiada świadectwo dopuszczenia wydane przez CNBOP-PIB. Producent wydał deklarację właściwości użytkowych.

Bezpośr. inf. POLON-ALFA

Tmaster CO/LPG/CNG G
trójgazowy detektor

Detektory **Tmaster CO/LPG/CNG G** stosuje się w stacjonarnych systemach detekcji tlenku węgla (CO), propanu-butanu (LPG) oraz metanu CH4 (CNG) poza strefami zagrożonymi wybuchem.

Detektory są przeznaczone do współpracy z typowymi centralami alarmowymi lub sterownikami przemysłowymi. Standardowe napięcie zasilania wynosi od 9 V do 28 V_{DC}. W zależności od wersji detektory mają wyjścia prądowe 4–20 mA, detekcyjne napięciowe (NC lub NO) lub cyfrowe (wyjście RS485 z protokołem Modbus RTU).

Do wykrywania tlenku węgla (CO) zastosowano selektywne, liniowe sensory elektrochemiczne o zakresie pomiarowym 0–550 ppm i progach alarmowych 40/100 ppm.

Do wykrywania propanu-butanu (LPG) i metanu (CNG) zastosowano nieselektywne sensory półprzewodnikowe o zakresie pomiarowym 0–50% DGW i progach alarmowych 10/30% DGW.

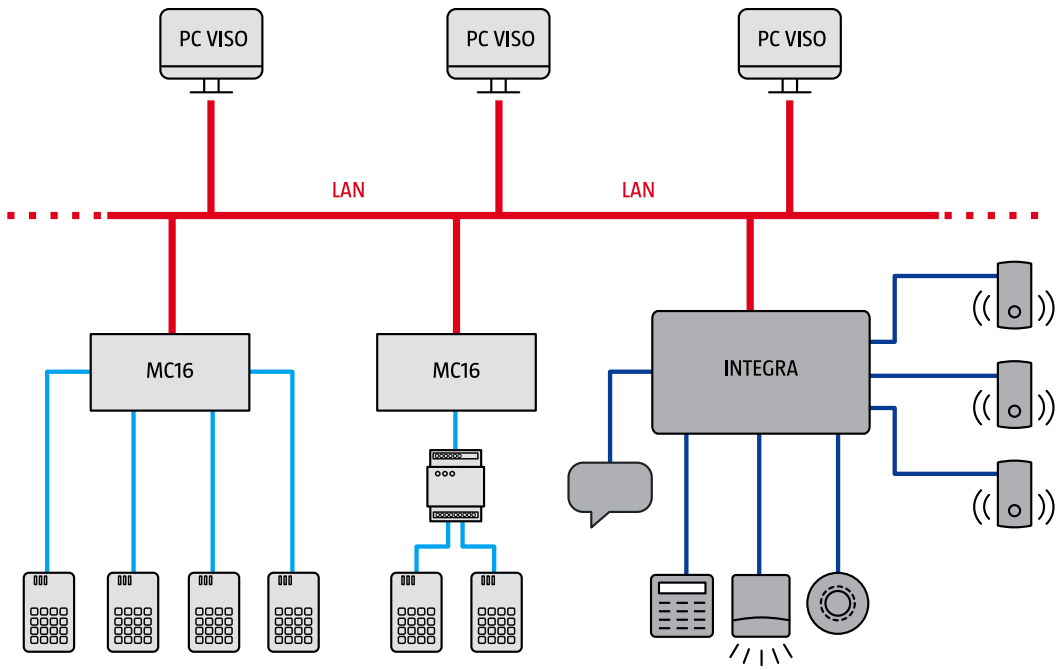
Detektory mają sygnalizację optyczną zasilania, przekroczenia progów alarmowych i awarii.

Detektor składa się z trzech modułów – głównego (CNG), modułu CO i modułu LPG –połączonych kablami. Obudowy modułów są wykonane z tworzywa sztucznego PS o stopniu ochrony IP33. Do podłączenia kabli służą wpusty kablowe (dławice) PG11 i PG9.

Główne miejsca zastosowania detektorów Tmaster CO/LPG/CNG G to systemy detekcji w garażach, na parkingach podziemnych i w stacjach diagnostycznych.

Bezpośr. inf. Przedsiębiorstwo Wdrożeniowe PRO-SERVICE
www.alarmgaz.com

Integracja systemu RACS 5
z centralami INTEGRA



System RACS 5 umożliwia integrację programową z centralami alarmowymi **INTEGRA** firmy SATEL. Integracja ta jest realizowana za pośrednictwem tzw. kontrolera wirtualnego, który po uruchomieniu na serwerze systemu kontroli dostępu komunikuje się z centralą alarmową INTEGRA za pośrednictwem interfejsu ETHM-1. Integracja umożliwia sterowanie stanem strefy alarmowej za pomocą terminali systemu RACS 5 oraz pokazywanie jej aktualnego stanu na ich wskaźnikach LED i wyjściach. Strefy systemu alarmowego można włączyć w dozór za pomocą identyfikatorów, przycisków funkcyjnych, przycisków podłączonych do linii wejściowych lub zdalnie – z poziomu oprogramowania zarządzającego systemem. Rejestr zdarzeń, które wystąpiły w systemie alarmowym, jest wyświetlany na bieżąco na stacji operatora systemu kontroli dostępu i zapisywany w jego bazie danych.

W reakcji na wybrane zdarzenia w systemie alarmowym system kontroli dostępu może podejmować wcześniej zaprogramowane akcje. Uprawnienia do sterowania systemem alarmowym podlegają definiowaniu jak wszystkie inne typy funkcji dostępnych w systemie RACS 5. Sterowanie systemem alarmowym z poziomu systemu kontroli nie tylko nie ogranicza sterowania strefami alarmowymi, ale zwiększa liczbę dostępnych metod sterowania. System RACS 5 może współpracować z wieloma centralami INTEGRA jednocześnie.

Charakterystyka systemu RACS5 połączonego z centralami INTEGRA:
- rejestracja zdarzeń z centrali alarmowej w bazie danych systemu kontroli dostępu,
- monitorowanie zdarzeń z centrali alarmowej w programie zarządzającym systemem kontroli dostępu,
- możliwość zaprogramowania reakcji systemu kontroli dostępu na zdarzenia z systemu alarmowego (programowa i sprzętowa),
- włączanie stref systemu alarmowego w dozór z poziomu terminali dostępu i oprogramowania systemu kontroli dostępu,
- pokazywanie stanu stref alarmowych na terminalach dostępu i wyjściach,
- definiowanie uprawnień do sterowania strefami alarmowymi,
- współpraca z wieloma centralami w ramach jednego systemu kontroli dostępu.

Bezpośr. inf. ROGER

System RACS w wersji 5.5

W **systemie RACS 5.5**, będącym kolejną, nową wersją systemu RACS 5, jest wiele nowych funkcji, spośród których najważniejsza jest programowa integracja z centralami alarmowymi z serii **INTEGRA**. Dzięki tej integracji zyskał on możliwość kompleksowej obsługi dużych systemów kontroli dostępu w zakresie zabezpieczenia antywłamaniowego na poziomie III (*Grade III*). W ramach wdrożonej integracji użytkownicy systemu mogą włączać strefy systemu alarmowego w dozór za pomocą czytników i klawiatur systemu kontroli dostępu, które pokazują jednocześnie aktualny stan powiązanych z nimi stref alarmowych. Rejestr zdarzeń, które wystąpiły w systemie alarmowym jest wyświetlany na bieżąco na stacji operatora systemu kontroli dostępu i zapisywany w jego bazie danych. System alarmowy można obsługiwać współbieżnie za pomocą klawiatur centrali alarmowej.

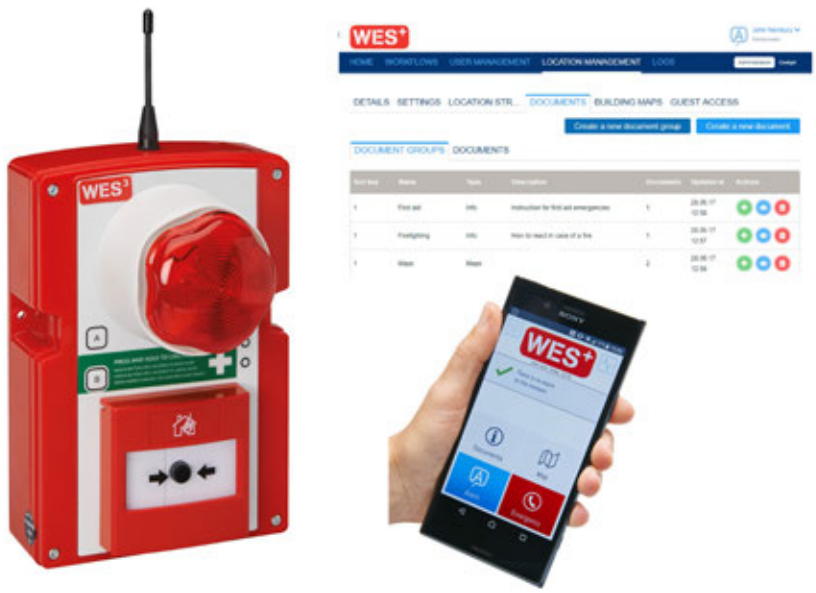
Integracja z centralami alarmowymi INTEGRA dostępna jest również w darmowej wersji programu RACS 5, czyli w VISO ST i wymaga instalacji na serwerze systemu kontroli dostępu.

Do zalet systemu RACS 5.5 należy również możliwość integracji kamer CCTV BCS Line i czytnika administratora HID OMNIKEY 5x27 CK, a także możliwość zdefiniowania własnych formatów wykorzystywanych do eksportu zdarzeń RCP.

W najnowszej wersji systemu RACS 5 aplikacja VISO WEB została rozszerzona o tzw. monitor obecności w strefie umożliwiający śledzenie osób przebywających w dowolnie określonym obszarze z użyciem przeglądarki internetowej.

Bezpośr. inf. ROGER

Zarządzanie on-line
sytuacjami kryzysowymi na budowie



Mobilny system detekcji pożaru **WES³** pomaga osobom odpowiedzialnym za bezpieczeństwo na placu budowy nie tylko klasycznym zestawem funkcji – poprzez wykrycie, sygnalizację i ułatwienie ewakuacji ludzi i sprzętu. **System WES REACT** korzysta z nowoczesnego rozwiązania wykorzystującego komunikację w chmurze, dając klientowi czas na przygotowanie własnych, optymalnych sposobów reagowania w sytuacjach kryzysowych.

Dzięki aplikacji mobilnej zainstalowanej w smartfonach pracownicy odpowiedzialni za bezpieczeństwo mogą otrzymywać powiadomienia o zdarzeniach. Funkcje systemu umożliwiają uwzględnienie planów urlopowych pracowników, blokady sygnalizacji dla osób znajdujących się poza terenem budowy (lokalizacja GPS) i tworzenie grup o zróżnicowanych uprawnieniach, co czyni system elastycznym narzędziem służącym do profesjonalnego zarządzania sytuacjami kryzysowymi na budowie.

Nowa linia produktowa firmy **Ramtech** wprowadza również udogodnienie w postaci dodatkowego przycisku do wzywania pomocy medycznej.

Całkowicie bezprzewodowy, bateryjnie zasilany system WES, uzupełniony nowoczesnymi funkcjami WES REACT, gwarantuje, że niebezpieczne sytuacje na chronionej przez system budowie spotkają się z błyskawiczną i przemyślaną reakcją przygotowanego na taką okoliczność personelu.

Więcej informacji o produktach firmy Ramtech znajduje się na stronie producenta (www.wesfire.com). Informacji udziela też **GEO-KAT** – wyłączny dystrybutor systemu WES w Polsce (www.geokat.com.pl).

Bezpośr. inf. GEO-KAT

WES³

Dagmara Pomirska
nowym dyrektorem ds. sprzedaży w firmie Axis Communications

Firma **Axis Communications** poinformowała, że od 3 grudnia Sales Managerem na Polskę, Ukrainę i Kraje Bałtyckie jest **Dagmara Pomirska**, która odpowiada za rozwój sieci sprzedaży w wymienionych krajach. Zastąpiła Jakuba Kozaka, który rozstał się z firmą pod koniec sierpnia.

– *Rok 2018 kończymy spektakularnym sukcesem w zakresie sprzedaży i dynamiki wzrostu. To najlepszy jak dotąd wynik w historii Axis Communications w tej części Europy, będący zasługą naszego zespołu profesjonalistów. Teraz dołącza do nas Dagmara, doświadczony menedżer, który podniesie poprzeczkę jeszcze wyżej. Oferta firmy Axis już od dawna nie ogranicza się tylko do prostego monitoringu. Axis proponuje złożone rozwiązania do optymalizacji ochrony i biznesu, a także komunikacji głosowej i kontroli dostępu* – powiedział Petr Tosner, dyrektor sprzedaży na Europę Wschodnią w firmie Axis Communications.

Dagmara Pomirska ma ponad 20-letnie doświadczenie w branży IT. Przez ostatnich sześć lat była związana z firmą Xerox (2012–2018), w której na stanowisku Office Business Director odpowiadała za sprzedaż i dostarczanie usług strategicznym klientom firmy oraz obecność na rynkach wertykalnych. Wcześniej pracowała m.in. w Tech Data Polska, TCH Components i Datrontech Poland, gdzie odpowiadała za rozwiązania z zakresu druku i sprzedaż rozwiązań do sieci komputerowych. Została laureatem nagrody dla managera i zespołu sprzedaży za największy wzrost sprzedaży w regionie w 2013 r., otrzymała nagrodę dla dystrybutora roku marki Xerox w 2009 r. oraz dla dystrybutora roku marki Samsung w 2008 r. Jest absolwentką Szkoły Głównej Handlowej w Warszawie na kierunku menadżerskim oraz na kierunku międzynarodowe stosunki gospodarcze i polityczne. Prywatnie oddaje się pasji ogrodniczej, wnętrzarstwu, fotografii i podróżom. Dla zachowania dobrej kondycji fizycznej gra w squasha.

Bezpośr. inf. Axis Communications

Rozpoczęło się przyjmowanie zgłoszeń wystąpień podczas konferencji IWMC 2019

Dziewiętnasta międzynarodowa konferencja **IWMC** poświęcona technikom gaszenia ognia z użyciem zawiesiny wodnej odbędzie się w **Berlinie w dniach 23–24 października 2019** roku. Impreza będzie miała miejsce w hotelu **Ameron Abion Spreebogen Waterside.**

15 stycznia rozpoczęło się przyjmowanie zgłoszeń wystąpień prelegentów. Streszczenia wystąpień będą przyjmowane do 15 maja. Prelegenci zostaną powiadomieni o akceptacji streszczeń do 17 czerwca. Końcowe wersje wystąpień będą przyjmowane do 15 września.

W celu ujednolicenia streszczeń i upewnienia się, że wszystkie niezbędne szczegóły zostały w nich zawarte, osoby, które chcą przesłać treść swoich wystąpień, proszone są o skorzystanie ze specjalnie opracowanych szablonów.

Sponsorzy imprezy już teraz mogą zarezerwować stoły na wystawę, która odbędzie się równolegle z konferencją.

–Zgłoszenia wystąpień i szablony streszczeń, a także formularze dla sponsorów mogą być ściągnięte ze strony IWMA lub pobrane w głównej siedzibie IWMA w Hamburgu – powiedziała **Bettina McDowell**, główny organizator konferencji IWMA.

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

Czy rynek technik budynkowych jest gotowy na przyszłe wyzwania?

Projekt BMS 2018 – podsumowanie

W dniach 7–8 listopada 2018 r. odbyła się trzecia edycja konferencji **Projekt BMS.** Sprawdzone rozwiązania oraz nowości zaprezentowali Złoci Partnerzy (Apa Group, BKT Elektronik, Global Control 5, WAGO ELWAG), Srebrni Partnerzy (Distech Controls, Finder, Honeywell, Salto) oraz Brązowi Partnerzy (Numeron, Positech, Produal, SmartIN).

Konferencję otworzyła Jowita Michalska, prezes Digital University – fundacji zajmującej się rozwojem strategicznych kompetencji cyfrowych. Tematem prelekcji były predykcje Raya Kurtzweila, najważniejszego futurologa na świecie.

Wykłady eksperckie wygłosili przedstawiciele organizacji NAPE, PLGBC i buildingSMART, a także firmy NUMERON.

Tematem panelu dyskusyjnego była sztuczna inteligencja w zastosowaniach budynkowych. Uczestnicy dyskutowali m.in. o tym, czy sztuczna inteligencja przyczyni się do optymalizacji zużycia energii w budynkach, jak wpłynie ona

na automatyzację pracy zarządcy budynku oraz w jaki sposób zostanie wykorzystana w systemach BMS.

Gościem specjalnym był Kajetan Broniewski – polski wioślarz, trzykrotny olimpijczyk, brązowy medalista XXV Igrzysk Olimpijskich w Barcelonie (1992 r.). Uczestnicy mieli okazję obejrzeć film *Historia polskiego olimpizmu* oraz wysłuchać komentarzy, wskazówek motywacyjnych Kajetana Broniewskiego i anegdot związanych z polskimi sportowcami.

Trzecia edycja Projektu BMS potwierdziła potrzebę istnienia miejsca spotkań wszystkich zainteresowanych rozwojem i użytkowaniem systemów zarządzania budynkiem i automatyki budynkowej. Projekt BMS pozostaje unikatowym ogólnopolskim wydarzeniem, które umożliwia konsolidację środowiska zajmującego się zintegrowanymi systemami budynkowymi.

Bezpośr. inf. Lockus
Opracowanie: Redakcja

Security Forum by Dahua
podsumowanie




29 listopada 2018 r. w Warszawie, w Renaissance Warsaw Airport Hotel, odbyła się pierwsza edycja **Security Forum by Dahua**. Organizatorem forum była firma Dahua Technology Poland. W imieniu organizatorów gości powitali Colin Wang – Managing Director of Dahua, CEE & Nordic – i Joanna Skarbek – Event & Training Manager, CEE & Nordic.

W spotkaniu wzięło udział siedem firm partnerskich z Polski i Europy i prawie trzystu uczestników, wśród których znaleźli się m.in. przedstawiciele służb mundurowych i instytucji publicznych, projektanci oraz osoby odpowiedzialne za infrastrukturę krytyczną.

Super platynowym partnerem spotkania była firma Seagate, platynowym Intel, złotym Axxon-Soft, a srebrnym QNAP i BFT Polska. Forum towarzyszyła wystawa produktów.

Podczas prelekcji gospodarz podał przykłady działających na świecie systemów Dahua Technology. Dzięki współpracy z firmą Intel i zaimplementowanym w produktach mechanizmom sztucznej inteligencji wykorzystującym algorytmy głębokiego uczenia się istnieje możliwość detekcji i rozpoznawania twarzy. Opracowany przez firmę Dahua Technology system rozpoznawania twarzy wykorzystywany w systemach dozoru wizyjnego w dużych miastach i w transporcie gwarantuje wysoki poziom bezpieczeństwa i ułatwia pracę służbom za nie odpowiedzialnym. Podczas forum zaprezentowano system ochrony węgierskiej granicy, w którym wykorzystane są rozwiązania firmy Dahua Technology.

W trakcie forum uczestnicy mogli poznać asortyment pamięci masowych firm QNAP i Seagate. Odpowiedni dobór pamięci

masowej do systemu monitorowania zapewnia bezpieczne przechowywanie i odzyskiwanie danych.

Integracja systemów zabezpieczeń musi być dokonana już na etapie projektowania każdego z nich, dlatego duże znaczenie ma zarządzanie projektami. To zagadnienie omówiła Wioletta Kastrau – dyrektor ds. rozwoju produktów i usług w International Project Management Association Polska (IPMA Polska). Stowarzyszenie IPMA Polska umożliwia wymianę doświadczeń wszystkim zainteresowanym zarządzaniem projektami.

Przykłady wdrożeń oprogramowania AxxonSoft służącego do obsługi wizyjnych systemów dozorowych omówił prezes zarządu AxxonSoft Polska – Paweł Trojak.

