a&S POLSKA
www.aspolska.pl

CZASOPISMO RYNKU SECURITY
nr 5/2018 (11)
wrzesień/październik
15 zł (w tym 8% VAT)

PRZEMYSŁ 4.0

TEMAT NUMERU

Wraz z pojawieniem się IIoT *(Industrial Internet of Things)*, stała się możliwa konwergencja OT *(Operational Technology)* i IT.

str. 64

ISSN 2451-5175
09
9 772451 517703

TELEWIZJA DOZOROWA

Fuzja obrazów

Obraz telewizyjny i termowizyjny można łączyć na wiele sposobów, uzyskując różne efekty.

str. 20

SIECI LPWA

Standard LoRaWAN

Wi-Fi czy Bluetooth sprawdzają się na niewielkim obszarze. A jak zapewnić komunikację w przemysłowym IoT w fabrykach czy miastach?

str. 68

BEZPIECZEŃSTWO BIZNESU

Dżungla miasta wg Jacka&Jacka

Nowy cykl o bezpieczeństwie autorstwa znanego reportera Jacka Pałkiewicza i security managera Jacka Tyburka.

str. 92

24/7 VIVID COLOR CAMERA

0.0005
Lux

Super
Aperture

HIKVISION

DEEP LEARNING DVR

False
Alarm Filter

Quick
Target Search

Target
Extraction

WIĘCEJ NIŻ MOŻESZ ZOBACZYĆ
TURBO HD 5.0

HIKVISION NR 1 NA ŚWIECIE

Hikvision to światowy lider w dostawie innowacyjnych produktów i rozwiązań do monitoringu wideo. Dzięki najsilniejszej w branży kadrze R&D, firma Hikvision rozwija kluczowe technologie kodowania audio i wideo, przetwarzania obrazu wideo oraz związanego z tym przechowywania danych. Aby uzyskać więcej informacji, odwiedź nas na stronie www.hikvision.com/pl/.

Hikvision Poland
The Park Warsaw
ul. Krakowiaków 50
02-255 Warszawa
T +48 22 4600150
info.pl@hikvision.com

ColorVu

Obrazy w żywych kolorach przez całą dobę

Kamery Hikvision ColorVu zapewniają obrazy w jasnych kolorach przez całą dobę, nawet w warunkach słabego oświetlenia. Dzięki zaawansowanym obiektywom i sensorom o wysokiej czułości doskonale radzą sobie z rejestrowaniem żywych obrazów w różnych, nawet trudnych do monitoringu miejscach.

AcuSense

Inteligentna precyzja

Oparty na algorytmach sztucznej inteligencji DVR AcuSense Turbo HD oferuje znacznie lepszą precyzję VCA.

@HikvisionPoland
www.hikvision.com/pl/

Drodzy Czytelnicy

Świat przemysłu zmienia się na naszych oczach. Cyfryzacja, konwergencja OT i IT, wykorzystanie biomateriałów do produkcji oraz sensorów do kontroli jakości czy ogromne możliwości, jakie niesie sztuczna inteligencja wsparta analizą *big data* – wszystko to istotnie wpływa zarówno na procesy wytwarzania, jak i sposób funkcjonowania obiektów przemysłowych. Zmiany te implikują nowe wyzwania dot. zapewnienia bezpieczeństwa. Dlatego **Przemysł 4.0** po raz kolejny jest tematem numeru. Opisujemy **Przemysłowy Internet Rzeczy**, który zwiększa „inteligencję" linii produkcyjnych (s. 64), oraz **standard LoRaWAN**, zapewniający komunikację między sensorami a urządzeniami działającymi w ramach IIoT w dużych fabrykach czy miastach (s. 68). **O złożoności zapewnienia ochrony w obiektach przemysłowych** piszą dla nas praktycy: Andrzej Kozłowki z PGNiG TERMIKA (s. 74) i Jacek Grzechowiak z Huty CELSA Ostrowiec (s. 76). Ekspercko temat **IV rewolucji przemysłowej (i jej wdrażania w Polsce)** opisuje Julia Patorska z Deloitte (s. 88).

Rynek security rozwija się dynamicznie. Opisujemy te zmiany i wskazujemy nowe trendy. Należy do nich niewątpliwie łączenie w jednej kamerze sygnałów telewizyjnych i termowizyjnych, czyli **fuzja obrazów** (s. 20). Niezwykle istotna w systemach dozoru wizyjnego jest także **transmisja sygnałów wizyjnych** – piszemy, co kryje się za skrótami PoE, PoC, EoC i w jakich zastosowaniach sprawdzą się te technologie (s. 26). Prezentujemy również przegląd oferty rynkowej **rejestratorów sieciowych NVR** (s. 49). Polecamy także opracowanie nt. **stosowania norm przy planowaniu ochrony** (s. 44).
W dzisiejszych cyfrowych czasach to nie mienie jest dla przedsiębiorstwa największą wartością, a dane – tajemnice firmowe, bazy klientów czy dane niezbędne do zachowania ciągłości produkcji. Dlatego kluczowe staje się odpowiednie **zabezpieczenie ppoż. serwerowni** (s. 54).

Rozpoczynamy nowy cykl artykułów **„Dżungla miasta wg Jacka & Jacka".** To autorskie podejście duetu: Jacek Pałkiewicz i Jacek Tyburek (s. 92). Znany reporter i podróżnik oraz wieloletni praktyk zarządzania bezpieczeństwem przedstawią swój punkt widzenia na bezpieczeństwo w jego różnych aspektach. Ponadto w dziale Bezpieczeństwo biznesu opisujemy także kwestię **centralnego zarządzania bezpieczeństwem organizacji** (s. 96) oraz **najnowsze statystyki dot. cyberzagrożeń** (s. 100).

Jesień to dla rynku security tradycyjnie czas wytężonej pracy i wielu branżowych spotkań. Uczestniczymy w licznych konferencjach, sympozjach i targach. Najciekawsze opisujemy na bieżąco na portalu **www.aspolska.pl** oraz w czasopiśmie – relacja z targów Security Essen na s. 16, pozostałe wydarzenia w serwisie informacyjnym (s. 102–109).

Życzymy przyjemnej lektury!

Marta Dynakowska
redaktor naczelna

Jan T. Grusznic
z-ca redaktora naczelnego

Mariusz Kucharski
dyrektor zarządzający

www.aspolska.pl

a&S POLSKA

Wydawca
A&S Polska Sp. z o.o.
ul. Rondo ONZ 1
00-124 Warszawa

Redakcja
ul. A. Branickiego 15
Wilanów Office Park, bud. 1
02-972 Warszawa
e-mail: info@aspolska.pl
www.aspolska.pl

Dyrektor zarządzający
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Z-ca redaktora naczelnego
Jan T. Grusznic

Stały felietonista
Andrzej Popielski

Dział marketingu i reklamy
Iwona Krawiec
Patrycja Sołtysik

Dział eventów i konferencji
Aleksandra Czapska

Kolegium redakcyjne
Norbert Bartkowiak
Edmund Basałyga
Sebastian Błażkiewicz
Janusz Bohdanowicz
Marek Domański
Jacek Grzechowiak
Roman Maksymowicz
Dariusz Mostowski
Przemysław Pierzchała
Janusz Sawicki
Stefan Jerzy Siudalski
Jerzy Sobstel
Paweł Wittich
Waldemar Wnęk
Aleksander M. Woronow

Korekta
Jolanta Kucharska

Projekt graficzny
Sylwester Dmowski

Skład
Dorota Cybulska
Sylwester Dmowski

Prenumerata
www.aspolska.pl/prenumerata

W numerze...

Bezpieczeństwo biznesu
JAK SKUTECZNIE CENTRALIZOWAĆ **ZARZĄDZANIE BEZPIECZEŃSTWEM ORGANIZACJI**

AXIS P3807-PVE: kamera kopułkowa z czterema przetwornikami obrazu

AXIS
www.axis.com/pl

AXIS P3807-PVE to stałopozycyjna sieciowa kamera kopułkowa z czterema przetwornikami obrazu. Jej instalacja jest łatwa i efektywna kosztowo dzięki skróceniu czasu montażu oraz zmniejszeniu okablowania i liczby licencji oprogramowania zarządzającego materiałem wizyjnym. Dzięki doskonałej jakości modułów optycznych, technologii Forensic WDR i Lightfinder kamera dostarcza wysokiej jakości materiał wizyjny niezależnie od warunków oświetlenia. Cztery moduły optyczne gwarantują płynny panoramiczny widok w zakresie 180° w rozdzielczości 8 Mpix przy 30 kl./s.

Kamera jest łatwa w instalacji i oferuje wiele wariantów montażu: wpuszczany, na płasko, wiszący i montaż tyłem do siebie dwóch kamer Axis. Urządzenie jest sprzedawane z ustawieniami fabrycznymi.

- Niezauważalne połączenie obrazów z różnych modułów optycznych
- Widok w zakresie 180° w poziomie i 90° w pionie
- Rozdzielczość 8 Mpix przy pełnej poklatkowości
- Technologia Axis Lightfinder umożliwia uzyskanie żywszych kolorów w warunkach słabego oświetlenia
- Technologia Forensic WDR skutecznie zmniejsza szum i artefakty, zapewniając obraz o wysokiej użyteczności w scenach o dużym kontraście oświetlenia między najciemniejszymi a najjaśniejszymi obszarami
- Technologia Axis Zipstream zmniejsza zapotrzebowanie na przepustowości i pamięć masową.

Nowe rejestratory BCS XVR

BCS
www.bcscctv.pl

Nowe rejestratory XVR serii BCS Line są przykładem innowacyjnego podejścia do zagadnienia telewizji analogowej wysokiej rozdzielczości. Korzystają z technologii i funkcjonalności do tej pory zarezerwowanych dla rejestratorów sieciowych NVR. Stosowanie kompresji Smart H.265+/H.265 pozwala zredukować zapotrzebowanie na przestrzeń dyskową nawet do 90% w porównaniu z dotychczas stosowaną w XVR-ach kompresją H.264 i znacząco obniżyć koszty inwestycji. Dzięki obsłudze kamer z interfejsem HDCVI w rozdzielczościach 4 Mpix czy nawet 4K nie trzeba przy tym rezygnować z wysokiej jakości nagrywanego obrazu.

Kolejne zalety: automatyczne rozpoznanie interfejsu (HDCVI/AHD/TVI/CVBS) podłączonej do rejestratora kamery, bez konieczności dodatkowej konfiguracji. Obsługa kamer HDCVI w rozdzielczości do 4K i kamer IP w rozdzielczości do 12 Mpix. Przesyłanie sygnałów audio i alarmów z kamer HDCVI kablem koncentrycznym nie wymaga użycia dodatkowego okablowania, a taki sygnał można przesłać na odległość nawet 1200 m (dla rozdzielczości 720p).

Wyposażenie rejestratora w drugie wyjście monitorowe HDMI2 pozwala na podłączenie monitora, na którym można ustawić spersonalizowany podgląd. W ten sposób operator uzyskuje stały podgląd z kamer o wyższym priorytecie.

W rejestratorach XVR zaimplementowano również algorytmy inteligentnej analizy obrazu znane do tej pory z rejestratorów NVR, takie jak przekroczenie linii, wtargnięcie w strefę, pojawienie się czy zniknięcie obiektu, a nawet detekcja twarzy.

Rejestratory Dahua zintegrowane z POS

Dahua Technology Poland
www.dahuasecurity.com/pl

Punkty sprzedaży (POS – *Point of Sale*) można zintegrować z rejestratorami Dahua, wchodzącymi w skład systemu dozoru wizyjnego. Rozwiązanie to jest przeznaczone do obiektów handlowych, takich jak wszelkiego rodzaju sklepy mało- i wielkopowierzchniowe czy punkty usługowe – praktycznie wszędzie tam, gdzie stosuje się kasy fiskalne. Taka integracja może przynieść właścicielom korzyści finansowe, gdyż umożliwia zminimalizowanie strat spowodowanych kradzieżami i fałszywymi transakcjami kasowymi. To jednak niejedyne straty, na jakie są narażeni właściciele obiektów handlowych.

Zintegrowanie systemu POS z rejestratorem pozwala zidentyfikować sprawcę oraz zebrać informacje i dowody popełnienia nadużycia przez sprzedawcę czy kasjera. Dzięki takim możliwościom pracodawca zyskuje dodatkowe narzędzie do walki z nieprawidłowościami pojawiającymi się w miejscu pracy.

Wszystkie operacje systemu fiskalnego są zapisywane w rejestratorze Dahua oraz przypisywane do materiału wizyjnego. Dzięki takiej rejestracji można bardzo szybko odnaleźć interesującą (np. podejrzaną) transakcję, odtworzyć cały jej przebieg na zarejestrowanym materiale wideo i stwierdzić ewentualne nieprawidłowości. Czas odnalezienia incydentu znacznie się skraca. Integracja rejestratorów Dahua z systemem POS wspomaga działania związane z zapobieganiem stratom w placówkach handlowych.

MAZi: kamera IP 8 Mpix IWH-84MR

GDE Polska
www.gde.pl

Coraz większą popularność zdobywają urządzenia obsługujące rozdzielczość 4K (3840 x 2160 pix, 8 Mpix). Nie może wśród nich zabraknąć kamer MAZi. Model IWH-84MR ma obiektyw moto-zoom 2,8…12 mm z autofokusem, doświetlenie o zasięgu 50 m oraz obudowę ze zintegrowaną puszką montażową. 8 Mpix to radykalnie lepsza jakość obrazu niż 2 Mpix – 4-krotnie większa rozdzielczość jest wyraźnie widoczna przy obserwacji twarzy, napisów czy innych detali obrazu, 20 klatek na sekundę daje płynne obrazy, kodek H.265+ pozwala na zachowanie wysokiej jakości obrazu 8 Mpix przy strumieniu jak z kamery 2 Mpix z kodekiem H.264, a funkcja WDR o dynamice 120 dB zapewnia bardzo dobrej jakości obraz nawet w niesprzyjających warunkach oświetlenia.
Kamera obsługuje funkcję ANR (*Automatic Network Replenishment*), kilka algorytmów analizy obrazu VCA (detekcja przekroczenia linii, detekcja wtargnięcia, wykrycie pozostawionego obiektu, wykrycie zniknięcia obiektu, detekcja twarzy). Dostępny jest uchwyt słupowy POLE-200, pasujący także do kamer IDH-84MR. Rodzina kamer 4K obejmuje modele IWH-84IR oraz IDH-84IR z obiektywem 2,8 mm, a także IDH-84MR wyposażony w obiektyw moto-zoom 2,8-12 mm. Wszystkie te kamery udostępniają identyczne funkcje jak model IWH-84MR, wymagają kompatybilnego rejestratora, np. INVR-04/08/16 KL/Q czy INVR-32K. Wyłącznym przedstawicielem firmy MAZi Security Systems GmbH jest GDE Polska.

Tiandy: 5-Mpix kamery TC-NC552S oraz TC-NC514S

Genway
www.tiandy.pl

Kolorowy obraz w nocy

Najnowsze kamery Starlight TC-NC552S oraz TC-NC514S firmy Tiandy przekazują kolorowy obraz nawet przy oświetleniu 0,002 luksa. Dla porównania Księżyc w pełni oświetla Ziemię z natężeniem 0,2 luksa, a oświetlenie uliczne w nocy ma 5 luksów. Urządzenia charakteryzują się rozdzielczością (maksymalną) 2560 x 1920 pikseli i obiektywami o ogniskowej 2,8 mm (obudowa kopułowa) oraz 4 mm (obudowa tubowa).

Wygoda i estetyka

W trosce o wygodę i estetykę montażu kamery wyposażono w metalowe obudowy specjalnego typu. Wszystkie połączenia wykonuje się wewnątrz urządzeń – znajduje się tam gniazdo RJ45. Przewód jest prowadzony przez dławik zapewniający szczelność. Nie ma potrzeby instalowania dodatkowych puszek.

Analiza obrazu

W kamerach zaimplementowano funkcje inteligentnej analizy obrazu IVA, takie jak przekroczenie linii pojedynczej i podwójnej, naruszenie obszaru, detekcja tłumu, detekcja pozostawionego lub usuniętego przedmiotu, detekcja szybko poruszającego się obiektu, nietypowego zachowania oraz nieprawidłowego parkowania. Mogą być również analizowane nieprawidłowości obrazu i dźwięku. Obie kamery są objęte 3-letnią gwarancją.

Praca w każdej przeglądarce

Obsługa kamer nie wymaga instalacji żadnych wtyczek do przeglądarki. Będą więc one działać w każdym systemie operacyjnym, m.in. Windows, MacOS czy Linux. Do wyświetlenia obrazu jest wymagana jedynie obsługa technologii Flash.

Hanwha Techwin: kamery PTZ do obiektów przemysłowych

Hanwha Techwin Europe
www.hanwha-security.eu

Hanwha Techwin wprowadza do oferty nową linię kamer PTZ przeznaczonych do pracy w najbardziej wymagających warunkach. Moduł kamery o rozdzielczości 1920 x 1080 pikseli z 32-krotnym zoomem optycznym jest dostępny w dwóch wersjach obudowy: tradycyjnej PTZ (model XNP-6320HS) oraz cylindrycznej z certyfikatem antywybuchowym ATEX (model TNU-6320E). Obie wersje są zamknięte w obudowie IP67 ze stali nierdzewnej, gwarantującej nieprzerwaną pracę w najbardziej wymagającym środowisku produkcji przemysłowej (pyły, czynniki korozyjne itp.). Kamery obsługują kompresję H.265 i H.264 do 10 niezależnie transmitowanych strumieni danych, WDR o dynamice 150 dB (model XNP-6320HS) lub 120 dB (TNU-6320E), żyroskopową stabilizację obrazu, zaawansowaną metodę transmisji WiseStream II ograniczającą pasmo do 75% w stosunku do standardowego H.264, a także bogaty zestaw funkcji analizy obrazu.
Całość uzupełnia wykrywanie i korekcja mgły, dwa gniazda kart SD o łącznej pojemności 512 GB oraz analityka dźwięku z klasyfikacją treści (wykrywanie strzałów z broni palnej, krzyku, eksplozji i stłuczenia szkła). Bezpieczeństwo cybernetyczne to duży atut nowych modeli. Szyfrowane pliki *firmware* i konfiguracji, brak haseł domyślnych, wymuszanie skomplikowanych haseł, autentykacja SSL i TLS/EAP, filtrowanie adresów IP to tylko niektóre technologie zapewniające najwyższą jakość zabezpieczeń, co w obiektach infrastruktury krytycznej jest kluczowe.

Kamera Hikvision ColorVu

Hikvision
www.hikvision.com/pl/

Kamery analogowe Turbo HD 5.0, o lepszych parametrach i wzbogacone o nowe funkcje, to kolejny przełom w dziedzinie analogowych systemów telewizji dozorowej. Pozwalają na całodobowe przesyłanie obrazu charakteryzującego się żywymi kolorami, jasnością i wyrazistością niespotykanymi w systemach z interfejsem HD-TVI. Nowością są kamery z technologią ColorVu, pozwalającą uzyskiwać kolorowy obraz przez całą dobę.
Zaawansowana zdolność kamer Hikvision ColorVu do rejestrowania szczegółów obrazu przy słabym oświetleniu wynika z zastosowania dwóch osiągnięć w dziedzinie technologii: jasnych obiektywów, przetworników obrazu o wysokiej czułości oraz doświetleniu sceny ciepłym białym światłem. Zastosowany w kamerze obiektyw o aperturze F1.0 rzutuje na przetwornik obrazu znacznie więcej światła niż tradycyjnie stosowane soczewki o większej liczbie F. Obiektywy są również pokryte szerokopasmową powłoką antyrefleksyjną (BBAR – *Broad Band Anti Reflection*) i wykonane ze szkła o bardzo niskiej dyspersji (ED – *Extra-low Dispersion*). Doskonale radzą sobie z rejestrowaniem żywych, kolorowych obrazów trudnych do monitorowania scen, takich jak miejsca publiczne nieoświetlone, parki przemysłowe w nocy, skrzyżowania ulic o słabym oświetleniu i wiele innych.
ColorVu obejmuje trzy modele kamer: DS-2CE12DFT, DS-2CE72DFT, DS-2CE10DFT. Ich podstawowe parametry: rozdzielczość 2 Mpix, czułość 0,005 lx, True WDR 120 dB, klasa szczelności obudowy IP67, zasięg doświetlenia do 40 m.

360 Vision: INVICTUS – hybrydowe kamery PTZ

Linc Polska
www.linc.pl

INVICTUS to seria hybrydowych kamer PTZ marki 360 Vision Technology (360 Vision). Zastosowana opatentowana technologia umożliwia połączenie w jednym rozwiązaniu dwóch technologii: analogowej oraz IP – HD. Dzięki temu kamery znajdują zastosowanie zarówno w istniejących, jak i w nowych systemach zabezpieczeń.
Serię INVICTUS wyróżnia:
- szczegółowy obraz kolorowy (przetwornik ULL 1/1,9", zoom optyczny x12);
- oświetlacz światła białego lub IR o zasięgu do 200 m;
- konstrukcja umożliwiająca nachylenie o 160°, widok i ciągły obrót 360° bez martwych stref;
- wbudowana pamięć do 256 GB;
- autokalibracja – automatyczny tryb wykrywania wymuszonych lub nienaturalnych ruchów i natychmiastowa ponowna kalibracja do prawidłowej pozycji i ustawień;
- wzmocniona obudowa z mechanizmem obrotu i pochyłu opartym na przekładni gwarantująca długą żywotność kamer;
- tryb niskiego poboru mocy przy braku aktywności, inteligentne sterowanie oświetleniem (zasilanie kamery z innych źródeł);
- możliwość specjalnego lakierowania o przedłużonej trwałości, np. do zastosowań na wybrzeżu i/lub w marynarce wojennej;
- dyskrecja – możliwość dostosowania koloru kamery do otoczenia;
- zdalna konfiguracja z jednego punktu w sieci, bez dodatkowych wtyczek do przeglądarki, specjalnych uprawnień i aktualizacji internetowych.

Kamery z serii INVICTUS marki 360 Vision sprawdzą się tam, gdzie liczy się niezawodność, skuteczność oraz prosta instalacja.

Głośnik tubowy IP ELSII-10H

Novatel
www.novatel.pl

Głośnik tubowy VoIP to idealne rozwiązanie uzupełniające system monitoringu wizyjnego. Badania i praktyka wykazały, że zapowiedź słowna nadana przez obsługę skutkuje tym, że w ponad 70% przypadków odnotowano odstąpienie sprawcy od niebezpiecznego czynu lub niepożądanego zachowania. Głośnik jest podłączany bezpośrednio do sieci IP i zasilany z PoE (jak kamera), co umożliwia użycie jednolitego okablowania oraz montaż w dowolnym miejscu w zasięgu sieci LAN.
Głośnik ELSII-10H cechuje: przesyłanie głosu wysokiej rozdzielczości „HD Voice", pasmo przenoszenia mowy od 200 Hz do 7 kHz, kodek g.722, wbudowany 10-watowy wzmacniacz mocy klasy D, bardzo wysoki poziom ciśnienia akustycznego (do 116 dB), klasa odporności obudowy na warunki atmosferyczne IP 67, szeroki zakres temperatury pracy od -40°C do 70°C, wbudowany przekaźnik oraz 6 WE/WY, wejście mikrofonowe oraz wyjście liniowe audio.
Po podłączeniu mikrofonu uzyskujemy możliwość zdalnego odsłuchu, można aktywować funkcję automatycznej regulacji głośności, która na bieżąco dostosowuje poziom głośności do hałasu otoczenia. Nadane komunikaty mogą być rejestrowane w systemie CCTV. Głośnik może pracować w kilku trybach VoIP: SIP, Pulse, AlphaCom, ma zaawansowane funkcje nadzoru pracy wykrywające błędy w sieci lub elektronice głośnika.
Status głośnika jest zgłaszany do jednostki centralnej, a także do zewnętrznych systemów za pomocą SNMP lub Syslog.
Szczegóły na stronie www.novatel.pl

System alarmu pożarowego Panasonic EBL G3

RAJ International
www.raj-international.net

EBL G3 – najnowszy produkt firmy Panasonic Eco Solutions Nordic AB – jest przeznaczony do ochrony średnich i rozległych obiektów o dużym zróżnicowaniu technicznym.
Centrala EBL G3 obsługuje analogowe adresowalne czujki dymu, czujki konwencjonalne, ręczne ostrzegacze pożarowe, moduły sterujące, sygnalizatory akustyczne i optyczne. Można do niej podłączyć do 1016 urządzeń pętlowych na 4 pętlach komunikacyjnych. Gdy 512 adresów dla punktów pożarowych i 512 adresów dla innych modułów to za mało, jest możliwość połączenia w sieć nawet 30 central. Zwiększa to pojemność systemu do ponad 15 tys. punktów pożarowych i 15 tys. innych modułów pętlowych. Centrale komunikują się za pomocą redundantnej sieci TLON, są równorzędne – każda centrala ma dostęp do informacji z innych central w sieci.
System jest monitorowany przez webserwer podłączony do Internetu lub wewnętrznej sieci LAN, przesyła informacje o alarmach pożarowych, serwisowych (np. brudne czujki), technicznych, uszkodzeniach, blokowanych strefach lub poszczególnych elementach systemu (powiadomienia na wybrane adresy e-mail).
System jest wstecznie kompatybilny z urządzeniami pętlowymi, więc przy modernizacji nie trzeba ich wszystkich wymieniać. Wystarczy zastąpić stare centrale nowymi EBL512 G3 i podłączyć istniejące pętle dozorowe (komunikacyjne).
System spełnia wymagania normy EN-54 i wewnętrzne wymagania krajowe. Dystrybutorem systemu EBL G3 w Polsce jest firma RAJ International.