Firma BFT Polska zaprezentowała zapory antyterrorystyczne pozwalające sterować ruchem samochodowym i zabezpieczające przed nieuprawnionym wjazdem pojazdu.

Spotkanie zakończyło się konkursem i rozdaniem nagród. Andrzej Jarzyna – Sales and Operations Director, CEE & Nordic, w Dahua Technology Poland – podziękował przybyłym gościom za uczestnictwo, a polskiemu zespołowi za organizację. Najprawdopodobniej kolejna edycja forum odbędzie się jesienią 2019 roku.

Serdecznie dziękujemy za zaproszenie, a zespołowi Dahua Technology Poland życzymy pomyślności i sukcesów w nowym roku.

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

Bezpośr. inf. Ela Końka

Gdyby nie te strzałki...

Znaki ewakuacyjne w budynkach wysokich i wysokościowych

Jan Dziedzic

Zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U.2010.109.719) właściciele, zarządcy lub użytkownicy budynków wysokich i wysokościowych powinni oznakować znakami zgodnymi z Polskimi Normami:

a) drogi i wyjścia ewakuacyjne (z wyłączeniem tych w budynkach mieszkalnych) oraz pomieszczenia, w których zgodnie z przepisami techniczno-budowlanymi wymagane są co najmniej dwa wyjścia ewakuacyjne (znaki powinny dostarczać informacji niezbędnych do ewakuacji);
b) miejsca usytuowania urządzeń przeciwpożarowych i gaśnic;
c) miejsca usytuowania elementów sterujących urządzeniami przeciwpożarowymi;
d) miejsca usytuowania nasady umożliwiającej zasilanie przeciwpożarowej instalacji wodociągowej, kurków głównych instalacji gazowej oraz materiałów niebezpiecznych pożarowo;
e) pomieszczenia i tereny z materiałami niebezpiecznymi pożarowo;
f) drabiny ewakuacyjne, rękawy ratownicze, pojemniki z maskami ucieczkowymi, miejsca zbiórki podczas ewakuacji, miejsca lokalizacji kluczy do wyjść ewakuacyjnych;
g) dźwigi dla straży pożarnej;
h) przeciwpożarowe zbiorniki wodne, zbiorniki technologiczne stanowiące uzupełniające źródło wody do celów przeciwpożarowych, punkty poboru wody, stanowiska czerpania wody;
i) drzwi przeciwpożarowe;
j) drogi pożarowe;
k) miejsca zaklasyfikowane jako strefy zagrożenia wybuchem.

Zadanie to jest proste w przypadku tego, co wymieniono w punktach b–k – wystarczy oznakowanie zgodne z normą PN-N-01256-01:1992 *Znaki bezpieczeństwa – Ochrona przeciwpożarowa* i normą PN-N-01256-04:1992 *Znaki bezpieczeństwa – Techniczne środki przeciwpożarowe*. W przypadku tego, co wymieniono w punktach c i d, możliwe są pewne problemy związane z właściwym doborem znaków (brak jednoznaczności i zrozumiałości znaków).

Oznaczanie dróg i wyjść ewakuacyjnych nie jest łatwe. W czasie obowiązywania normy PN-N-01256-02:1992 *Znaki bezpieczeństwa – Ewakuacja – Symbole graficzne – Barwy bezpieczeństwa i znaki bezpieczeństwa* występowały problemy z właściwym doborem znaków/piktogramów. Brak jednolitego standardu czy wzorca powodował, że stosowano różne znaki w różnych budynkach, na bardzo podobnych do siebie drogach ewakuacyjnych. Problemów tych nie ograniczyło wprowadzenie nowej normy PN-EN ISO 7010:2012 *Symbole graficzne – Barwy bezpieczeństwa i znaki bezpieczeństwa*. Nie dość, że przetłumaczono (z języka angielskiego) tylko pierwszą stronę normy, to zrozumiałość znaków stała się mniejsza.

Przyjmijmy założenie, że znaki ewakuacyjne powinny jednoznacznie, w sposób nie budzący wątpliwości, określić, którędy – z danego miejsca na kondygnacji – należy udać się do najbliższego wyjścia ewakuacyjnego – z budynku lub na ewakuacyjną klatkę schodową (pomińmy przejście do

innej strefy pożarowej). Na szczęście sprawę nieco ułatwiają przepisy przeciwpożarowe, tzn. rozporządzenie Ministra Infrastruktury z 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U. z 15 czerwca 2002 r. z późniejszymi zmianami), które nie pozwalają na powstawanie bardzo skomplikowanych przebiegów dróg ewakuacyjnych na skutek ograniczenia długości przejścia ewakuacyjnego, długości dojścia ewakuacyjnego oraz powierzchni strefy pożarowej. W strefach ZL III przejścia (w pomieszczeniach) mają długości od 40 m do 80 m, zaś dojścia ewakuacyjne (korytarzem ewakuacyjnym do przedsionka ppoż. ewakuacyjnej klatki schodowej) mają długości od 60 m do 120 m. Dodatkowo – m.in. ze względu na funkcjonalność i wynikającą z niej aranżację – droga ewakuacyjna nie powinna być swego rodzaju labiryntem. Ma to wpływ także na wielkość stosowanych znaków/piktogramów. Ponieważ maksymalna odległość od znaków nie przekracza 12 m, w budynkach wysokich i wysokościowych stosuje się najczęściej znaki o wymiarach 15 cm x 30 cm.

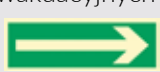
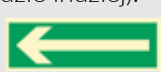
Jednymi z najlepiej sprawdzających się były następujące znaki (na folii fotoluminescencyjnej lub podświetlane):

1. Znak 

lub 

, naklejany na drzwiach ewakuacyjnych lub zawieszony nad drzwiami.

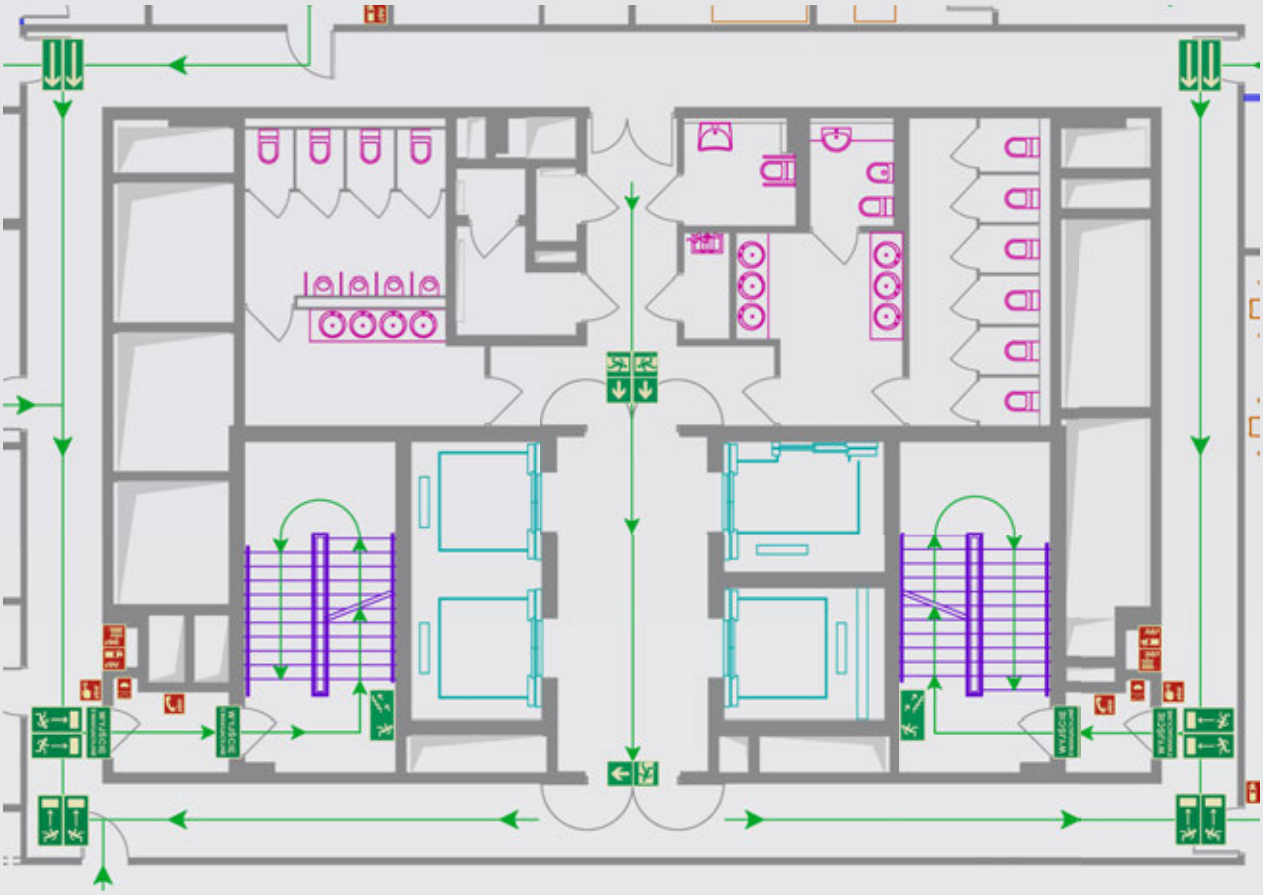
2. Znak  lub  , zawieszany pod sufitem, w najbliższym sąsiedztwie drzwi ewakuacyjnych (nigdzie indziej).

3. Znak  lub  , zawieszany w miejscach zmiany kierunku przebiegu drogi ewakuacyjnej (przejścia/dojścia).

4. Znak  lub  , ewentualnie znak  lub  w przypadku wskazywania kierunku przemieszczania się do wyjścia ewakuacyjnego – na wprost, np. wzdłuż długiego korytarza. Wskazania strzałki zależały (i nadal zależą) od osoby decydującej o doborze znaków (większość decydujących wybiera jeden z dwóch pierwszych znaków – ze strzałką skierowaną w dół). Niezrozumiały jest znak z sylwetką ludzką w otwartych drzwiach (niczego nie wyjaśnia, a wręcz wprowadza w błąd, sugerując obecność drzwi na drodze ewakuacyjnej).

5. Znaki  lub  , ewentualnie  lub  (najczęściej na folii fotoluminescencyjnej), umieszczane na ewakuacyjnych klatkach schodowych, w nadziemnej lub podziemnej (garażowej) części budynku.

Przedstawiona na rys. 1 koncepcja doboru znaków i ich rozmieszczenia jest bardzo prosta i zrozumiała. W przypadku alarmu pożarowego i ewakuacji udaj się w stronę wskazaną przez strzałki. Gdy zobaczysz znak  lub  , będziesz bardzo blisko wyjścia ewakuacyjnego, przez które albo wyjdziesz z budynku, albo wejdziesz (przez przedsionek ppoż.) na ewakuacyjną klatkę schodową. Jeżeli musisz przejść przez jakiekolwiek drzwi, znak poinformuje Cię, czy po przejściu przez nie masz iść dalej prosto czy zmienić kierunek (za drzwiami zobaczysz kolejny znak).



Rys. 1. Przykład zastosowania znaków ewakuacyjnych według „starej” normy

Zgodnie z aktualną normą PN-EN ISO 7010:2012 *Symbole graficzne – Barwy bezpieczeństwa i znaki bezpieczeństwa* powinno się stosować następujące znaki:

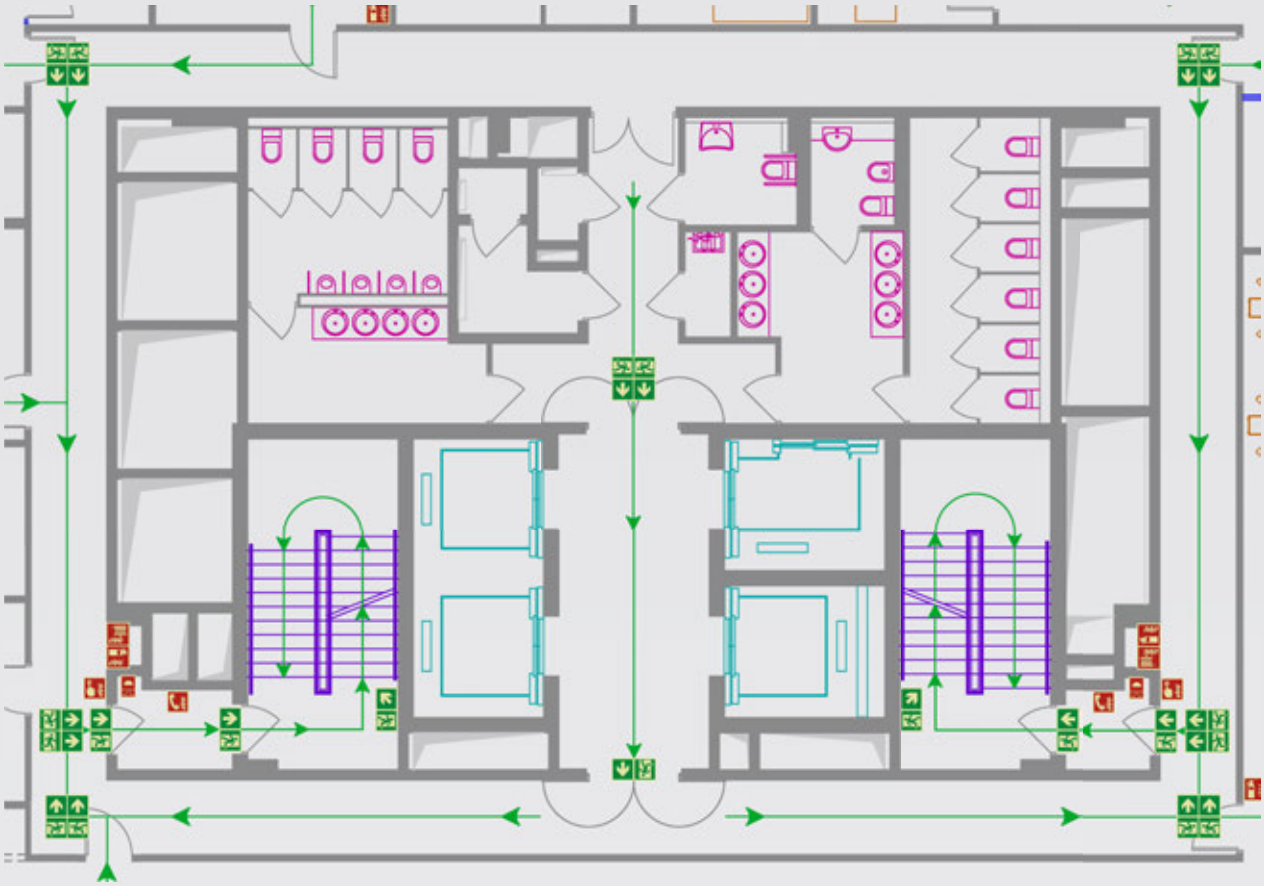
1. Znak  lub  , naklejony na drzwiach ewakuacyjnych lub zawieszony nad drzwiami (drzwi otwierające się w lewą lub w prawą stronę).

2. Znak  lub  , wskazujący albo drzwi ewakuacyjne (znajduje się w pobliżu tych drzwi), albo kierunek (zmiany kierunku) przemieszczania się drogą ewakuacyjną.

3. Znak  lub  , ewentualnie znak  lub  . Znaki te wskazują drogę do wyjścia ewakuacyjnego – na wprost, np. wzdłuż długiego korytarza. Ustawienie strzałki zależy od osoby decydującej o doborze znaków (większość wybiera jeden z dwóch pierwszych znaków – ze strzałką skierowaną w dół). Niezrozumiały jest znak z sylwetką ludzką w otwartych drzwiach (niczego nie wyjaśnia, a wręcz wprowadza w błąd, sugerując obecność drzwi na drodze ewakuacyjnej).

4. Znaki  lub  , ewentualnie znaki  lub  (najczęściej na folii fotoluminescencyjnej), umieszczane na ewakuacyjnych klatkach schodowych, w części nadziemnej lub podziemnej (garażowej) budynku. Niezrozumiały jest znak z sylwetką ludzką w otwartych drzwiach (niczego nie wyjaśnia, a wręcz wprowadza w błąd, sugerując obecność drzwi na klatce schodowej). Także brak symbolu schodów na znaku może wprowadzać w błąd, sugerując, że droga ewakuacyjna może przebiegać po pochylni, a nie po schodach (co jest ważne dla osób niepełnosprawnych).

Przedstawiona na rys. 2 koncepcja doboru znaków i ich rozmieszczenia nie jest prosta i zrozumiała. Na każdym znaku znajduje się sylwetka



Rys. 2. Przykład zastosowania znaków ewakuacyjnych według „nowej" normy

ludzka w otwartych drzwiach – nawet na klatce schodowej, gdzie nie ma żadnych drzwi ewakuacyjnych (oprócz tych na parterze budynku).

Porównując dwa przykłady oznaczenia dróg i wyjść ewakuacyjnych, można wysnuć wniosek, że oznaczenia według „starej" normy są bardziej zrozumiałe. Gdyby nie strzałki na znakach, według „nowej" normy nie byłoby wiadomo, w którą stronę kierować się do wyjścia ewakuacyjnego.

Zamiast zmieniać dobre na lepsze, może – dla podkreślenia, że jesteśmy w Unii Europejskiej i „dajemy szansę" osobom obcojęzycznym – należałoby jedynie zalecić stosowanie znaku uzupełniającego 

zamiast znaków 

lub 

.

Jednym z najlepszych przykładów problemów z doborem znaków ewakuacyjnych jest znak zastosowany w jednym z biurowców na warszawskim Mokotowie. Znak  może znaczyć „jeżeli już tu doszedłeś, zawróć", choć bardziej prawdopodobne jest to, że znaczy „po przejściu przez drzwi otwierające się w lewą stronę udaj się w lewo." Znak jest umieszczony w holu windowym, drzwi prowadzące z holu na korytarz są dwuskrzydłowe, a lewe skrzydło tych drzwi jest tzw. skrzydłem czynnym. Czy strona, w którą otwierają się drzwi, jest istotna podczas ewakuacji? Może chodzi o osoby leworęczne? Przecież w przypadku drzwi dwuskrzydłowych najczęściej tylko jedno skrzydło jest wyposażone w klamkę!

Uważam, że przewaga „nowej" normy nad „starą" jest wątpliwa, nie jest ona bardziej zrozumiała, w przypadku ewakuacji nie jest szczególnie istotne, w którą stronę otwierają się drzwi (w lewą czy w prawą), a umieszczenie na znaku postaci przechodzącej przez lewe lub prawe drzwi niczego nie wnosi.

Jan Dziedzic

ZETTLER nieprzerwanie tworzy nowatorskie rozwiązania w dziedzinie systemów sygnalizacji pożarowej

Od 1877 roku firma ZETTLER jest kojarzona z systemami sygnalizacji pożarowej, ochrony przeciwpożarowej oraz przywoławczymi. Może pochwalić się wieloma innowacyjnymi i sprawdzonymi rozwiązaniami. Przyczynia się do rozwoju branży i zapewnia swoim klientom ochronę życia, mienia oraz spokój. Systemy ZETTLER są zgodne z normami, niezrównanie elastyczne i łatwe w obsłudze. To wszystko przekłada się bezpośrednio na długoterminowe oszczędności, wszechstronny rozwój w przyszłości i pewność, że wygoda nie jest osiągana kosztem bezpieczeństwa.

Firma ZETTLER była pierwszym producentem systemów sygnalizacji pożarowej, który przeszedł z techniki analogowej na cyfrową, co poprawiło ich odporność i niezawodność. Wprowadziła ona również pierwszą czujkę CO, a także tzw. logikę rozmytą, która polega na wykorzystaniu wielu czujników w celu określenia zarówno prawdopodobieństwa wystąpienia pożaru, jak i jego lokalizacji.

PROFILE Flexible – kolejna innowacja firmy ZETTLER

System sygnalizacji pożarowej PROFILE Flexible to idealny przykład naszej tradycji tworzenia innowacyjnych rozwiązań przeciwpożarowych. Centrale PROFILE Flexible korzystają z zaawansowanej technologii MZX, oryginalnie zaprojektowanej z myślą o pracy w najtrudniejszych warunkach, dzięki czemu są niezwykle odporne na oddziaływanie czynników zewnętrznych, takich jak zakłócenia elektryczne. Jednocześnie można je dostosować do określonych wymogów dotyczących chronionego obiektu i łatwo rozbudować, aby spełniły nowe wymagania. System łączy łatwość obsługi, wydajność i elastyczność, a koszty jego eksploatacji są niskie.

Innowacyjna pętla dozorowa zapewniająca elastyczność i funkcjonalność

Ten zaawansowany system sygnalizacji pożarowej został zaprojektowany z myślą o zwiększeniu pojemności pętli dozorowych i umożliwieniu ich współdzielenia, co zapewnia większą elastyczność w zakresie projektowania systemu oraz obniża koszty instalacji – nie tylko na początkowym etapie, ale także w całym okresie jej eksploatacji. Dzięki zastosowaniu mechanizmu wtykowych kart rozszerzeń centrale PROFILE Flexible można jeszcze lepiej dopasować. W przypadku zmian w projekcie system można łatwo rozbudować i przystosować do nowych wymogów.

Wraz z wprowadzeniem normy EN54-23 (europejskiej normy dotyczącej pożarowych sygnalizatorów optycznych) nastąpił znaczny wzrost zapotrzebowania na prąd elektryczny w pętli, co często przekłada się na konieczność zastosowania większej liczby pętli dozorowych i central pożarowych chroniących budynki i osoby w nich przebywające. System PROFILE Flexible można rozbudować. Liczbę pętli można zwiększyć z czterech do 32, stosując nawet 4000 adresów na pętlach w jednej centrali. Centrale sygnalizacji pożarowej mogą być połączone w jedną sieć. W sieci może pracować maksymalnie 99 central PROFILE.

ZETTLER PROFILE Flexible dostarcza do pętli prąd o natężeniu 1 A, czyli dwa razy większym niż w większości dostępnych na rynku rozwiązań innych producentów. Oznacza to także, że potrzebna jest mniejsza liczba pętli i central, co upraszcza projektowanie oraz obniża koszty okablowania i instalacji systemu. Adresowalne pętle dozorowe mogą być włączane do centrali jako pętle współdzielone (SP) lub pętle dużej mocy (HP), dzięki czemu projektanci mogą przydzielić całą dostępną moc pojedynczej pętli HP lub podzielić zasoby na dwie współdzielone pętle SP. Daje to większą swobodę projektowania systemu i umożliwia maksymalne wykorzystanie pojemności pętli – od układu budynku często zależą użyteczne rozmiary pętli dozorowych, co zazwyczaj skutkuje niepełnym wykorzystaniem zasobów. Systemy PROFILE Flexible bazują na tej samej technologii MZX, która jest wykorzystana w innych systemach firmy ZETTLER.

Łatwiejsza instalacja i modernizacja

Centrala PROFILE Flexible jest dostarczana wraz z łatwą w montażu ramą, dzięki której urządzenie jest w stanie zainstalować nawet tylko jedna osoba. Ramę i okablowanie można zainstalować przed przymocowaniem centrali do ściany System można skonfigurować przesyłając dane z komputera do centrali poprzez interfejs z gniazdem USB, dzięki czemu można zaoszczędzić czas i ograniczyć koszty instalacji. Centrala ma nowoczesną konstrukcję, estetyczny wygląd

Fot. 1. Centrala nie tylko jest łatwa w obsłudze, ale także wygląda estetycznie w miejscach ogólnodostępnych

i możliwe są różne sposoby jej montażu. Jest łatwa w obsłudze i wygląda atrakcyjnie w miejscach ogólnodostępnych, takich jak recepcja.

Dzięki wstecznej zgodności central PROFILE Flexible ze starszymi rozwiązaniami administrator obiektu może zaktualizować elementy starszego systemu, więc nie jest potrzebna jego wymiana w całości.

PROFILE Flexible zaprojektowano z myślą o potrzebach zarówno projektantów, jak i użytkowników końcowych. Przejrzysty kolorowy ekran dotykowy TFT o przekątnej 8,4" zapewnia błyskawiczny dostęp do informacji, co może przyczynić się do uratowania czyjegoś życia. Pomimo wielu funkcji nowy interfejs użytkownika jest łatwy w obsłudze. Recepcjoniści oraz inni operatorzy mogą bez problemu uzyskać dostęp do dokładnych informacji o systemie, korzystając z ekranu dotykowego.

Prostsza obsługa i monitorowanie

Obsługę centrali PROFILE Flexible ułatwia interfejs dostępny w wielu wersjach językowych, ergonomiczny układ ikon oraz podświetlane diodami LED przyciski, których wciśnięcie powoduje wyświetlenie podstawowych informacji o stanie systemu Informacje są wyświetlane na ekranie głównym centrali w sposób uporządkowany i czytelny. Dodatkowo możliwa jest personalizacja z wykorzystaniem firmowych znaków. Dostępne na ekranie mapy budynku ułatwiają sprawdzenie układu pięter lub lokalizacji czujek. Można je skonfigurować tak, aby zawsze pokazywane były najbardziej aktualne informacje, co w razie pożaru pozwoli przyspieszyć jego zwalczanie.

W systemie zastosowano przemyślane udogodnienia, takie jak przycisk Info, który służy do szybkiego wyświetlenia informacji i instrukcji zależnych od kontekstu, co jest szczególnie pomocne dla początkujących użytkowników. System posiada również obszerny rejestr mieszczący 10 tys. zdarzeń, który można pobrać na nośnik USB. Dostępne są dynamiczne filtry pozwalające na selektywne przejrzenie rejestru lub jego zapisanie w celu późniejszego wydrukowania i analizy. Obsługa kart RFID umożliwia identyfikację użytkowników i monitorowanie aktywności centrali sygnalizacji pożarowej. Jest to szczególnie przydatne w obiektach specjalnych, gdzie konieczne jest monitorowanie działań o znaczeniu krytycznym. Te wysoce efektywne narzędzia pomagają szybko rozpoznawać sytuacje w obiekcie i znacznie usprawniają wykrywanie usterek.

Niezawodność

Odporność i niezawodność to podstawowe i najważniejsze cechy każdego systemu sygnalizacji pożarowej. Technologia MZX zastosowana w systemach ZETTLER PROFILE Flexible została stworzona z myślą o ich pracy w najtrudniejszych warunkach. Systemy te charakteryzują się wysoką odpornością na czynniki zewnętrzne i źródła fałszywych alarmów.

Fot. 2. Przejrzysty kolorowy ekran dotykowy TFT o przekątnej 8,4" zapewnia błyskawiczny dostęp do informacji

Dzięki wbudowanym zabezpieczeniom nawet awaria procesora nie zmniejsza skuteczności systemu. W przypadku uszkodzenia procesora głównego jego funkcje przejmie procesor pętli, a system zachowa sprawność. Żadne z wejść alarmowych nie zostanie utracone, a wszystkie czujki i ostrzegacze pożarowe nadal będą funkcjonować. Urządzenia przeciwpożarowe nadal będą prawidłowo uruchamiane, a wyświetlacz centrali będzie pokazywał punkty i strefy objęte alarmem.

Niższe koszty eksploatacji

W celu zredukowania całkowitego kosztu systemu centrale PROFILE Flexible mają szereg funkcji stworzonych z myślą o większej elastyczności – od momentu instalacji aż do końca cyklu eksploatacyjnego systemu. Kompatybilność wsteczna gwarantuje, że zastosowane wcześniej centrale pożarowe z MZX mogą być połączone z nowymi centralami PROFILE. 4000 adresów pętlowych dostępnych w centralach PROFILE Flexible umożliwia projektowanie dużych systemów bazujących na pojedynczej centrali.

Klient na pierwszym miejscu

ZETTLER nieustannie poszukuje nowych sposobów modernizacji produktów i rozwija systemy, które przewyższają oczekiwania klientów. Przy wsparciu firmy-matki, Johnson Controls, jesteśmy w stanie osiągnąć nowy poziom globalnej siły z wykorzystaniem lokalnej specjalistycznej wiedzy. Firma Johnson Controls jest działającym w wielu branżach globalnym liderem w tworzeniu zróżnicowanych rozwiązań technologicznych, mającym klientów w ponad 150 krajach. Ponad 120 tysięcy naszych pracowników tworzy współdziałające ze sobą rozwiązania z dziedzin automatyki budynkowej, wydajnych systemów energetycznych, zintegrowanej infrastruktury oraz systemów transportowych nowej generacji, przyczyniając się do rozwoju inteligentnych miast. Firma Johnson Controls, którą utworzono w 1885 roku, po wynalezieniu przez Warrena S. Johnsona pierwszego elektrycznego termostatu do zastosowań w pomieszczeniach, od początku dba o zrównoważony rozwój. Z kolei strategiczne koncentrowanie się na rozwoju naszych platform zarządzania budynkami i na rozwoju energetycznym dowodzi, jak dużą wagę przywiązujemy do sukcesu naszych klientów. ZETTLER PROFILE Flexible to po prostu kolejny przykład dążenia do rozwoju firm, które powierzają nam swoje bezpieczeństwo. PROFILE Flexible sprawdza się doskonale w hotelach, biurach, placówkach medycznych, a także w środowiskach przemysłowych i w obiektach produkcyjnych.

PROFILE Flexible firmy ZETTLER łączy w sobie nowoczesne rozwiązania techniczne z wydajnością Takie systemy zapewniają ochronę, nie zakłócając codziennych czynności – chronią życie ludzi, działając w tle. Oferują najbardziej zaawansowane rozwiązania do wykrywania pożaru. Charakteryzują się najwyższą jakością i najmniejszą szkodliwością dla środowiska naturalnego. Systemy ZETTLER dają coś więcej niż ochronę przeciwpożarową, a mianowicie spokój wynikający z poczucia bezpieczeństwa.

Więcej informacji o firmie ZETTLER i linii produktów PROFILE Flexible znajduje się na stronie www.zettlerfire.com.

Johnson Controls

Domowy IoT, chmura i media społecznościowe to główne cele hakerów w 2019 roku

Magdalena Grochala

W roku 2019 nastąpi konsolidacja grup cyberprzestępczych, które w swoich działaniach wykorzystają sztuczną inteligencję. Najpopularniejszym celem ataków staną się urządzenia IoT zlokalizowane w prywatnych domach, smartfony, media społecznościowe oraz dane zmagazynowane w chmurze. Takie są przewidywania specjalistów z McAfee przedstawione w raporcie *McAfee Labs 2019 Threats Predictions Report*

Cyberprzestępcze podziemie

Cyberprzestępcy rozwijają rynek oprogramowania jako usługi (ang. *software as a service*), oferując sprzedaż złośliwych programów w formie komponentów gotowych do wykorzystania. Dzięki temu nawet hakerzy z niewielkim doświadczeniem i małymi umiejętnościami mogą skutecznie atakować. Ten trend będzie się utrzymywał w 2019 roku, co przełoży się na konsolidację grup przestępczych. Gangi cybernetyczne będą ściśle współpracować z czołowymi dostawcami takich usług jak pranie pieniędzy czy ataki z wykorzystaniem luk w zabezpieczeniach.

W 2019 r. może nastąpić intensyfikacja wykorzystania złośliwego oprogramowania mobilnego, botnetów, ransomware'u, a także zwiększenie się liczby oszustw bankowych i prób obejścia uwierzytelnienia dwuskładnikowego.

Sztuczna inteligencja i dezinformacja w służbie hakerów

Ponieważ zabezpieczenia stosowane w firmach i organizacjach są coraz bardziej wyrafinowane, również cyberprzestępcy muszą wykazywać się większą kreatywnością. Dostępność złośliwych programów w formie gotowych komponentów pozwoli atakującym integrować ze sobą znane taktyki i techniki oraz rozszerzać zakres ich działania, aby realizować nowe cele.

Cyberprzestępcy będą coraz śmielej sięgać po sztuczną inteligencję. Dzięki niej będą mogli zautomatyzować wybór celu, skanować sieć w poszukiwaniu luk i oceniać kondycję oraz szybkość reakcji zainfekowanych środowisk. Wszystko to będzie miało na celu uniknięcie wykrycia przed przejściem do kolejnych etapów ataku.

Boty do rozsyłania fałszywych komunikatów już powstały i można je kupić w cyberprzestępczym podziemiu. Idąc w ślad za niedawnymi niechlubnymi kampaniami pewnych państw, mającymi na celu wpływanie na opinię publiczną, cyberprzestępcy prawdopodobnie przystosują boty i użyją mediów społecznościowych przeciwko znanym firmom. Będą zamieszczać nieprawdziwe informacje na ich temat i żądać okupu za zaprzestanie takich działań.

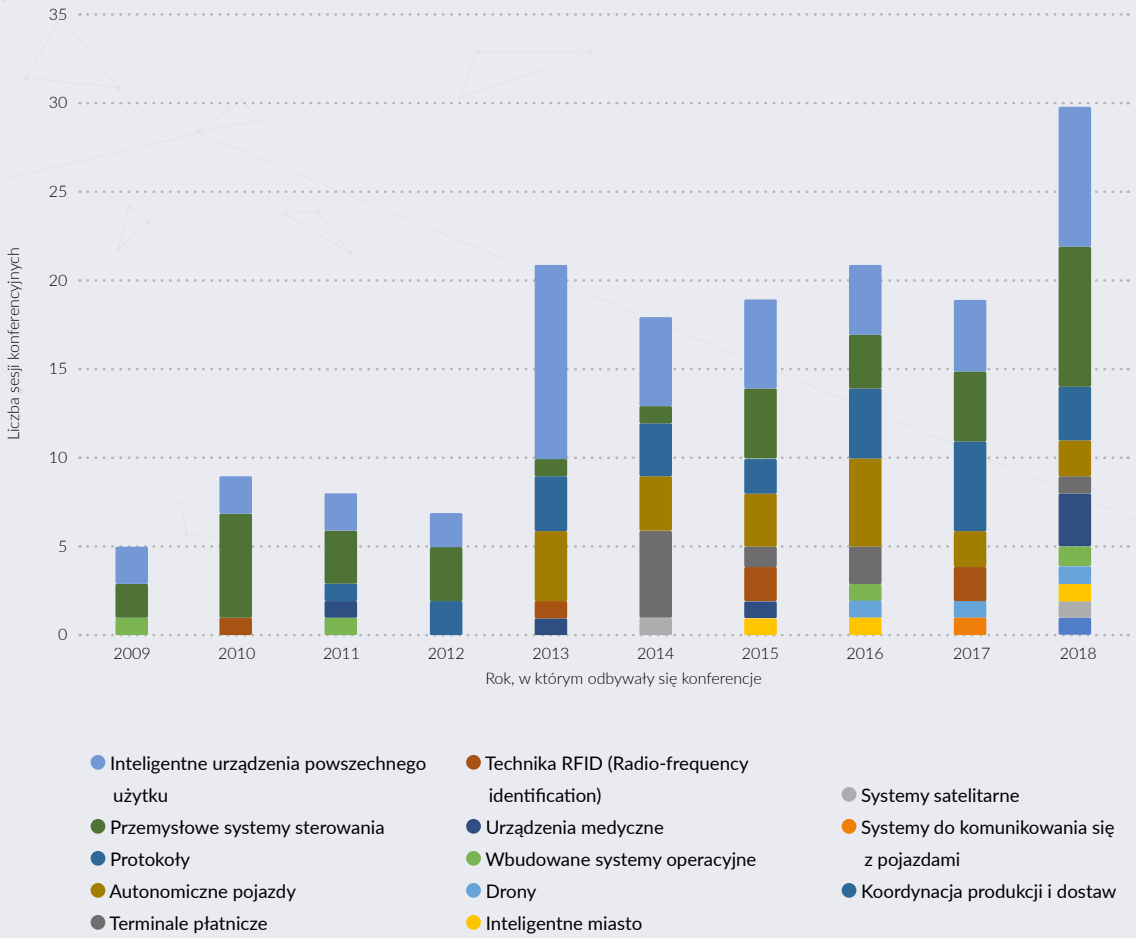
McAfee przewiduje również, że cyberprzestępcy zastosują strategię łączenia kilku rodzajów ataków, aby skutecznie obchodzić zabezpieczenia. Przykładem może być integracja phishingu, steganografii i wirusów bezplikowych w celu przeprowadzenia ataku na wiele celów jednocześnie. Wprowadzi to spore zamieszanie i skomplikuje proces identyfikacji i przeciwdziałania atakom.

Chmura, domowy IoT i media społecznościowe w stanie oblężenia

Dzięki dostępowi do coraz skuteczniejszych taktyk i strategii cele działań cyberprzestępców mogą być bardziej złożone, a zakres tych celów może być szerszy. Przewiduje się, że w roku 2019 na ich celowniku znajdą się własność intelektualna, domowe urządzenia IoT, dane uwierzytelniające przechowywane w chmurze, cyfrowi asystenci i platformy społecznościowe.

Eksperci prognozują znaczny wzrost liczby ukierunkowanych ataków mających na celu uzyskanie dostępu do ogromnych ilości danych korporacyjnych przechowywanych w chmurze. Według informacji zawartych w *Cloud Adoption & Risk Report* 21% zasobów zarządzanych obecnie za pośrednictwem chmury zawiera materiały poufne i o szczególnym znaczeniu, np. własność intelektualną, informacje o klientach i dane osobowe. Możliwe scenariusze obejmują ataki skierowane na słabe interfejsy API lub niestrzeżone punkty końcowe API, rozszerzony rekonesans i eksfiltrację danych z baz chmurowych, a także użycie chmury do ataków kryptologicznych MITM (ang. *man-in-the-middle*) w celu cryptojackingu lub wykorzystania ransomware'u.

Liczba sesji poświęconych urządzeniom IoT podczas konferencji Black Hat i DEF CON na przestrzeni ostatnich 10 lat



Na popularności zyskają także ataki na domowe urządzenia IoT za pośrednictwem smartfonów, tabletów i ruterów. Nowe złośliwe programy mobilne będą wykorzystywać smartfony, tablety i rutery po to, by dotrzeć do cyfrowych asystentów i sterowanych przez nich prywatnych urządzeń IoT. Po infekcji takie urządzenia będą wytrychem do naszych domów, stając się częścią botnetów, które mogą uruchomić ataki DDoS, lub dając cyberprzestępcom dostęp do danych osobowych oraz możliwość podjęcia innych złośliwych działań, np. otwarcia drzwi lub połączenia z serwerem sterującym.

Cyberprzestępcy nie ominą też mediów społecznościowych. Co prawda w 2019 roku duże platformy społecznościowe wdrożą dodatkowe środki ochrony danych użytkowników, jednak wraz z rozwojem tego rodzaju mediów hakerzy będą z coraz większą determinacją rozpracowywać te obfitujące w dane środowiska. Skuteczne naruszenia zabezpieczeń mediów społecznościowych, platform tożsamościowych i urządzeń brzegowych pozwolą przestępcom ponawiać podobne ataki w przyszłości.

W roku 2018 byliśmy świadkami coraz lepszej współpracy między cyberprzestępcami, którzy usprawniali swoje techniki i taktyki. Ta tendencja będzie się utrzymywać także w roku 2019, jednak najbliższa przyszłość przyniesie też nowe sposoby tworzenia zabezpieczeń i sojusze po stronie firm pracujących nad rozwiązaniami do walki z atakami.

Opracowała Magdalena Grochala na podstawie materiałów firmy McAfee

Podczas konferencji Black Hat i DEF CON, jakie odbyły się w roku 2018, trzydzieści wystąpień dotyczyło urządzeń IoT. Jest to duży skok naprzód w porównaniu z rokiem 2017, gdy takich wystąpień było tylko dziewiętnaście. Wzrost zainteresowania dotyczył głównie zintegrowanych systemów komputerowych, urządzeń medycznych, zagadnień związanych z inteligentnymi miastami i inteligentnymi urządzeniami konsumenckimi (patrz rysunek).