Czujka zasysająca dymu AIRSCREEN ASD 535/ASD 531

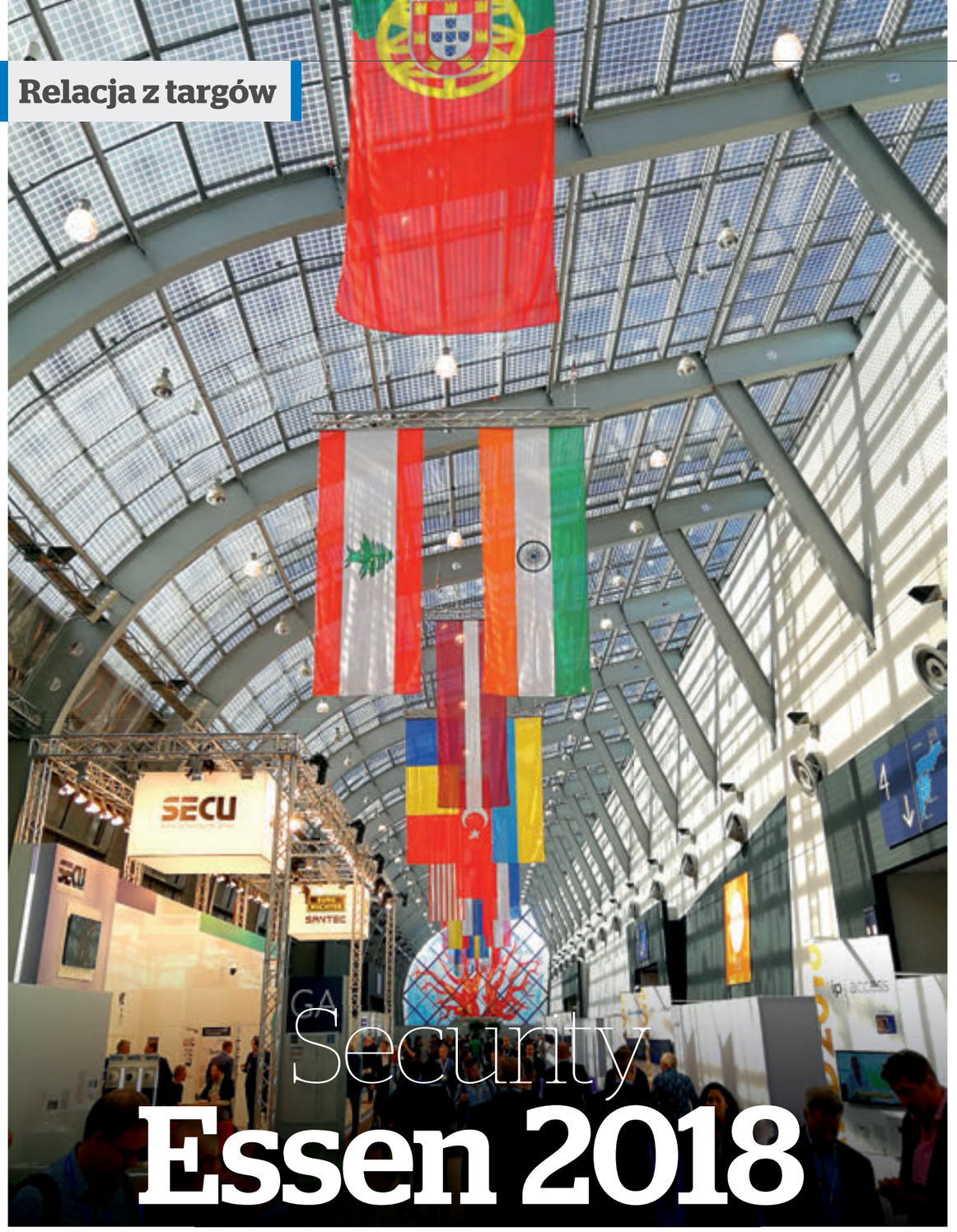
Schrack Seconet Polska
www.schrack-seconet.pl

W wymagających warunkach środowiskowych detekcję pożaru należy powierzyć rozwiązaniom specjalnym, m.in. czujkom zasysającym dymu typu ASD 535 przeznaczonym do większych instalacji (do 600 m całkowitej długości orurowania na system) oraz ASD 531 – do mniejszych instalacji (do 75 m).
Czujki zasysające charakteryzują się aktywną detekcją pożaru polegającą na próbkowaniu (zasysaniu) powietrza przez otwory ssące i jego transporcie przez układ orurowania do jednostki centralnej, gdzie następuje ocena pod kątem obecności dymu przez czujnik dymu wysokiej czułości (nawet 0,002%/m).
Czujki mogą być projektowane w klasach A, B i C zgodnie z PN-EN 54-20.
Rurki zasysające mogą być zlokalizowane bezpośrednio w trudnym środowisku o wysokim poziomie zakłóceń el.-mag. (np. rozdzielnie elektryczne), a jednostka centralna – w bezpiecznej strefie zapewniającej prawidłową pracę systemu oraz obsługę i testowanie. Bardzo długie układy orurowania (do 300 m/czujnik dla ASD 535) i wysoka czułość chronią pomieszczenia o dużej kubaturze, np. hale produkcyjne. Zastosowanie filtrów przeciwpyłowych czy układów automatycznego przedmuchiwania orurowania pozwala na pracę całego systemu w obszarach dużego zapylenia. Inne obszary zastosowań to strefy zagrożone wybuchem (przy zastosowaniu zaworu przeciwwybuchowego).
Czujki zasysające współpracują bezpośrednio (integracja cyfrowa) z systemem sygnalizacji pożarowej Integral IP, co znacznie ułatwia ich obsługę i serwisowanie.

TP-Link: EAP225-Wall Kompaktowy naścienny punkt dostępowy

TP-Link
www.tp-link.com.pl

EAP225-Wall to urządzenie o nowoczesnym designie, które świetnie sprawdza się np. w pokojach hotelowych. Jego obudowa ma zaledwie 15 mm grubości. Punkt dostępowy idealnie wkomponuje się w każde wnętrze, zapewniając jednocześnie silny sygnał sieci bezprzewodowej.
Access Point zapewnia łączną przepustowość do 1200 Mb/s, gwarantując dużą wydajność transmisji nawet przy wielu podłączonych klientach bezprzewodowych. Pozwala na stworzenie wielu SSID z logowaniem przez stronę powitalną, vouchery lub jednorazowe hasła dostępu.
Instalacja EAP225-Wall jest niezwykle łatwa. Obsługa zasilania PoE w standardzie 802.3af/at eliminuje konieczność zastosowania dodatkowego okablowania, a konstrukcja urządzeń ułatwia montaż w standardowej obudowie naściennej.
EAP225-Wall nie jest standardowym punktem dostępowym, zawiera również trzy porty Ethernet, w tym jeden port PoE-Out, który może służyć do zasilania urządzeń przewodowych, takich jak telefony IP, kamery IP czy interkomy.
Bezpłatne oprogramowanie TP-Link Omada Controller umożliwia centralne zarządzanie siecią bezprzewodową składającą się z setek urządzeń z dowolnego komputera znajdującego się w sieci. Do każdego urządzenia z serii Omada można zastosować fizyczny sprzętowy kontroler Omada Cloud OC200, który umożliwia zarządzanie siecią zarówno lokalnie, jak i przez chmurę.



Security Essen 2018

Ponad 950 wystawców z 43 krajów, ponad 36 tys. gości ze 125 krajów zainteresowanych najnowszymi osiągnięciami technologicznymi w systemach zabezpieczeń technicznych, mechanicznych i cybernetycznych – tak targi Essen wyglądają w liczbach. Co ciekawe, w tym roku aż 40% odwiedzających stanowili goście z zagranicy.

Jan T. Grusznic

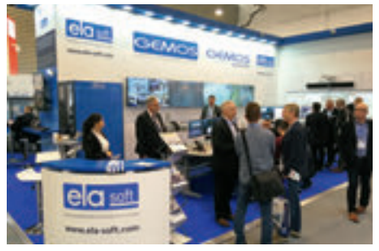
Pomimo dużej liczby odwiedzających, tłok nie był odczuwalny – być może dzięki temu, że ta czterodniowa impreza była po raz pierwszy zorganizowana w odrestaurowanej części Messe Essen, gdzie zadbano o optymalną komunikację dla gości i wystawców. Przestronne parterowe hale, dużo światła dziennego i nowe obiekty usługowe oraz przestrzeń do wypoczynku pozwalały na „złapanie oddechu" podczas długich wędrówek między stoiskami. W tym roku organizator stworzył siedem tematycznie zaplanowanych hal poświęconych kontroli dostępu, telewizji przemysłowej, systemom przeciwpożarowym, włamania i napadu, rozwiązaniom ochrony perymetrycznej oraz bezpieczeństwu cybernetycznemu.

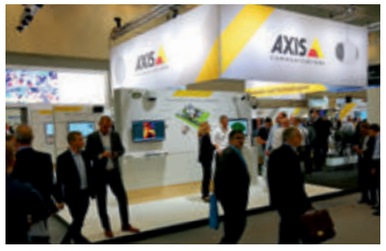
Podczas targów w Niemczech dało się zauważyć coraz większą rolę integracji, zwłaszcza w systemach kontrolujących dostęp. Rozwiązania te stają się coraz inteligentniejsze, coraz częściej też opierają się na aplikacjach wgranych w urządzenia mobilne i na identyfikacji biometrycznej. Sztuczna inteligencja pomaga dokładniej, a przy tym w coraz krótszym czasie oceniać zawartość obrazu, dzięki czemu prezentowane systemy rozpoznania twarzy czy geometrii dłoni naprawdę robiły wrażenie. Jeden z wystawców, firma TBS, wskazywał, że to właśnie systemy bezdotykowe są przyszłością systemów przyznawania dostępu.

W tym roku uwagę zwracał ogrom rozwiązań inteligentnych zamków, rygli czy klamek, w których proces wymiany informacji i autoryzacji jest oparty w większym lub mniejszym stopniu na chmurze. Również dyspozytory kluczy czy szafki miały własne podłączenie do Internetu, aby właściwie zarządzać dostępem i powierzoną zawartością. Ciekawą koncepcją była wspólna przestrzeń, na której swoje rozwiązania prezentowali zarówno przedstawiciele wysublimowanych systemów kontroli dostępu, jak i producenci zabezpieczeń mechanicznych – okuć okiennych, drzwiowych, wkładek do zamków i maszyn do dorabiania kluczy. Widać, że mechanika nie ustępuje pola nowej technologii, która staje się coraz bardziej zależna od rozwiązań tradycyjnych, czego dowodem było ogromne stoisko firmy ABUS prezentującej synergię tych dwóch światów.

Głośno mówiło się o otwartości i standardach wymiany informacji zapewniających lepszy stopień integracji. Przedstawiciele firmy Nedap, producenta m.in. systemów kontroli dostępu, wskazywali na zalety takiego podejścia w postaci choćby oszczędności i szybszego czasu wdrożenia. Nedap, oprócz rozwiązań opartych na produktach swoich partnerów biznesowych, pokazał na swoim stoisku również niewielkich rozmiarów własny czytnik serii MACE, obsługujący karty zbliżeniowe, jak również wspierający rozwiązania mobilne typu NFC, BLE i kody QR. Jak twierdzą przedstawiciele firmy, to obecnie jedyne takie urządzenie na rynku, zapewniające obsługę tak wielu standardów.

Podczas rozmów wystawcy wskazywali na istotę zabezpieczania systemów przed atakami od strony sieci teleinformatycznej i rosnącą potrzebę stosowania kryptografii. Coraz większa popularność podejścia Security as a Service (SECaaS), a wraz z nią liczba urządzeń podłączonych do globalnej sieci spowodowała, że w tym roku organizatorzy postanowili zaprosić również specjalistów związanych z cyberbezpieczeństwem. Na targach w Essen pojawiły się firmy dostarczające profesjonalne rozwiązania do zarządzania urządzeniami w sieciach rozproszonych. Skanując urządzenia pod kątem podatności, umożliwiają wgranie oprogramowania układowego lub ich izolację. Są również w stanie wspomagać działania serwisowe i konserwacyjne, szybciej wykrywając uszkodzenia lub powstające błędy transmisyjne. Podczas odbywających się równolegle prelekcji temu tematowi poświęcono sporo miejsca.





Relacja z targów

Nie rozczarowała również oferta firm związanych z telewizją dozorową. Axis postawił na otwartość i łatwość integracji, udostępniając znaczną część swojego stoiska partnerom technologicznym i programistycznym, którzy prezentowali własne rozwiązania oparte na urządzeniach tego producenta. Podobną koncepcję ekspozycji miał Milestone. Firma zademonstrowała korzyści z integracji, m.in. BriefCam (producent oprogramowania do analizy obrazu wideo umożliwiającego streszczenie wielogodzinnych nagrań do kilkuminutowych migawek; od maja br. w grupie Canon) i technologii LIDAR. Dahua pokazała możliwości swojej chmury wideo, algorytmów analizy obrazu wspartej sztucznymi sieciami neuronowymi i rozwiązania machine vision, czyli widzenia maszynowego. W trakcie targów w Essen Dahua oficjalnie uruchomiła program DIPP (*Dahua Integration Partner Program*), koncentrujący się na tworzeniu kompleksowych, zintegrowanych rozwiązań z partnerami zewnętrznymi. Do programu dołączył już AxxonSoft, który prezentował swoje osiągnięcia z zakresu analizy obrazu wspartej sztuczną inteligencją.

Hikvision postawił na promocję linii DarkfighterX, nowej serii kamer ColorVu, nowego oprogramowania VMS HIKCentral i dalsze umacnianie swojego AI na rynku zabezpieczeń. Wraz ze swoimi partnerami – Eagle Eye (znany z dbałości o bezpieczeństwo dostawca rozwiązań wideodozoru opartych na chmurze), IPS (producent zaawansowanej analizy obrazu zintegrowanej m.in. z kamerami HEOP Hikvision), SeeTec (uznana platforma VMS, zwłaszcza w segmentach handlu detalicznego, transportowym i logistycznym), Skilu (producent sprzętu do transmisji sygnałów wizyjnych opartego na technologii bezprzewodowych włókien światłowodowych o wysokiej częstotliwości), Seagate (producent pierwszego dysku przeznaczonego specjalnie do rozwiązań dozoru wizyjnego opartych na sztucznej inteligencji) oraz Milestone – Hikvision przekonywał, że jego produkty można stosować dużo szerzej niż tylko do zabezpieczeń technicznych.

Firma Flir promowała w Essen multispektralną kamerę serii Saros do kompleksowego zabezpieczenia przestrzeni zewnętrznych. Kamera Saros jest wyposażona w wiele czujników termicznych, jedną lub więcej kamer 1080p lub 4K, reflektory na podczerwień i światła widzialnego, ma wbudowane zaawansowane funkcje analizy, dwukierunkowe audio i cyfrowe wejścia/wyjścia. Flir zdecydował się pokazać po raz pierwszy w Europie autorskie oprogramowanie VMS Latitude, sprawdzone wielokrotnie w aplikacjach militarnych.

Coraz większa z każdym rokiem moc obliczeniowa procesorów kamer wspierająca algorytmy oparte na sztucznej sieci neuronowej pozwala traktować kamery jako wieloaspektowe urządzenia detekcyjno-pomiarowe, a nie tylko jako urządzenia do przechwytywania obrazu. Hasło „kamera jako czujnik" pojawiało się na targach w Essen pod postacią „Software Define Camera", które jakiś czas temu zaczął promować Google, a za nim Huawei. W skrócie chodzi o kamery, które wspierają kilka lub kilkanaście równolegle pracujących algorytmów analizujących obraz i zbierających różnorodne dane w ramach projektów związanych z BIG DATA (np. poziom oświetlenia w scenie, poziom hałasu, zliczanie pojazdów i osób, pomiar średniego czasu przebywania w strefie, kierunkowość ruchu itp.). To właśnie w tej dziedzinie zapowiada się rewolucja. Pomimo nieobecności firmy Bosch na targach w Essen, o jej projekcie SAST (*Security and Safety Things*) mówiło się w kuluarach. Bosch zamierza bowiem w przyszłym roku udostępnić otwarty system operacyjny Camera OS oparty na Android Open Source Project i otworzyć sklep z aplikacjami tworzonymi przez społeczność SAST.

Z polskich akcentów – można było zobaczyć ofertę firm Satel, Pulsar, Ambient, EBS, Merawex, Metalkas, Advanced Protection Systems S.A., Ambient, Kanex, Ela-compil (twórca rozwiązania MOSAIC dla systemu GEMOS).

Rys. 1. **Przykład połączenia czterech zdjęć w jedno zdjęcie HDR** (autor: Jakub Sobek)

SZTUKA ŁĄCZENIA

czyli o fuzji obrazów

W najbliższych latach coraz częściej będziemy spotykali zarówno zastosowania fuzji danych z różnych sensorów, jak i fuzji wizyjnej. Warto eksperymentować, łączyć i poszukiwać „nowych smaków”...

Jakub Sobek

Smaczne danie łączy smaki poszczególnych składników w spójną, czasem zaskakującą całość. W filharmonii spodziewamy się wzruszających połączeń nie tyle smaków, co dźwięków. W branży zabezpieczeń technicznych takie połączenia także można spotkać. Należy do nich m.in. fuzja obrazów.

Dobrego kucharza poznaje się nie po tym, że potrafi przygotować smaczne danie z wyjątkowych produktów. Prawdziwego kunsztu kulinarnego wymaga przygotowanie smacznego dania z podstawowych jedynie produktów. Smaczne danie łączy smaki poszczególnych składników w spójną, czasem zaskakującą całość. Najczęściej właśnie dlatego lubimy chodzić do restauracji.

W filharmonii spodziewamy się wzruszających połączeń nie tyle smaków, ile dźwięków. Piękny koncert łączy grę wielu instrumentów i tylko ich prawidłowe współbrzmienie tworzy wyjątkowość danego dzieła. Gdyby każdy instrument kolejno odgrywał swoją partię, efekt byłby rozczarowujący. Zarówno zmysł smaku, jak i słuchu lubią umiejętne połączenia. Podobnie wzrok – sztuka może być jednym z takich przykładów.

W branży zabezpieczeń technicznych takie połączenia także można spotkać. Należy do nich m.in. fuzja obrazów. Rzadko jeszcze spotykana, dla wielu niezrozumiała, zyskuje na popularności. Tym umiejętnym połączeniom warto przyjrzeć się bliżej.

Co można ze sobą połączyć?

Fuzja oznacza łączenie wielu rzeczy w całość. W odniesieniu do systemów wizyjnych to np. połączenie dwóch lub większej liczby pojedynczych obrazów, a nawet sekwencji wizyjnych w jeden obraz wynikowy. Można ze sobą łączyć nie tylko media pochodzące ze źródeł tego samego typu, można np. połączyć obrazy z danymi uzyskanymi z urządzenia Lidar (skaner laserowy) w celu utworzenia przestrzennych map otoczenia.

Coraz popularniejsze roboty i autonomiczne samochody, które za chwilę wkroczą w naszą rzeczywistość, właśnie z takiej fuzji korzystają. W wielu koncepcjach jest ona niejednokrotnie nawet bardziej złożona – łączą się ze sobą obrazy z kamery, dane ze skanera Lidar, z czujników ultradźwiękowych oraz radarów krótkiego zasięgu. Takie heterogeniczne rozwiązanie tworzy mapę otoczenia, łącząc różne zarejestrowane atrybuty środowiska. Dzięki temu pojazd widzi znaki zarówno poziome, jak i pionowe, może oceniać prędkość poruszających się obiektów i odległość od nich oraz prowadzić złożoną analizę ruchu wszystkich rejestrowanych obiektów.

W klasycznej fotografii przykładem fuzji wizyjnej jest metoda HDR (*High Dynamic Range* – wysoki zakres dynamiki). Polega ona na połączeniu dwóch lub kilku zdjęć wykonanych z różnym czasem ekspozycji w jedno zdjęcie o znacznie szerszym zakresie kolorów (skali szarości) i poziomów jasności niż każda ramka z osobna. Takie zdjęcie ma dla wielu osób dodatkowe walory estetyczne i artystyczne. Istnieje wiele metod i technologii HDR, efekt zastosowania HDR dla tych samych zdjęć będzie inny – może zależeć od tego, czy użyjemy obrazów już skompresowanych, np. JPEG, czy obrazów typu RAW. Często obraz uzyskany w technologii HDR ma na tyle dużą rozpiętość tonalną, że nie można go prawidłowo wyświetlić na monitorze lub wydrukować. Konieczne jest wówczas przeskalowanie otrzymanej dynamiki, często nazywane mapowaniem tonalnym. Przykładowo na *rys. 1* przedstawiono połączenie zdjęć wykonanych z różnym czasem naświetlania oraz końcowy efekt w postaci zdjęcia HDR.

Kamery dozorowe często mają funkcję WDR (*Wide Dynamic Range* – szeroki zakres dynamiki). W zależności od producenta lub modelu kamery efekt ten może być uzyskiwany na różne sposoby. Pierwsza z metod polega na rejestracji obrazu o większej głębi tonalnej niż ten, który rzeczywiście może być wyświetlony. Następnie przeskalowuje się cały zakres, zwracając szczególną uwagę na miejsca prześwietlone i niedoświetlone. Druga metoda jest taka sama jak stosowana w fotografii metoda HDR (czasem tych nazw używa się zamiennie). Polega na tym, że kamera w czasie rzeczywistym wykonuje dwie ekspozycje obrazu i następnie składa je ze sobą. Również w tym przypadku można mówić o fuzji wizyjnej. Funkcja WDR wymaga procesorów sygnałowych o większej mocy obliczeniowej. Szybko poruszające się obiekty mogą być w obrazie wynikowym rozmazane, co jest efektem przemieszczenia się obiektu między pierwszą a drugą klatką. W ostatnich latach nastąpił rozwój technologii WDR, które stosują dodatkowo algorytmy redukcji szumów oraz wzmocnienia obrazu. Wybierając kamery z funkcją WDR, należy pamiętać, że mogą one działać w zupełnie inny sposób, dając obraz znacznie różniący się jakością, mimo że parametry fizyczne kamer mogą być do siebie bardzo zbliżone.

Fuzja wizyjno-termowizyjna

Jedną z odmian fuzji wizyjnej, która coraz częściej zaczyna pojawiać się w systemach telewizji dozorowej, jest łączenie obrazów światła widzialnego z obrazami termowizyjnymi. Dzieje się tak m.in. dlatego, że upowszechniły się przetworniki termowizyjne o niskich rozdzielczościach, np. 80 x 60 pikseli lub 160 x 120 pikseli. Uzyskiwane z nich obrazy mają niską szczegółowość. Aby nadać im większą szczegółowość, producenci decydują się na fuzję wizyjną. Użytkownik ma wrażenie pracy z kamerą termowizyjną o znacznie wyższej rozdzielczości niż jest w rzeczywistości. Taka kamera termowizyjna potrzebuje jednak światła widzialnego, aby generować szczegółowy obraz,

Rys. 2. **Testowe obrazy wejściowe. Z lewej strony obraz z kamery światła widzialnego, z prawej – obraz z kamery termowizyjnej** (źródło: baza TNO)

co tak naprawdę jest zaprzeczeniem idei termowizyjnej. Dla wielu celów takie ograniczenie nie stanowi większej przeszkody, ale to pewna słabość tych rozwiązań, którą trzeba brać pod uwagę podczas planowania pracy systemu i przy ocenie ryzyka.

W przypadku termowizji obrazy można łączyć na wiele sposobów. Ich wynik czasem zachwyca, czasem jest daleki od ideału. To, z jakiej metody korzysta producent danej kamery, najczęściej wprost zależy od jej mocy obliczeniowej. Trzeba pamiętać, że procesor sygnałowy musi w czasie rzeczywistym połączyć ze sobą dwa strumienie obrazu – z przetwornika światła widzialnego i przetwornika termowizyjnego. Obraz tradycyjny ma zazwyczaj rozdzielczość full HD lub większą, termowizyjny natomiast znacznie niższą, np. 80 x 60, 320 x 240 lub 640 x 480 pikseli. Pierwszym krokiem, jaki należy wykonać, jest przeskalowanie tych obrazów, by ich rozmiary były takie same. Najczęściej powiększa się obraz termowizyjny, stosując jego interpolację. Może się też zdarzyć, że proporcje obrazu będą inne, np. obraz wizyjny w formacie 16:9, termowizyjny – w formacie 4:3. W takim przypadku nałożenie i fuzja obrazów mogą być wykonane tylko na ich obszarze wspólnym. W celu zaprezentowania, jak działa taka fuzja, posłużę się dwoma zdjęciami wejściowymi z kamery światła widzialnego i kamery termowizyjnej (*rys. 2*).

Przenikanie obrazów

Jedną z najprostszych metod wykonania fuzji obrazu wizyjnego i obrazu termowizyjnego jest nałożenie ich na siebie, a następnie procentowe ustawienie przenikalności obrazu znajdującego się na wierzchu. Często taką metodę stosuje się także do porównania dwóch obrazów niewiele się różniących między sobą. Nałożenie obrazów i ustawienie ich przenikania jest często wygodniejsze niż porównywanie obrazów ustawionych obok siebie. Często z funkcji „przeźroczystości" obrazów korzystają graficy komputerowi, tworząc np. kolaże w programach graficznych. Większość najpopularniejszych programów umożliwia takie operacje.

Rys. 3. **W tym przykładzie z obrazu termowizyjnego została odcięta część histogramu z jasnymi odcieniami skali szarości, które reprezentują chłodniejsze obiekty. Pozostałą część obrazu nałożono z 50-proc. przenikalnością na obraz z kamery światła widzialnego** (źródło: Baza TNO, modyfikacja obrazu: Jakub Sobek)

Najczęściej w dostępnych na rynku budżetowych kamerach termowizyjnych właśnie ta metoda fuzji jest stosowana. Obraz wizyjny stanowi podkład, na niego nakłada się z pewną przeźroczystością obraz termowizyjny. W niektórych aplikacjach metoda ta się sprawdza, jednak zazwyczaj otrzymany obraz wyjściowy nie ma zbyt wysokiej jakości.

W tej metodzie istotny jest dobór właściwej palety barwnej dla obrazu termowizyjnego, aby obserwowana scena była czytelna, a kolory najbardziej jaskrawe podkreślały np. najcieplejsze jej elementy.

Spotyka się również nieco bardziej złożone metody ustawiania przenikalności, polegające na definiowaniu tego parametru osobno dla każdego piksela. W ten sposób całkowitą przenikalność można ustawić dla obszarów z dolnego zakresu histogramu, co może reprezentować chłodniejsze obiekty, a zerową przepuszczalność dla górnych zakresów histogramu – obiekty cieplejsze. Dzięki temu na obraz wizyjny nakładane są tylko najcieplejsze obiekty w danej scenie. Odnosi się wówczas wrażenie, że obraz termowizyjny jest „progowany" temperaturowo.

Dodawanie krawędzi

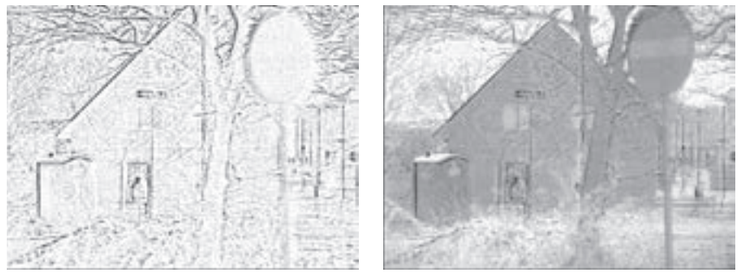
Nieco bardziej złożoną metodą tworzenia obrazu multimodalnego jest wykorzystanie obrazu światła widzialnego i dołożenie do niego jedynie krawędzi obiektów, które pochodzą z obrazu termowizyjnego. Tutaj złożoność obliczeniowa jest zazwyczaj nieco większa. Trzeba bowiem pamiętać, że filtracja obrazu jest operacją kontekstową, w której wartość każdego piksela obrazu wyjściowego wyznacza się jako kombinację pikseli z sąsiedztwa. Istnieje wiele algorytmów detekcji krawędzi – od korzystających z prostego filtrowania obrazu, poprzez coraz bardziej złożone i ciągle doskonalone.

Jedną z podstawowych metod detekcji krawędzi jest filtrowanie obrazu tzw. Krzyżem Robertsa. To operator łatwy w implementacji i nie wymaga dużej złożoności obliczeniowej, dlatego jest często stosowany w prostych aplikacjach. Aby obliczyć wartość każdego piksela na obrazie, wystarczy analiza tylko czterech pikseli, przy czym obliczenia są wykonywane tylko za pomocą operacji dodawania i odejmowania. Nie jest też wymagana dodatkowa parametryzacja tych obliczeń. Liczone są różnice luminancji pikseli położonych koło siebie po przekątnych, a następnie dodawane ich wartości bezwzględne. W ten sposób filtr wykrywa obszary o wysokiej częstotliwości, co często odpowiada rzeczywistym krawędziom obiektów. Najczęściej dane wejściowe dla takich filtrów stanowi obraz w skali szarości. Główną wadą tego operatora jest jego duża wrażliwość na szumy w obrazie i niezbyt skuteczna detekcja krawędzi wtedy, gdy są niewyraźne i nieostre na obrazie wejściowym.

> Z kilku podstawowych produktów można przygotować wiele różnych dań. Dwa wielomodalne obrazy także można łączyć na wiele sposobów, uzyskując różne efekty. Istotne, by zrozumieć sposób działania fuzji wizyjnej i wiedzieć, jakie daje możliwości, by lepiej je wykorzystywać w realnych aplikacjach.

Rys. 4. **Obraz po wykryciu krawędzi maską Robertsa i fuzja z obrazem z kamery światła widzialnego** (źródło: Baza TNO, modyfikacja obrazu: Jakub Sobek)

Rys. 5. **Obraz po wykryciu krawędzi maską Sobela i fuzja z obrazem z kamery światła widzialnego** (źródło: Baza TNO, modyfikacja obrazu: Jakub Sobek)



Rys. 6. **Obraz po wykryciu krawędzi operatorem Laplace'a i fuzja z obrazem z kamery światła widzialnego** (źródło: Baza TNO, modyfikacja obrazu: Jakub Sobek)

1	0
0	-1

Maska Robertsa

-1	0	1
-2	0	2
-1	0	1

Przykładowa maska Sobela

Lepsze rezultaty można uzyskać za pomocą dwuwymiarowej maski Sobela o wielkości 3 x 3. Jest ona szczególnie skuteczna przy detekcji krawędzi pionowych i poziomych. Z powodu większej maski złożoność obliczeniowa tego algorytmu jest większa, jednak jest on operatorem znacznie mniej wrażliwym na zaszumienie obrazu, generuje także znacznie wyższe wartości wyjściowe dla podobnych krawędzi obrazu w porównaniu z metodą Robertsa.

Trzecią metodą wartą uwagi jest różniczkowy operator Laplace'a. Główna różnica między Laplasjanem a innymi operatorami, takimi jak Robertsa czy Sobela, polega na tym, że są to maski pochodne pierwszego rzędu, a Laplasjan jest maską pochodną drugiego rzędu. Ponadto Laplasjan nie pomaga w wyszukiwaniu pionowych i poziomych krawędzi, a wyznacza zewnętrzne i wewnętrzne krawędzie obiektów. Od

tego, które z tych krawędzi zostaną wykryte, zależy, czy zastosowana maska będzie negatywna, czy pozytywna – środkowe elementy maski mają znak dodatni lub ujemy. Jest to zatem filtr, który gładkim zmianom jasności obrazu nadaje wartości bliskie zeru, a silnie wzmacnia nagłe zmiany jasności obrazu związane z krawędziami i brzegami obiektów obrazu.

0	1	0
1	-4	1
0	1	0

Pozytywna maska Laplace'a

0	-1	0
-1	-4	-1
0	-1	0

Negatywna maska Laplace'a

W zależności od użytych masek każdy obraz wyjściowy wygląda nieco inaczej, inny jest też efekt końcowy polegający na fuzji obrazu wizyjnego z obrazem termowizyjnym po zastosowaniu jednego z operatorów różniczkujących.

Dekompozycja i łączenie

Kolejny sposób tworzenia obrazów wielomodalnych jest oparty na tzw. dekompozycji dwóch obrazów, a następnie wykonaniu operacji odwrotnej – ich połączenia. Dekompozycję obrazu można wykonać metodą DWT (*Discrete Wavelet Transform* – dyskretna transformacja falkowa). Ma ona szerokie zastosowanie zarówno w przetwarzaniu, jak i kompresji obrazów. Opublikowany przez komitet JPEG standard kodowania obrazu JPEG 2000 opiera się właśnie na DWT. Dekompozycja DWT każdego z obrazów może być wykonywana wielokrotnie. Każdy obraz (sygnał) wejściowy poddawany takiej dekompozycji jest dzielony na dwa odrębne obrazy zawierające po połowie próbek. Możliwe jest także odtworzenie bezstratne obrazu wejściowego. Każdy zdekomponowany obraz można poddać kolejny raz transformacji DWT. Metodę tę w przetwarzaniu obrazów często wykorzystuje się do redukcji szumów czy filtracji obrazu.

Rys. 8. **Obraz wielomodalny wykonany za pomocą dekompozycji metodą DWT** (źródło: Baza TNO, modyfikacja obrazu: Jakub Sobek)

Dekompozycja dwóch obrazów, a także wszystkie wcześniej opisane metody (przenikanie obrazów, detekcja krawędzi za pomocą różnych operatorów) mogą zostać wykonane także w tym środowisku matlab.
Proces łączenia obrazów rozpoczyna się od wczytania obrazów o tej samej wielkości. Gdy różnią się wielkością, są przeskalowywane. Następnie jest wykonywana dekompozycja falkowa z wykorzystaniem konkretnego rodzaju falki. W tym przykładzie zastosowano falkę Daubechiesa. Tak zdekomponowane obrazy można ponownie połączyć. Zastosowana w tym przykładzie fuzja obrazu wymaga maksymalnej selekcji, porównuje się współczynniki DWT obu obrazów i zawsze wybiera współczynnik maksymalny, jedynie dla pasma niskiego liczy się średnią z obu współczynników. Po takim zespoleniu niskich i wysokich pasm dokonuje się rekonstrukcji obrazu za pomocą szybkiej dyskretnej transformacji odwróconej. W ten sposób obraz wynikowy jest kolejną odmianą multimodalnego obrazu z kamery światła widzialnego i kamery termowizyjnej.

Podsumowanie

Z kilku podstawowych produktów można przygotować wiele różnych dań. Dwa wielomodalne obrazy także można łączyć na wiele sposobów, a efekty mogą być różne.
Istotne jest, aby zrozumieć sposób działania fuzji i wiedzieć, jakie daje możliwości, by lepiej ją wykorzystywać w realnych aplikacjach. Ułatwi to podjęcie właściwej decyzji, czy w konkretnym zastosowaniu obraz prezentowany w takiej formie będzie użyteczny. Obraz wielomodalny nie tylko musi być obserwowany przez operatora systemu monitoringu, może też być obrazem wejściowym dla systemów analizy wizji.
Warto pamiętać, że kiedy kolejny producent oferuje kamerę łączącą obraz światła widzialnego z obrazem termowizyjnym, powinniśmy bliżej przyjrzeć się temu, jak taka fuzja jest realizowana. Same hasła marketingowe nie wystarczą, by móc podjąć właściwą decyzję – często tak naprawdę mają tylko zamaskować niską rozdzielczość oferowanej kamery.

Literatura

[1] Varuna De Silva, Jamie Roche and Ahmet Kondoz: *Robust Fusion of LiDAR and Wide-Angle Camera Data for Autonomous Mobile Robots*, Institute for Digital Technologies, Loughborough University, London 2018

[2] Rafał K. Mantiuk, Karol Myszkowski and Hans-Peter Seidel: *High Dynamic Range Imaging*, Wiley Encyclopedia of Electrical and Electronics Engineering, 2016

[3] Dipalee Gupta, Siddhartha Choubey: *Discrete Wavelet Transform for Image Processing*, International Journal of Emerging Technology and Advanced Engineering, 2015

[4] Alexander Toet: *TNO Image Fusion Dataset*, Netherlands Organisation for Applied Scientific Research, 2014

[5] Andrzej Materka, Paweł Strumiłło: *Wstęp do komputerowej analizy obrazów*, Politechnika Łódzka, Instytut Elektroniki, 2009

[6] http://homepages.inf.ed.ac.uk/rbf/HIPR2/featops.htm

[7] https://www.tutorialspoint.com/dip

[8] https://www.mathworks.com/matlabcentral/fileexchange/56494-image-fusion-based-wavelet-transform

BIO

Jakub Sobek
Absolwent Politechniki Poznańskiej na Wydziale Robotyki i Automatyki, specjalność Systemy wizyjne i multimedialne. Po studiach rozpoczął pracę w firmie Linc Polska na stanowisku trenera technicznego. W 2012 r. zdał egzamin trenera technicznego MOBOTIX, do dziś jest jedynym certyfikowanym trenerem MOBOTIX w Polsce. Posiada także certyfikat trenera rozwiązań FLIR Security Products. Od roku 2015 jest pracownikiem dydaktycznym oraz doradcą zarządu PISA.

Efektywny przesył danych i mocy

Nie trzeba nikogo przekonywać, że transmisja jest kluczowym elementem zapewniającym prawidłowe działanie systemów dozoru wizyjnego w dużych obiektach. Z tego względu wybór odpowiednich urządzeń do transmisji nabiera szczególnego znaczenia. **Wraz z postępem migracji systemów monitoringu wizyjnego do technologii IP wielu użytkowników przekonuje się, jak użyteczne i ekonomiczne mogą być rozwiązania *Ethernet-over-Coaxial* (EoC).**

William Pao
a&s International

W systemach dozoru wizyjnego transmisja sygnału ma ogromne znaczenie. W dużych organizacjach, chcących zapewnić sobie wgląd w otoczenie oraz ochronę pracowników i mienia, niezakłócony przesył obrazu wideo z kamer IP do rejestratora NVR jest sprawą kluczową. Oprócz danych infrastrukturą przesyłową dostarczana jest moc.

Technologie takie, jak PoE (*Power-over-Ethernet*) i PoC (*Power-over-Coaxial*) umożliwiają dostarczanie zasilania poprzez infrastrukturę sieciową IP lub opartą na okablowaniu koncentrycznym. Szczególnie PoE staje się podstawową metodą zasilania energią elektryczną kamer IP, dostarczając moc przez sieć Ethernet, a nie z dodatkowych źródeł prądu.

Dozór wizyjny oparty na połączeniach sieciowych IP zaczyna dominować, duży wzrost odnotowuje sprzedaż produktów i sprzętu PoE. Jak przewiduje firma analityczna Markets&Markets, wartość rynku rozwiązań PoE powinna osiągnąć 1 mld USD w 2022 r. (przy średniej rocznej stopie wzrostu szacowanej w latach 1016–2022 na 12,6 proc.). Zwiększające się wykorzystanie technologii PoE – wynikające z zalet tego rozwiązania, takich jak niski koszt instalacji, wygoda i niezawodność – doprowadziło do zwiększenia zapotrzebowania na sprzęt zapewniający zasilanie *Power-over-Ethernet* oraz urządzenia kompatybilne z tym standardem transmisji. Przekłada się to na większą sprzedaż rozwiązań PoE.

Największy wzrost na rynku rozwiązań *Power-over-Ethernet* w segmencie sterowników zasilanych urządzeń i układów scalonych jest spodziewany w latach 2016–2022. Będzie on stymulowany coraz większą sprzedażą urządzeń zasilanych PoE, szczególnie telefonów VoIP, bezprzewodowych punktów dostępowych i kamer IP.

Czego poszukują użytkownicy

W przypadków dużych obiektów użyteczności publicznej, lotnisk czy elektrowni poszczególne elementy wdrożonej na dużym obszarze infrastruktury przesyłowej mogą być oddalone o kilometry od siebie albo od centrum sterowania. Wysłanie pracowników po to, by sprawdzili każdy element systemu, jest wtedy kosztowne i czasochłonne, dlatego przy rozległych instalacjach znaczenia nabiera możliwość zdalnej kontroli stanu urządzeń.

To dlatego wielu operatorów dużych systemów zdecydowało się na stworzenie zarządzanego środowiska. Przykładowo, gdy jeden z przełączników sieciowych w obiekcie zaczyna nagle otrzymywać duże ilości danych, należy przydzielić mu szersze pasmo dla określonego typu ruchu, np. strumieniowania wideo, aby zapobiec „gubieniu" danych. Jeśli można zrobić to zdalnie, nie trzeba wysyłać pracownika do urządzenia. Dostępne są nie tylko rozwiązania umożliwiające zdalne zarządzanie switchami, ale także oprogramowanie zarządzające urządzeniami dozoru wizyjnego. Przy użyciu intuicyjnego interfejsu graficznego typowy użytkownik komputera może zdalnie zarządzać sprzętem, kontrolować i go monitorować. Pozwala to ograniczyć personel techniczny i liczbę pracowników zajmujących się utrzymaniem ciągłości pracy systemu.

Innym parametrem transmisji, wymaganym przez użytkowników dużych obiektów, jest niezawodność, czyli zapewnienie stabilnego przesyłu danych i mocy – bez przerw w działaniu i nieplanowanych przestojów. Systemy często działają w trudnym środowisku i są narażone na niesprzyjające warunki atmosferyczne. W zakładach produkcyjnych dochodzi obecność substancji chemicznych, które powodują korozję. Dlatego kluczowe staje się posiadanie sprzętu o wzmocnionej konstrukcji odpornej na wpływ środowiska pracy.

W przypadku instalacji związanej z mediami użytkowymi będą pracowały w terenie, trzeba więc zapewnić ich działanie w szerokim zakresie temperatury od -40 do +75°.

JAKĄ TOPOLOGIĘ SIECIOWĄ WYBRAĆ DLA DANEGO PROJEKTU

Sieć spełnia ważną rolę w systemie zabezpieczeń dużych obiektów. Sprzęt do transmisji nie tylko powinien być wzmocniony i niezawodny, ale także musi zapewniać optymalny przesył danych i mocy.

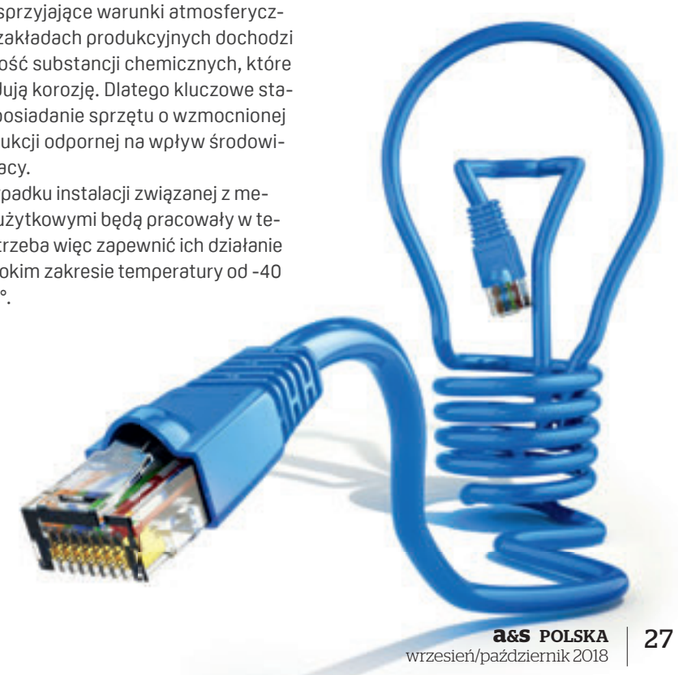
Z tego względu, już na etapie projektowania systemu należy określić potrzeby w zakresie topologii sieci. Do wyboru są różne topologie sieci oraz sposoby implementowania urządzeń i sprzętu sieciowego w systemie ochrony. Trzy podstawowe to: magistrala, pierścień i gwiazda. Każda z nich ma zalety i wady.

W układzie magistrali wszystkie węzły lub urządzenia są połączone z głównym przewodem, którym dane są transmitowane z jednego punktu do drugiego. Ponieważ topologia opiera się na jednym przewodzie, jest stosunkowo tania i łatwa. Gdy w użyciu jest natomiast jeden kabel, jego awaria prowadzi do unieruchomienia całego systemu.

Z kolei topologia gwiazdy zakłada istnienie centralnego węzła (którym jest hub lub switch), łączącego urządzenia w trybie punkt-punkt. Wszystkie dane przechodzą przez switch, który następnie przekazuje je do odpowiedniego odbiorcy. „Gwiazdę" także łatwo się instaluje i łatwo rozbudowuje, ponieważ użytkownik musi tylko dodać nowy przewód, który połączy kolejną kamerę z systemem. Ponieważ każde urządzenie wymaga oddzielnego przewodu, ta topologia może być droższa. A skoro wszystkie dane przechodzą przez switch, to staje się on pojedynczym punktem awarii – gdy przełącznik sieciowy się zepsuje, nie działa cały system.

Wreszcie topologia pierścienia, która jest najbardziej niezawodna. Do pierścienia są podłączone wszystkie urządzenia. Gdy jedno z nich się zepsuje, dane są przekierowywane do pierścienia zapasowego, który przejmuje jego pracę.

Wybór odpowiedniej topologii zależy od wielu czynników, w tym aplikacji, a także budżetu, jakim dysponuje użytkownik, oraz jego oczekiwań względem niezawodności. W przypadku magistrali urządzenia są połączone szeregowo – przykładem jej zastosowania mogą być autostrady. Z kolei w topologii gwiazdy mamy do czynienia z transmisją punkt-punkt, więc będzie przydatna, gdy wszystkie urządzenia muszą łączyć się z pojedynczą lokalizacją, np. centrum monitoringu.



JAK WYLICZYĆ BILANS MOCY

Większość współczesnych kamer IP jest zasilana poprzez sieć Ethernet, a nie z oddzielnego źródła prądu. Dlatego na etapie projektowania tego rodzaju instalacji trzeba obliczyć, jaka całkowita moc jest potrzebna w danej lokalizacji.

Obliczanie bilansu mocy sprowadza się do określenia liczby wymaganych kamer i mocy pobieranej przez każdą z nich. Użytkownik musi obliczyć całkowitą moc pobieraną przez wszystkie kamery podłączone do tego samego switcha PoE, a następnie dobrać najbardziej odpowiadający wynikowi przełącznik sieciowy. Przykładowo, jeśli mamy osiem kamer wymagających mocy 15,4 W oraz dwie kamery 30-watowe, to bilans mocy wynosi 183,2 W. Należy wybrać 10-portowy switch z technologią *Power-over-Ethernet*, który jest w stanie dostarczyć moc 183,2 W.