NOVUS®

2000 SERIA IP • 4000 SERIA IP

IDEALNE DOPASOWANIE

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

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

Bezpieczeństwo
inteligentnych systemów dozorowych

Axis Communications

O bławę można śledzić na ekranach. Wiadomo, gdzie nasz antybohater się znajduje, gdyż widać go dzięki kamerom służącym do monitoringu miejskiego, a także urządzeniom zamontowanym w prywatnych autach i pojazdach służących do transportu publicznego. Sieć złożona z systemów publicznych, prywatnych kamer oraz kompatybilnych sensorów oplata „złego" i ogranicza jego pole manewru. Dane z systemów detekcji twarzy oraz analizy sylwetki, ruchu i głosu docierają do policji, a z głośników dobywa się skierowany do zbiega komunikat ostrzegawczy.

Historia z wizyjnym systemem dozorowym w roli głównej wcale nie musi kończyć się happy endem, zwłaszcza jeśli zdobycze techniki zostaną użyte w złym celu. Wyobraźmy sobie, że ktoś wykorzystuje taki system do śledzenia i zdyskredytowania innego człowieka z przyczyn zawodowych lub politycznych. Ktoś może próbować przejąć kontrolę nad systemem bezpieczeństwa, w porcie lotniczym, a nawet w obiekcie rządowym czy wojskowym. Przejęcie kontroli może ponadto skutkować uzyskaniem dostępu do bazy danych o szczególnym znaczeniu. Niemożliwe? Bynajmniej! Im bardziej będziemy rozwijać świat IoT, tym większe będzie ryzyko łamania

Wyobraźmy sobie, że jest rok 2022. Więzień zbiega z policyjnego konwoju. Próbuje ukryć się w wąskiej uliczce, ale dostrzega go lokalny patrol. Wbiega więc na główną arterię, schodzi do metra, ale zostaje rozpoznany przez ochronę, zmienia plan i udaje się do pobliskiego sklepu, a stamtąd, przez zaplecze, dociera na parking, gdzie kradnie auto, po czym ucieka dalej. Policyjne syreny są co raz głośniejsze. Rozpoczyna się szaleńczy pościg i obława.

zabezpieczeń. W Polsce coraz wyraźniej widać popularność koncepcji tzw. inteligentnego miasta, w tym inteligentnego nadzoru wizyjnego. To cieszy, jednak zdaje się, że ciągle zbyt słabo rozpoznaje się zagrożenia, zwłaszcza problem możliwości włamania się do wizyjnego systemu dozorowego.

Bezpieczeństwo inteligentnego miasta

Inteligentne miasto to przestrzeń, w której infrastruktura bazuje na najnowszych osiągnięciach techniki. Chodzi także o świadczenie usług publicznych w takim stopniu, aby ułatwić życie mieszkańcom. Do istoty funkcjonowania inteligentnego miasta należy integracja, komplementarność, automatyzacja i bezpieczeństwo systemów, za pośrednictwem których dokonywana jest wymiana danych – np. podczas indywidualnych rozliczeń, zakupów, użytkowania publicznych i prywatnych środków transportu, sprawdzania lokalizacji, korzystania z ułatwień dla niepełnosprawnych, dostępu do informacji i źródeł rozrywki. Potrzebny jest dostęp do konkretnych urządzeń, np. telewizorów, smartfonów, kamer i czujników. Wykorzystuje się wymagające ciągłego doskonalenia i testowania zaawansowane systemy informatyczne, sztuczną inteligencję, uczenie się przez maszyny lub systemy (ang. *machine learning*), analizę dużych zasobów danych (ang. *big data*).

Ze względu na ważność rejestrowanych, przetwarzanych i przesyłanych danych systemy informatyczne będące elementami inteligentnego miasta trzeba szczególnie chronić przed ingerencjami

fizycznymi i cyberatakami. Jak wynika z badań przeprowadzonych m.in. przez Wi-Sun Alliance i Fundację Bezpieczna Cyberprzestrzeń w Szwecji, Danii, Wielkiej Brytanii, USA, a także w Polsce, inwestowanie w IoT jest coraz bardziej popularne i uważane za potrzebne do wdrażania rozwiązań charakterystycznych dla inteligentnego miasta. Mimo to w praktyce wiele projektów nie doczekuje się realizacji z powodu ich wadliwości, niezapewnienia dostatecznego poziomu bezpieczeństwa, ograniczeń infrastrukturalnych, zastanych uwarunkowań prawnych i administracyjnych, nienadążania przez niektóre instytucje za postępem w dziedzinie techniki, niewystarczających kompetencji użytkownika końcowego.

Pokonywanie zabezpieczeń systemów inteligentnego miasta może przebiegać na różne sposoby. Atak może być wymierzony w operatora lub nadzorcę, sprzęt i oprogramowanie. Rodzaje zagrożeń są różne.

Konieczność zabezpieczenia systemu monitorującego

Wizyjne systemy dozorowe, w których zastosowane są zminiaturyzowane moduły i które wyposażono w dodatkowe czujniki, są jak komputery, których funkcją jest wychwytywanie określonego rodzaju danych. Należy zabezpieczyć system monitorujący, aby ochronić te dane, a zwłaszcza wizerunki osób i konteksty sytuacyjne, w których się pojawiają. Dane te nie powinny dostać się w niepowołane ręce, więc firmy oferujące systemy dozorowe muszą zagwarantować odpowiednie zabezpieczenia. Trzeba podkreślić, że wszędzie tam, gdzie mamy do czynienia z mniej lub bardziej rozbudowanym systemem obserwacji bazującym na sieciowych kamerach i czujnikach, istnieje potrzeba magazynowania danych w serwerach i chmurach, które również wymagają specjalnej ochrony. Słabe algorytmy szyfrujące bądź niewystarczające uświadamianie sobie zagrożeń przez administratorów mogą wykorzystać hakerzy, których ostatecznych celów możemy nigdy nie poznać. Kamera może posłużyć jako urządzenie szpiegujące. Nie bez przyczyny amerykańska administracja zakazała swoim urzędnikom użytkowania urządzeń niektórych chińskich producentów.

Możliwy jest atak na system sterowania ruchem ulicznym, system służący do rozpoznawania numerów rejestracyjnych i poboru opłat za parkowanie, system oświetlenia ulic i przystanków. Wyobraźmy sobie manipulowanie przy systemach do wykrywania zanieczyszczeń powietrza czy detekcji wzrostu temperatury lub intensywnych opadów deszczu. Dodajmy do tego ataki na kamery wielosensorowe czy czujniki w ogóle, na przykład te, które służą do ochrony przyrody lub dziedzictwa kulturowego, lub są wykorzystywane w inteligentnych urządzeniach gospodarstwa domowego. Niepożądana ingerencja w systemy dozorowe może doprowadzić do zwiększenia liczby fałszywych alarmów i w konsekwencji do paraliżu służb, które muszą na nie reagować. Może ona być też elementem tzw. wojny hybrydowej. Na pojedyncze i skomasowane ataki powinny być przygotowane nie tylko odpowiednie służby, ale także każdy podmiot, który korzysta z systemu, który może być źródłem danych wymagających ochrony.

Hakowanie w praktyce

O skutecznych przejęciach kontroli nad monitoringiem miejskim nie pisze się często, gdyż nie jest to powód do chwały – tym bardziej, że w niektórych przypadkach próbowano naruszyć bezpieczeństwo wewnętrzne, co podano do wiadomości dopiero po dłuższym czasie. Ataki złośliwego oprogramowania powodują z reguły zmiany w ustawieniach obrazowania i w kalibracji obserwowanych scen, zmiany zawartości lub właściwości zapisywanych plików, a także modyfikację ustawień kart sieciowych. Niektóre mogą doprowadzić do chwilowego zatamowania lub przekierowania jakiegoś strumienia informacji, inne mogą spowodować większe szkody. Oczywiście aranżowane są też testy i ataki kontrolowane.

Badanie Vasiliosa Hioureasa oraz Thomasa Kinseya ujawniło, że sieci, które mają chronić przed przestępcami i terrorystami, mogą stać się niebezpiecznym narzędziem w ich rękach. Wykazali oni, że w jednym z miejskich systemów monitorowania nie było stosowane żadne szyfrowanie, mimo że urządzenia posiadały odpowiednie funkcje. Hioureas i Kinsey w dość prosty sposób stworzyli własną wersję oprogramowania, które umożliwiło pełną kontrolę nad kamerami, dzięki czemu byli w stanie przechwycić obraz z każdego miejsca, dokonywać manipulacji, zamieniać rzeczywiste nagrania na fałszywe. Mechanika

ataku polegała na wykorzystaniu podatności sieci miejskiej na ataki, takie jak ARP, podczas którego użytkownik podszywa się pod jeden z węzłów rutujących, przesyłając pakiety, a następnie zmienia dane wysyłane do rutera i z rutera. W ten sposób atakujący uzyskuje bezpośredni dostęp do strumieni wizyjnych, np. dostępnych na posterunku policji, a dzięki imitowaniu węzła sprawia, że pobliskie kamery przesyłają swoje pakiety danych bezpośrednio do niego. Konfiguracja ta umożliwia tzw. atak man-in-the-middle, znany także z niektórych gier strategicznych. Dzięki zhakowaniu systemu przestępcy mogą zobrazować fikcyjne przestępstwo lub inne zdarzenie wymagające pilnej interwencji i w efekcie skłonić policję lub inne służby do wysłania grupy operacyjnej we wskazane miejsce. Mogą w ten sposób spowodować interwencję w jednym miejscu, by odwrócić uwagę, i dokonać przestępstwa w innym. To scenariusz rodem z Hollywood, ale wcale nie musi być fikcją.

W ramach audytów bezpieczeństwa polscy specjaliści przeprowadzili kontrolowane ataki na wizyjne systemy dozorowe. Dzięki przysłowiowej jednej linijce kodu w 2017 roku zhakowano kamery w stopniu umożliwiającym nagrywanie obrazów i dźwięków na własnych nośnikach, a nawet dostęp do nagrań archiwalnych. Co ciekawe, w systemie zastosowane były popularne kamery jednej z japońskich firm, wykorzystywane m.in. w więzieniach, a także przez nowojorską policję i FBI. W przypadku innych kamer, przeznaczonych do miejskich systemów obserwacyjnych, poprzez nieuwierzytelnione zapytanie HTTP udało się pobrać zawartość pamięci i uzyskać dane potrzebne do zalogowania się jako administrator. Popularny staje się również Google hacking umożliwiający dostęp do strumieni wizyjnych z kamer publicznych lub prywatnych (w przedsiębiorstwach lub w domach) poprzez użycie domyślnego hasła producenta kamer. W Internecie można znaleźć wiele przykładów takiego prostego łamania zabezpieczeń.

Jeden z poważniejszych ataków hakerskich, o charakterze kryminalnym, miał miejsce w Waszyngtonie, gdzie dwójka rumuńskich hakerów opanowała większość zewnętrznych kamer obserwacyjnych stołecznej policji. Przejęli oni kontrolę nad 123 z 187 kamer używanych przez MPDC na cztery dni, od 9 do 12 stycznia 2017 r. Ich celem nie była inwigilacja czy działania terrorystyczne. Według śledczych usiłowali jedynie użyć elementów systemu podłączonych do Internetu by rozprowadzić oprogramowanie szantażujące (ransomware), szyfrujące dane na dyskach użytkowników w celu wyłudzenia okupu za odzyskanie danych.

Rozwiązania z dziedziny inteligentnego monitorowania są możliwe do realizacji za pośrednictwem wielu różnych urządzeń przynależnych do IoT. Jak dowodzą audytorzy, np. podczas pokazów na konferencji DEF CON, możemy być – jakkolwiek to zabrzmi – szpiegowani przez lodówki czy odkurzacze. Przejęcie kontroli nad inteligentnym odkurzaczem pewnej koreańskiej firmy uświadamia nam, że należy ciągle doskonalić zabezpieczenia sprzętowe, programowe i sieciowe. Poprzez jedno połączone z siecią za pośrednictwem inteligentnego urządzenia atakujący może dotrzeć do innych urządzeń i mogą wśród nich być również te, na których przechowywane są ważne dla użytkownika dane, które wymagają szczególnej ochrony. Badania pokazują, że w coraz liczniejszych inteligentnych urządzeniach RTV i AGD z wbudowanymi kamerami, mikrofonami i czujnikami można znaleźć luki w zabezpieczeniach. Mogą one zostać wykorzystane do niewykrywalnych naruszeń prywatności, nieinwazyjnego szpiegowania, niewidocznych przestępstw.

Jak się bronić?

Nie ma potrzeby wymieniać tu poszczególnych działań producentów, projektantów, osób zarządzających bezpieczeństwem itd. Podstawą jest analiza dokonanych i przewidywanie potencjalnych ataków w celu projektowania odpowiednich łat i aktualizacji systemów. Jeśli chodzi o wizyjne systemy dozorowe, można wskazać kilka sposobów zapobiegania naruszeniom, zarówno na poziomie technicznym jak i operacyjnym.

Jedną z podstawowych metod, jakimi należy się posługiwać, jest odpowiednie planowanie i rozdzielanie uprawnień użytkowników systemów. To wydaje się oczywiste, ale w praktyce bywa różnie. Firma Axis Communications zawsze zwraca uwagę na to, że zakres i zasady uwierzytelniania powinny odpowiadać stanowiskom i kompetencjom poszczególnych osób.

Urządzenia, oprogramowanie i powiązane zabezpieczenia powinny być odpowiedniej jakości.

Mowa tu przede wszystkim o odpowiednich algorytmach szyfrujących, procedurach logowania się i potwierdzania tożsamości, procedurach zmiany haseł i uprawnień, a także o funkcjach kodowania obrazu, które umożliwiają zamazywanie sylwetek i twarzy ludzkich na określonym poziomie dostępu.

Potrzebne jest systematyczne aktualizowanie zabezpieczeń, a także stosowanie się do zaleceń i instrukcji. Z cyberatakami jest jak z grypą. Ciągle powstają nowe mutacje wirusa i żadna szczepionka nie jest w pełni skuteczna. Każdy producent kamer powinien wyraźnie ostrzegać o możliwości ataku cyfrowego, a także informować o tym, co należy w danym przypadku zrobić. Axis Communications od lat spełnia tę powinność, ale nie wszyscy dostawcy to robią.

Zauważalny jest problem po stronie użytkownika końcowego – większości ataków można by uniknąć, gdyby na etapie konfiguracji zastosowano dobre praktyki. W tym kontekście warto wspomnieć np. o *Hardening Guide* firmy Axis Communications – tekście, w którym opisano zasady i procedury, których należy przestrzegać podczas wdrożenia, aby uodpornić system na cyberataki.

Tę krótką analizę warto zakończyć dwoma wnioskami generalnymi. Ograniczanie cyberzagrożeń jest szczególnie ważne w zarządzaniu bezpieczeństwem w dziedzinach i sektorach strategicznych. Tym bardziej, że domena cyberbezpieczeństwa monitorowania sięga obecnie nawet poziomu geopolityki i geostrategii. W związku z tym należy dbać o bezpieczeństwo nie tylko systemów służących do obserwacji ruchu drogowego lub kolejowego, ale też systemów dozorujących obiekty rządowe, przedsiębiorstwa i instytucje, które są szczególnie ważne ze względu na bezpieczeństwo państwa i społeczeństwa.

Na zakończenie warto dodać, że jeśli zależy nam na bezpieczeństwie w inteligentnym mieście, sami również musimy działać inteligentnie. Niewiele da nam kolejna „mądra” aplikacja w pracy lub domu, jeśli nie będziemy używać bezpiecznego hasła. Nie będzie możliwa większa wygoda podczas zakupów i w podróży, energooszczędność, optymalizacja finansów czy walka ze smogiem z wykorzystaniem najnowocześniejszych technik, jeżeli zapomnimy o potencjalnych cyberzagrożeniach, odpowiednich zabezpieczeniach i nie wyciągniemy wniosków z ataków, które mamy za sobą.

Axis Communications

ZAWSZE WIESZ CO JEST GRANE

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

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

WarAn i GekOn

narzędzia dla projektanta instalacji niskoprądowych

Andrzej Warzywoda

Czy zastanawiałeś się, jakiego narzędzia najbardziej brakuje Ci podczas projektowania instalacji? Na tak postawione pytanie 70% projektantów odpowiada, że automatycznego numerowania elementów! Faktycznie – nie da się zapomnieć tego uczucia, gdy okazuje się, że trzeba dodać jeszcze jedną czujkę na początku pętli pożarowej albo „upchnąć" w koncentratorze dodatkowy detektor PIR, albo wstawić gniazdo LAN na początku panelu. Dodanie każdego z tych elementów wymaga ponumerowania od nowa pozostałej części urządzeń systemowych w projekcie. W przypadku rozbudowanej instalacji zajmie to bardzo dużo czasu i nieuchronnie pociągnie za sobą dodatkowe koszty projektowania. Jak wspominasz rysowanie schematów blokowych czy przygotowywanie zestawień urządzeń? Czy pamiętasz, jak tuż przed wydaniem projektu okazało się, że jeden albo dwa głośniki DSO nie zostały włączone w linię? To są chwile, w których uzmysławiasz sobie, że dobrze byłoby mieć narzędzie, które te wszystkie czynności wykona za Ciebie. Prawda?

WarAn to zbiór narzędzi rozszerzających funkcjonalność oprogramowania CAD (BricsCAD, AutoCAD, ZwCAD, GstarCAD), których zadaniem jest automatyzacja pracy przy projektowaniu wszystkich instalacji logicznych, szczególnie systemu sygnalizacji pożarowej, dźwiękowego systemu ostrzegawczego, systemu sygnalizacji włamania i napadu, okablowania strukturalnego i podobnych.

WarAn łączy obiekty (czujki, głośniki, gniazda etc.) w logiczną całość, umożliwiając ich numerowanie, rysowanie schematów, przygotowywanie zestawień i list, a także wyszukiwanie potencjalnych błędów.

Są dwa typy logicznych połączeń elementów w systemach niskoprądowych – magistrala i drzewo. Magistrala to połączenie urządzeń jedno za drugim. Jest ono typowe dla systemu sygnalizacji pożarowej czy dźwiękowego systemu ostrzegawczego.

Połączenie typu drzewo umożliwia przypisanie urządzeń w układzie wiele-do-jednego. W strukturę drzewa łączone są wszystkie systemy wyposażone w koncentratory adresów – system sygnalizacji włamania i napadu, system kontroli dostępu czy okablowanie strukturalne.

WarAn ma zaimplementowaną logikę dla struktur połączeń typu magistrala i typu drzewo. Dzięki temu jest w stanie obsłużyć praktycznie każdą instalację wymagającą adresowania. Właśnie ta uniwersalność wyróżnia go spośród innych narzędzi przeznaczonych dla projektantów instalacji niskoprądowych.

Podstawowym elementem w WarAnie jest aparat. Aparaty są logicznie łączone w magistrale lub drzewa, z których kolejno powstają logiczne obrazy całych systemów. Aparatem

może być to, co akurat potrzebujesz przyłączyć, czyli czujka pożarowa, czujka włamaniowa, gniazdo sieciowe LAN, oprawa awaryjna lub jakiekolwiek inne urządzenie do aktualnie projektowanego systemu.

Aparaty budowane są na zasadzie dokładania kolejnych bloków – symboli. Dzięki temu można błyskawicznie dodać do czujki pożarowej np. obudowę przeciwwietrzną, podstawę z przekaźnikiem lub izolator zwarć. Jeśli jest to potrzebne, można nawet przypisać każdej czujce pomieszczenie, w którym ma zostać zainstalowana. WarAn jest na tyle uniwersalny, że można w nim odwzorować urządzenia każdego producenta.

Do tworzenia projektów można użyć symboli dostarczonych z WarAnem albo własnych, z których korzysta się na co dzień.

Po dokonaniu logicznego połączenia aparatów (w strukturze drzewa lub magistrali) można to połączenie w dowolny sposób modyfikować. Takie operacje jak dodawanie i usuwanie elementów, zmiana kierunku połączenia czy sortowanie urządzeń nie stanowią problemu. Oczywiście połączenie można wielokrotnie numerować i generować schematy blokowe.

Zarówno numerowanie, jak i rysowanie schematów blokowych w WarAnie jest zautomatyzowane i zajmuje nie więcej niż kilkanaście sekund, niezależnie od wielkości projektowanych systemów – mogą to być systemy z pojedynczymi czujkami albo z kilkunastoma tysiącami czujek. Właśnie w przypadku dużych systemów WarAn jest doceniany najbardziej. Jego moduł do sprawdzania i identyfikowania błędów jest w nich niezastąpiony.

Gdy projekt zostanie narysowany, aparaty będą ponumerowane, a schematy gotowe, warto przygotować zestawienie albo listę systemową, która odzwierciedla dany system w formie tabelarycznej. To również automatycznie wykona WarAn.

Na koniec polecamy jeszcze jedno sprytne narzędzie, które pozwala między innymi szybko i w pełni automatycznie przygotować profesjonalnie wyglądającą wersję PDF wszystkich rysunków w projekcie na raz (wraz z automatycznym wyborem i przycięciem rozmiaru arkuszy w PDF-ie dopasowanym do faktycznego rozmiaru obszaru wydruku). Tym narzędziem jest GekOn, czyli jeszcze jedna – obok WarAna – nakładka CAD naszej produkcji. Dzięki niej projekt będzie gotowy do wydania.

Zapraszamy do pobrania pakietu instalacyjnego ze stron www.warancad.pl i www.gekoncad.pl. Można przetestować WarAna i GekOna, żeby sprawdzić ich funkcje. Użyj kodu AIDCAD01 przy zamówieniu, a otrzymasz pakiet na 90 dni gratis.

WarAn i GekOn to polskie produkty stworzone przez projektantów dla projektantów. Zastosowane w nich rozwiązania mają skutkować przede wszystkim ergonomią pracy, łatwością konfiguracji i intuicyjnością obsługi. W razie konieczności dodania jakiejś nowej funkcji deweloperzy są w stanie przygotować odpowiednie rozwiązanie w krótkim czasie.

Producentem i dystrybutorem WarAna i GekOna jest AidCAD.

Andrzej Warzywoda
AidCAD
andrzej.warzywoda@gekoncad.pl
www.warancad.pl, www.gekoncad.pl

Systemy ochronne
do sieci strukturalnych i instalacji CCTV

Mirosław Gondek

Firma Ewimar od wielu lat zdobywa doświadczenie w zakresie projektowania i produkcji urządzeń przeznaczonych do ochrony przeciwprzepięciowej w systemach teleinformatycznych. Podstawowa oferta obejmuje ograniczniki LAN do sieci 100 Mbit, przeznaczone głównie do zastosowania w instalacjach IP-CCTV, oraz – od niedawna – wysokiej jakości ograniczniki do sieci Gigabit Ethernet

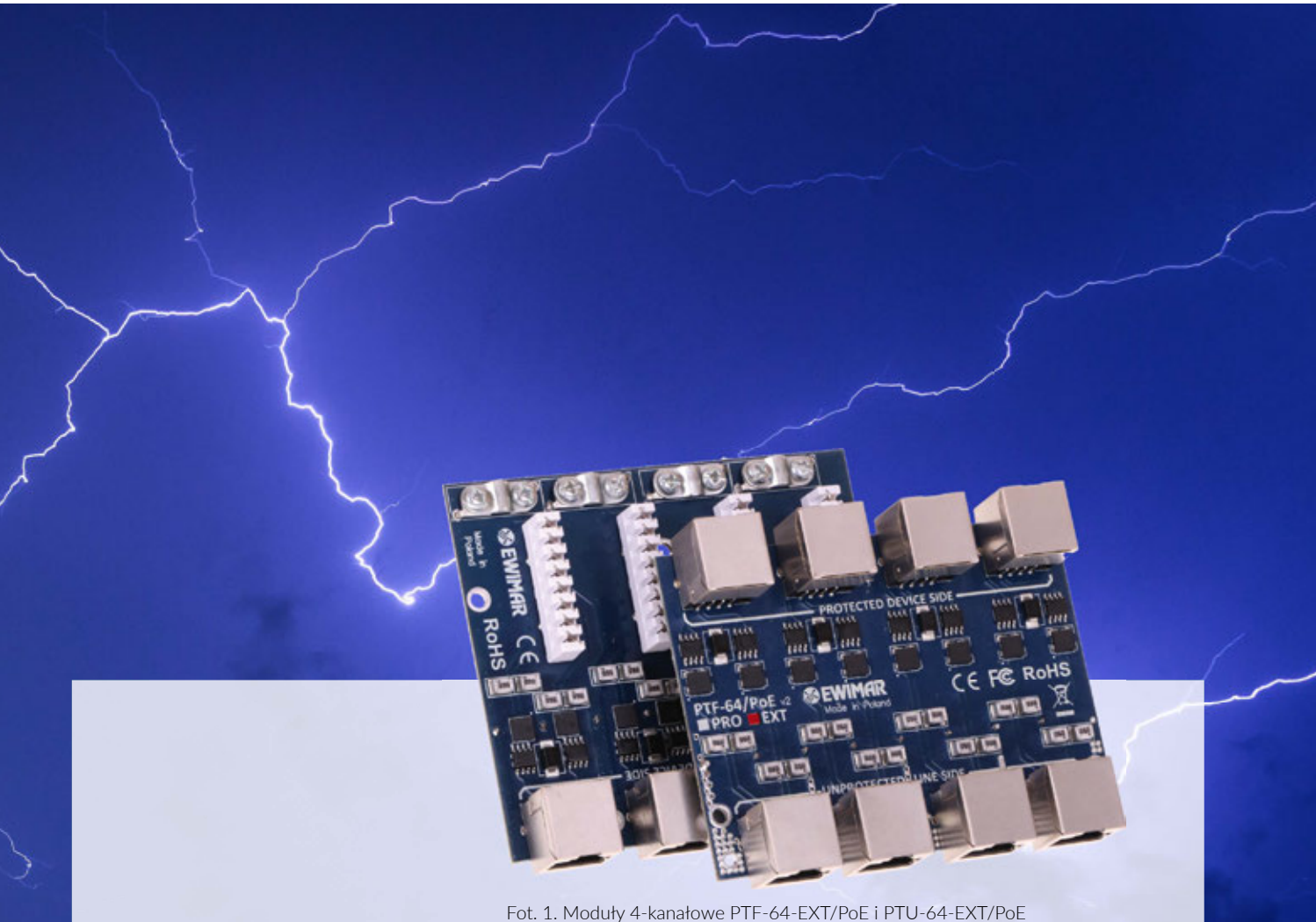
Zdecydowana większość systemów CCTV wykorzystuje sieć 100Base-T, pomimo dosyć częstego stosowania przewodów kategorii 6 lub wyższej. Taka szybkość sieci LAN jest narzucana przez producentów kamer IP, które dzięki wykorzystaniu nowych metod kompresji obrazu generują strumienie wizyjne o niskiej przepływności i nie są w stanie przekroczyć przepustowości 100 Mbit.

Wśród czołowych producentów firma Ewimar ma jeden z najbogatszych asortymentów ograniczników do IP-CCTV, uwzględniający zróżnicowaną skuteczność działania, różne rozwiązania montażowe, liczby kanałów, sposoby łączenia przewodów i budowę modułową.

Dlaczego warto stosować systemy ochronne?

Ochronniki przeciwprzepięciowe należy stosować z wielu powodów. Oto niektóre z nich:

1. Wyraźnie zmieniający się od lat 80. XX wieku klimat powoduje wiele anomalii pogodowych,



Fot. 1. Moduły 4-kanałowe PTF-64-EXT/PoE i PTU-64-EXT/PoE

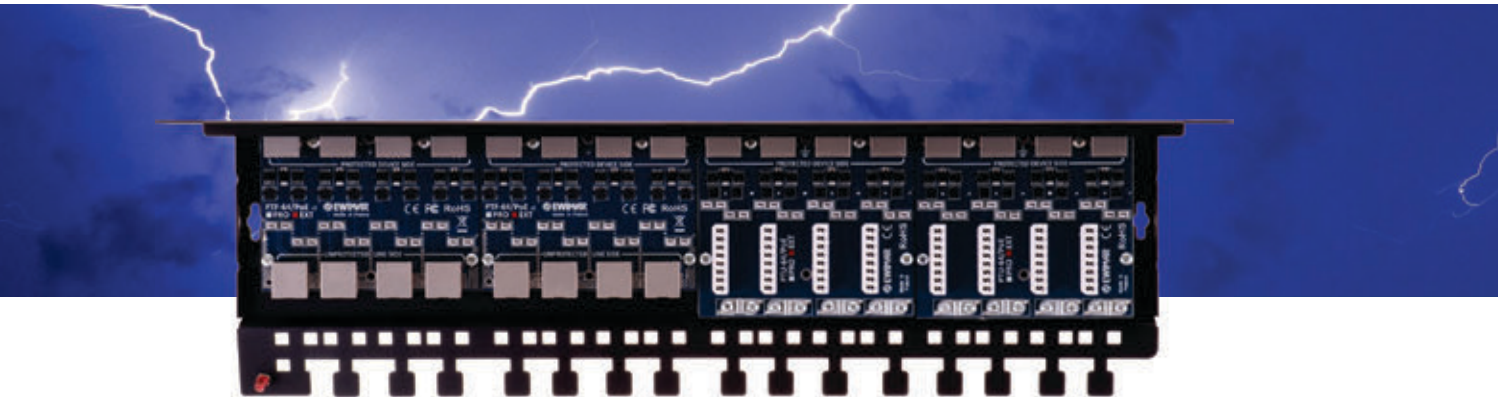
w tym coraz częstsze i intensywniejsze wyładowania atmosferyczne. Statystycznie rzecz biorąc, urządzenia elektroniczne z roku na rok są coraz częściej narażone na udary prądowe.

2. Postępująca miniaturyzacja (a tym samym mniejsza zdolność do odprowadzania ciepła i niższe napięcia zasilania) nieporównywalnie zwiększa ryzyko uszkodzenia współczesnych urządzeń elektronicznych (ryzyko jest znacznie większe niż w przypadku urządzeń wyprodukowanych dawniej, na przykład 30 lat temu).
3. Wymiana danych i sterowanie z wykorzystaniem cyfrowych metod transmisji jest podstawą działania firm, nowoczesnych systemów bezpieczeństwa oraz procesów technologicznych. Przeważnie wymagana jest nieprzerwana praca infrastruktury sieciowej, a odpowiedniej jakości ograniczniki przepięciowe są w stanie ochronić ją przed awarią i czasowym wyłączeniem.
4. Firma instalacyjna, która uwzględnia wszystkie zabezpieczenia przed przepięciami, jest ceniona jako profesjonalny wykonawca.

Bezkompromisowe zabezpieczenie sieci gigabitowych

Częste zapytania ze strony firm projektujących sieci strukturalne zobligowały firmę Ewimar do rozpoczęcia prac nad ogranicznikami pracującymi w sieciach 1000Base-T oraz 1000Base-TX. W sieciach LAN może występować wiele zakłóceń, które mogą powodować przerwy w transmisji lub jej spowalnianie. Najbardziej niekorzystne z nich to odbicia, tłumienia oraz przesłuchy międzykanałowe – w przypadku sieci 100Base-T są to dwa oddziaływania: para A na parę B i para B na parę A. W standardzie 1000Base-T wykorzystywane są cztery pary transmisyjne, przy czym każda para oddziaływuje na każdą inną – łącznie jest 12 przypadków oddziaływania. Te i inne czynniki powodują, że wykonanie urządzenia ochronnego dostosowanego do sieci 1 Gbit jest o wiele trudniejsze i bardziej kosztowne od wykonania równie dobrego produktu dla sieci 100 Mbit.

Prace nad urządzeniami chroniącymi Gigabit Ethernet trwały w firmie Ewimar ponad półto-



Fot. 2. Przykład montażu modułów z serii PTU i PTF w jednej obudowie

Fot. 3. Widok 16-kanałowego ogranicznika z przodu

ra roku i obejmowały szereg symulacji zjawisk fizycznych występujących w projektowanych obwodach, a także wiele obliczeń i badań wytrzymałościowych. Dzięki skrupulatnej analizie wyników udało się dobrać optymalne parametry obwodów i technologię wytwarzania płyt PCB, a także przeprowadzono selekcję komponentów, które będą mieć odpowiednią wytrzymałość udarową i jednocześnie znikomy wpływ na degradację sygnałów.

Zastosowanie wielowarstwowych płyt PCB z bardzo grubą warstwą miedzi i zapewnienie jak najlepszego sprzężenia par symetrycznych wymagało specjalnego procesu ich wytwarzania, z procedurą kontroli impedancji, czemu mogli sprostać tylko nieliczni spośród producentów obwodów drukowanych.

Dzięki powyższym zabiegom oraz bardzo wysokiej jakości komponentom, w tym gniazdom RJ-45 uzyskaliśmy znakomite parametry transmisyjne, które są zdecydowanie lepsze niż parametry urządzeń firm konkurencyjnych. Testy wykonane za pomocą certyfikowanych testerów LAN potwierdziły, że spośród dwunastu testowanych urządzeń kilku wiodących producentów jedynie produkty firmy Ewimar całkowicie spełniły wymagania dotyczące kabli kategorii 6, natomiast niektóre spośród konkurencyjnych produktów nie zostały na podstawie testów zaliczone nawet do kabli kategorii 5e. Wszystkie testy wykonano identycznie, poprzez bezpośrednie podłączenie ograniczników do interfejsów testera.

Komponenty MOSFET, które firma Ewimar wykorzystuje z powodzeniem od kilku lat, umożliwiły uzyskanie bardzo niskiego napięciowego poziomu ochrony Up, który jest niewiele wyższy od znamionowego napięcia pracy Uc (maksymalne napięcie, jakie dotrze do chronionego urządzenia przy maksymalnym poziomie udaru). Oznacza to bardzo wysoką skuteczność ochrony. Ponadto komponenty MOSFET stanowią czasową izolację o wytrzymałości od 650 V do 850 V pomiędzy poszczególnymi urządzeniami LAN. Ogranicza to ryzyko przebicia transformatorów izolujących warstwy fizycznej urządzeń, zasilanych z różnych źródeł lub lokalnie uziemionych.

W najczęściej stosowanej sieci Gigabit 1000Base-T – wykorzystuje się kodowanie PAM-5 i częstotliwość taktowania 125 MHz, dlatego wystarczą przewody kategorii 5e (a nawet kategorii 5). Czy konieczne są ograniczniki do przewodów kategorii 6? Tak samo konieczne, jak konieczne jest stosowanie ekranowanych przewodów kategorii 6 w dużych infrastrukturach sieciowych. W rozproszonych instalacjach interferuje ze sobą niewiele sygnałów, natomiast na trasach kablowych i w rackach może zbiegać się nawet kilkaset przewodów. Nałożenie się dużej liczby sygnałów cyfrowych generuje tak wiele zakłóceń interferencyjnych, że bez odpowiedniego zapasu jakościowego sieć LAN nie będzie funkcjonować poprawnie. Stosując wielokanałowe ograniczniki firmy Ewimar montowane w racku, mamy pewność, że dzięki ich wysokiej jakości sieć LAN będzie działać stabilnie.

Fot. 4. Ogranicznik 1-kanałowy PTF-61-EXT/PoE

Na szczególną uwagę zasługują specjalne rozwiązania służące do ochrony przed przepięciami i niekontrolowanym wzrostem napięcia w kablach, za pośrednictwem których urządzenia są zasilane metodą PoE. Zabezpieczenia te chronią przełączniki sieciowe oraz zasilacze urządzeń końcowych przed uszkodzeniem. Obsługują one każdy dostępny standard PoE, włącznie z Hi PoE.

Aktualny asortyment urządzeń do sieci Gigabit Ethernet obejmuje trzy produkty, które wykazują odporność udarową do 2 kA na każdą żyłę przewodu:

1. PTF-61-EXT/PoE – 1-kanałowy ogranicznik instalowany przy urządzeniach końcowych, produkowany jako wolnostojący lub przykręcany do ściany, zapewniający również ciągłość ekranowania.
2. Moduł PTF-64-EXT/PoE – 4-kanałowy moduł z gniazdami RJ-45 po stronie wejściowej i wyjściowej, montowany w nowo skonstruowanym racku 19". Jest w nim miejsce dla czterech modułów tego samego typu lub różnych typów.
3. Moduł PTU-64-EXT/PoE – 4-kanałowy moduł z gniazdami RJ-45 po stronie wyjściowej i złączami LSA (dawniej Krone) po stronie wejścia. Takie rozwiązanie upraszcza instalację i obniża koszty ze względu na możliwość bezpośredniego zaszycia przewodów LAN na ogranicznikach. Moduły mają obejmy do przewodów ekranowanych, więc właściwości przewodu FTP są wykorzystane w pełni. Moduły montowane są również w nowym racku.

Nowe oblicze ograniczników przepięć do sieci LAN 100 Mbit

Dzięki doświadczeniom zdobytym podczas budowy urządzeń do sieci Gigabit Ethernet całkowicie od podstaw została zbudowana nowa seria urządzeń dostosowanych do sieci 100 Mbit. Korzystając z identycznych sposobów symulacji i testowania obwodów, stworzyliśmy serię urządzeń o znacznie lepszych parametrach udarowych oraz transmisyjnych. Uwzględniliśmy również wiele uwag instalatorów i projektantów, dotyczących zarówno elektroniki, jak i mechaniki. Docelowo nowe produkty zastąpią dotychczasowe serie PTF-1, PTF-4 oraz PTU-4 i zdecydowanie poprawią jakość i stabilność transmisji sieciowej, zwłaszcza w bardzo dużych instalacjach.

W momencie ukazania się niniejszego artykułu powinny być już dostępne następujące produkty:

1. PTF-51-(ECO/PRO/EXT)/PoE – 1-kanałowe zabezpieczenia do ochrony kamer i innych punktów końcowych LAN.
2. PTF-54-(ECO/PRO/EXT)/PoE – moduły 4-kanałowe z gniazdami RJ-45 po obydwu stronach, instalowane w nowym racku.
3. PTU-54-(ECO/PRO/EXT)/PoE – moduły 4-kanałowe ze złączami LSA po stronie wejść i gniazdami RJ-45 po stronie wyjść. Nowością w porównaniu do poprzedniej wersji PTU jest kompatybilność z przewodami FTP i zachowanie ciągłości ekranu.

Mirosław Gondek
Ewimar
www.ewimar.pl

Ocena działań na rynku zabezpieczeń w 2018 roku

i ich potencjalny wpływ na aktywność w roku 2019

Ray Mauritsson

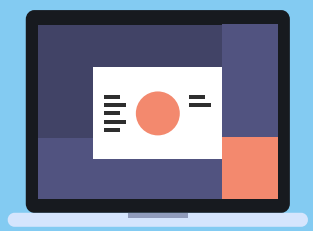
Chociaż Axis Communications jest firmą, która stara się patrzeć w przyszłość, czasami warto zrobić przerwę, żeby pomyśleć o niedalekiej przeszłości. Zakończył się rok 2018, nadszedł właściwy czas na to, by przyjrzeć się niektórym spośród najbardziej znaczących zeszłorocznych działań i trendów, które ukształtowały branżę zabezpieczeń i które, jak sądzimy, będą miały na nią wpływ także w roku 2019 i później

Rozwój i konsolidacja

Szybkość zmian w branży zabezpieczeń nadal rośnie. Firma Axis Communications powstała w połowie lat 80. ubiegłego wieku, a stworzyła pierwszą na świecie kamerę sieciową zaledwie 20 lat temu. W ciągu tylko dwóch dekad nastąpiło niemal całkowite zastąpienie produkowanych wcześniej urządzeń analogowych urządzeniami cyfrowymi. Kamery są coraz lepsze, ich jakość i wydajność poprawia się wykładniczo, a potencjał sztucznej inteligencji i tzw. głębokiego uczenia się przez maszyny lub systemy stworzy możliwości innowacji, o których nam się nie śniło. Takie tempo zmian obarcza wymaganiami rynkowych graczy, którzy muszą za nimi nadążyć. Wielu z nich chce rozszerzyć swoją ofertę lub działalność międzynarodową poprzez przejęcie innych firm.