Obecne standardy PoE – IEEE 802.3af i IEEE 802.3at – zapewniają odpowiednio: 15,4 W i 30 W na każdym porcie switcha z PoE. Coraz więcej dostępnych na rynku kamer wymaga jednak mocy przekraczającej 30 W. Są i takie, które pobierają 60 W, jeśli korzystają z rozwiązań do ogrzewania bądź chłodzenia w celu ochrony przed ekstremalnymi warunkami środowiskowymi. Gdy tego rodzaju kamera nie korzysta z ogrzewania, nie potrzebuje nawet 15 W, gdy jednak ogrzewanie musi być włączone, urządzenie wymaga większej mocy, niż są w stanie zapewnić obecne standardy PoE. Wychodząc naprzeciw tym trendom, producenci przełączników sieciowych oferują urządzenia posiadające obok portów 15,4 W i 30 W także takie, które zapewniają 60 W. Ich użytkownicy mogą wtedy rozdzielać moc według swoich potrzeb. Określenie bilansu mocy nie jest więc procesem skomplikowanym, ponieważ zależy tylko od liczby kamer i mocy pobieranej przez każdą z nich. Jeśli klient będzie potrzebował pomocy, to dostawca albo integrator systemów poprowadzi go przez ten proces i pomoże w wyborze najbardziej odpowiedniego do danego projektu produktu bądź rozwiązania.

EoC – nowe życie starszych instalacji

Globalnie niemal wszystkie nowe projekty systemów zabezpieczeń są oparte na IP. Klienci wybierają tę technologię ze względu na korzyści, jakie oferują systemy dozoru wizyjnego IP (wyższa rozdzielczość i możliwości zastosowania bardziej zaawansowanej analityki, zapewniającej większy wgląd w monitorowane środowisko). W przypadku starszych obiektów i dużych projektów opartych na infrastrukturze analogowej całkowita migracja do technologii IP może być jednak posunięciem kosztownym. Bardziej ekonomiczną alternatywą dla wymiany infrastruktury może być jej modernizacja z wykorzystaniem rozwiązań EoC (*Ethernet-over-Coaxial*).

Na całym świecie nowe budynki i projekty wykorzystują sieciowe systemy dozoru wizyjnego, gdyż to rozwiązanie oferuje wyższą jakość obrazu, lepszą integrację kamer z innymi urządzeniami sieciowymi, a także większe możliwości analityczne.

O tym, że IP podbija branżę dozoru wizyjnego, świadczą badania rynkowe. Firma Stratistics MRC światowy rynek monitoringu wizyjnego wyceniała na 19,5 mld dol. w 2015 r., a do 2022 r. jego wartość ma wynieść już 63,2 mld dol., przy średnim wzroście rocznym rzędu 18,3 proc. Sprzedaż systemów dozorowych IP ma natomiast rosnąć szybciej, bo o 25 proc. rocznie.

Także właściciele dużych istniejących systemów VSS, opartych na okablowaniu koncentrycznym myślą o migracji do IP, by móc wykorzystać zalety tej technologii. Muszą jednak się liczyć z różnymi wyzwaniami, z których największym jest koszt pełnej wymiany infrastruktury analogowej.

W przypadku starszych instalacji trzeba ocenić stopień trudności zamontowania nowych kabli, przewodów i gniazd. Taka operacja może doprowadzić do zniszczenia kosztownego wystroju i umeblowania obiektu. Jeśli przewód ma być wprowadzany w ścianę, trzeba będzie wykonać w niej korytka. Innym problemem jest wpływ wymiany infrastruktury na prowadzoną działalność. Jeśli zależy nam na jak najmniejszym jej zakłóceniu, prace będą musiały być prowadzone jedynie w uzgodnionych godzinach.

Rozwiązaniem jest EoC

W związku z takimi wyzwaniami wymiana tylko urządzeń końcowych, czyli kamer i rejestratorów, oraz pozostawienie koncentrycznej infrastruktury kablowej mogłaby być bardziej ekonomicznym i niewymagającym tak dużego nakładu pracy rozwiązaniem. Z pomocą przychodzi technologia *Ethernet-over-Coaxial* (EoC), która łączy urządzenia IP z adapterami EoC, konwertując sygnał cyfrowy na analogowy, by mógł być dalej przesyłany po kablu koncentrycznym. Także moc generowana przez przełączniki sieciowe PoE może być przesyłana przewodem koncentrycznym, dzięki wykorzystaniu technologii *Power-over-Coaxial* lub *Power-over-Link*.

By zaspokoić potrzeby użytkowników, dostawcy oferują wiele różnych produktów i rozwiązań EoC, które umożliwiają łączenie kamer IP i innych urządzeń poprzez kabel koncentryczny na dystansie do 500 m, dzięki czemu modernizacja używanego dotychczas systemu staje się łatwiejsza i tańsza. Rozwiązania obejmują jedno- i wieloportowe adaptery i odbiorniki z wbudowanymi przełącznikami oraz komunikacją sieciową, która zapewnia generowanie PoC lub przekazywanie mocy. Dostępne są produkty do stosowania zarówno we wnętrzach, jak i na zewnątrz obiektów.

Są też oferowane rozwiązania *Ethernet-over-UTP* (EoUTP), które zwiększają długość przesyłu nawet do 2,4 km oraz dostarczają moc 30 W przez pojedynczy przewód UTP. W rezultacie technologia *Ethernet-over-Coaxial* okazuje się świetnym, bo efektywnym zarówno jeśli chodzi o koszty, jak i nakłady pracy rozwiązaniem dla użytkowników końcowych, chcących migrować do dozoru wizyjnego opartego na protokole IP.

Dobrą rekomendacją jest udane wdrożenie w mieście liczącym ponad 2 mln mieszkańców, którego władze doszły do wniosku, że konieczna jest modernizacja miejskiego systemu monitoringu i przejście z systemu analogowego na cyfrowy. System obejmował ponad 100 większych węzłów (w każdym zainstalowano od 6 do 8 kamer) oraz wiele małych, które nie posiadały własnych źródeł prądu do zasilania kamer IP. Miasto oczekiwało niezawodnego rozwiązania, które mogłoby sobie poradzić z dużym ruchem sieciowym i byłoby zabezpieczone przed dłuższymi przestojami w razie awarii łącza. Firma EtherWAN poradziła sobie z tym złożonym projektem, stosując połączenie tradycyjnej topologii sieciowej z rozwiązaniami własnymi. Problemem były zwłaszcza te obszary, które wymagały monitoringu, ale nie dysponowały lokalnym źródłem zasilania i były oddalone o więcej niż 100 m od najbliższego węzła (co uniemożliwiało zastosowanie technologii PoE). W takich przypadkach zastosowano przełączniki sieciowe w połączeniu z przedłużaczami sieci Ethernet, co umożliwiło transmisję zarówno danych, jak i mocy poprzez istniejące okablowanie (w tym przypadku kabel koncentryczny z wcześniejszej instalacji monitoringu wizyjnego).

Ethernet-over-Coaxial (EoC) łączy urządzenia IP z adapterami EoC, konwertując sygnał cyfrowy na analogowy, by mógł być dalej przesyłany po kablu koncentrycznym.

Ponieważ udało się spełnić wymogi dotyczące mocy i przepustowości za pomocą istniejącego okablowania koncentrycznego, zaoszczędzono zarówno pieniądze, jak i czas. Rozwiązanie zwiększyło możliwości policji w zakresie monitoringu w obszarach, które wcześniej były trudno dostępne.

INNOVACJA

Tego jeszcze nie było! Kamera termowizyjna i tradycyjna w jednej obudowie plus dodatkowe funkcje...

FLIR Saros

Ochrona obwodowa i monitorowanie terenów otwartych to temat ważny dla wszystkich instytucji, które priorytetowo traktują zabezpieczenie dużych powierzchni i znajdującego się na nich mienia. **Wydaje się to dość proste w realizacji, jednak jeśli przeanalizować możliwe scenariusze naruszeń i rodzaje realnych zagrożeń, okazuje się, że skuteczne zabezpieczenie danego obiektu stanowi nie lada wyzwanie.**

FLIR Systems (FLIR) opracował kamerę Saros przeznaczoną do ochrony obwodowej, która może sprostać wielu wymaganiom. To kompaktowe rozwiązanie łączące w jednym urządzeniu technologię termowizyjną z technologią światła widzialnego oraz analityką wizji obejmujące:

- przetwornik termowizyjny,
- przetwornik światła widzialnego o rozdzielczości 1080p lub 4K,
- oświetlacze LED w zakresach bliskiej podczerwieni i światła widzialnego,
- analitykę wideo.

Całość zamknięto w kompaktowej obudowie, łącząc różne funkcjonalności i minimalizując liczbę wymaganego dodatkowo sprzętu.

Tradycyjne systemy alarmowe stosowane w ochronie obwodowej nie są tanie podczas wdrażania, montażu czy w trakcie późniejszego użytkowania, a możliwy odsetek fałszywych alarmów, zależnie od stosowanej technologii, może być znaczny. Projektując system, należy mieć świadomość tego, że kamery światła widzialnego w ochronie obwodowej są narażone na różne czynniki zakłócające, takie jak deszcz, mgła czy nawet próby oślepienia kamery przez odbite promienie słoneczne. Aby je wyeliminować, rozwiązanie FLIR Saros wykrywa potencjalnego intruza z wykorzystaniem termowizji i zaawansowanej analityki obrazu, a weryfikację tego zdarzenia ułatwia kamera światła widzialnego o rozdzielczości nawet 4K doświetlana przez oświetlacze LED emitujące w paśmie światła widzialnego i bliskiej podczerwieni. W najbardziej zaawansowanym modelu do dyspozycji jest 6 rdzeni termicznych połączonych w matrycę o łącznym poziomym kącie widzenia minimum 270° i dodatkowo 3 moduły kamerowe 4K każdy, oferujące sumaryczną rozdzielczość nawet 24 Mpix. Rozwiązanie to idealnie nadaje się do nadzorowania otwartych terenów o zróżnicowanej powierzchni. FLIR Saros, bazując na czterech technologiach, dostarcza służbom mundurowym i ratowniczym dokładnie zlokalizowane, zweryfikowane alarmy oraz sprawdzone dane (bez względu na słabe oświetlenie czy niesprzyjające warunki atmosferyczne). W efekcie czas reakcji i interwencji zostaje skrócony, co zapobiega utracie sprzętu, towarów czy klientów. Ponadto większy zasięg monitorowanego obszaru pozwala zmniejszyć liczbę potrzebnych urządzeń. Zastosowanie kamer FLIR Saros zapewnia:

- całodobowy monitoring bez konieczności stosowania dodatkowych kamer tradycyjnych,
- dwukierunkowe audio w czasie rzeczywistym,
- możliwość integracji z czujnikami alarmowymi poprzez wejścia I/O,
- działanie prewencyjne z użyciem oświetlenia światłem białym,
- zmniejszenie liczby fałszywych alarmów, zachowując dobrą wykrywalność i klasyfikację,
- identyfikację niechcianych przedmiotów i obiektów,
- integrację z centralnymi platformami monitoringu i systemami zarządzania wideo.

Dzięki kompaktowej budowie i połączeniu wielu technologii w jednym urządzeniu FLIR Saros jest rozwiązaniem atrakcyjnym pod względem technologicznym i ekonomicznym. Kamera jest łatwa i szybka w montażu, minimalizuje wydatki na infrastrukturę i zwiększa wydajność wdrażania. To idealna propozycja jako skuteczna alternatywa dla tradycyjnych metod ochrony perymetrycznej. Rozwiązania FLIR Saros z pewnością zostaną docenione również przez centra monitoringu, stosujące niezawodne, nowoczesne metody weryfikacji wizyjnej.

SATEL
ul. Budowlanych 66
80-298 Gdańsk
www.satel.pl

Monitorowanie zdarzeń

w systemach alarmowych INTEGRA i INTEGRA Plus

Powiadomienie centrum monitoringu o zagrożeniu to jedno z kluczowych zadań systemu alarmowego. Istotne są szybkość wysłania informacji oraz gwarancja jej dostarczenia. Jak rozwiązać problem skutecznego monitoringu w obiektach o najwyższym stopniu zabezpieczenia, takich jak banki czy infrastruktura krytyczna?

Na rynku dostępnych jest wiele central alarmowych, co pozwala dobrać model odpowiedni do danego obiektu. Jednym z kryteriów wyboru może być właśnie sposób realizacji monitoringu zdarzeń.

Chcąc mieć pewność, że nadany przez system komunikat zostanie szybko doręczony do odbiorcy, warto sięgnąć po rozwiązanie umożliwiające korzystanie z monitoringu dwutorowego *(Dual Path Reporting)*, spełniające wymagania normy EN 50136. Przykładem może być instalacja bazująca na spełniającej wymagania Grade 3 centrali INTEGRA Plus.

Monitoring w systemach INTEGRA/INTEGRA Plus

Centrale INTEGRA zawierają dialer telefoniczny (monitoring przez PSTN) lub telefon GSM (tylko INTEGRA 128-WRL, monitoring: GPRS, SMS, audio).

W razie konieczności wyboru innych opcji niezbędne jest dołączanie modułów rozszerzających, np. ETHM-1 Plus (monitoring TCP/UDP).

Aby dane mogły być przesyłane za pośrednictwem sieci komórkowej, należy sięgnąć po moduł GSM/GPRS. Do tej pory na rynku brakowało urządzeń, które komunikowałyby się z centralami w sposób natywny. Uzupełniając tę lukę, SATEL wprowadził do oferty magistralowy moduł INT-GSM.

Praca w tandemie i Dual Path Reporting

INT-GSM może pracować z centralą INTEGRA na dwa sposoby. Pierwszy polega na podłączeniu modułu do magistrali manipulatorów oraz portu RS-232. Drugi zakłada współpracę z ETHM-1 Plus – komunikatory są spięte ze sobą przez RS-485, a magistrala manipulatorów centrali oraz jej port RS-232 podłączone do modułu ethernetowego. Z punktu widzenia monitoringu zdarzeń największą zaletą tego rozwiązania jest obsługa monitoringu *Dual Path Reporting*. Wykorzystuje on kanały Ethernet i GPRS, a komunikacja przez każdy z nich jest stale testowana. Ponadto można określić priorytety przesyłania informacji przez Ethernet, GPRS (karta SIM1), GPRS (karta SIM2), SMS (SIM1) i SMS (SIM2).

Co istotne, INT-GSM może wykorzystywać GPRS jako zapasowy tor łączności dla sieci Ethernet.

Co jeszcze potrafi moduł INT-GSM?

Moduł realizuje monitoring GPRS i SMS, ale także informuje o zdarzeniach wiadomościami SMS, e-mail (INTEGRA Plus) oraz powiadomieniami PUSH. Komunikaty bazują na pamięci zdarzeń centrali i nie ma konieczności ręcznej konfiguracji ich treści. Dzięki INT-GSM można zdalnie sterować funkcjami systemu alarmowego – przez SMS i CLIP. Nowością jest zastosowanie modułu telefonicznego, który może jednocześnie odbierać wiadomości SMS i połączenia przychodzące przez obie karty SIM. Zdalne sterowanie systemem jest dostępne również z aplikacji mobilnej INTEGRA CONTROL (Android i iOS) oraz programu administracyjnego GUARDX.

Dzięki możliwości korzystania z usługi zestawiania połączeń SATEL konfiguracja komunikacji między centralą a ww. oprogramowaniem jest bardzo szybka. Opcja ta znajduje zastosowanie także przy zdalnym połączeniu i konfiguracji systemu z poziomu programu DLOADX. Ponadto program UpServ umożliwia aktualizowanie firmware'u modułu przez GPRS, bez konieczności dojazdu do obiektu i demontażu urządzenia.

Administratorzy rozproszonych systemów bezpieczeństwa bazujących na centralach INTEGRA i INTEGRA Plus mogą zastosować moduł INT-GSM przy ich integracji za pomocą oprogramowania INTEGRUM.

Izba Technicznej Ochrony Mienia EUROALARM
ul. Piękna 25,
85-303 Bydgoszcz
www.euroalarm.com.pl

Zadymiacz pilnie poszukiwany

Z analizy materiałów wideo wynika, że w 40% przypadków włamywacz, po sforsowaniu zabezpieczeń mechanicznych, przebywa w strefie chronionej od 3 do 6 minut. **Łatwo oszacować, o ile mniejsze byłyby straty, gdyby intruz, ze względu na dynamicznie pogarszającą się w pomieszczeniu widoczność, miał do dyspozycji tylko 30 sekund.**

Systemy zadymiające są znane od lat. Popularność tego technicznego środka w systemach sygnalizacji włamania była jednak umiarkowana ze względu na wysoką cenę, a także rozmiary urządzenia nieprzystające do wielu aranżacji.

UKARA DyM to innowacyjny antykradzieżowy system ochrony pozbawiony wymienionych wad, który całkowicie zmienia filozofię rozwiązania. Elementem wykonawczym jest kapsuła generująca w krótkim czasie dużą ilość dymu. Wytworzony dym stanowi środowisko o bardzo niskiej przejrzystości, uniemożliwiając intruzowi swobodne i dokładne działanie. Próba szybkiej kradzieży staje się niemożliwa. Czas zadymienia i stopień przejrzystości powietrza zależą od kubatury chronionego pomieszczenia. Jedna kapsuła zadymia pomieszczenie o kubaturze do 100 m^3 w kilkanaście sekund.

Docelowo oferta urządzeń zostanie rozszerzona o rozwiązania do montażu sufitowego nawierzchniowego i dyskretnych wersji do sufitów podwieszanych. Obecnie firma Euroalarm uruchomiła sprzedaż wersji do montażu naściennego na wysokości od 1,8 o 3,0 m od posadzki. Niewielkie wymiary i kilkakrotnie niższa cena kapsuły wymiennej (ok. 300 zł netto) czynią z tego urządzenia alternatywę w zabezpieczeniu niektórych dóbr.

UKARA DyM z kapsułą zadymiającą jest wyposażona w układ elektroniczny i zasilacz z podtrzymaniem akumulatorowym. Urządzenie zostało przygotowane pod kątem kilku scenariuszy aktywowania kapsuły, również z możliwością dezaktywowania akcji na etapie prealarmu. Może pracować zarówno jako element wykonawczy istniejącego systemu sygnalizacji włamania i napadu, jak i samodzielnego urządzenia wyzwalanego z czujki PIR, sterownika radiowego, przycisku napadowego itp.

Zastosowanie takiego zabezpieczenia może być wielorakie: od witryn sklepowych, pomieszczeń z bronią palną, po przedsionki bankomatów. Montowane są również w bliskim sąsiedztwie drzwi wejściowych jako prewencyjne zabezpieczenie przed siłowym wtargnięciem rozbójniczym.

Jednak głównym odbiorcą systemu UKARA DyM są jednostki organizacyjne, w których przetwarza się informacje niejawne o klauzuli „tajne" lub „ściśle tajne", oraz instytucje o wyższych obostrzeniach dotyczących ochrony danych wrażliwych (RODO).

Należy podkreślić, że substancje chemiczne w dymie nie stanowią zagrożenia życia ludzi, a po aktywacji kapsuły pomieszczenie należy jedynie starannie przewietrzyć. Po przewietrzeniu nie jest wymagane sprzątanie lub mycie, gdyż środek nie pozostawia żadnych śladów.

Producent przeprowadził analizę składu chemicznego dymu, zakładając krótkotrwałe wystawienie się na jego działanie. Zaleca się, aby po aktywacji zadymienia okres pobytu ludzi nie był dłuższy niż 15 minut. Wszystkie wartości zmierzonych substancji mieszczą się w limitach określonych w aneksie do Dyrektywy UE 2017/164. Przykładowo: tlenek węgla (CO) – wartość wykryta: 28 mg/m^3, limit wg dyrektywy: 117 mg/m^3, chlorek metylenu – wartość wykryta <1,5 mg/m^3, limit wg dyrektywy 706 mg/m^3. Dokładna specyfikacja jest dostarczana z instrukcją urządzenia.

To rozwiązanie z pewnością zrewolucjonizuje rynek systemów sygnalizacji włamania i usług Agencji Ochrony.

SALTO Systems Sp. z o.o. Oddział w Polsce
ul. 17 Stycznia 45 A, Warszawa
tel. +48 609 017 777
info.pl@saltosystems.com | **www.saltosystems.com**

Modnie i wygodnie

Technologia mobilna w systemach kontroli dostępu

Technologia bezprzewodowa w systemach kontroli dostępu staje się już standardem. Zapewnia większą wygodę menedżerom i użytkownikom systemu, a także wszechstronność, dzięki której współczesne systemy KD zwiększają sprawność działania, bezpieczeństwo i kontrolę.

W Salto jesteśmy tego świadomi, dlatego najnowsze innowacje w tej dziedzinie prezentowaliśmy klientom na targach Ifsec i w Essen, dzięki czemu nasze rozwiązania są coraz bardziej popularne. Dotyczy to np. Salto SPACE, platformy z funkcjami wirtualnej sieci SVN, a także Salto KS, kompleksowej i niezawodnej platformy kontroli dostępu opartej na chmurze – mówi Marc Handels, dyrektor ds. marketingu i sprzedaży w Salto Systems.

Jedna aplikacja, kilka technologii

Salto JustIN Mobile to aplikacja mobilna stosowana na platformie Salto SPACE, oparta na firmowej i sprawdzonej technologii SVN (*Salto Virtual Network*). Klucz mobilny JustIN zaprojektowano do komunikacja pomiędzy smartfonem a zamkiem elektronicznym, aby usprawnić działanie systemu. Według Marca Handelsa podstawą jest funkcjonalność, która zwiększa wygodę użytkownika.

– Nasza aplikacja klucza mobilnego JustIN jest dostępna na systemy iOS i Android, czyli pokrywa 98% rynku smartfonów. Zapewnia dodatkową zaletę, ponieważ w przypadku Androida do bezprzewodowego połączenia z elektronicznym zamkiem aplikacja korzysta z technologii BLE (Bluetooth Low Energy) – Bluetooth Smart oraz NFC (Near Field Communications) – wyjaśnia. Dzięki temu mobilne rozwiązania Salto są kompatybilne z prawie wszystkimi produktami dostępnymi w portfolio firmy: okuciami, czytnikami naściennymi, a także wkładkami. Użycie NFC w połączeniu z aplikacją klucza mobilnego JustIN Mobile zwiększa zainteresowanie klientów dostarczanymi przez Salto przyszłościowymi systemami, ponieważ nawet już oferowane okucia i wkładki mogą korzystać z tej innowacyjnej technologii po uaktualnieniu oprogramowania *firmware*.

Dwukierunkowa komunikacja

– Zawsze byliśmy świadomi, że technologia mobilna może przynieść dodatkowe możliwości naszym produktom, co ostatecznie pozwala dostarczać klientom znacznie więcej funkcjonalności. Klucz mobilny JustIN Mobile został zaprojektowany na tych założeniach, a dzięki naszej technologii SVN opracowaliśmy technologię mobilną z dwukierunkową komunikacją. W ten sposób JustIN Mobile konwertuje praktycznie każde urządzenie kontroli dostępu w trybie offline na urządzenie online bez dodatkowego sprzętu i bez instalacji – dodaje M. Handels.

Dzięki tej aplikacji administrator systemu może zdalnie zarządzać kluczami online, a także łatwo i szybko przedłużać ich ważność. Wszystkie prawa dostępu są wysyłane z oprogramowania zarządzającego Salto ProAccess SPACE bezpośrednio do smartfona użytkownika, bez względu na to, gdzie on się znajduje. Dzięki temu zawsze będzie miał dostęp do swoich danych, będzie także mógł natychmiast zmienić uprawnienia lub aktywować swoją kartę.

W tym samym czasie aplikacja JustIN Mobile przesyła informację z urządzenia offline do oprogramowania zarządzającego, powiadamiając, że np. użytkownik uzyskał dostęp do drzwi. Ponieważ platforma JustIN Mobile korzysta z technologii wirtualnej sieci SVN, możliwe jest również otrzymanie statusu baterii zamka (okucia) lub wkładki, co zwiększa ilość informacji o systemie. Zapobiega to potencjalnym awariom i ułatwia prace konserwacyjne. Inną kluczową cechą jest dystrybucja zaktualizowanych czarnych list, która zwiększa kontrolę nad uprawnieniami osób, a tym samym podnosi poziom bezpieczeństwa obiektu.