Jednym z przykładów może być przejęcie Avigilonu przez Motorolę na początku roku [2018 – przyp. red.], a wcześniej dodanie przez nią funkcji nadzoru wizyjnego do dotychczas oferowanych urządzeń radiokomunikacyjnych stosowanych w sektorze bezpieczeństwa publicznego. Ostatnio firma UTC – najbardziej znana jako producent systemów chłodniczych, ogrzewania, wentylacji i klimatyzacji – zakończyła proces wykupu S2 Security.

Nie należy oczekiwać spowolnienia konsolidacji firm w 2019 roku, gdyż coraz więcej z nich dostrzega, że bogatszy asortyment to sposób na rozwój, a przejęcie może być sposobem na szybsze wprowadzenie innowacji aniżeli rozwój w obrębie jednego przedsiębiorstwa, o ile wyzwania związane z połączeniem dwóch firm, które mają różne struktury, dorobki i specyfiki, zostaną szybko przezwyciężone. Chociaż fuzje i przejęcia mogą szybko pomóc organizacjom rozszerzyć ich oferty, połączenie osobnych produktów w jedno spójne rozwiązanie może stać się dodatkowym wyzwaniem. Niezwykły rozwój rozwiązań technicznych przeznaczonych na rynek konsumencki, jaki nastąpił w ostatnich dwóch



dekadach, ma wpływ na oczekiwania dotyczące zdobyczy techniki wykorzystywanych w biznesie. Łatwość użycia i zarządzania są szczególnie ważne. W końcu dlaczego ktoś miałby oczekiwać, że zabezpieczenia będą trudniejsze w użyciu niż telefon komórkowy? Istotne są również parametry użytkowe systemu, sposób instalacji, wzornictwo i intuicyjny interfejs.

Ograniczenie i ochrona prywatności

Nie sposób zignorować widocznego w ostatnich 12 miesiącach zwiększonego nacisku na zachowanie prywatności, zwłaszcza w odniesieniu do danych osobowych. Uderzające jest uwydatnienie się kulturowych i geograficznych różnic w postawach i podejściach do tego tematu – zarówno pozytywnych, jak i negatywnych.

W Europie nacisk na ochronę danych osobowych jest prawdopodobnie największy. Nie jest to zaskakujące, gdyż to właśnie Parlament Europejski stworzył najbardziej rygorystyczne na świecie regulacje, zawarte w rozporządzeniu o ochronie danych osobowych (RODO), które określają, jak dane osobowe mogą być gromadzone, przetwarzane, przechowywane, udostępniane i używane. Ponieważ każda firma z branży zabezpieczeń, która jest w posiadaniu danych osobowych obywateli Unii Europejskiej, będzie oczywiście musiała przestrzegać RODO, regulacje będą miały konkretne skutki dla tych, którzy korzystają z nadzoru wizyjnego (o czym można przeczytać w naszej białej księdze).

Poza Europą postawy są inne. Na przykład w USA jest, jak się zdaje, większe zainteresowanie cyberbezpieczeństwem niż prywatnością, przynajmniej w porównaniu z Europą. Obywatele USA są bardziej skłonni udostępniać swoje dane osobowe (o ile są pewni, że firmy, które je przechowują, zabezpieczą je przed cyberprzestępcami) i zezwalać na dostęp do nich organom rządowym. Finansowany przez państwo program nadzorczy PRISM, który za zgodą sądu umożliwia Agencji Bezpieczeństwa Narodowego (NSA) dostęp do danych osobowych gromadzonych przez firmy działające w Internecie, prawdopodobnie spowodowałby oburzenie, gdyby został wprowadzony w Europie.

Te odmienne pod wieloma względami podejścia wskazują na różnice w priorytetach. Po prostu w USA kładzie się nacisk na ochronę państwa, a w Europie najważniejsza jest ochrona jednostki. W innych regionach i krajach świata – od Kanady po Chiny, od Brazylii po Rosję – postawy, działania i prawa także się różnią. Podejścia są zróżnicowane bardziej niż kiedykolwiek wcześniej – przynajmniej w tej dziedzinie nastąpiła regionalizacja, a nie globalizacja.

Wzrost podatności na cyberataki

Niestety nigdy nie przestaniemy poruszać kwestii cyberbezpieczeństwa. Magazyn *Wired UK* opisuje wiele naruszeń bezpieczeństwa, a są to tylko te najbardziej znane, dotyczące ogólnodostępnych danych. Faktem jest, że bardzo dobrze finansowani, wprawni i zorganizowani cyberprzestępcy wprowadzają innowacje w takim tempie, że trudno za nimi nadążyć (zwłaszcza że nie są skrępowani żadnymi krajowymi czy regionalnymi przepisami). Ponadto jest coraz więcej dowodów na to, że niektóre państwa przeprowadzają wyrafinowane cyberataki wymierzone w inne państwa, organizacje handlowe i publiczne oraz infrastrukturę krytyczną.

Zwiększa się liczba połączeń między urządzeniami, które mogą być również punktami końcowymi systemów i poprzez które cyberprzestępcy mogą próbować uzyskać dostęp do tych systemów i zgromadzonych w nich danych. Bez efektywnych środków zabezpieczających przed cyberatakami poprzez któreś z połączonych urządzeń – drukarkę, inteligentne urządzenie domowe czy kamerę sieciową – może nastąpić wtargnięcie do systemu. Z kolei w związku z niepokojącymi dowodami na to, że urządzenia wytwarzane

w niektórych krajach są infekowane już na etapie produkcji, znajomość pochodzenia wszystkich urządzeń, które podłącza się do systemów, jest niezbędna.

Konsekwencje etyczne

Wygląda na to, że będziemy żyć w świecie, w którym będzie się próbowało uzyskać finansowany przez państwo wzmożony nadzór – na większych obszarach i w większej liczbie państw niż kiedykolwiek wcześniej. To coraz ważniejsza kwestia, która powinna być wysoko na liście priorytetów wszystkich firm, zwłaszcza tych z branży zabezpieczeń (i każdej organizacji, która kupuje produkty od tych firm). Każda organizacja powinna wyraźnie określić, jakiego wykorzystania swoich produktów oczekuje (chodzi zarówno o aspekt techniczny, jak i etyczny). Powinna informować swoich partnerów i prowadzić działania marketingowe, żeby uczynić to jasnym. W niektórych przypadkach może to oznaczać także podjęcie decyzji o tym, komu produkty zostaną sprzedane i (co ważniejsze) komu nie zostaną sprzedane, jeżeli nie ma pewności, że ich wykorzystanie nie przekroczy etycznych granic wyznaczonych przez producenta.

Technika przyniosła ogromne korzyści społeczeństwu i nadal je przynosi. Firma Axis Communications wierzy, że jej wizja lepszego i bezpieczniejszego świata urzeczywistni się właśnie dzięki postępowi w dziedzinie techniki. W związku z innowacjami i postępem – zwłaszcza w takich dziedzinach jak sztuczna inteligencja i uczenie się przez maszyny lub systemy – kwestie etyczne jeszcze bardziej zyskają na znaczeniu. Samo to, że możemy coś zrobić, nie zawsze oznacza, że powinniśmy. Czy jednak każda organizacja ma niezbędne narzędzia kontroli i rozstrzyga kwestie natury etycznej? To sprawa wewnętrzna każdej z nich, jednak wspieranie takich inicjatyw jak *The Copenhagen Letter* jest ważnym publicznym obowiązkiem.

Zaufanie

Zaufanie zawsze było jednym z najważniejszych aspektów relacji biznesowej, ale tradycyjnie to, co o nim przesądzało, było bardziej namacalne, konkretne – mogło to być dostarczenie czegoś w terminie, za uzgodnioną cenę. Można jednak dostrzec, że bardziej „miękkie" wyznaczniki zaufania wysuwają się na pierwszy plan. Tak jest dziś i z pewnością było tak w minionym roku. Ważne jest na przykład to, czy mogę Ci zaufać, by powierzyć Ci swoje dane, czy wyznajemy podobne wartości, czy popierasz firmy lub kraje, których metody działania są uczciwe i przyzwoite itd.

Bycie godnym zaufania będzie coraz częściej postrzegane jako szczególnie istotny atut, jako coś o rzeczywistej wartości, podobnie jak aktywa firmy. Z pewnością oczywiste nadużycie zaufania wpływa niekorzystnie na wartość i wyniki firmy. W biznesie nie ma przerw, ale koniec jednego roku i początek następnego jest dobrym momentem na refleksję i planowanie. Chociaż powitałem rok 2019, wiedząc, że pojawią się nowe i nieprzewidziane wyzwania, którym trzeba będzie sprostać, jestem nastawiony optymistycznie. Mam pewność, że ogromna większość ludzi, organizacji i rządów podziela nasz pogląd, że możemy sprawić, że świat będzie lepszym i bezpieczniejszym miejscem dla każdego.

Ray Mauritsson
Axis Communications
Tłumaczenie: Paweł Karczmarzyk

Nowoczesne zamki sejfowe

Jarosław Marciniak

Obecnie przechowywanie gotówki, dokumentów i rzeczy wartościowych to już nie tylko trzymanie ich pod kluczem. Powinno ono być rozpatrywane jako proces operacyjny wspomagany najnowszymi technikami

Takie rozwiązanie wymusza intensyfikacja obrotu gotówką, a także rozwój nowych form i organizacji handlu. Nowe techniki dają możliwość poprawy jakości życia i pracy. Powinno się uwzględniać wpływ czynnika ludzkiego, indywidualne procedury operacyjne, ochronę pracowników, politykę prywatności i wiele innych aspektów charakterystycznych dla danej branży i podmiotu gospodarczego.

Od przeszło 20 lat obserwujemy rozwój zamków sejfowych. W 2013 roku rozpoczęliśmy pionierski projekt wymiany zamków kluczowych na elektroniczne, dostarczone przez firmę Lock4Safe z Limburgii, w sieci obiektów usytuowanych na terenie całej Polski. Wszystkie prace były prowadzone u klientów podczas normalnego działania sejfu. W krótkim czasie po instalacji dział IT mógł rozpocząć centralne zarządzanie sejfami poprzez sieć internetową.

Zamki są dostępne w wersjach HOME, BUSINESS i PROFESSIONAL. Wszystkie zamki szyfrowe, które oferujemy na polskim rynku, są przeznaczone do sejfów, które dotychczas były otwierane za pomocą kluczy. Zamki z linii HOME są przeznaczone do zainstalowania w sejfach domowych i biurowych. Użytkownik może wybrać odpowiadający mu produkt spośród zamków różniących się funkcjami i rozwiązaniami technicznymi.

Fot. 1. Zamki z linii HOME

Fot. 2. Zamki z linii BUSINESS

Fot. 3. Zestaw PROFESSIONAL

W przypadku przedsiębiorstwa należy zastanowić się, jakie ryzyko wiąże się z przechowywaniem gotówki w sejfie, jakie są koszty zabezpieczenia, jak zrównoważyć sprawne funkcjonowanie firmy i bezpieczeństwo, a także nad tym, czy istnieją dziedziny, w których warto przekazać odpowiedzialność pracownikom. Dla firm przeznaczone są zamki z linii BUSINESS.

Linia PROFESSIONAL to zamki przeznaczone do pracy w sieci. Praca zamka podlega stałemu nadzorowi, przy czym możliwe jest też dokonywanie ustawień. Dodatkowo zamki mogą być otwierane **jednorazowymi kodami dynamicznymi**, ważnymi tylko w przypadku określonej osoby i w określonym przedziale czasowym.

Główne korzyści wynikające z zastosowania systemu tych zamków to:

1. Wysoki poziom bezpieczeństwa. Pracownik używa sześciocyfrowego kodu osobistego, który w każdej chwili może być zmieniony. Kody użytkowników mogą być blokowane lub usuwane przez menedżerów.
2. Redukcja kosztów. Poważne problemy związane z obsługą kluczy zostają całkowicie wyeliminowane. Nie ma kosztów usług i zarządzania kluczami. Nie ma już problemu wynikającego ze złamania albo zgubienia klucza.
3. Możliwość określenia procedury wyznaczania osoby odpowiedzialnej za gotówkę. Zmiana osoby, która ma być odpowiedzialna za gotówkę, odbywa się zgodnie z ustaloną i wdrożoną procedurą. Nie można podać kodu nieupoważnionemu pracownikowi i poprosić go o otworzenie sejfu. Nie można też przekazać kodu kierownikowi następnej zmiany.
4. Możliwość kontroli (przeprowadzenia audytu). Dzienniki dotyczące otwarć, zmiany kodów i innych czynności są przechowywane w pamięci zamka i mogą być odczytane w centrum zarządzania.
5. Możliwość podłączenia zamka do systemu alarmowego obiektu. Pracownicy mogą wyzwolić cichy alarm w przypadku zagrożenia. Możliwe jest zdalne zablokowanie zamka przez system alarmowy.
6. Możliwość zastosowania programów czasowych. Poza godzinami otwarcia sklepu można uniemożliwić dostęp do sejfu wybranym lub wszystkim pracownikom. Nawet po wprowadzeniu poprawnego kodu otwarcie zamka nie będzie możliwe.
7. Możliwość wskazania osoby odpowiedzialnej za sejf. W godzinach roboczych jedna osoba jest odpowiedzialna za sejf. Po pracy pracownik jest całkowicie zwolniony z tej odpowiedzialności, a więc również wolny od wszelkich podejrzeń.

Firmy i osoby zainteresowane nawiązaniem współpracy zachęcamy do bezpośredniego kontaktu z nami. Chętnie zademonstrujemy możliwości zamków elektronicznych wszystkim zainteresowanym.

Jarosław Marciniak

Selprima
ul. Kazachska 1/20
02-999 Warszawa
www.selprima.pl
tech@selprima.pl
tel.: +48 513 756 202

NOVUS®

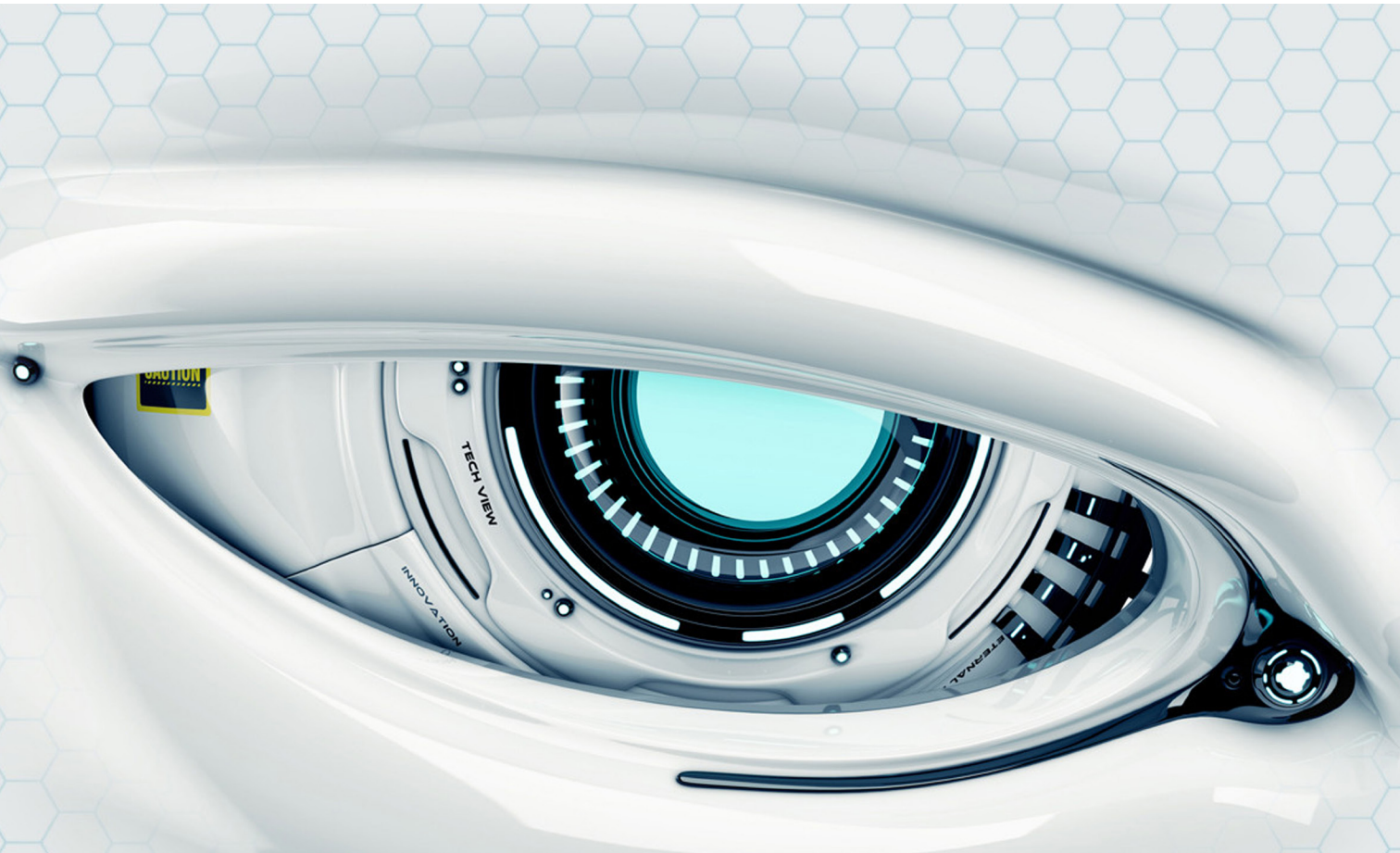
3000 SERIA IP • 6000 SERIA IP

NOVUS IP · NMS Compatible · ONVIF

SKUTECZNE ROZPOZNAWANIE TWARZY

W REJESTRATORACH SERII 6000 W POŁĄCZENIU Z KAMERAMI SERII 3000

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



AI dla każdego.

Część 1

Piotr Rogalewski

Branża zabezpieczeń od dawna czerpie pełnymi garściami z IT. Z każdym rokiem granica między rozwiązaniami z dziedziny IT i z dziedziny zabezpieczeń staje się coraz bardziej zatarta i nic w tym dziwnego, bo znaczna część urządzeń na rynku zabezpieczeń to w istocie mniej lub bardziej zminiaturyzowane komputery, a chyba trudno obecnie o bardziej fascynujące zastosowanie komputerów niż rozwój sztucznej inteligencji. Proponuję lekturę całego cyklu artykułów na ten temat. Czego będzie można się z nich dowiedzieć?

Między innymi tego, czym jest szeroko rozumiana sztuczna inteligencja, jak ewoluowały rozwiązania leżące u jej podstaw, jakie są przykładowe rodzaje konkretnych systemów wykorzystujących sztuczną inteligencję, co to jest deep learning, jak działają sieci neuronowe, jakie są i mogą być praktyczne zastosowania systemów wykorzystujących sztuczną inteligencję, a także jakie zagrożenia mogą one spowodować. Cykl artykułów będzie napisany językiem prostym, bez skomplikowanej nomenklatury matematycznej, bez odwoływania się do funkcji różniczkowalnych czy teorii zbiorów rozmytych. Trochę matematyki będzie, wszak to królowa nauk i bez niej sztuczna inteligencja by nie powstała. Obiecuję jednak, że wstawki matematyczne będą minimalne, a wszystko krok po kroku i bardzo dokładnie wyjaśnię. Nadrzędnym celem artykułów jest odczarowanie sztucznej inteligencji, konsolidacja wiedzy w tym zakresie i przekazanie jej w formie przystępnej dla każdego

Nazwy i slogany

W świecie techniki, a szczególnie technik informacyjnych (IT), jest moda na slogany, podchwytywane natychmiast przez specjalistów od marketingu. A że moda, jak wiadomo, ulega ciągłym zmianom, również slogany się zmieniają.