Nie ma potrzeby dodatkowej infrastruktury

– A wszystko to bez dodatkowej infrastruktury – podkreśla Marc Handels. *– Wyobraźmy sobie posiadanie samodzielnego zamka elektronicznego offline (okucia), gdzie nie można zainstalować systemów bezprzewodowych z powodu braku połączenia z Internetem. JustIN Mobile pozwala monitorować wejście, wiedzieć, kto miał do niego dostęp, jaki jest stan baterii, a nawet nadać zdalnie uprawnienia natychmiastowego dostępu do drzwi każdemu zweryfikowanemu użytkownikowi. Wystarczy przyłożyć smartfon do drzwi bez potrzeby noszenia różnych poświadczeń i posiadania zawsze aktualnych danych uwierzytelniających. To również udogodnienie dla*

menedżerów obiektu, ponieważ będą mogli uzyskać wszystkie informacje dotyczące punktów dostępu (przejść kontrolowanych), a tym samym osób znajdujących się w obiekcie w czasie rzeczywistym – przedstawia zalety tego rozwiązania.

Więcej niż klucz

Aplikacja JustIN Mobile udostępnia również inne funkcje, które zapewniają użytkownikowi większą funkcjonalność. Pozwala przechowywać więcej niż jeden klucz, bez względu na to, czy jest to klucz do biura, czy do pokoju w hotelu na wyjazd służbowy na następny dzień. Oba mogą być przetwarzane i udostępniane przez aplikację bez zakłóceń. Aplikacja może też wysyłać do użytkownika wiadomości dotyczące jego różnych kluczy, a nawet informacje o lokalizacji hotelu, do którego ma jechać. To nie tylko klucz do drzwi, ale także wszelkie informacje potrzebne użytkownikowi.

Wszystkie te korzyści są już doceniane, JustIN Mobile jest stosowany w setkach tysięcy drzwi na całym świecie, głównie w hotelach, a coraz częściej także w obiektach komercyjnych i opieki zdrowotnej. Salto czerpie wiele z tych praktycznych doświadczeń i nadal rozwija tę technologię, podczas gdy inni dopiero zaczynają stosowanie technologii mobilnej w swoich rozwiązaniach.

Klucze mobilne w rozwiązaniach w chmurze

– Od wielu lat jesteśmy pionierami w dziedzinie systemów kontroli dostępu w chmurze. Dlatego uważamy, że nasza platforma Salto KS Keys (Keys as a Service) jest najbardziej zaawansowanym i elastycznym rozwiązaniem – mówi Marc Handels. *– Oferujemy kontrolę dostępu niezawodną i stabilną, stosowaną w dziesiątkach tysięcy drzwi na całym świecie. Dzięki temu zdobywamy doświadczenie, którego nie ma żaden inny dostawca.*

Salto KS proponuje rozwiązanie, które redukuje potrzebę złożonej infrastruktury IT, nie wymaga nawet instalowania oprogramowania. W porównaniu z tradycyjnymi rozwiązaniami zabezpieczeń zapewnia doskonałą funkcjonalność i wydajność. Teraz Salto KS korzysta również z mobilnego dostępu dzięki nowej funkcjonalności kluczy mobilnych włączonych do aplikacji w celu zwiększenia elastyczności i wygody systemu kontroli dostępu opartego na rozwiązaniach w chmurze.

Zwiększona elastyczność dla administratorów i użytkowników

Aplikacja zapewnia administratorom pełną elastyczność, ponieważ pozwala bezpośrednio ze smartfona zarządzać kontrolą dostępu użytkowników i drzwi z dowolnego miejsca i w dowolnym czasie. Zablokowanie uprawnień użytkownika lub zdalne otwarcie drzwi było od początku możliwe, ale oprócz nowej funkcji kluczy mobilnych administrator może wysłać referencje bezpośrednio na smartfon użytkownika, eliminując konieczność przekazywania klucza fizycznego.

– Tylko ze smartfonem możesz kontrolować swoją nieruchomość lub uzyskać do niej dostęp, zwiększając w ten sposób elastyczność naszej kontroli dostępu opartej na chmurze – dodaje Marc Handels. *– Użytkownicy mogą również czerpać korzyści, ponieważ klucze mobilne Salto KS eliminują potrzebę posiadania poświadczeń fizycznych. Dodatkową zaletą jest możliwość wysyłania referencji bezpośrednio do użytkownika, ponieważ poświadczenia można rozpowszechniać automatycznie bez konieczności oczekiwania na ich fizyczne otrzymanie. Jest to idealne rozwiązanie np. dla korzystających ze wspólnych przestrzeni do pracy, w których użytkownicy mogą przemieszczać się z jednej lokalizacji do drugiej z jeszcze większą łatwością.*

ASSA ABLOY Poland
ul. Jana Olbrachta 94, 01-102 Warszawa
tel. 22 751-53-54
www.assaabloy.com.pl

Pionierski system zabezpieczeń dla branży telekomunikacyjnej

Jednym z kluczowych sektorów infrastruktury krytycznej jest branża telekomunikacyjna, umożliwiająca przesyłanie wszelkich informacji i danych – podstawę funkcjonowania każdej działalności gospodarczej.

Case Study

Zapewnienie ciągłości działania infrastruktury krytycznej staje się jednym z najważniejszych wyzwań dla firm projektujących kompleksowe systemy zabezpieczeń. Aby ograniczyć ryzyko wszelkich zdarzeń niepożądanych, niezbędne jest stworzenie dedykowanego i pionierskiego rozwiązania. Jakie rozwiązania w tym zakresie proponuje światowy lider branży security, marka ABLOY?

Wyzwanie rzeczywistości cyfrowej

Zapewnienie bezpieczeństwa wszelkich danych przesyłanych drogą elektroniczną oraz nieprzerwalności świadczenia usług stanowi jedno z najważniejszych zadań dla operatorów sieci komórkowych. Wyzwaniem XXI wieku jest kompleksowe zabezpieczenie całej infrastruktury komunikacyjnej, złożonej m.in. z anten przesyłowych, wież transmisyjnych i koncentratorów sieciowych. Kluczowa staje się zatem integracja rozproszonych na dużych odległościach obiektów. Tego typu innowacyjne rozwiązanie zostało zaprojektowane i wdrożone dla jednego z liderów branży telekomunikacyjnej – firmy Orange Polska. *Dzięki wdrożeniu technologii ABLOY Protec Cliq 2 możliwe było skonsolidowanie rozwiązań elektronicznych i mechanicznych, a tym samym zapewnienie zdalnej kontroli i elastycznej obsługi we wszystkich obiektach. To elektroniczny system kontroli dostępu połączony z mechanicznym systemem wkładek i cylindrów. Administrator systemu, za pomocą dziennika zdarzeń zyskuje pełną informację odnośnie wszystkich operacji w czasie rzeczywistym* – mówi Paweł Banach, przedstawiciel marki ABLOY.

Elastyczność i gwarancja pełnej kontroli

Rozwiązanie zaprojektowane dla Orange umożliwia integrację kilkunastu tysięcy rozproszonych obiektów w jednym zdalnie programowanym systemie. ABLOY PROTEC CLIQ to inteligentny system pozwalający zarządzającemu infrastrukturą w sposób efektywny kontrolować pracę wszystkich pracowników, którzy mieli do niego dostęp. Rejestr zdarzeń pozwala na uzyskanie informacji kto, kiedy i gdzie przebywał w każdym obiekcie – znika konieczność prowadzenia administracji kluczami. *W tak rozbudowanej organizacji jak Orange Polska (OPL), dużym wyzwaniem jest zapewnienie kontrolowanego dostępu do obiektów i infrastruktury technicznej wszystkim osobom uprawnionym. Poszukiwaliśmy rozwiązania, które spełni nasze wymagania, zarówno w zakresie technicznym, jak i finansowym. Zdecydowaliśmy się na ABLOY z uwagi na elastyczność rozwiązań i możliwość ich dopasowania do różnorodnej infrastruktury występującej w Orange Polska. Co warto podkreślić, ABLOY dostarcza nam rozwiązanie kompleksowe, tzn. zapewnia zarówno sprzęt, montaż na obiektach, uruchomienie systemu oraz pakiet szkoleń dedykowanych zarówno operatorom, jak i administratorom systemu. Wybrana technologia, czyli programowalne klucze z pamięcią wewnętrzną zarówno w zamku, jak i w samym kluczu spełnia nasze oczekiwania i pierwotne założenia projektu. Orange Polska (OPL), jako firma innowacyjna i wiodący operator rynku telekomunikacyjnego poszukiwała nowoczesnego rozwiązania, które przyniesie wartość dodaną do klasycznych zamknięć mechanicznych. Zaimplementowany system pozwolił ograniczyć liczbę incydentów bezpieczeństwa w naszych obiektach, jednocześnie ułatwiając dostęp służbom technicznym do infrastruktury, co wprost przekłada się na jakość usług, jak i satysfakcję naszych klientów* – mówi Łukasz Grabiński, Dyrektor Bezpieczeństwa Obiektów i Urządzeń w Orange Polska.

Wymierne korzyści

Innowacyjny system spełnia najwyższe standardy zabezpieczeń i gwarantuje niezawodność. Wprowadzenie tego typu rozwiązania pozwala przede wszystkim znacznie ograniczyć liczbę zdarzeń niepożądanych w obrębie całego ogólnopolskiego systemu. Wpływa również na zwiększenie funkcjonalności i usprawnienie pracy działu bezpieczeństwa, zapewniając tym samym znaczne oszczędności czasu pracy i kosztów zagwarantowania pełni bezpieczeństwa.

Bosch Security Systems
ul. Jutrzenki 105, 02-231 Warszawa
tel. 22 715 41 00
www.pl.boschsecurity.com/pl/

HALA KOSZYKI – warszawski tygiel kulturowy zabezpieczony systemami Bosch

Warszawa dołączyła do grona największych światowych metropolii, takich jak Londyn, Oslo, Rotterdam czy Florencja, gdzie w halach targowo-restauracyjnych pod jednym dachem tętni życie i spotykają się smaki z całego świata. **Miejsce w tej ekskluzywnej grupie zapewniła jej Hala Koszyki.**

Hala Koszyki została wzniesiona w latach 1906–1908 przy ul. Koszykowej w Warszawie. Przez ponad 100 lat była związana z handlem. Zlokalizowana w bogatej i inteligenckiej części miasta, przetrwała pomimo licznych przemian społeczno-politycznych. Jesienią 2016 r. wróciła po modernizacji jako wyjątkowy punkt towarzyski i kulinarny, gdzie można zjeść w kilkunastu restauracjach i barach, a także kupić produkty spożywcze do domu.

CASE STUDY

Mając w perspektywie ochronę tak wyjątkowego obiektu, firma Bosch – dostawca sprzętu i rozwiązań zabezpieczeń – uwzględniła następujące aspekty:

- wymagania estetyczne, zapewniające klientom komfort i przyjemną atmosferę, w której mogą robić zakupy;
- różne obszary zastosowania: sklepy, kawiarnie, bary, restauracje, magazyny, parking, powierzchnie biurowe, serwerownie;
- kompleksowe procedury ewakuacji: duży budynek, wiele osób, które muszą być ewakuowane szybko i bezpiecznie;
- integracja różnych systemów zabezpieczeń Bosch i innych dostawców w celu zapewnienia maksymalnej ochrony obiektu.

Bosch sprostał wyzwaniom, zadbał o bezpieczeństwo obiektu i zadowolenie inwestora. Hala Koszyki została wyposażona w systemy telewizji dozorowej, systemy sygnalizacji włamania i napadu, systemy kontroli dostępu. W obiekcie zainstalowano kamery obrotowe i stałopozycyjne. Kamery obrotowe skutecznie monitorują rozlegle powierzchnie, np. patio przed halą od ul. Koszykowej, kamery stałopozycyjne natomiast zamontowano w miejscach wymagających identyfikacji osób i zdarzeń. W kluczowych obszarach obiektu zastosowano kamery z inteligentną analizą obrazu.

Każda kamera sieciowa w takim systemie staje się urządzeniem inteligentnym, analizującym rejestrowany obraz i ostrzegającym pracowników ochrony o potencjalnych zagrożeniach, takich jak pozostawione bez opieki podejrzane przedmioty, gromadzenie się ludzi, blokowanie stref ewakuacyjnych czy przekraczanie stref bezpieczeństwa. Możliwe jest też szybkie i skuteczne przeszukiwanie zarejestrowanego materiału wg dowolnych kryteriów. Dla ułatwienia pracy na stanowiskach ochrony zastosowano Bosch VMS, którego ergonomiczny interfejs sprawia, że zarządzanie sygnałem wizyjnym staje się prostsze, a personel może pracować wydajnie i skutecznie.

W dbałości o ochronę pracowników i gości przed wejściem osób nieupoważnionych cały obiekt wyposażono w czytniki kontroli dostępu, dzięki którym możliwe jest nadawanie uprawnień wejścia do różnych pomieszczeń, a także rejestracja czasu wejścia oraz wyjścia pracowników.

W Hali zastosowano również czujki serii Professional, które zabezpieczają obiekt przed intruzami. Dzięki połączeniu ich z centralą MAP 5000 zapewniono najwyższy poziom bezpieczeństwa, a zwarcie lub przerwa w dostawie prądu nie spowodują awarii systemu. Ponadto system można rozbudowywać wraz z wymaganiami klienta.

Wszystkie systemy integruje i kompleksowo zarządza całością Building Integration System, który – niezależnie od stopnia złożoności wymagań – zapewnia elastyczność, łatwość obsługi i szybkość reakcji ochrony.

Honeywell sp. z o.o.
ul. Domaniewska 39,
02-672 Warszawa
www.security.honeywell.com/ee/

Honeywell Security Solutions:

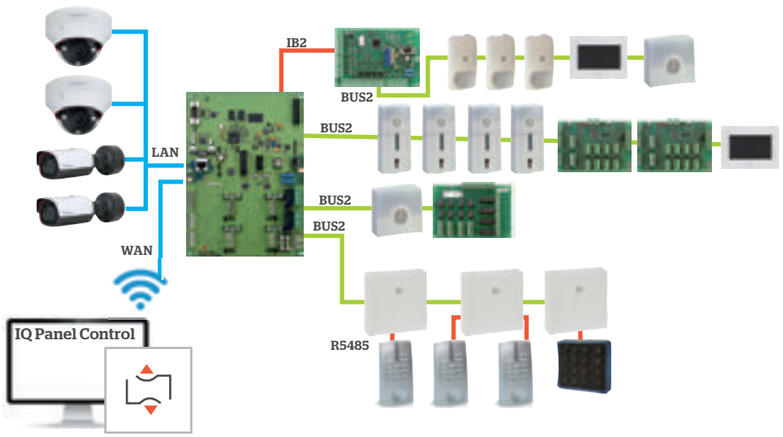
Modułowa platforma MB-Secure v7

MB-Secure to system bezpieczeństwa nowej generacji. Dzięki unikatowej budowie stanowi nowy typ platformy technologicznej, która umożliwia integrację różnych systemów (SSWiN, SKD, CCTV), łącząc sprzęt, oprogramowanie układowe i usługi. W artykule opisano najważniejsze opcje dodane w ostatniej wersji oprogramowania.

Zespół Honeywell PL
Security Solutions

Na początek kilka faktów i liczb na temat platformy MB-Secure, która jest nową generacją popularnej centrali MB-Classic: **2752** to maks. liczba urządzeń adresowalnych obsługiwanych przez jedną centralę, **44 032** konwencjonalne urządzenia, jest w stanie (teoretycznie) obsłużyć pojedyncza centrala, **10 tys.** to liczba użytkowników, a **512** – maks. liczba stref głównych i czasowych oraz przejść zarządzanych przez jedną centralę. Z kolei maks. liczba zaawansowanych scenariuszy akcja – reakcja(e) wynosi **2 tys.**
Już to pokazuje, że MB-Secure ma olbrzymie możliwości, a w zanadrzu nadal pozostaje kilka ciekawych opcji, o które w ramach licencji można rozszerzyć funkcjonalność systemu. Platforma jest modułowa, skalowalna, a jej bazą, niezależnie od wielkości instalacji, jest jedna i ta sama płyta główna. Dzięki takiemu podejściu to użytkownik decyduje, kiedy i o jakie elementy wzbogaca swój system.
Jedną z ciekawszych nowości jest funkcja rejestratora obsługującego 4 kamery kompatybilne z protokołem ONVIF S i G. W rezultacie można zbudować mały system zabezpieczeń składający się z kontroli dostępu, sygnalizacji włamania i napadu oraz dozoru wizyjnego, którego „sercem" jest jedna płyta. Takie zintegrowane rozwiązanie idealnie sprawdzi się w małych obiektach, takich jak bankomat czy paczkomat. Obraz z kamer jest rejestrowany w przypadku wystąpienia zdarzeń zaprogramowanych przez użytkownika za pomocą funkcji makro. Materiał można odtworzyć z poziomu klawiatury systemu SSWiN TouchCenter plus, czyli na panelu LCD do zarządzania systemem, znajdującym się np. w pomieszczeniu ochrony.
Konfigurację i serwisowanie systemu ułatwia dodana do centrali opcja połączeń zdalnych. Połączenie z centralą działa z „pominięciem" routera, bez konieczności przekierowywania portów, konfiguracji DDNS czy posiadania stałego adresu IP. Dzięki temu można skonfigurować dostęp zdalny, nie mając specjalistycznej wiedzy sieciowej.
Nowa licencja Mifare Parametry DESFire umożliwia dodanie używanych przez klienta nośników Mifare DESFire (karta dostępu, pastylka itp.), które mają własne szyfrowanie. Z poziomu funkcji serwisowych IQ PanelControl można dopisać i skonfigurować podstawowe parametry dostępu oraz klucz szyfrujący.
W przypadku aplikacji wymagających bardzo wysokiego poziomu bezpieczeństwa, np. BSI *(Bundesamt für Sicherheit und Informationstechnik)* wprowadzono szyfrowaną komunikację AES-128 z czytnikami Honeywell LuminAXS mifare DESFire. Nowe oprogramowanie centrali umożliwia podłączenie nawet 32 takich czytników bezpośrednio do centrali na magistrali RS485. Zaletą jest możliwość ustawienia indywidualnego klucza szyfrującego osobno dla każdego czytnika. Dla klientów zainteresowanych integracją centrali z systemami wizualizacji firm trzecich opracowano pakiety integrujące. Korzystając z jednej z trzech dostępnych opcji, można monitorować stany poszczególnych elementów, wywoływać ich funkcje czy też w najwyższym pakiecie uzyskać niemal pełną dwukierunkową integrację z centralą. Taka elastyczność rozwiązania MB Secure sprawdza się tam, gdzie w projekcie istnieje już oprogramowanie wizualizacyjne albo użytkownik ma takie oprogramowanie narzucone z góry.

Platforma MB-Secure to wydajny i wszechstronny system, łatwy w obsłudze i konfiguracji. Mnogość opcji sprawia, że każdy może zbudować swój własny, unikatowy i dopasowany do potrzeb system zabezpieczeń, który może się powiększać wraz z rosnącymi potrzebami, bez konieczności wymiany centrali.



TP-Link Polska
ul. Ożarowska 40/42
05-850 Duchnice
www.tp-link.com/pl/

Infrastruktura sieciowa elementem integrującym systemy w przedsiębiorstwie

Kluczem do efektywnego zarządzania jest umiejętność spojrzenia na organizację i zachodzące w niej procesy w sposób integralny. Dynamicznie zmieniające się środowisko pracy wymusza na przedsiębiorcach implementację systemów zintegrowanych, które pozwalają szybko identyfikować wszelkiego rodzaju problemy i zagrożenia oraz im zapobiegać.

T1600G-28TS
Przełącznik zarządzalny wyposażony w 24 gigabitowe porty RJ45 oraz 4 sloty SFP

T1600G-52PS
Przełącznik zarządzalny wyposażony w 48 portów PoE 802.3at/af może zasilać np. punkty dostępowe lub kamery IP

EAP225
Gigabitowy bezprzewodowy punkt dostępowy. Obsługuje zarówno PoE 802.3af, jak i pasywne PoE, co umożliwia jego szybki i wygodny montaż

Iwo Ostalski

Oprócz szeroko pojętych zintegrowanych systemów zarządzania przedsiębiorstwa dysponują systemami CCTV, systemami ppoż., systemami sygnalizacji włamania i napadu oraz systemami kontroli dostępu. Stale rosnąca liczba urządzeń i rozwiązań, które muszą ze sobą współpracować, wymaga budowy infrastruktury sieciowej stanowiącej nośnik informacji płynących z poszczególnych systemów.
Odpowiedzią TP-Link na zwiększające się potrzeby rynku jest seria przełączników zarządzalnych, które dzięki technologii VLAN 802.1Q umożliwiają podział istniejącej sieci na odseparowane wirtualne sieci lokalne. Popularne VLAN-y pozwalają szybko i efektywnie wydzielić w sieci segmenty dla poszczególnych działów, pracowników czy gości. Za pomocą zarządzalnych przełączników można wyizolować np. sieci CCTV, aby pracownicy i goście nie mieli dostępu do urządzeń z tego systemu, z kolei osoby odpowiedzialne za nadzór obiektu miały dostęp jedynie do systemów zabezpieczeń, a nie do zasobów firmy – drukarek, dysków sieciowych czy serwerów. Z kolei poszczególne działy przedsiębiorstwa mogą mieć dostęp tylko do wybranych przez administratora segmentów sieci, np. dział marketingu nie będzie miał dostępu do serwerów księgowych. Gościom czasowo przebywającym na terenie firmy system może udostępniać sieć WiFi z przypisaniem do konkretnego VLAN-u – to bezpieczny sposób na udostępnienie Internetu, z wyłączeniem jakichkolwiek zasobów firmy. Takie rozwiązania gwarantują bezpieczeństwo wrażliwych danych przedsiębiorstwa.
Wybór punktów dostępowych i przełączników dysponujących zasilaniem PoE znacznie ułatwia instalację i obniża jej koszty. Ten typ zasilania jest także stosowany w kamerach IP monitorujących obiekt, telefonach IP i innych urządzeniach sieciowych systemów KD czy ppoż. Całość tworzy zintegrowany system połączony z przełącznikiem, co ułatwia zarządzanie.
We współczesnym przedsiębiorstwie nie może też zabraknąć dostępu do sieci bezprzewodowej. Ze względu na liczbę użytkowników jednocześnie korzystających z WiFi oraz powierzchnię, przedsiębiorstwa są wymagającym środowiskiem dla infrastruktury sieciowej. Obecnie priorytetem powinno być bezpieczeństwo. Nieprawidłowo skonfigurowana sieć bezprzewodowa naraża firmę na zagrożenia cybernetyczne.
TP-Link oferuje gotowe rozwiązanie w postaci punktów dostępowych serii Omada, które umożliwiają administratorowi utworzenie odseparowanych sieci WiFi: osobnych dla gości, osobnych dla pracowników i administracji obiektu. Izolacja sieci wykorzystuje technologię 802.1Q VLAN. Do dyspozycji są różne funkcje zabezpieczeń, począwszy od hasła do sieci WiFi, logowania poprzez Facebook lub SMS, skończywszy na stronie powitalnej, pozwalającej weryfikować użytkowników za pomocą voucherów dostępowych.
Portfolio produktów skierowanych do klienta biznesowego jest stale poszerzane. Obecnie w ofercie TP-Link znajduje się wiele urządzeń: od podstawowych jednozakresowych montowanych do sufitu o prędkości do 300 Mb/s, poprzez montowane w ścianie odporne na warunki atmosferyczne w klasie szczelności IP65, aż po urządzenia obsługujące najnowsze standardy ac Wave2-MU-MIMO.
Siecią zbudowaną z serii urządzeń Omada można w łatwy, niewymagający szkolenia sposób zarządzać za pomocą bezpłatnej aplikacji lub kontrolera sprzętowego, a także zdalnie – za pośrednictwem interfejsu WEB, aplikacji na smartfon lub chmury.

Stosowanie norm przy planowaniu ochrony – problemy

Normy są spisanym, zaakceptowanym i stale uzupełnianym przez europejską branżę security zasobem aktualnej wiedzy i wymagań dotyczących technicznych środków ochrony. Stanowią zbiór wiedzy kilku tysięcy fachowców z kilkudziesięciu krajów Europy.