W latach 80. na początku dynamicznego rozwoju mikroprocesorów mieliśmy modę na mikroprocesorowe centrale telefoniczne, regulatory temperatury, sterowniki czy prostowniki samochodowe. Gdy komputery upowszechniły się na dobre przyszła kolej na slogany komputerowe. Pojawiło się zatem komputerowe wspomaganie projektowania, badanie wzroku, badanie pojazdów czy projektowanie kuchni.

Najnowszy krzyk mody to „inteligentne" rzeczy. Mamy więc smartfony ze sztuczną inteligencją, inteligentne systemy zarządzania ruchem, inteligentne odkurzacze, oświetlenie, meble, domy, a w naszej branży np. kamery IP i rejestratory. W wielu przypadkach mamy do czynienia ze zwykłymi marketingowymi frazesami, jednak szeroko rozumiana sztuczna inteligencja jest jedną z dziedzin nauki i techniki, która faktycznie całkowicie zmieni świat, jaki znamy. Zmiany rozpoczęły się już dawno.

Zacznijmy od uporządkowania nazewnictwa i definicji. W artykułach niniejszego cyklu będę zamiennie używał nazwy s*ztuczna inteligencja* i angielskiego skrótowca *AI* pochodzącego od terminu *artificial intelligence*. Czym jest sztuczna inteligencja? Zacznijmy może od inteligencji sensu *stricto*.

Fot. 1. Pomnik Alana Turinga w Bletchley Park (fot.: Jon Callas, San Jose, USA)

Naturalna inteligencja

Miało być łatwo i przyjemnie, a już na początku pojawia się pewien problem. Otóż nie ma jednej, uniwersalnej definicji inteligencji. Jest to pojęcie tak szerokie, iż nie można stworzyć nawet jednej, spójnej kategorii zjawisk i procesów, które można by przypisać do inteligencji. Mówi się o inteligencji emocjonalnej, kognitywnej (abstrakcyjnej), werbalnej, społecznej itd. Nawet standardowe testy psychometryczne na iloraz inteligencji (IQ) sami naukowcy uznają za kontrowersyjne, bo umożliwiają one ocenę zaledwie bardzo niewielkiej części spektrum inteligencji jako sprawności umysłowej.

Dokonam pewnego uproszczenia i połączę dwie definicje inteligencji zaproponowane przez psychologów – Williama Sterna i G. A. Fergusona. Pierwszy z nich zdefiniował inteligencję jako umiejętność przystosowania się do nowych warunków przez wykorzystanie dostępnych środków poznawczych[1]. Drugi postulował, że to zdolność do uczenia się[2]. Przyjmijmy więc, że inteligencja to zdolność do uczenia się z wykorzystaniem dostępnych źródeł wiedzy oraz zdolność do przystosowania się do różnych, nawet nieprzewidzianych wcześniej sytuacji. Zdolność adaptacyjna wynika tu wprost z nauki. Taka definicja bardzo dobrze nadaje się m.in. do opisania procesów uczenia maszynowego, o czym przekonamy się już niebawem.

Sztuczna inteligencja

Za ojca sztucznej inteligencji uważa się Alana Turinga – brytyjskiego kryptologa i matematyka. Jego praca *On computable numbers (O liczbach obliczalnych)*[3] z 1936 r. była punktem odniesienia przy definiowaniu algorytmu komputerowego i kamieniem węgielnym informatyki.

W 1950 r. Turing postawił pytanie: „Czy maszyna jest zdolna do zachowań inteligentnych?"[4]. Aby znalezienie odpowiedzi było łatwiejsze, matematyk opracował prosty test – grę, w której bierze udział przynajmniej trzech graczy: człowiek-sędzia oraz dwaj rozmówcy – maszyna i drugi człowiek. Zadaniem sędziego (testera) jest ustalenie na podstawie dialogu, prowadzonego w języku naturalnym, który z rozmówców jest maszyną, a który człowiekiem. Brak możliwości wydania przez sędziego jednoznacznego werdyktu oznacza pozytywny wynik testu – maszyna jest uznawana za zdolną do inteligentnej komunikacji. Ta procedura to test Turinga[5]. Do jego przeprowadzenia wymaga się teraz obecności wielu sędziów. Maszyna przejdzie test pomyślnie, jeżeli uzna ją za człowieka przynajmniej 30% sędziów. Pozytywny wynik testu Turinga udało się maszynie uzyskać dopiero 7 czerwca 2014 roku, dokładnie 60 lat po śmierci słynnego matematyka[6].

Pojęcie sztucznej inteligencji wprowadził w 1956 r. podczas konferencji w Dartmouth[7] amerykański informatyk i matematyk John McCarthy[8], późniejszy laureat Nagrody Turinga[9] przyznawanej za wybitne osiągnięcia w dziedzinie informatyki.

Sztuczną inteligencję jest trudno zdefiniować, podobnie jak naturalną. Ma ona związek z wieloma dziedzinami, m.in. logiką rozmytą (teorią zbiorów rozmytych), obliczeniami ewolucyjnymi, sieciami neuronowymi, głębokim uczeniem (ang. *deep learning*), informatyką, robotyką. Tak jak w przypadku definicji inteligencji naturalnej, proponuję uproszczenie definicji AI. Działanie sztucznej inteligencji opiera się w głównej mierze na pracy komputerów i oprogramowania, a udział informatyki w tym procesie jest największy. Zdefiniujmy zatem sztuczną inteligencję jako dziedzinę informatyki zajmującą się tworzeniem rozwiązań technicznych naśladujących zachowania wynikające z inteligencji naturalnej.

Początki

Podstawy matematyczne sztucznej inteligencji zostały stworzone na długo przed pierwszymi praktycznymi realizacjami. Po pracach Alana Turinga pierwszy matematyczny model ludzkiego neuronu opracowali w 1947 r. neurofizjolog Warren McCulloch i matematyk Walter Pits. Model ten, od nazwisk uczonych, zwany jest modelem McCullocha-Pitsa[10] i stał się on teoretycznym fundamentem sztucznych sieci neuronowych. Często określany jest też jako sztuczny neuron lub perceptron[11].

Pierwsze próby utworzenia inteligentnych systemów miały miejsce dopiero dekadę po powstaniu modelu McCullocha-Pitsa. W 1966 r. Joseph Weizenbaum z Massachusetts Institute of Technology (MIT) stworzył program komputerowy ELIZA

Fot. 2. Asimo firmy Honda – pierwszy autonomiczny robot chodzący (fot.: Honda Motor Co., Ltd.)

posługujący się językiem skryptowym i udający prawdziwego rozmówcę. Tego typu program jest nazywany czatbotem. Najbardziej znany skrypt ELIZY to DOCTOR, który wcielał się w rolę psychoterapeuty[12]. Była to jedna z pierwszych prób stworzenia procesora języka naturalnego. Algorytm programu był stosunkowo prosty i bazował na technice dopasowania do wzorców i generowaniu pytań na podstawie treści wprowadzanych przez użytkownika. Nie posiadał on żadnych zaawansowanych mechanizmów analizy kontekstu, jednak mimo tego radził sobie całkiem dobrze jak na swoje czasy. Fragment przykładowej konwersacji między czatbotem, a studentką:

***ELIZA**: Czy coś Cię trapi?*
***Człowiek**: Mój chłopak mnie tu przyprowadził.*
***ELIZA**: Czy to jest dla Ciebie ważne, że Twój chłopak Cię tu przyprowadził?*
***Człowiek**: On mówi, że jestem przygnębiona przez większość czasu.*
***ELIZA**: Przykro mi słyszeć, że jesteś przygnębiona.*
***Człowiek**: To prawda, jestem nieszczęśliwa.*
***ELIZA**: Czy myślisz, że przyjście tutaj pomoże Ci przestać być nieszczęśliwą?*

ELIZA była bardzo zręcznym rozwiązaniem dającym iluzję inteligencji, jednak była pozbawiona najistotniejszego elementu AI – nie potrafiła się uczyć, a w celu zdemaskowania faktu, że jest programem komputerowym, wystarczyło zadać pojedyncze, nietypowe pytanie lub zmienić wątek podczas konwersacji.

Rozwój

Dynamiczny rozwój sztucznej inteligencji stał się możliwy dzięki coraz lepszym komputerom. Coraz szybsze procesory i coraz większa moc obliczeniowa umożliwiały realizację coraz bardziej złożonych zadań. Ostatnią dekadę XX w. i początek nowego tysiąclecia można uznać za okres przełomowy.

11 maja 1997 r. – wynikiem 3 ½ do 2 ½ – superkomputer IBM Deep Blue wygrywa mecz szachowy z mistrzem świata Garrim Kasparowem. Wprawdzie inżynierowie z firmy IBM modyfikowali oprogramowanie w trakcie meczu, w przerwach między partiami, i pojawiło się też kilka innych kontrowersji, jednak sam Kasparow mówił w późniejszych wywiadach o czynniku ludzkim, jaki momentami dostrzegał w grze komputera[13].

31 października 2000 r., po 18 latach pracy, firma Honda zaprezentowała Asimo – humanoidalnego robota poruszającego się na wzór człowieka. Był to pierwszy i najbardziej zaawansowany technicznie autonomiczny robot chodzący, wykorzystujący m.in. algorytmy symulujące pracę elementów

ludzkiego rdzenia kręgowego. Projekt Asimo rozwijany jest do dziś. Obecnie robot potrafi m.in. biegać, chodzić po nierównej powierzchni, skakać na jednej nodze, płynnie komunikować się głosowo z ludźmi, a nawet dyrygować orkiestrą[14].

16 lutego 2011 r., po trzydniowej rozgrywce, superkomputer IBM Watson wygrał w amerykańskim teleturnieju *Jeopardy!* (polski odpowiednik to *Va banque*) z ówczesnymi mistrzami tej zabawy – Bradem Rutterem i Kenem Jenningsem[15]. Komputer wykorzystywał najnowsze algorytmy przetwarzania języka naturalnego i rozpoznawania mowy. W trakcie rozgrywki komunikowano się z nim dokładnie tak samo jak z pozostałymi uczestnikami. Wygrane przez Watsona pieniądze przekazano w całości na cele charytatywne.

7 czerwca 2014 r., w 60. rocznicę śmierci Alana Turinga, czatbot Eugene Goostman jako pierwszy w historii osiągnął pozytywny wynik testu Turinga, przekonawszy 30 sędziów, że jest 13-letnim chłopcem. Niektórzy kwestionują wynik testu, gdyż czatbot sprytnie maskował swoje słabe strony humorystycznymi odpowiedziami[16].

15 marca 2016 r. program komputerowy AlphaGo do gry w go, uznawanej za najtrudniejszą grę świata, pokonał po pięciu rundach koreańskiego mistrza – Lee Sedola. AlphaGo wykorzystuje kombinację technik głębokiego uczenia i przechodzenia drzewa (więcej o tym w kolejnych artykułach)[17].

Mam nadzieję, że podstawowe definicje, trochę historii i kilka ciekawostek ze świata sztucznej inteligencji zachęciło Czytelników do lektury kolejnych części cyklu, w których przedstawię konkretne systemy wykorzystujące sztuczną inteligencję – także te, które są od niedawna wykorzystywane w branży zabezpieczeń.

Piotr Rogalewski

Bibliografia

1. J. T. Lamiell, *William Stern (1871-1938): A Brief Introduction to His Life and Works*, Pabst Science Publishers, Langerich 2010.
2. G. A. Ferguson, *On learning and human ability*, (w:) „Canadian Journal of Psychology", nr 8/1954.
3. A. M. Turing, *On Computable Numbers, with Application to the Entscheidungsproblem, (w:) Proceedings of the London Mathematical Society*, seria 2, wol. 42, Londyn 1937.
4. A. M. Turing, *Computing Machinery and Intelligence*, (w:) „Mind", nr LIX (236)/1950.
5. G. Oppy, D. Dowe, *The Turing Test, (w:) Stanford Encyclopedia of Philosophy*, Stanford 2003.
6. J. Schofield, *Computer chatbot 'Eugene Goostman' passes the Turing test*, https://www.zdnet.com/article/computer-chatbot-eugene-goostman-passes-the-turing-test, data wyświetlenia: 27.12.2018.
7. J. Moor, *The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years*, (w:) „AI Magazine", nr 4/2006.
8. https://en.wikipedia.org/wiki/John_McCarthy_(computer_scientist), data wyświetlenia: 27.12.2018.
9. https://en.wikipedia.org/wiki/Turing_Award, data wyświetlenia: 27.12.2018.
10. W. McCulloch, W. Pitts, *A logical calculus of the ideas immanent in nervous activity*, (w:) „Bulletin of Mathematical Biophysics", nr 5/1943.
11. https://en.wikipedia.org/wiki/Perceptron, data wyświetlenia: 28.12.2018.
12. M. Baranovska, S. Höltgen, *Hello, I'm Eliza. Fünfzig Jahre Gespräche mit Computern*, Projekt Verlag, Bochum/Freiburg 2018.
13. Garri Kasparov, *Deep Thinking: Where Machine Intelligence Ends And Human Creativity Begins*, Perseus Books, Nowy Jork 2017.
14. http://asimo.honda.com, data wyświetlenia: 28.12.2018.
15. https://money.cnn.com/2011/01/13/technology/ibm_jeopardy_watson, data wyświetlenia: 29.12.2018.
16. https://en.wikipedia.org/wiki/Eugene_Goostman, data wyświetlenia: 27.12.2018, *Turing test success marks milestone in computing history*, http://www.reading.ac.uk/news-and-events/releases/PR583836.aspx, data wyświetlenia: 27.12.2018.
17. https://deepmind.com/research/alphago, data wyświetlenia: 29.12.2018.

Oprogramowanie AxxonSoft

Przykłady zastosowania

AxxonSoft

Firma AxxonSoft jest producentem wyspecjalizowanego oprogramowania do obsługi wizyjnych systemów dozorowych i w tej dziedzinie plasuje się w ścisłej czołówce światowej. Oprogramowanie AxxonSoft nie tylko umożliwia zarządzanie pracą kamer, rejestratorów i innych urządzeń wizyjnych, lecz także integrację różnych systemów zabezpieczających i ich obsługę z poziomu wspólnej platformy programowej. Zaawansowana technicznie inteligentna analiza treści obrazu pozwala na stosowanie oprogramowania AxxonSoft w systemach wspomagających handel detaliczny i inne gałęzie biznesu

obiektach jak muzea, dworce kolejowe i lotnicze, budynki biurowe itp., co przekłada się na poprawę bezpieczeństwa w przestrzeniach miejskich.

Oprogramowanie AxxonSoft oddaje do dyspozycji operatorów systemów wizyjnych liczne narzędzia ułatwiające im pracę. Możliwe jest interaktywne działanie z wykorzystaniem map miasta, na których wyświetlane są powiadomienia o wypadkach i incydentach z możliwością oceny sytuacji na obrazach z kamer. Dostępne są takie funkcje jak obsługa ściany wizyjnej, kompresja czasu, automatyczne sterowanie pracą kamer PTZ i wiele innych. Rozbudowane inteligentne funkcje do wyszukiwania wydarzeń w zgromadzonym materiale archiwalnym ułatwiają prowadzenie śledztw i dochodzenie przyczyn zaistniałych wypadków czy incydentów.

Oprogramowanie AxxonSoft jest szczególnie użyteczne w systemach nadzoru wizyjnego rozległych obszarów publicznych. Stwarza ono możliwość szybkiego wykrywania niebezpiecznych sytuacji w gęsto zaludnionych środowiskach miejskich oraz błyskawicznego podejmowania odpowiednich decyzji. Dzięki inteligentnym mechanizmom analizy materiału wizyjnego z wielu kamer możliwe jest rozpoznawanie i śledzenie osób w ruchu ulicznym, kontrolowanie ruchu pojazdów, tworzenie danych statystycznych pozwalających na usprawnienie funkcjonowania miasta.

Oprogramowanie AxxonSoft jest skalowalne i elastyczne. Może pobierać i przetwarzać dane z lokalnych systemów zabezpieczających w takich

Oprogramowanie AxxonSoft znajduje zastosowanie również w dużych obiektach budowlanych, takich jak galerie handlowe, hotele, wyższe uczelnie.

Przykładem pierwszego z takich obiektów jest Al Ain Mall w Abu Dhabi. Ze względu na lokalne przepisy budynek jest monitorowany nieprzerwanie, całodobowo i całotygodniowo. W systemie, w którym zastosowano 12 serwerów, rejestrowanych jest 744 strumieni wizyjnych pochodzących z odpowiednio rozmieszczonych kamer. Wykorzystane są inteligentne funkcje usprawniające handel detaliczny, takie jak wykrywanie tworzących się kolejek, zliczanie osób odwiedzających poszczególne sklepy, tworzenie map cieplnych. Kontrolowane są punkty kasowe w celu uniknięcia

„podarunków", czyli przenoszenia towarów przez punkty kasowe z pominięciem odczytu kodu kreskowego.

Drugim z przykładowych obiektów jest hotel Atlantis, The Palm, w Dubaju, który stanowi jedną z największych atrakcji turystycznych tego miasta. Ten nadmorski hotel o monstrualnych rozmiarach i wyszukanej stylistyce oferuje jedne z najbardziej luksusowych i najdroższych apartamentów na świecie. Odwiedza go rocznie około pół miliona gości. System AxxonSoft zastąpił zastosowany wcześniej, przestarzały system wizyjny, zainstalowany jeszcze podczas budowy hotelu. We wstępnym etapie modernizacji systemu firma AxxonSoft musiała sprostać konkurencji, którą stanowili niemal wszyscy liczący się na całym świecie dostawcy wizyjnych systemów dozorowych, jednak jej rozwiązania okazały się najlepsze i przebiły ofertę konkurencji. Zaważyły takie cechy systemu jak łatwy w obsłudze interfejs użytkownika, stabilność pracy i doskonałe wsparcie techniczne. Nie bez znaczenia była elastyczność systemu i możliwość jego łatwej integracji z zabezpieczeniami dostarczanymi przez innych producentów. W systemie zbudowanym z wykorzystaniem 16 serwerów rejestrowanych jest 2050 strumieni wizyjnych z kamer CCTV.

Trzecim z przykładowych obiektów jest Cambridge Trinity College w Wielkiej Brytanii. Jest to rozległy teren akademicki wypełniony zabytkowymi budynkami o różnym charakterze. Na szczególną uwagę zasługuje biblioteka i katedra, które stanowią wielką atrakcję dla osób zwiedzających uczelnię. Także ten prestiżowy obiekt został zabezpieczony przez firmę AxxonSoft. Zainstalowano tam ponad 100 kamer oraz uruchomiono zaawansowane technicznie funkcje analizy treści obrazu i rozpoznawania twarzy. Oprogramowanie AxxonSoft sprostało zadaniu zapewnienia bezpieczeństwa w tym ruchliwym, odwiedzanym przez setki tysięcy turystów obiekcie.

Na koniec warto wspomnieć o działalności firmy AxxonSoft na terenie Polski. Jedną z najnowszych instalacji firmy jest służący do monitorowania miasta Kraków wizyjny system dozorowy, w którym zastosowano sześć serwerów, rejestrujący obraz z 700 kamer i obejmujący swoim zasięgiem całą aglomerację. System jest stale rozbudowywany i w niedalekiej przyszłości osiągnie jeszcze większe rozmiary. W Krakowie nie tylko należało zapewnić bezpieczeństwo mieszkańcom oraz tłumnie odwiedzającym to zabytkowe miasto turystom, ale także rozwiązać problem plagi wandalizmu. Efektem chuligańskich wybryków pseudokibiców są znaczne zniszczenia dokonywane przy okazji meczów piłki nożnej. Dzięki rozbudowanym funkcjom analitycznym system AxxonSoft jest w stanie wesprzeć służby porządkowe i policję w walce z chuligaństwem i wandalizmem. Pełni on także rutynowe funkcje typowe dla dużych miast, to znaczy jest wykorzystywany do kontroli ruchu ulicznego i do szybkiego wykrywania niebezpiecznych zdarzeń i wypadków. Warto zwrócić uwagę zwłaszcza na funkcje analityczne, które umożliwiają gromadzenie metadanych z kamer obrotowych PTZ. Wszystko wskazuje na to, że dzięki rozwiązaniom w systemie Axxon NEXT poziom bezpieczeństwa obywateli oraz turystów odwiedzających Kraków znacznie się podniesie.

AxxonSoft
Opracowanie: Redakcja

axxonSOFT

EXPERIENCE THE NEXT®

OTWARTA PLATFORMA INTEGRUJĄCA SYSTEMY BEZPIECZEŃSTWA

Pobierz darmową wersję na axxonsoft.com/pl

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

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

Hala Koszyki
zabezpieczona przez systemy **Bosch**

Agnieszka Augustyniak

Hala Koszyki została wzniesiona w latach 1906-1908 przy ul. Koszykowej w Warszawie i przez ponad 100 lat była obiektem handlowym. Zlokalizowana w bogatej i inteligenckiej części miasta hala przetrwała do dziś pomimo licznych przemian społeczno-politycznych

Jesienią 2016 roku Halę Koszyki otwarto po gruntownej modernizacji i od razu stała się wyjątkowym punktem towarzyskim i kulinarnym Warszawy. Można tutaj zjeść potrawy charakterystyczne dla różnych krajów świata w kilkunastu restauracjach i barach, a także kupić produkty spożywcze. Po remoncie Hala Koszyki dołączyła do grupy podobnych obiektów funkcjonujących w innych miastach europejskich, np. w Londynie, Oslo, Rotterdamie czy Florencji, gdzie w halach targowo-restauracyjnych tętni życie i pod jednym dachem można zakosztować smaków z całego świata.

Taki obiekt wymaga kompleksowego zabezpieczenia. Bosch jako dostawca systemów zabezpieczających musiał uwzględnić następujące aspekty:

- wymagania estetyczne, które mają zapewniać klientom komfort,
- różnorodność chronionych miejsc (sklepy, kawiarnie, bary, restauracje, magazyny, parking, powierzchnie biurowe, serwerownie),
- kompleksowe procedury ewakuacji (duży budynek, ogromna liczba osób, które muszą być ewakuowane szybko i bezpiecznie),
- integracja różnych systemów bezpieczeństwa firmy Bosch i innych dostawców w celu zapewnienia maksymalnej ochrony obiektu.

– Jako Property Manager Hali Koszyki zwracam szczególną uwagę na systemy, które ułatwiają pracę osób odpowiedzialnych za bezpieczeństwo. Chcę mieć pewność, że nic nie umknie naszej uwadze. Jest to szczególnie ważne w miejscach, gdzie gromadzą się tłumy, coś się dzieje, a następnie trzeba odtworzyć materiał nagraniowy, znaleźć konkretną osobę lub sprawdzić, do kogo należy pozostawiony przedmiot. Nasz obiekt codziennie odwiedza wielu gości, organizujemy ogólnodostępne imprezy, przy czym nie weryfikujemy tożsamości odwiedzających. Przy takim założeniu nie możemy sobie pozwolić na to, aby osoby nieupoważnione miały dostęp do pomieszczeń technicznych czy też wynajętej powierzchni – powiedziała Sylwia Orzeł, Property Manager Hali Koszyki.

Hala Koszyki została wyposażona w systemy telewizji dozorowej, systemy sygnalizacji włamania i napadu, systemy kontroli dostępu. W obiekcie zainstalowano kamery obrotowe oraz stałopozycyjne. Kamery obrotowe skutecznie obserwują rozlegle powierzchnie, takie jak patio przed halą od ul. Koszykowej, natomiast kamery stałopozycyjne zamontowano w miejscach wymagających identyfikacji osób i zdarzeń. W kluczowych miejscach w obiekcie zastosowano kamery dokonujące inteligentnej analizy treści obrazu. Każda kamera sieciowa w takim systemie staje się urządzeniem inteligentnym, które jest w stanie analizować rejestrowany obraz i ostrzegać pracowników ochrony o potencjalnych zagrożeniach, takich jak pozostawione podejrzane przedmioty, gromadzenie się ludzi, blokowanie stref ewakuacyjnych, przekraczanie stref bezpieczeństwa. Ponadto możliwe jest szybkie i skuteczne przeszukiwanie zarejestrowanego materiału według dowolnych kryteriów. Dla ułatwienia pracy na stanowiskach ochrony zastosowano system Bosch VMS z ergonomicznym interfejsem, co sprawia, że zarządzanie sygnałem wizyjnym jest proste, a personel może pracować wydajnie i skutecznie.

Aby zapobiec wejściu osób nieupoważnionych do chronionych stref, cały obiekt wyposażono w czytniki kontroli dostępu. W systemie możliwe jest nadawanie uprawnień do wejścia do różnego rodzaju pomieszczeń, a także rejestrowanie czasu przebywania pracowników w tych pomieszczeniach.

– Dzięki kontroli dostępu tylko upoważnieni pracownicy mogą poruszać się po przestrzeni niepublicznej. Ponadto w każdej chwili możemy sprawdzić, kto i w jakim czasie przebywał w danym pomieszczeniu. Rozwiązanie to jest bardzo wygodne. Dzięki jednej karcie identyfikacyjnej pracownicy poruszają się swobodnie po dozwolonych dla nich obszarach obiektu. Bez względu na to, co dzieje się w hali, nasza ochrona widzi wszystko w centrum monitorowania i na bieżąco reaguje. Funkcje, jakie oferują systemy Bosch, w pełni odpowiadają naszym oczekiwaniom. Bardzo dobrze współpracuje nam się z firmą Bosch, która zapewnia nam wsparcie i doradztwo techniczne – powiedziała Sylwia Orzeł.

Wszystkimi instalacjami kompleksowo zarządza Building Integration System, który niezależnie od stopnia złożoności wymagań zapewnia elastyczność, łatwość obsługi oraz szybkość reakcji ochrony obiektu.

Agnieszka Augustyniak
Bosch Security and Safety Systems

NVIP-5DN2008V/IR-1P

Kamera wandaloodporna IP marki NOVUS z obiektywem typu rybie oko

Kamera wandaloodporna IP marki NOVUS **z obiektywem typu rybie oko** (ogniskowa 1,1 mm, przysłona 2.0) o stopniu szczelności IP66. Urządzenie pracuje z wybranymi modelami rejestratorów IP NOVUS z serii 4000 i aplikacją NMS, pozwala na multiplikowanie obrazów i sterowanie elektroniczną funkcją PTZ dla optymalnego wyboru obserwowanej sceny.

Obraz	
Przetwornik obrazu	6 MPX, matryca CMOS, 1/2.9", SONY Exmor R STARVIS
Liczba efektywnych pikseli	3096 (H) x 2202 (V)
Czułość	0,03 lx/F2.0 - tryb kolorowy (DSS), 0 lx (IR wł.) - tryb czarno-biały
DSS/WDR/DNR/F-DNR/BLC	do 1/5 s /tak/2D, 3D/tak/tak
Obiektyw	
Typ obiektywu	„rybie oko", f=1.1 mm/F2.0
Dzień/Noc	
Rodzaj przełączania	mechanicznie odsuwany filtr podczerwieni
Sieć	
Prędkość przetwarzania	15 kl./s dla 2160 x 2160 30 kl./s dla 1520 x 1520 i niższych rozdzielczości
Kompresja obrazu/dźwięku	H.264, H.265/-
Liczba jednoczesnych połączeń/Tryb wielostrumieniowy/ Przepustowość	maks. 10/3 strumienie/łącznie 16 Mb/s
Zgodność z ONVIF	Profil S
Pozostałe funkcje	
Strefy prywatności	4
Detekcja ruchu	tak
Reakcja na zdarzenia alarmowe	e-mail z załącznikiem, zapis na FTP
Oświetlacz IR	
Liczba diod/Zasięg/Kąt świecenia	3/5 m/120°
Interfejsy	
Interfejs sieciowy	1 x Ethernet - złącze RJ-45, 10/100 Mbit/s
Parametry instalacyjne	
Obudowa	IP 66, wandaloodporna aluminiowa, biała
Temperatura pracy	-30°C ~ 55°C

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

NVIP-9DN2018V/IR-1P

Kamera wandaloodporna IP marki NOVUS z obiektywem typu rybie oko

Kamera wandaloodporna IP marki NOVUS **z obiektywem typu rybie oko** (ogniskowa 2.0 mm, przysłona 2.4) o stopniu szczelności IP66. Urządzenie pracuje z wybranymi modelami rejestratorów IP NOVUS z serii 4000 i aplikacją NMS, pozwala na multiplikowanie obrazów i sterowanie elektroniczną funkcją PTZ dla optymalnego wyboru obserwowanej sceny.

Obraz	
Przetwornik obrazu	12 MPX, matryca CMOS, 1/1.7", SONY Exmor R STARVIS
Liczba efektywnych pikseli	4072 (H) x 3046 (V)
Czułość	0,04 lx/F2.4 - tryb kolorowy 0 lx (IR wł.) - tryb czarno-biały
DSS/WDR/DNR/F-DNR/BLC	do 1/5 s /tak/2D, 3D/tak/tak
Obiektyw	
Typ obiektywu	„rybie oko", f=2.0 mm/F2.4
Dzień/Noc	
Rodzaj przełączania	mechanicznie odsuwany filtr podczerwieni
Sieć	
Prędkość przetwarzania	30 kl./s dla 3000 x 3000 i niższych rozdzielczości
Kompresja obrazu/dźwięku	H.264, H.265/G.711, G.726, ADPCM
Liczba jednoczesnych połączeń/Tryb wielostrumieniowy/ Przepustowość	maks. 10/3 strumienie/łącznie 40 Mb/s
Zgodność z ONVIF	Profil S
Pozostałe funkcje	
Strefy prywatności	4
Detekcja ruchu	tak
Reakcja na zdarzenia alarmowe	e-mail z załącznikiem, zapis na FTP, zapis na kartę SD, aktywacja wyjścia alarmowego
Oświetlacz IR	
Liczba diod/Zasięg/Kąt świecenia	3/10 m/120°
Interfejsy	
Wejścia/wyjścia akustyczne	+ wbudowany mikrofon
Wejścia/wyjścia alarmowe	1 (NO/NC)/1
Gniazdo kart pamięci	microSD - pojemność do 128GB
Parametry instalacyjne	
Obudowa	IP66, wandaloodporna aluminiowa, biała
Temperatura pracy	-30°C ~ 55°C

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

MC16-PAC-2-KIT

Zestaw do systemu kontroli dostępu RACS 5

Zestaw **MC16-PAC-2-KIT** obejmuje elementy niezbędne do kontroli dwóch przejść. W skład zestawu wchodzi metalowa obudowa z zasilaczem, sieciowy kontroler dostępu i ekspander we/wy. Zestaw umożliwia obsługę dwóch przejść dwustronnych z wykorzystaniem czytników RS485 (czytniki serii MCT), RACS CLK/DTA (czytniki serii PRT) lub czytników z interfejsem Wiegand. Do zasilania czytników mamy do dyspozycji dwa wyjścia o wydajności prądowej 0,2 A, a do zamków i pozostałych elementów kontrolowanego przejścia 2 x 1,0 A. Prąd ładowania akumulatora może być ustawiony na 0,3 A, 0,6 A lub 0,9 A.

Charakterystyka

- Zestaw do kontroli dwóch przejść dwustronnie
- Sieciowy kontroler dostępu MC16-PAC-2
- Ekspander we/wy MCX2D
- Interfejs do 4 czytników RACS CLK/DTA (seria PRT)
- Interfejs do 4 czytników z interfejsem Wiegand
- 2 wyjścia zasilające o wydajności prądowej 0,2 A (do zasilania czytników)
- 2 wyjścia zasilające o wydajności prądowej 1,0 A (do zasilania zamków)
- 1 wyjście zasilające o wydajności prądowej 0,3 A/0,6 A/0,9 A (do ładowania akumulatora)
- Zabezpieczenie przed głębokim rozładowaniem akumulatora
- Czujnik antysabotażowy
- Miejsce na akumulator 7 Ah
- Zasilacz sieciowy 13,8 V/3 A
- Metalowa obudowa
- Wymiary (zewnętrzne): 295,0 x 285,0 x 90,0 mm

roger®

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

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

MC16-PAC-4-KIT

Zestaw do systemu kontroli dostępu RACS 5

Zestaw **MC16-PAC-4-KIT** obejmuje elementy niezbędne do kontroli czterech przejść. W skład zestawu wchodzi metalowa obudowa z zasilaczem, sieciowy kontroler dostępu i ekspander we/wy. Zestaw umożliwia obsługę czterech przejść dwustronnych z wykorzystaniem czytników RS485 (czytniki serii MCT) lub czterech przejść jednostronnych w przypadku współpracy z czytnikami Wiegand lub RACS CLK/DTA. Do zasilania czytników mamy do dyspozycji cztery wyjścia o wydajności prądowej 0,2 A, a do zamków i pozostałych elementów kontrolowanego przejścia cztery wyjścia o wydajności prądowej 1,0 A. Prąd ładowania akumulatora może być ustawiony na 0,3 A, 0,6 A lub 0,9 A.

Charakterystyka

- Zestaw do kontroli czterech przejść dwustronnie
- Sieciowy kontroler dostępu MC16-PAC-4
- Ekspander we/wy MCX4D
- Interfejs do 4 czytników RACS CLK/DTA (seria PRT)
- Interfejs do 4 czytników z interfejsem Wiegand
- 4 wyjścia zasilające o wydajności prądowej 0,2 A (do zasilania czytników)
- 4 wyjścia zasilające o wydajności prądowej 1,0 A (do zasilania zamków)
- 1 wyjście zasilające o wydajności prądowej 0,3 A/0,6 A/0,9 A (do ładowania akumulatora)
- Zabezpieczenie przed głębokim rozładowaniem akumulatora
- Czujnik antysabotażowy
- Miejsce na akumulator 17 Ah
- Zasilacz sieciowy 13,8 V/5 A
- Metalowa obudowa
- Wymiary (zewnętrzne): 305,0 x 325,0 x 100,0 mm

roger®

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

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

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

D PROD S

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

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

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

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

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

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

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

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

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

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

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

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

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

D I

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

D PROD PROJ S

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

D PROD PROJ S

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

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

D PROD S

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

D I PROJ S

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

D

P.W.H. BRABORK LABORATORIUM Sp. z o.o.
ul. Ratuszowa 11
03-450 Warszawa
Tel. kom. 604 569 775
e-mail: brabork@braborklab.pl
www.braborklab.pl

D I PROD PROJ

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

D I PROD PROJ S

CBC (Poland) Sp. z o.o.
ul. Anny German 15
01-794 Warszawa
tel. 22 633 90 90
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; faks 22 855 00 19
e-mail: biuro@cs.pl
www.cs.pl

D I PROD PROJ S

DAHUA TECHNOLOGY POLAND Sp. z o.o.
ul. Salsy 2
02-823 Warszawa
tel. 22 395 74 00
e-mail: biuro.pl@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. B. Czecha 59
04-555 Warszawa
tel. 22 518 84 00; faks 22 518 84 99
e-mail: sales@ebs.pl
www.ebs.pl

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

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

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

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

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

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

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

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

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

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

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

EUROPEAN SECURITY TRADING POLSKA Sp. z o.o.
ul. Nowogrodzka 11
00-513 Warszawa
tel. 22 629 53 49
e-mail: kontakt@estpolska.pl
www.estpolska.pl

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

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

Komfort & Bezpieczeństwo

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

HANWHA TECHWIN EUROPE LTD.
Biuro w Polsce
ul. Posag 7 Panien 1
02-495 Warszawa
Tel. kom. 518 346 039
e-mail: k.dulin@hanwha.com
https://www.hanwha-security.eu/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

C D I PROD PROJ S

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

I PROJ

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

D PROJ S

KATON Sp. z o.o.
ul. Bajana 31E
01-904 Warszawa
tel. 22 869 43 92; faks 22 869 43 93
e-mail: biuro@katon.eu
www.katon.eu

C D S

KOLEKTOR
K. MIKICIUK I R. RUTKOWSKI Sp. J.
ul. Obrońców Westerplatte 31
80-317 Gdańsk
tel. 58 553 67 59; faks 58 553 48 67
e-mail: info@kolektor.pl
www.kolektor.pl

D I PROJ

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

D PROD PROJ S

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

PROD

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

D

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

PROD

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

D PROJ S

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

D I PROD PROJ S

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

D PROJ S

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

ROPAM Elektronik s.c.
Polanka 301
32-400 Myślenice
tel. 12 272 39 71, 341 04 07; faks 12 379 34 10
www.ropam.com.pl

D PROD S

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

PROD PROJ S

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

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

ul. Św. Czesława 7 lok. 18, 61-575 Poznań
tel./faks 61 833 31 53, 833 50 37
e-mail: poznan@schrack-seconet.pl

ul. Mydlana 1, 51-502 Wrocław
tel./faks 71 345 00 95
e-mail: wroclaw@schrack-seconet.pl

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

D PROJ S

Zakład Rozwoju Technicznej Ochrony Mienia
TECHOM Sp. z o.o.
Al. Wyzwolenia 12
00-570 Warszawa
tel. 22 625 34 00
faks 22 625 26 75
e-mail: techom@techom.com
www.techom.com

B C S

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

B D PROD PROJ

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

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

D I PROD PROJ

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

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

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

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

Legenda

Kategorie*

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

Działalność*

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

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

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Paweł Karczmarzyk
Andrzej Walczyk

Korekta
Paweł Karczmarzyk

Dział marketingu i reklamy
Ela Końka

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

Współpraca
Marcin Buczaj
Piotr Czernoch
Marcin Pyclik

Projekt graficzny, skład i łamanie
Piotr Przybylski

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

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

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

Dostępne formy reklamy

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

Reklama na okładkach
pierwsza strona
druga strona
przedostatnia strona
ostatnia strona

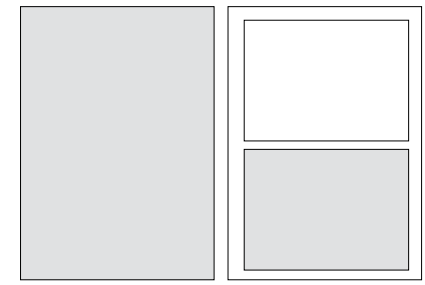
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie

Spis teleadresowy
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Ceny negocjujemy indywidualnie

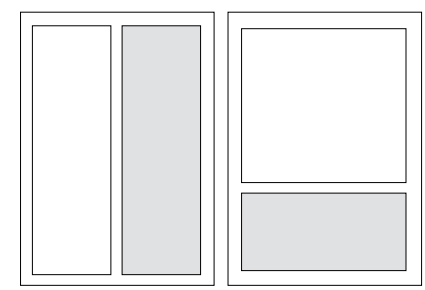
Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej http://www.zabezpieczenia.com.pl w dziale Reklama

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



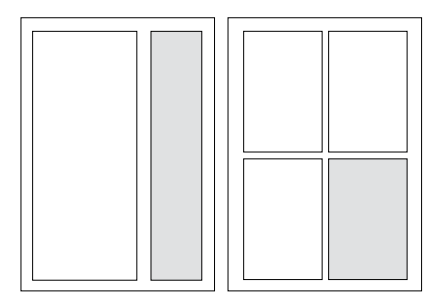
cała strona
(200 x 282 mm + 3mm spad)

1/2 strony
(170 x 125 mm)



1/2 strony
(83 x 260 mm)

1/3 strony
(170 x 80 mm)



1/3 strony
(54 x 260 mm)

1/4 strony
(83 x 125 mm)

Spis reklam

NOVUS®

3000 SERIA IP • 6000 SERIA IP

IDEALNE DOPASOWANIE

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

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

Ulisse evo

Bądź świadkiem ewolucji wizyjnych systemów zabezpieczających

Kamera ULISE EVO PTZ firmy Videotec to kolejny, innowacyjny krok naprzód w dążeniu do tworzenia coraz skuteczniejszych i niezawodnych składników wizyjnych systemów dozorowych. Ta nowa, wszechstronna kamera PTZ jest konkurencyjna cenowo i ma niespotykany dotychczas wygląd.

VIDEOTEC

VIDEO SECURITY PRODUCTS
www.videotec.com
info@videotec.com
Made in Italy since 1986

deLux technology

ONVIF | SQ