Stefan Jerzy Siudalski

Normy zawierają nie tylko wymagania dotyczące technicznych i użytkowych parametrów urządzeń. Są w nich zapisane także procedury badań i ich kolejność, wytyczne projektowania i eksploatacji systemów zabezpieczeń, a nawet przygotowywania wymagań na zabezpieczenia jeszcze przed przetargiem. Normy umożliwiają porównywanie cech urządzeń i systemów, co stanowi duże ułatwienie zarówno dla projektantów, jak i użytkowników systemów.

Ta wiedza jest jednak wykorzystywana szczątkowo, a często nawet bez sensu. Są dwa tego powody. Po pierwsze – bariera językowa. Nie wystarczy dobra znajomość języka angielskiego, aby nawet na własny użytek dokładnie przetłumaczyć normę wprowadzoną w języku oryginału. Po drugie – bariera językowa w trakcie wprowadzania norm do spisu w Polsce. Aby normy weszły do spisu jako przetłumaczone, trzeba:

- znaleźć sponsora zarówno tłumacza, jak i czynności wykonywanych z wprowadzaniem przetłumaczonej normy w samym PKN,
- znaleźć tłumacza, który ma opanowany zakres słownictwa technicznego, następnie zlecić tłumaczenie, sprawdzić np. w KT 52 zgodność tłumaczenia z innymi normami oraz zlecić i opłacić wprowadzenie.

Stan aktualny norm

Z każdym rokiem zmniejsza się odsetek norm opublikowanych w języku polskim. Od ponad czterech lat praktycznie zanikło w KT52 (Systemy alarmowe) tłumaczenie norm z języka angielskiego na polski. W efekcie większość z ponad 80 aktualnych norm dotyczących systemów elektronicznych z serii PN EN jest wprowadzona do spisu polskich norm jako tzw. normy okładkowe – przetłumaczona jedynie pierwsza strona, reszta w języku oryginału. Jedynie normy obronne są po polsku, ponieważ powstały w Polsce[1]. Ze względu na to, że mogą być powoływane tylko normy w języku polskim, więc zapisy norm są w minimalnym stopniu wykorzystywane w ustawach, rozporządzeniach, a nawet w innych normach, np. normach obronnych. Ponieważ wprowadzane nowe normy okładkowe powodują wycofywanie norm starszych, które były przetłumaczone, to:

- powołania (jeśli są) odnoszą się do starych wycofanych norm,
- są montowane urządzenia spełniające (lub nie) dawno wycofane normy.

Odwoływanie się do wycofanych norm nie jest zakazane. Na stronie PKN można znaleźć informację, jak długo po wycofaniu konkretnych norm producenci mogą się powoływać na stare normy[2]. Ten mechanizm jest konieczny, by nie powstała przerwa w dostawie na rynek urządzeń, których parametry są zgodne z normami. Niestety często w nowo powstających dokumentach są odwołania do norm sprzed 2000 r., nawet z 1995 r.[3]

Innym czynnikiem wpływającym na mierne stosowanie norm jest brak na uczelniach przedmiotu: normy[4]. Nawet na uczelniach cywilnych szkolących ludzi w branży security w Polsce nie ma tego przedmiotu, a przynajmniej nie natrafiłem na jego ślad. Wyjątkowo mała liczba składanych patentów w Polsce wskazuje na istotne braki w przekazywanej na studiach wiedzy i umiejętności jej wykorzystania, by z patentów i publikacji osiągać zyski. Dotyczy to również branży ochrony. Patentować

1) Uwaga odnosi się do 10 norm dotyczących zabezpieczeń elektronicznych i mechanicznych.

2) Laboratoria także mogą przez określony czas wydawać „atesty" wg wycofanych norm.

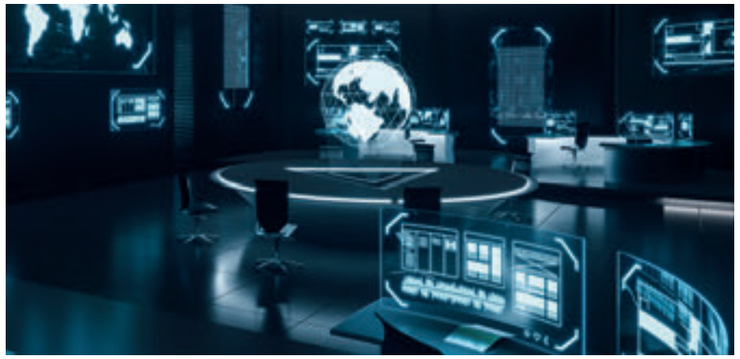
3) W aktualnych normach obronnych wymagania na zasilanie systemów alarmowych są przepisane z normy z 1995 r.

4) W lutym br. miałem prelekcję na temat norm. W sali było ok. 60 słuchaczy, studia skończyło 55 osób. Zapytałem, czy mieli przedmiot: normy. Jedna osoba podniosła rękę, ale okazało się, że dotyczyło to norm związanych z budownictwem.

WYMAGANIA DOT. POMIESZCZEŃ DO PRZECHOWYWANIA BRONI W RÓŻNYCH ROZPORZĄDZENIACH (opis tabeli na następnej stronie)

ROZPORZĄDZENIE	WYMAGANIA – CYTATY	UWAGI
Rozporządzenia Ministra Finansów z 12 lipca 2013 r.	…znajdować się w budynku murowanym, będącym pod całodobową uzbrojoną ochroną lub wyposażonym w urządzenia sygnalizacyjne (alarmowe) połączone z najbliższą uzbrojoną formacją, w której pełniony jest całodobowy dyżur…	• budynkiem murowanym jest także budynek wykonany z lekkich pustaków, ochrona jest więc na poziomie szkieletu kanadyjskiego, • brak minimalnego stopnia ochrony i wymagań na transmisję sygnału alarmu, • nie wskazano, jaki system ma być zamontowany: antywłamaniowy, ppoż. z sygnalizacją napadu czy bez
Rozporządzenie Ministra Spraw Wewnętrznych z 30 maja 2014 r. – straże gminne /miejskie	…sygnalizację alarmową przeciwwłamaniową podłączoną do stanowiska osoby pełniącej całodobowy dyżur lub stanowiska objętego całodobową uzbrojoną ochroną	• brak wymagań dotyczących systemu alarmowego, • brak wskazania, czy system ma mieć przyciski antynapadowe, • brak wymagań na zabezpieczanie transmisji sygnału alarmu
Rozporządzenie Ministra Środowiska z 1 lipca 2014 r. w sprawie przydziału, ewidencjonowania i przechowywania w regionalnej dyrekcji Lasów Państwowych i nadleśnictwie broni, amunicji…	Magazyn broni jest objęty całodobową ochroną oraz posiada następujące wyposażenie: 1) podręczny sprzęt gaśniczy, instalację alarmową…	• brak informacji, o jaki system alarmowy chodzi – ppoż. czy antywłamaniowy, • brak wskazania, czy system ma mieć przyciski antynapadowe, • brak informacji o przesyłaniu sygnału alarmu poza obiekt
Rozporządzenie Ministra Kultury i Dziedzictwa Narodowego z 2 września 2014 r. (zał. Nr 2)	…system sygnalizacji włamania i napadu: a) zabezpiecza wszystkie otwory drzwiowe i okienne oraz kubaturę magazynu zbiorów, b) zapewnia sterowanie zabezpieczeniem magazynu zbiorów w obrębie wydzielonego podsystemu, c) do ochrony przestrzennej pomieszczeń wykorzystuje czujki z antymaskingiem, d) obejmuje ochroną indywidualną szafy, w których przechowywana jest broń palna; …system telewizji dozorowej zapewnia obserwację i nagrywanie obrazu sprzed wejścia do magazynu zbiorów; …jest zainstalowany system sygnalizacji pożarowej	• są dwa odniesienia, które mogą wskazywać na wymagany stopień ochrony: pierwsze – miejsca wykrywania agresji pokrywają się z wymaganiami PN EN 50131-7 dla stopnia ochrony 3; drugie – wymóg posiadania przez czujki antymaskingu, co sugeruje stopień ochrony co najmniej 3 wg tej normy*, lecz określenie miejsca wykrywania agresji jest na tyle mało precyzyjne, że może dotyczyć zarówno 2., jak i 3. stopnia ochrony, • w innym miejscu tego rozporządzenia podano wymagania dla systemów alarmowych z powołaniem się na stopnie ochrony (2 klasa) i telewizji przemysłowej (3 klasa)
Rozporządzenie Ministra Spraw Wewnętrznych z 26 sierpnia 2014 r.	…zabezpieczenie systemem sygnalizacji włamania i napadu spełniającym wymagania co najmniej normy PN-EN 50131-1 z transmisją sygnału alarmu do uzbrojonego stanowiska interwencyjnego, pełniącego całodobowy dyżur…	• brak stopnia ochrony wg powołanej normy, • brak wymagań dotyczących transmisji alarmu
	dopuszcza się zastosowanie drzwi spełniających co najmniej wymagania, o których mowa w normie PN-EN 1627, plombowanych lub zaopatrzonych w inny wskaźnik sygnalizujący wejście osób nieuprawnionych	• brak zaleceń co do powiązania lub nie z systemem alarmowym, • w powołanej normie jest 6 klas drzwi, a klasa najniższa chroni jedynie przed atakiem ręką lub nogą
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 21 października 2011 r. (powtórzone w Obwieszczeniu z 18 czerwca 2015 r.)	…zabezpieczenie systemem sygnalizacji włamania i napadu z transmisją sygnału alarmu do uzbrojonego stanowiska interwencyjnego, pełniącego całodobowy dyżur…	• brak wymagań na system alarmowy
Rozporządzenie Ministra Infrastruktury i Rozwoju z 11 kwietnia 2014 r. w sprawie rodzaju i sposobów ewidencjonowania, przechowywania w straży ochrony kolei broni, amunicji…	…lub zaopatrzone w inny wskaźnik nieuprawnionego wejścia…	• może to oznaczać elektroniczną kontrolę wejścia, lecz to jest domniemanie, • brak wzmianki o konieczności zamontowania systemu alarmowego
Obwieszczenie Ministra Spraw Wewnętrznych z 18 czerwca 2015 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia MSWiA w sprawie zasad uzbrojenia specjalistycznych uzbrojonych formacji ochronnych i warunków przechowywania oraz ewidencjonowania broni i amunicji	…na trwałe przymocowanych do elementów konstrukcyjnych budynku, zabezpieczonych systemem sygnalizacji włamania i napadu z transmisją sygnału alarmu do uzbrojonego stanowiska interwencyjnego, pełniącego całodobowy dyżur	• brak wymagań na system alarmowy

*Wykrywanie sabotażu - Rodzaje sabotażu, które powinny być wykryte - PN EN 50131-1.



można nie tylko urządzenia czy ich części składowe, ale także metody ochrony, oprogramowania, procedury, a jeśli już nie da się opatentować, to przynajmniej prawo autorskie powinno chronić publikowaną wiedzę.

Niechęć do norm

Bariera czasowa. Czas zapoznania się ze wszystkimi zapisami zawartymi w normach dotyczących zabezpieczeń elektronicznych, i to tylko w tych przetłumaczonych, oceniam na ok. 600 godzin[5], a przecież jedynie ok. 20 ze 100 aktualnych norm jest po polsku. Zwykle w ciągu roku pojawiają się dwie, trzy nowe lub zaktualizowane normy – dochodzi więc dodatkowe ok. 100 godzin do zapoznania się także z treścią norm wycofanych.

Bariera kosztowa. Czas poświęcony na zapoznanie się z normami to niejedyny koszt. Na zakup norm w najtańszej wersji, czyli jako plik, trzeba przeznaczyć w sumie nie mniej niż 8 tys. zł – bez norm dotyczących zabezpieczeń mechanicznych. Norma, która ma 50 stron, kosztuje ponad 120 zł, natomiast książka omawiająca wybrane aspekty zapisów w normach, w podobnej objętości – ok. 25 zł!

Decydenci nie wiedzą, że nie wiedzą[6]. To zjawisko powszechne, tym częstsze, im wyższe stanowisko decyzyjne. Przykład: w 2014 r. NIK skontrolowała kilkadziesiąt systemów monitoringu wizyjnego miast. Brano pod uwagę wiele czynników, m.in. ochronę danych osobowych. Po kontroli powstał raport, podczas prelekcji przedstawiciel NIK omawiał jej wyniki. Byłem na tym spotkaniu – zorientowałem się, że kontrolujący nie wiedzieli o istnieniu polskich norm dotyczących systemów wizyjnych, nie znali zapisów norm serii PN EN 50132 ani PN EN 62676 dotyczących monitoringu. Sprawdzano, o ile zmniejszyła się przestępczość[7], jak dobierano obsługę stacji monitorowania, ale już o tym, czy spełniały one wymagania albo chociaż część wymagań zapisanych w normach PN EN 50518 dotyczących zabezpieczeń stacji monitorowania, w raporcie nie było żadnej wzmianki.

Skoro na poziomie NIK nie są znane normy dotyczące monitoringu, to czego wymagać od decydentów na znacznie niższych szczeblach? Cztery ministerstwa np. wydały sześć rozporządzeń dotyczących przechowywania broni. Przed ich opublikowaniem nie przeprowadzono konsultacji, więc:

- wymagania są różne, chociaż kraj ten sam i broń taka sama,
- we wszystkich ministerstwach zapomniano, że magazyny broni mają podłogi i stropy,
- odwołania do norm są na poziomie..., a to widać w zamieszczonej tabeli.

W żadnym rozporządzeniu nie ma wymagań na transmisję alarmu. W ministerstwach nie ma też wiedzy, jak bardzo różnią się wymagania na poszczególne stopnie ochrony systemów SSWiN i CCTV (cyt. *zabezpieczenie systemem sygnalizacji włamania i napadu spełniającym wymagania co najmniej normy PN-EN 50131-1 z transmisją sygnału alarmu…* grade 1 też spełnia wymagania wymienionej normy, lecz dla tego stopnia nie jest przewidywana transmisja alarmu. Nagminne jest przekonanie, że należy montować systemy dawnej klasy SA3 lub SA4, mimo że od 9 lat norma określa stopnie ochrony systemów, a dawna klasa SA3 nie odpowiada systemom Grade 3 wg nowych norm – nie ma takiego prostego przełożenia. Zwykle dawna klasa SA3 ledwie odpowiada stopniowi ochrony 2.

Nie poruszam tu odwołań lub ich braku do norm dotyczących zabezpieczeń mechanicznych, podam tylko kilka przykładów, by można było się zorientować w skali braku wiedzy decydentów. W jednym z rozporządzeń sformułowanie *co najmniej* pojawia się 19 razy, wielokrotnie jest użyte bez sensu, np. *co najmniej w klasie 7* według normy PN-EN 12209. Nie ma przecież klasy wyższej niż 7, więc zapis wskazuje na niewiedzę piszącego. Są i takie zapisy: *drzwi spełniające co najmniej wymagania, o których mowa w Polskiej Normie PN-EN 1627* albo *szyby o zwiększonej odporności na włamanie, co najmniej w klasie P-4*. Ani słowa o klasyfikacji antywłamaniowej drzwi, błędnie wpisana klasa szyby (od 2000 r. nie ma klasy P-4 tylko P-4A).

Jeśli wymienia się klasę szyby, to z przypisaną klasą drzwi – tu nie ma o tym ani słowa. Mylona jest klasa C zamków do drzwi z klasą C zamków do sejfów, a szyby bezpieczne z antywłamaniowymi, zakładając, że szyby kuloodporne mają automatycznie klasę antywłamaniową!!!

Wyszukiwarka na stronie PKN została błędnie skonfigurowana. Na stronie www.pkn.pl wkleiłem skopiowaną nazwę normy. Wyszukiwarka podała, że takiej nie ma. Dopiero ręczne wpisanie nazwy do wyszukiwarki dało efekt. Prawdopodobnie wyszukiwarka nie akceptuje innych rodzajów czcionki niż te, na które została zaprogramowana.

5) Dotyczy także poznania norm, do których są odwołania.

6) *...nie wiemy, że nie wiemy...* – Donald H. Rumsfeld.

7) Sprawdzianem skuteczności monitoringu jest nie tylko zmniejszenie się przestępczości liczonej wg liczby zdarzeń, ale także skrócenie czasu trwania zdarzeń i ograniczenie strat, o czym w dokumencie nie wspomniano.

BIO

Stefan Jerzy Siudalski
Autor ponad 340 artykułów i 8 książek oraz ponad 200 opinii (dla ubezpieczycieli, agencji ochrony i sądów) nt. systemów ochrony. Przez ponad 27 lat był biegłym sądowym z dziedziny systemów alarmowych i systemów ochrony. Szkolił agentów ochrony, instalatorów systemów i inwestorów.

Hikvision Poland
ul. Krakowiaków 50, 02-255 Warszawa
tel. 22 460 01 50, faks 22 464 32 11
e-mail: info.pl@hikvision.com

NVR CZY VMS

Jako centralny punkt systemu monitoringu wizyjnego może funkcjonować zarówno wysokiej jakości rejestrator wizji, jak i system zarządzania oparty na oprogramowaniu VMS. **Które rozwiązanie zapewni większą niezawodność i funkcjonalność, a także komfort pracy z systemem monitoringu?**

Dominika Mazurek
Hikvision

Każde rozwiązanie ma zalety i wady, które determinują możliwość jego wykorzystania w określonej instalacji. Każde ma szansę sprawdzić się lepiej w konkretnym środowisku pracy lub w aplikacji w konkretnym systemie. Przed dokonaniem wyboru dobrze jest więc dokładnie przeanalizować potrzeby.

Instalacja

Jedną z oczywistych zalet rejestratora NVR w porównaniu z oprogramowaniem VMS jest jego cena oraz łatwość instalacji i konfiguracji. Uruchomienie rejestratora nie wymaga instalowania dodatkowego oprogramowania, a dodawanie kamer jest znacznie łatwiejsze i szybsze w porównaniu ze złożoną konfiguracją oprogramowania VMS. Jednak VMS zapewnia większą swobodę w doborze sprzętu, na którym zostanie zainstalowane, a także w późniejszej wymianie jego komponentów, co jest w zasadzie niemożliwe w przypadku rejestratorów.

Integracja i kompatybilność

Podstawowym zadaniem rejestratorów jest zapis materiału wizyjnego na dyskach twardych oraz wyświetlanie obrazu bieżącego lub zarejestrowanego. Dzięki wbudowanym wejściom i wyjściom alarmowym możliwa jest też współpraca z urządzeniami zewnętrznymi, takimi jak automatyka domowa, system alarmowy lub kontroli dostępu. Funkcjonalność ta jest jednak ograniczona. Jeśli więc mowa o integracji systemu monitoringu IP z innymi systemami, warto przyjrzeć się możliwościom oferowanym przez VMS.

Skalowalność

Jednym z kluczowych parametrów wyboru rejestratora jest liczba obsługiwanych przez to urządzenie kamer. W praktyce projektowej często dochodzi jednak do sytuacji wymagającej rozbudowy istniejącego systemu monitoringu wizyjnego. Wówczas konieczny staje się zakup dodatkowej jednostki – nawet gdy jest potrzebny tylko jeden dodatkowy kanał wizji. Trudno przewidzieć, jak będzie ewoluował projektowany dziś system telewizji dozorowej, niełatwo więc jednoznacznie określić zasoby sprzętowe, które go obsłużą w przyszłości. W przypadku platformy VMS można wykupić kolejną licencję, więc jest to bardziej elastyczne rozwiązanie, pozwalające na rozbudowę w dowolnym momencie i korzystanie z tylu kanałów, ile jest aktualnie potrzebnych.

Użyteczność

To aspekt, w którym zawierają się również intuicyjność obsługi, wsparcie czy uniwersalność. Tym, na co należy zwrócić uwagę przed podjęciem decyzji, jest scenariusz zastosowania. Rejestratory NVR są przeznaczone do obsługi mniejszych systemów, natomiast oprogramowanie VMS – do zarządzania systemami rozproszonymi. Wady i zalety należałoby więc rozpatrywać w kontekście rozmiaru systemu, skalowalności i celu zastosowania.

Czy trzeba wybierać?

Firma Hikvision wprowadziła do oferty nową platformę zarządzającą HikCentral, która łączy oba te rozwiązania. Oprócz realizacji zapisu na macierzach dyskowych HikCentral pozwala też użyć do zapisu rejestratorów NVR i DVR. Umożliwia to zarówno elastyczną rozbudowę istniejącego systemu, i to niezależnie od zastosowanej metody transmisji sygnału, jak też realizację nowej instalacji o dowolnej wielkości, przy zachowaniu pełnego zarządzania parametrami zapisu i wyświetlania. Nowe rozwiązanie zapewnia możliwość budowy kompleksowego, inteligentnego systemu zabezpieczeń, wyposażonego w zaawansowane funkcje zarządzania oraz otwartego na potrzeby dalszej rozbudowy i inteligencji.

Przegląd rejestratorów NVR

Galopujący postęp technologiczny i miniaturyzacja skutkują upakowaniem wielu funkcji do jednego urządzenia. Dotyczy to również rejestratorów sieciowych obrazu i dźwięku, które – oprócz gwarantowanej, prawidłowej archiwizacji – coraz częściej integrują dane z systemów zewnętrznych (np. ciągi tekstowe, transakcje z systemu POS) lub z rozkładu danych wizyjnych (np. odczyt tablic rejestracyjnych, rozpoznanie twarzy) w celu szybszego wyszukiwania materiału. Znacząca większość rejestratorów ma wbudowane mechanizmy analizy obrazu wspomagane algorytmami wywodzącymi się z uczenia maszynowego. Współpracę z urządzeniami firm trzecich zapewnia popularność i dojrzałość standardu ONVIF, który w tym roku kończy 10 lat. Nie dotyczy to tylko możliwości podłączenia bieżącego strumienia wizyjnego czy sterowania PTZ, wyjściami alarmowymi i przekaźnikami, ale również replikacji danych zapisanych w kamerze do pamięci centralnej. Na rynku zaczynają dominować jednostki typu *appliance,* czyli urządzenia „wszystko-w-jednym" zbudowane na bazie płyty głównej komputerów PC lub serwerowych (najczęściej Microsoft lub Linux).

Axis Communications: AXIS Camera Station S20

AXIS Camera Station S20 to seria sieciowych rejestratorów wizji, umożliwiających niezawodny dozór w wysokiej rozdzielczości. Aby zminimalizować czas montażu, urządzenia AXIS S20 mają wbudowany switch PoE przeznaczony do zapisu obrazów w rozdzielczości nawet 4K, oprogramowanie do zarządzania obrazem AXIS Camera Station, potrzebne licencje oraz pozostałe niezbędne oprogramowanie systemowe.
Wraz z kamerami z bogatej oferty firmy Axis i monitorami rejestratory tworzą kompleksowe rozwiązanie dla średnich instalacji (do 24 kanałów), zapewniając efektywny dozór. Wstępna konfiguracja pozwala skrócić do minimum czas instalacji.
Rejestrator został wyposażony w sprawdzone rozwiązania sprzętowe, jest objęty 3-letnią gwarancją.
Oprogramowanie AXIS Camera Station ma intuicyjny interfejs użytkownika i zapewnia swobodę korzystania ze wszystkich zalet szerokiej gamy kamer i innych urządzeń sieciowych Axis. Współpracuje z kamerami także innych producentów.
Seria sieciowych rejestratorów AXIS S20 obejmuje urządzenia mające wbudowany switch w wersjach: 8-, 16- i 24-kanałowej.

- Zintegrowane urządzenie z wbudowanym przełącznikiem PoE
- Szeroki zakres funkcjonalności
- Dozór w wysokiej rozdzielczości do 4K
- Oprogramowanie AXIS Camera Station w zestawie
- Pełna kompatybilność z produktami Axis

BCS NVR6408-4K-RR

Sieciowy rejestrator BCS NVR6408-4K-RR to najwyższej klasy urządzenie zapewniające niespotykaną dotąd jakość obrazu. Zastosowanie 4-rdzeniowego procesora Intel umożliwia prowadzenie podglądu w rozdzielczości do 12 Mpix. Rejestrator jest kompatybilny z urządzeniami innych producentów (wsparcie standardu Onvif 2.4), co pozwala na wykorzystanie go w dużych centralnie zarządzanych systemach monitoringu. Idealnie sprawdzi się w obiektach administracji rządowej, użyteczności publicznej, hotelach, centrach handlowych, instytucjach finansowych. Niezawodność i odporność na ewentualne usterki dysków twardych podnoszą technologia Hotspare umożliwiająca wymianę uszkodzonego dysku bez konieczności wyłączania rejestratora oraz obsługa RAID 0/1/5/10 pozwalająca na bezpieczniejsze przechowywanie danych.

Rejestrator BCS NVR6408-4K-RR współpracuje z kamerami z obiektywami typu „rybie oko" (*fisheye*), obsługując *dewarping* – funkcję podziału i dostosowania obrazu, działającą przy podglądzie na żywo i odtwarzaniu. Wsparcie dla funkcji mapy ciepła (nanoszenia graficznego natężenia ruchu na obraz z kamery) dostarcza operatorom dodatkowych danych do analizy systemu. A to wszystko w rozdzielczości do 12 Mpix zarówno w trybie nagrywania, odtwarzania, jak i podglądu na żywo.
W rejestratorze tej klasy nie zabrakło funkcji zaawansowanej analizy obrazu: przekroczenia linii, wtargnięcia w strefę, pojawienia się i zniknięcia obiektu, detekcji twarzy, zmniejszających liczbę fałszywych alarmów.
W obiektach handlowych przydatna jest możliwość integracji rejestratora z kasami fiskalnymi (POS). Dane z paragonu fiskalnego rejestrator nanosi na obraz z kamery. Algorytm wyszukiwania pozwala znaleźć na nagraniu dany produkt i zweryfikować poprawność transakcji. Z kolei współpraca z kamerami do identyfikacji tablic rejestracyjnych umożliwi identyfikację nadjeżdżającego pojazdu, ewentualne otwarcie szlabanu i późniejsze łatwe wyszukanie nagrania na podstawie numerów rejestracyjnych.

BCS P-NVR12816-4KR

To najbardziej zaawansowany rejestrator w ofercie BCS Point. Może obsłużyć do 128 kamer IP w rozdzielczości do 12 Mpix. Ze względu na liczbę obsługiwanych kamer i możliwość zamontowania do 16 dysków twardych o pojemności do 8 TB każdy stanowi idealne rozwiązanie dla dużych systemów monitoringu. Znajduje zastosowanie tam, gdzie wymagana jest niezawodność i duża liczba funkcji, zarówno związanych z jakością obrazu, odbieraniem zdarzeń czy odtwarzaniem nagrań, jak i tych, dzięki którym codzienna obsługa odbywa się intuicyjnie. Pozostaje jeszcze możliwość rozbudowy urządzenia.
Rejestrator obsługuje całą gamę funkcji zaawansowanej analizy obrazu, m.in. przekroczenie linii, wtargnięcie w strefę, detekcję twarzy, liczenie osób, zmianę sceny czy ostrości kamery, detekcję audio oraz *autotracking* w przypadku kamer PTZ.
Prosta obsługa i łatwy dostęp do najważniejszych funkcji, poszerzone o szybkie wyszukiwanie nagrań na podstawie zdarzenia czy wyszukiwanie Smart, które znacząco skraca czas potrzebny na przeszukanie nawet bardzo dużego archiwum, odciąża operatora systemu, który może się skupić na bieżącej sytuacji.
Rejestrator jest wyposażony w dwa wyjścia HDMI do podłączenia dwóch niezależnych monitorów. Można go rozbudować, montując w nim dwie karty dekodujące po 6 wyjść HDMI każda. W rezultacie do urządzenia można podłączyć aż 14 monitorów, tworząc w ten sposób małe centrum monitoringu oparte tylko na jednym urządzeniu.
Niezawodność rejestratora zapewniają m.in. dwa równolegle pracujące zasilacze – w przypadku usterki jednego z nich drugi automatycznie, w sposób niezachwiany dla systemu, kontynuuje pracę. Co ważne, uszkodzony zasilacz można wymienić również w trakcie normalnej pracy rejestratora.
Niezawodność systemu zwiększa również obsługa dysków w systemie *hot swap* oraz organizowanie ich pracy za pomocą RAID 0/1/5/6/10.
Ze względu na liczbę obsługiwanych kamer i dostępne pasmo na poziome 512 Mb/s rejestrator został wyposażony w 4 karty sieciowe oraz 2 sloty na wkładki SFP.

Miwi Urmet: Urmet 1093/932H5 z serii Boost 3.0

Innowacyjny model 1093/932H5 wspiera najnowszy standard kompresji H.265, który w stosunku do H.264 zmniejsza wielkość strumienia wizji nawet o połowę. Tak duża oszczędność przekłada się bezpośrednio na zmniejszenie ruchu sieciowego i mniejszą przestrzeń dyskową potrzebną na zarejestrowanie materiału o porównywalnej jakości. Możliwość obsługi dysków o pojemności do 8 TB znacznie wydłuża czas rejestracji.
Rejestrator monitoruje podstawowe funkcje dysku twardego S.M.A.R.T, dzięki czemu może zaalarmować serwis o ewentualnej niesprawności.
Model 1093/932H5 rejestruje materiał w rozdzielczości 4K, a wbudowane wyjście HDMI pozwala wyświetlić obrazy w pełnej jakości bezpośrednio z rejestratora. Inną istotną funkcją rejestratora jest ochrona nagrań znakiem wodnym (mogą one stanowić niepodważalny dowód w sądzie).
Rejestrator umożliwia również zarządzanie analityką wizji VDect zaimplementowaną w kamerach Urmet. Można skonfigurować m.in. przecięcie wirtualnej linii, wejście w strefę, opuszczenie strefy, pozostawienie, zabranie przedmiotu, zliczanie obiektów, detekcję twarzy.
Co ważne, praca rejestratora jest oparta na bezpiecznym systemie operacyjnym Linux. W cenę rejestratora wliczono też koszt oprogramowania klienckiego z intuicyjnym interfejsem użytkownika, pozwalającym na obsługę wielu rejestratorów URMET różnych typów (IP, AHD, HD-SDI, CVBS) za pomocą jednej stacji klienckiej.
Dla użytkownika ważne jest to, że rejestrator wspiera technologię chmury (P2P), dzięki której można uzyskać zdalny dostęp do systemu bez obowiązku posiadania publicznego adresu IP, przekierowania portów rejestratora w routerze czy tłumaczenia zmiennego adresu IP na domenę. Do podglądu i odtwarzania obrazów z kamer podłączonych do rejestratora Urmet z każdego miejsca na Ziemi (z dostępem do Internetu) wystarczy połączenie rejestratora poprzez złącze RJ45 z dowolną poprawnie działającą siecią internetową w obiekcie.
Więcej informacji: **www.miwiurmet.pl**

GDE: rejestrator 32-kanałowy INVR-32K MAZi

Urządzenia o rozdzielczości 4K (3840 x 2160 pix, 8 Mpix) są coraz bardziej popularne. Spadające ceny monitorów 4K, pojawienie się kodeków H.265/H.265+ oraz rejestratorów w cenach zbliżonych do urządzeń H.264 zachęcają do stosowania kamer o większej rozdzielczości.
MAZi od dawna ma w ofercie gamę urządzeń zgodnych z 4K. Jednym z najpopularniejszych jest 32-kanałowy rejestrator INVR-32K ze względu na doskonały stosunek ceny do funkcjonalności.
Oprócz obsługi H.265/H.265+ udostępnia wiele użytecznych funkcji: • ANR (*Automatic Network Replenishment*) – w przypadku przerwania połączenia z rejestratorem pozwala na nagrywanie na karcie SD w kamerze, a po przywróceniu połączenia następuje przesłanie brakujących nagrań na rejestrator • pełną współpracę z kamerami wyposażonymi w VCA (algorytmy analizy obrazu, m.in. detekcja przekroczenia linii, detekcja wtargnięcia, wykrycie pozostawionego obiektu, wykrycie zniknięcia obiektu, detekcja twarzy i inne) • dwa porty LAN do połączenia zapasowego lub do równoczesnego podłączenia do sieci LAN oraz wydzielonej sieci CCTV.
Dzięki wyjściu HDMI o rozdzielczości 4K można łatwo, jednym kliknięciem myszy i bez potrzeby powiększania, obserwować obraz z kamer 8 Mpix na monitorze 4K podłączonym bezpośrednio do rejestratora. Niezależne wyjście VGA umożliwia pracę dwumonitorową. Typowe zastosowanie to ciągły podgląd na monitorze 4K ze wszystkich kamer oraz podgląd obrazów z wybranej kamery, w tym z kamer PTZ, lub przeglądanie nagrań za pomocą funkcji *Smart Search* (inteligentne przeszukiwanie zdarzeń w wybranym fragmencie pola widzenia kamery).
Rejestrator może być zarządzany przez smartfon, przeglądarkę, a także przez zaawansowane oprogramowanie Windows pozwalające na zarządzanie ponad 200 urządzeniami mającymi łącznie ponad 100 kanałów.
Rozdzielczość 4K obsługują także inne rejestratory MAZi, np. modele INVR-04KL/KLPOE, INVR-08KL/KPOE, INVR-16KL/KL1, HSVR-16HT4 oraz HSVR-32HT.
Wyłącznym przedstawicielem firmy MAZi Security Systems GmbH jest GDE Polska.

Hikvision: iDS-7208HUHI-K2/4S AcuSense TURBO HD 5.0

Firma Hikvision – międzynarodowy lider w produkcji urządzeń i rozwiązań monitoringu wizyjnego – rozszerza portfolio o nową serię produktów TURBO HD 5.0, w tym rejestrator iDS-7208HUHI-K2/4S. Urządzenie działa z zastosowaniem technologii AcuSense opartej na algorytmach *deep learning*, poprawiającej dokładność analizy obrazu (VCA).
Rejestrator Turbo HD 5.0 AcuSense obsługuje wszystkie standardy transmisji – HDTVI, HDCVI, AHD, CVBS, udostępnia również nową techniką kompresji wizji H.265 Pro+, H.265 Pro, H.265, która znacząco poprawia wydajność kodowania.
Jedną z funkcji rejestratora jest filtrowanie fałszywych alarmów. Jeżeli zostanie wyzwolona detekcja przekroczenia linii albo wykrycie intruza w strefie, algorytm głębokiego uczenia sprawdza, czy w kadrze znajduje się człowiek. Jeśli tak, alarm zostaje przekazany dalej, jeśli nie – trafia do puli alarmów fałszywych. Kolejną funkcją jest inteligentne wyszukiwanie obiektu w zarejestrowanym materiale, pozwalające wyodrębnić osoby i pojazdy w celu szybkiego przeszukania zarejestrowanych obrazów.
Rejestrator obsługuje do 8 kamer HDTVI w rozdzielczości 8 Mpix oraz umożliwia podłączenie do 16 kamer IP w rozdzielczości 8 Mpix. Dzięki dodatkowemu wyjściu wizyjnemu HDMI w rozdzielczości 4K podgląd obrazu z kamer 4K można obserwować na monitorze, z zachowaniem szczegółowości obrazu.

Hikvision: iDS-7700NXI-I/S

Firma Hikvision wprowadziła nowe rozwiązania EASY IP 4.0, m.in. serię rejestratorów sieciowych AcuSense, które umożliwiają efektywniejsze zarządzanie systemem ochrony. Zastosowana technologia AcuSense jest oparta na algorytmach sztucznej inteligencji, które wzbogacają systemy telewizji dozorowej. Technologia znacząco zwiększa dokładność wystąpienia alarmów, umożliwiając łatwiejsze i przede wszystkim skuteczniejsze przeszukiwanie nagrań wideo.
Rejestrator AcuSense iDS-7700NXI-I/S ma następujące cechy:

- filtrowanie alarmów, dzięki precyzyjnemu rozpoznaniu system może odfiltrować nawet do 90% zdarzeń wywołujących fałszywe alarmy. Znaczące zmniejszenie liczby fałszywych alarmów przyczynia się do obniżenia kosztów pracy. Funkcja filtrowania fałszywych alarmów odbywa się na 4 kanałach;
- inteligentne wyszukiwanie obiektu na nagraniu wideo.

W NVR AcuSense wyszukiwanie plików, w których pojawiają się określony obiekty, np. ludzie i pojazdy, jest bardziej wydajne i efektywne. Opcje szybkiego inteligentnego wyszukiwania są dostępne w lokalnym GUI, zapewniającym dostęp do nagrań z zarejestrowanymi osobami czy pojazdami.
Rejestrator iDS-7700NXI-I/S może obsłużyć 16 lub 32 kamery IP o rozdzielczości do 12 Mpix. Dzięki wyjściu HDMI w rozdzielczości 4K podgląd obrazu można obserwować z zachowaniem jego szczegółowości. Ponadto jest możliwość nakładania metadanych (np. informacji POS) na obraz, a także skonfigurowania alarmu POS w celu wyzwolenia nagrania.
Rejestratory z nową technologią AcuSense znajdują zastosowanie w infrastrukturze krytycznej, ochronie perymetrycznej, parkingach itd.

Hikvision: iDS-9632nxi-i8/4f

Firma Hikvision konsekwentnie rozwija swoje produkty z serii DeepInMind. Skuteczna ochrona mieszkańców, ich własności i miejsc publicznych stanowi stałe wyzwanie władz miejskich na całym świecie. Technologia *deep learning* firmy Hikvision została wdrożona do rozpoznawania osób oraz analizowania zachowań ludzi i pojazdów na obrazie. Pozwala to na wyszukiwanie zbiegów, odnajdywanie zaginionych, zapobieganie potencjalnym przestępstwom, wykrywanie podejrzanego zachowania czy niewłaściwego parkowania itp.
Obecnie do oferty wprowadzono rejestrator sieciowy ids-9632nxi-i8/4f, w którym działanie funkcji analitycznych opiera się głównie na karcie graficznej. W połączeniu z odpowiednią kamerą **na 4 kanałach** umożliwia rozpoznawanie i porównywanie twarzy z wcześniej utworzoną bazą. Oparcie całej mocy obliczeniowej na karcie graficznej znacznie przyspiesza pracę urządzenia oraz poprawia dokładność rozpoznawania. Rejestrator umożliwia wyszukanie w zarejestrowanym materiale intruza na podstawie zdjęcia otrzymanego np. od policji. Zaimplementowany kodek H.265+ pozwala znacznie wydłużyć czas rejestracji, oszczędzając miejsce na dysku o około 75%. Rejestrator może nagrywać strumienie wizji z kamer o rozdzielczości do 12 Mpix, maks. liczba obsługiwanych kamer to 32. Możliwość nagrywania w rozdzielczości 12 Mpix ma bezpośredni wpływ na jakość zarejestrowanych obrazów – to ważny argument przy przeszukiwaniu nagrań po wystąpieniu niepożądanego zdarzenia. Inteligentne systemy zapewniają firmom przewagę w obszarze marketingu, możliwości w zakresie konwersji oraz korzyści na wielu płaszczyznach.

Hikvision: iDS-96128NXI-I24 – rejestrator sieciowy serii DeepInMind

Rejestrator sieciowy NVR o symbolu iDS-96128NXI-I24 firmy Hikvision może obsługiwać do 128 kanałów IP, dekodować do 20 kanałów o rozdzielczości do 1080 pix, a maksymalna rozdzielczość podłączanych kamer to 12 Mpix. Co istotne, można do niego podłączyć do 24 dysków HDD z funkcją *hot swap* (do 8 TB każdy). Ponadto w rejestratorze zaimplementowano funkcje analizy obrazu oparte na głębokim uczeniu, a wśród wielu algorytmów są m.in. rozpoznawanie twarzy, rozpoznawanie pojazdów, rozpoznawanie budowy ludzkiego ciała, filtrowanie alarmów.
Sygnał alarmu wyzwolony po wykryciu przekroczenia linii lub naruszenia strefy chronionej mogą również powodować liście poruszające się na wietrze czy deszcz, dlatego NVR DeepInMind przeprowadza drugą, pomocniczą analizę obrazu. Znacząco zwiększa to wiarygodność wygenerowanego alarmu.

Tym, co wyróżnia rejestrator na tle innych, jest zastosowanie 8 procesorów graficznych Nvidia. NVR umożliwia przypisanie konkretnej funkcji analitycznej do danego silnika graficznego, dzięki czemu zyskuje się większe możliwości kontroli nad zasobami urządzenia. Rozpoznawanie twarzy może odbywać się jednocześnie na 32 kanałach, a baza danych może pomieścić do 100 tys. zdjęć.
Rejestrator może być stosowany w każdych – małych i średnich – projektach wymagających funkcjonalności rozpoznawania twarzy. Jest w stanie sprostać wymaganiom różnych branż. To idealne urządzenie do takich obiektów, jak kasyna, budynki mieszkalne, szkoły czy centra handlowe.

Bezpieczne serwerow nie

W dzisiejszych cyfrowych czasach to nie przedmioty materialne stanowią dla przedsiębiorstw największą wartość. W tej hierarchii coraz częściej na jej szczycie znajdują się dane, takie jak tajemnice przedsiębiorstwa, bazy klientów lub – w przypadku zakładów produkcyjnych – zachowanie ciągłości procesu produkcji.

Iza Trzeciak, Renata Trojanowska

Dane mogą być przechowywane w formie elektronicznej lub papierowej – na nośnikach elektronicznych w serwerowniach lub w tradycyjnych teczkach w archiwach. Najcenniejsze dobra wymagają szczególnej ochrony, również przeciwpożarowej. Ani serwerownie, ani archiwa w przypadku pożaru nie mogą być gaszone wodą, gdyż przyniesie to skutek odwrotny do zamierzonego. Wprawdzie woda uchroni mienie przed ogniem, ale i je zniszczy. W takich przypadkach stosuje się stałe urządzenia gaśnicze gazowe.

Właściwości gazów gaśniczych

Gazy gaśnicze mogą być używane do gaszenia pożarów grup A, B i C, z wyjątkiem specyficznych substancji chemicznych. Bezsprzecznymi zaletami ich zastosowania w tych miejscach są czystość gaszenia oraz nieprzewodzenie prądu elektrycznego przez gazy.

Zasada działania SUG gazowego

Stałe urządzenie gaśnicze gazowe składa się z dwóch części: elektrycznej i hydraulicznej. System detekcji pożaru i sterowania gaszeniem odbiera sygnał o wykryciu pożaru oraz wysterowuje urządzenia według przyjętego algorytmu sterowania. Część hydrauliczna magazynuje i uwalnia gaz gaśniczy.

Na system detekcji pożaru i sterowania gaszeniem składają się następujące urządzenia: centrala sterowania gaszeniem (CSG), czujki pożarowe, przycisk „start gaszenia", sygnalizatory optyczno-akustyczne, klapy odciążające i wyzwalacz na zaworze butli.

Centrala jest zazwyczaj programowana na tryb alarmowania dwustopniowego z koincydencją dwuczujkową. Przyjęcie takiego trybu alarmowania ogranicza prawdopodobieństwo fałszywego alarmu i niepotrzebnego wyładowania gazu. Po wystąpieniu alarmu pierwszego stopnia (zadziałaniu jednej czujki) zostaje uruchomiony sygnalizator optyczno-akustyczny w pomieszczeniu.

Wejście systemu w stan alarmu drugiego stopnia powoduje szereg sterowań: uruchomienie sygnalizatorów optycznych, otwarcie klapy odciążającej oraz rozpoczęcie odliczania czasu zwłoki do wyładowania gazu. Czas zwłoki (opóźnienie wyładowania gazu w stosunku do wystąpienia alarmu drugiego stopnia) jest potrzebny z dwóch powodów – aby zapewnić ewakuację ludzi z pomieszczenia gaszonego oraz zamknąć przeciwpożarowe klapy odcinające na wentylacji i otworzyć klapę odciążającą. Klapa odciążająca pozwala odprowadzić nadciśnienie powstające przy wyładowaniu gazu. W ten sposób ogranicza się możliwość zniszczenia pomieszczenia. Klapa jest otwarta na czas wyładowania gazu, dając ujście nadciśnieniu, zamyka się po zakończeniu wyładowania, aby doszczelnić pomieszczenie. Po upływie zaprogramowanego czasu na ewakuację następuje wysterowanie zaworu na butli – wyładowanie środka oraz uruchomienie sygnalizatora optycznego z informacją „uwaga gaz, nie wchodzić" na zewnątrz pomieszczenia.

Po wyzwoleniu gazu gaśniczego pomieszczenie należy pozostawić zamknięte przez co najmniej 10 minut. Następnie można skontrolować efekty gaszenia – to zadanie dla strażaków wyposażonych w aparaty ochrony dróg oddechowych (w pomieszczeniu mogą znajdować się trujące produkty spalania). Po akcji gaśniczej pomieszczenie należy dokładnie przewietrzyć.

Rys. 1. **Czworościan spalania**

Gazy gaśnicze

National Fire Protection Association (NFPA – stowarzyszenie znane z opracowywania standardów, prowadzenia badań i szkoleń z zakresu ppoż.) w standardzie NFPA 2001 dzieli gazy gaśnicze na trzy grupy: gazy obojętne, chlorowcopochodne węglowodorów oraz dwutlenek węgla stanowiący samodzielnie trzecią grupę. Podział ten uwzględnia właściwości gazów: od sposobu, w jaki gaszą pożar, do postaci magazynowania gazu. Gazy obojętne i chlorowcopochodne węglowodorów NFPA określa się jako „czyste środki gaśnicze" (*clean agents*).

Gazy obojętne są nazywane również gazami inertyzującymi (*inert gases*) ze względu na sposób ich oddziaływania na pożar – inertyzacja to częściowe lub całkowite zastąpienie powietrza lub palnej atmosfery przez gaz obojętny. W uproszczeniu ta grupa gazów redukuje zawartość tlenu w atmosferze do ok. 12%. (Przyjmuje się, że średnia zawartość tlenu w powietrzu potrzebna do podtrzymania reakcji spalania wynosi ok. 15%; dokładna wartość zależy od materiału palnego). Stosowane stężenia gazów obojętnych sięgają 40–50% i są największymi stężeniami projektowymi wśród wszystkich gazów gaśniczych. Do tej grupy należą cztery gazy: IG-01 (argon), IG-100 (azot), IG-541 (mieszanina zawierająca 52% azotu, 40% argonu i 8% dwutlenku węgla), IG-55 (50% azotu i 50% argonu).

Gazy obojętne magazynowane w butlach znajdują się pod wysokim ciśnieniem – 150–300 barów (15–30 MPa), pozostając przy tym w stanie gazowym. Ich zaletą jest naturalne pochodzenie – są składnikiem atmosfery, więc nie oddziałują na środowisko.

Chlorowcopochodne węglowodorów są też określane jako zamienniki halonów lub gazy chemiczne. Ich działanie gaszące polega na blokowaniu reakcji łańcuchowych zachodzących w strefie spalania oraz chłodzeniu (ponieważ mieszanina gazu z powietrzem ma większą pojemność cieplną niż powietrze). Stężenia potrzebne do uzyskania tego efektu nie przekraczają 10%. Jedną z cech charakterystycznych tych gazów jest to, że skraplają się przy dość niskich ciśnieniach, a skroplone zajmują mniejszą objętość – najmniejszą ze wszystkich gazów gaśniczych. Najczęściej stosowanymi w Polsce zamiennikami halonów są gazy: HFC-227ea oraz FK-5-1-12.

Dwutlenek węgla. Jako jedyny spośród gazów gaśniczych w stosowanych stężeniach gaśniczych jest szkodliwy dla ludzi. Stężenia projektowe CO_2 mieszczą się w granicach 34–66%. Już stężenia rzędu 2–6% mogą mieć negatywny wpływ na zdrowie człowieka i powodować różne objawy, np. ból i zawroty głowy, dreszcze. Stężenie przekraczające 17% powoduje śmierć w ciągu minuty. Stałe urządzenia gaśnicze wykorzystujące dwutlenek węgla jako środek gaśniczy są stosowane do ochrony pomieszczeń, w których nie przebywają ludzie. Drugim zastosowaniem SUG na dwutlenek węgla jest ochrona urządzeń (maszyn) – poprzez działanie miejscowe. Pod względem magazynowania CO_2 wykazuje się podobnymi cechami jak zamienniki halonów – skrapla się przy ciśnieniu do 52 barów, a pod względem oddziaływania gaśniczego, podobnie jak gazy obojętne, odbiera tlen, dodatkowo chłodząc strefę spalania.

Inertyzacja sposobem na pożary

Oprócz rozwiązań gazowych przy zabezpieczeniu serwerowni można również zastosować m.in. inertyzację pomieszczeń chronionych. Ma ona działanie zarówno przeciwpożarowe, jak i przeciwwybuchowe. Inertyzacja to kontrolowane wyparcie tlenu za pomocą gazu obojętnego, takiego jak azot lub dwutlenkiem węgla w celu zapobiegania pożarom i tworzeniu się atmosfery wybuchowej. Gaz obojętny nie reaguje z innymi obecnymi substancjami. W przypadku ochrony ppoż. pomieszczeń, w tym serwerowni, w których woda mogłaby spowodować poważne szkody, użycie gazu obojętnego znacznie redukuje lub eliminuje ryzyko wybuchu pożaru. Inertyzacja w tym przypadku to zabezpieczenie polegające na ciągłym zmniejszaniu ilości tlenu do poziomu uniemożliwiającego powstawanie i podtrzymywanie reakcji spalania.

Odkrycie chemicznej strony reakcji spalania spowodowało, że do trójkąta spalania dodano czwarty element, jakim są wolne rodniki. Od tego czasu występuje także pojęcie czworościanu spalania *(rys. 1).*

Do powstania pożaru są niezbędne: źródło zapłonu/ciepło, wolne rodniki, dostęp do odpowiedniej ilości tlenu oraz paliwo/substancja niebezpieczna. Źródła zapłonu nie da się przewidzieć i trudno go uniknąć, są to np. iskry czy elektryczność, w serwerowniach natomiast kumulacja energii. Wolne rodniki to powstające w trakcie reakcji utleniania związki chemiczne lub pierwiastki mające wolne wiązania, które mogą wchodzić w reakcje chemiczne z innymi substancjami lub pierwiastkami. Tlen jest najłatwiejszy do kontrolowania, dzięki temu można uniknąć zagrożeń pożarowych. Paliwo/substancja niebezpieczna po prostu jest.

Serwerownie są wydzielonymi pomieszczeniami będącymi środowiskiem pracy komputerów pełniących funkcję serwerów przechowujących bazy danych, często wrażliwych z punktu widzenia prowadzenia biznesu. Dlatego tak ważne jest zabezpieczenie tych pomieszczeń przed wystąpieniem pożaru – nawet tlący się ogień może mieć niszczący wpływ na miejsce, gdzie znajduje się zaawansowane technicznie wyposażenie.

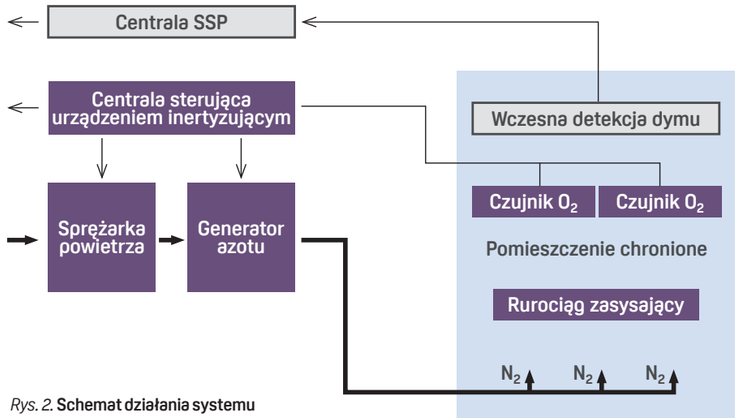
Na rynku są dostępne systemy intertyzujące, które utrzymują stężenie tlenu w pomieszczeniu chronionym na takim poziomie, aby proces spalania nie mógł nastąpić. Zapłon substancji staje się trudny, gdy stężenie tlenu nie przekracza 17% objętościowych, a przy 15% obj. tlenu jest już praktycznie niemożliwy. Taki system składa się z:

– kompresorów powietrza (dostarczone spoza pomieszczenia powietrze zostaje sprężone do wymaganego ciśnienia roboczego),
– generatora azotu rozkładającego dostarczone ze sprężarki powietrze na tlen i azot,
– centrali sterującej, swoistego centrum dowodzenia, gdzie są zapisywane wszelkie informacje dotyczące działania systemu. Centrala uruchamia lub wyłącza dostarczanie azotu do pomieszczenia chronionego po przeanalizowaniu danych wchodzących dotyczących stężenia tlenu
– rurociągów,
– czujników stężenia tlenu, które w sposób ciągły dokonują pomiarów. W pomieszczeniu chronionym instaluje się co najmniej dwa czujniki pracujące niezależnie od siebie,
– przełączników trybu pracy, które umożliwiają przełączanie trybu, np. z 15 % obj. tlenu na 17%. Powietrze o stężeniu tlenu powyżej 17% nie jest traktowane jako powietrze zubożone w tlen, tym samym ludzie mogą w nim przebywać bez ograniczeń czasowych,
– urządzeń alarmowych i informacyjnych,
– instalacji wczesnej detekcji dymu.

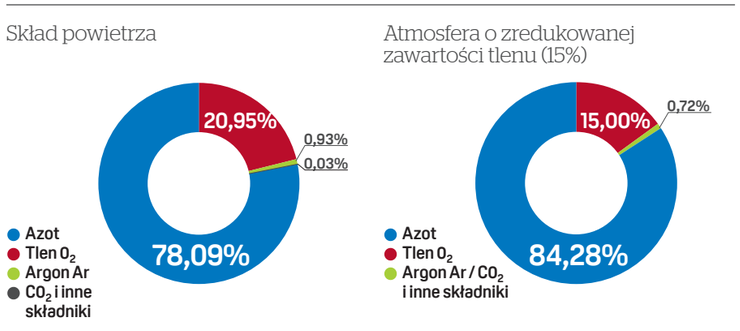
Zasada działania tej technologii polega na kontrolowanym wtłaczaniu azotu do pomieszczenia, co w efekcie zmienia udział procentowy tlenu w powietrzu (*rys. 3* i *rys. 4*).

Ponieważ azot jest składnikiem powietrza, mieszanina tlenu i azotu jest nietoksyczna i nie zagraża człowiekowi, który do 13% obj. tlenu nawet może pracować bez zastosowania sprzętu oddechowego, tyle że krócej. Poniżej 13% obj. tlenu obowiązuje jednak zakaz wstępu do pomieszczenia chronionego. Ze względów bezpieczeństwa należy dokładnie prowadzić pomiary i kontrolować stężenie tlenu zarówno wewnątrz, jak i na zewnątrz pomieszczenia chronionego.

Producenci takiego systemu (*rys. 5*) wymieniają szereg jego zalet, m.in. zapewniają, że w pomieszczeniu chronionym nie ma możliwości powstania pożaru wywołanego przez urządzenie, system zaś wykorzystuje do ochrony wyłącznie powietrze, a dokładnie rzecz biorąc azot w nim występujący. Dzięki temu łatwo go pozyskać w niezbędnej ilości także w pomieszczeniu chronionym. Azot ma najlepszą skuteczność gaśniczą wśród wszystkich gazów obojętnych (z wyjątkiem CO_2). Ponadto urządzenie nie wymaga wymiany gazu gaśniczego (jak w standardowych instalacjach SUG gazowych po wyładowaniu) ani regularnych badań zbiorników ciśnieniowych.



Rys. 2. **Schemat działania systemu**



Rys. 3. **Skład objętościowy powietrza**

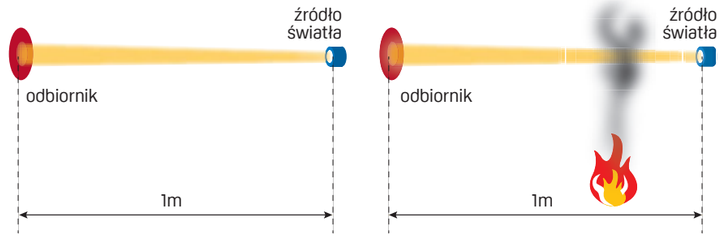
Rys. 4. **Skład objętościowy powietrza po wtłoczeniu azotu**

Rys. 5. **Urządzenie instalacji inertyzującej (fot. WAGNER Group GmbH)**

System zasysający – po prostu bezpiecznie

Techniczne zabezpieczenie serwerowni przed pożarem ma zasadniczy cel, jakim jest niedopuszczenie do pożaru. W miejscu, gdzie znajdują się wyjątkowo cenne (ważne) urządzenia, warto zainstalować – oprócz instalacji gaśniczej gazowej lub urządzenia inertyzującego – system wczesnej detekcji dymu. System aspiracyjny wykrywa zagrożenie pożarowe w jego najwcześniejszym stadium, gdy dym nie jest jeszcze widoczny. Tym samym umożliwia wcześniejszą reakcję użytkownika i ewentualną eliminację źródła pożaru.

System funkcjonuje na zasadzie czujki dymu. Sieć rurek z precyzyjnie dobranymi otworami zasysającymi bez przerwy, 24 godziny na dobę próbkuje powietrze, doprowadzając je do detektora, w którym są wykrywane i analizowane wszystkie cząstki dymu. Zanim jednak powietrze dotrze do głowicy detektora, wszelkie zanieczyszczenia, np. kurz, zostają przefiltrowane. Pozwala to na szybkie i niezawodne wykrywanie nawet najmniejszych cząstek dymu oraz zapobiega powstawaniu fałszywych alarmów. Czujki te, zależnie od klasy, mają możliwość ustawienia różnych progów czułości dokładnie dopasowanych do specyficznych warunków i potencjalnych zagrożeń, a także poziomu tła występującego w pomieszczeniu chronionym. Czułość czujki dymu to nic innego, jak stopień zaciemnienia wyrażony w procentach na metr [%/m]. Stopień zaciemnienia przedstawiono na *rys. 6.*



Rys. 6. **Stopień zaciemnienia**

Zgodnie z normą EN54-20 występują 3 klasy czułości czujek zasysających: A, B i C. W *tabeli* podano przykładowe zakresy (jednego z producentów systemu zasysającego):

Klasa czujki zasysającej	Zakresy czułości czujki
A	0,02–10% / m
B	0,1–10% / m
C	0,5–10% / m

Klasa A – bardzo wysoka czułość; czujki tej klasy nadają się głównie do ochrony pomieszczeń czystych, serwerowni, centrów komputerowych, a także obiektów szczególnie chronionych z racji prowadzonej w nich produkcji lub znajdujących się w nich cennych przedmiotów (np. muzea, archiwa).

Klasa B – zwiększona czułość; czujka przeznaczona do obiektów, w których dym jest trudny do wykrycia, czyli występują w nich duże przepływy powietrza lub pomieszczenia są wysokie.

Klasa C – typowa czułość; czujka doskonała do obiektów, w których konserwacja czujek punktowych jest utrudniona lub inne metody wykrywania pożaru są nieodpowiednie lub niemożliwe.

W przypadku pożaru czujka zasysająca przesyła sygnały do centrali systemu sygnalizacji pożarowej (SSP) budynkowej oraz do centrali sterującej. System wczesnej detekcji dymu może być traktowany jako główne urządzenie wykrywające pożar, a następnie sterujące gaszeniem w standardowych instalacjach SUG gazowych. Może też uruchomić dostarczanie azotu w systemach inertyzujących lub jako system wspomagający, informacyjny.

Trzeba jednak pamiętać, że w systemie SUG gazowym w serwerowni ustawienie detektora zasysającego w klasie A i o zbyt dużej czułości, zbliżonej do czułości tła otoczenia, będzie prowadziło do częstych fałszywych alarmów. Jeśli system wczesnej detekcji będzie sterował gaszeniem, to może wywoływać niepotrzebne wyładowania gazu, co będzie się wiązało z kosztami ponownego napełnienia butli. Jako system wspomagający natomiast w tym wypadku będzie idealny, pozwoli obsłudze na zorientowanie się w sytuacji.

Reasumując – warto i należy poszukiwać odpowiednich metod służących zapobieganiu powstawania pożaru i realnie stosować rozwiązania, by nie ponosić skutków powstałego pożaru.

Literatura

[1] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (DzU z 2010 r. nr 109, poz. 719)
[2] NFPA 2001: *Standard on Clean Agent Fire Extinguishing Systems, edition 2012.*
[3] *Gazem w ogień*, „Przegląd Pożarniczy" 12/2012
[4] EN 54-20:2006 *Fire detection and fire alarm systems – Part 20: Aspirating smoke detectors*
[5] www.wagnergroup.com
[6] *OxyReduct Removing the threat of fire* – broszura handlowa
[7] www.vesda.pl

BIO

Renata Trojanowska
Absolwentka Wydziału Inżynierii Bezpieczeństwa Pożarowego w Szkole Głównej Służby Pożarniczej w Warszawie, zawodowo zajmuje się projektowaniem systemów gaszenia.

Iza Trzeciak
Absolwentka Wydziału Inżynierii Bezpieczeństwa Pożarowego w Szkole Głównej Służby Pożarniczej. Założycielka bloga o ochronie przeciwpożarowej blog-ppoz.pl.

Schrack Seconet Polska
ul. A. Branickiego 15
02-972 Warszawa
http://schrack-seconet.pl

System bezpieczeństwa pożarowego w obiektach przemysłowych

Bezpieczeństwo pożarowe obiektów przemysłowych wymaga szczególnej uwagi. Inwestorzy planujący lub realizujący inwestycje w Polsce konsultują swoje wizje i założenia z firmami konsultingowymi lub wybranym ubezpieczycielem, który wskazuje kierunki działań w zakresie ochrony obiektu, oceny ryzyka, określenia ewentualnych aspektów związanych z procesami produkcyjnymi i zagrożeniem wybuchem (m.in. zgodnie z §4 Rozporządzenia Ministra Gospodarki z 8 lipca 2010 r. w sprawie minimalnych wymagań dotyczących bezpieczeństwa i higieny pracy, związanych z możliwością wystąpienia w miejscu pracy atmosfery wybuchowej). Na tym etapie nadrzędną sprawą jest dostosowanie obiektu do aktualnych wymagań ppoż. i budowlanych oraz ochrona pracowników.

Schrack Seconet Polska

W Polsce wymagania formalne w zakresie systemów sygnalizacji pożarowej bazują na normach serii PN-EN 54. W przypadku inwestorów zagranicznych najczęściej brane są dodatkowo pod uwagę wytyczne VdS – Stowarzyszenia Niemieckich Towarzystw Ubezpieczeniowych od wielu lat dbającego o bezpieczeństwo i zaufanie w zakresie ochrony ppoż. i systemów zabezpieczeń. VdS jest instytucją, która opracowuje zaawansowane koncepcje bezpieczeństwa pożarowego zarówno dla znaczących zakładów przemysłowych i obiektów handlowych, jak i czołowych producentów i integratorów systemów komputerowych. W zakresie wytycznych VdS systemy sygnalizacji pożarowej i sterowania stałymi urządzeniami gaśniczymi (SUG) projektowane są wg wytycznych VdS 2095pl i VdS 2496pl. Obiekty przemysłowe dzielą się na kilka podstawowych kategorii, z których każda wymaga bardzo indywidualnego podejścia na etapie projektowania – niezbędne są szerokie konsultacje z rzeczoznawcą do spraw ppoż. oraz skrupulatne weryfikowanie wymagań formalnych.

SEKTOR ENERGETYCZNY – w najbardziej wymagających przypadkach charakteryzują go zagrożenia wybuchem związane z wszechobecnym pyłem węglowym, gospodarką olejową itp. Wszystkie komponenty systemu sygnalizacji pożarowej muszą mieć odpowiedni stopień ochrony IP ze względu na warunki pracy związane z wymogiem częstego mycia wodą zmywną obszarów, gdzie może występować zagrożenie pożarowe (np. galerie nawęglania). Różnice w stosowaniu odpowiedniej ochrony ppoż., w tym również w zakresie detekcji pożaru, występują w przypadku węgla brunatnego lub kamiennego – oba surowce różnią się między sobą pod względem procesu tlenia, żarzenia czy zagrożeń związanych z występowaniem pyłów. Dlatego w celu ochrony głównych przenośników taśmowych czy galerii nawęglania należy stosować dedykowane rozwiązania bazujące na detekcji gazów pożarowych powstających we wczesnym etapie rozwoju pożaru (tlenie), żarzenia się węgla, czy zmian temperaturowych, oraz występujących w tym obszarze innych zagrożeń.
Głównie w galeriach nawęglania powinno się stosować dedykowane stałe urządzenia gaśnicze oparte na systemach zalewowych lub mgły wodnej, sterowane przez zintegrowany system sygnalizacji pożarowej i sterowania gaszeniem, np. w oparciu o centralę Integral IP MXE/MXF. Z uwagi na znaczną długość galerii nawęglania należy zastosować specjalistyczne czujki pożarowe. Ich zadaniem jest nie tylko szybka detekcja pożaru już na etapie tlenia, ale także dokładne określenie lokalizacji, aby konkretna sekcja gaśnicza została uruchomiona. Ze względu na bardzo częste występowanie w tego typu obiektach kilkunastu, a nawet kilkudziesięciu stref gaszenia zastosowany system sygnalizacji pożarowej i sterowania gaszeniem musi realizować funkcję gaszenia wielostrefowego.

Dodatkowo obiekt energetyczny składa się często z kilkudziesięciu różnego rodzaju budynków, w których zainstalowane centrale sygnalizacji pożarowej i sterowania gaszeniem wymagają połączenia ze sobą w sieć central – w wielu istniejących i powstających aktualnie tego typu obiektach znajduje swoje zastosowanie najnowszej generacji system rozproszony Integral WAN (wprowadzony w miejsce sieci SecoNET) pozwalający na połączenie w jedną sieć bardzo dużej liczby central, dający możliwość inwestorowi czy generalnemu wykonawcy zrealizowania jednego spójnego systemu sygnalizacji pożarowej i sterowania gaszeniem Integral IP – z możliwością wydzielenia podsystemów dla poszczególnych części zakładu lub rozdzielenia części detekcyjnej i sterowania gaszeniem. Takie podejście jest podyktowane wymogiem odłączania jak najmniejszej części systemu przy prowadzeniu jakichkolwiek prac w zakresie rozbudowy czy serwisu, aby pozostała część systemu mogła realizować swoje funkcje bezpieczeństwa w sposób nienaruszony.

SEKTOR GAZOWY I CHEMICZNY (analiza zagrożenia i temperatura zapłonu produktów) – ma ogromne znaczenie dla bezpieczeństwa ludzi, chronionych obiektów i procesów produkcji. W sektorze chemicznym ze względu na występujące zagrożenie wybuchem bardzo często muszą być stosowane dedykowane urządzenia przeciwpożarowe spełniające dyrektywę ATEX. Funkcjami detekcji i sterowania zarządzają centrale sygnalizacji pożarowej i sterowania gaszeniem.

SEKTOR HUTNICZY I GÓRNICZY (analiza zagrożenia i zmiany temperaturowe w różnych obiektach huty) – szczególną

Bezpieczeństwo pożarowe

uwagę zwraca się na obszary związane z tunelami kablowymi, którymi prowadzone są instalacje elektryczne zasilające urządzenia produkcyjne i piece hutnicze. W zakresie detekcji pożaru można zastosować liniową czujkę ciepła Listec lub inne czujki pożarowe o podwyższonym stopniu ochrony IP przystosowane do pracy w trudnych warunkach otoczenia oraz system gaszenia SUG oparty na mgle wodnej lub aerozolach sterowanych przez wielostrefową centralą sterowania gaszeniem Integral IP MXF/MXE.

SEKTOR LOGISTYCZNY – charakteryzuje się zmiennością wynikającą z wprowadzania i magazynowania produktów, które mają różne temperatury zapłonu, co musi być uwzględnione w kontekście doboru urządzeń przeciwpożarowych. Świadomy inwestor powinien zwracać szczególną uwagę na sposoby zabezpieczenia swojego mienia i jego odpowiednie magazynowanie. Straty związane z błędnym określeniem sposobu zabezpieczenia takiego obiektu mogą być ogromne. W obiektach tego typu znajdują zastosowanie czujki zasysające AIRSCREEN ASD 535 szczególnie do zabezpieczania magazynów wysokiego składowania.

SEKTOR MOTORYZACYJNY (analiza zagrożenia, strefy zagrożone wybuchem, biura, strefy magazynowania itp.) – ze względu na różnorodność materiałów stosowanych i składowanych w tym sektorze należy przeprowadzić szczegółową analizę zagrożeń. W tym sektorze stosuje się bardzo wiele materiałów i rozwiązań praktycznie z każdej grupy urządzeń ppoż. Dla przykładu – mogą być tu zastosowane czujki w osłonach przeciwwietrznych przystosowane do zabezpieczania kanałów wentylacyjnych lub czujki zasysające zabezpieczające hale produkcyjne. Dodatkowo należy zwrócić szczególną uwagę na pomieszczenia lakierni, gdzie występują strefy zagrożone wybuchem. W tych obiektach również znajdują zastosowanie wielostrefowe centrale gaszenia współpracujące z każdym typem SUG.

SEKTOR SPOŻYWCZY – wiąże się z magazynowaniem m.in. mąki, wody, mięsa i jego przetworów (chłodnie i mroźnie). Znane są przypadki, kiedy ubezpieczyciel obliczył

Obiekty przemysłowe dzielą się na kilka podstawowych kategorii, z których każda wymaga bardzo indywidualnego podejścia na etapie projektowania.

straty związane ze zdarzeniem pożarowym na ok. 100 mln PLN. Schrack Seconet ma w swojej ofercie dedykowane rozwiązania przeznaczone do wczesnej detekcji pożaru w mroźniach – tj. czujki zasysające dymu wyposażone w specjalne układy automatycznego rozmrażania zatkanych lodem (oblodzonych) otworów ssących.

SEKTOR DROGOWY – wyróżniają go tunele, nisze ewakuacyjne, MOP-y. W zakresie tego obszaru szczególną uwagę zwraca się na niezawodne wykrycie zagrożenia, a także na zastosowanie odpowiedniego stopnia ochrony IP urządzeń. W zakresie detekcji pożaru w tunelach drogowych znajduje zastosowanie liniowa czujka ciepła. Zainstalowany w tunelu aktywny element detekcyjny czujki, a więc kabel sensoryczny, ma zintegrowane, rozmieszczone na całej swojej długości czujniki ciepła pozwalające na identyfikację miejsca pożaru i charakteryzuje się wysoką odpornością na panujące warunki atmosferyczne. Dodatkowo szczególnie długie tunele mogą być wyposażone w dźwiękowy system ostrzegawczy (DSO), gdzie należy również zastosować specjalistyczne głośniki przeznaczone do pracy w trudnych warunkach atmosferycznych.

Wszystkie ww. sektory budownictwa przemysłowego w związku z zagrożeniami pożarowymi, które mogą w nich wystąpić, wymagają zastosowania systemu sygnalizacji pożarowej zapewniającego szybkie i niezawodne wykrycie pożaru. Punktowe czujki pożarowe chroniące część administracyjną, jak też pomieszczenia produkcyjne niewymagające rozwiązań specjalnych muszą dostosowywać swoje parametry detekcji do panujących warunków otoczenia. Taką funkcjonalność zapewniają interaktywne czujki pożarowe serii CUBUS, np. MTD 533X, które stale analizują parametry otoczenia i podwyższają swoją czułość w momencie wykrycia przyrostu temperatury w związku z rozwijającym się pożarem. Dzięki temu czujki mają optymalną czułość zapewniającą niezawodne wykrycie prawdziwego pożaru, a przy tym są odporne na alarmy mylne.

W obiektach przemysłowych wymagających bardzo często indywidualnego podejścia do spełnienia wymagań bezpieczeństwa pożarowego bardzo kluczowa jest elastyczność oprogramowania central sygnalizacji pożarowej i sterowania gaszeniem, pozwalająca na realizację scenariusza pożarowego, przy jednoczesnym uwzględnieniu ciągłości działania procesów produkcyjnych. Dodatkowo do realizacji funkcji bezpieczeństwa na najwyższym poziomie stosowany jest system integrujący urządzenia przeciwpożarowe SIS-FIRE, który ściśle współpracuje z systemem Integral IP.

System sygnalizacji pożarowej i sterowania gaszeniem INTEGRAL IP firmy Schrack Seconet znacznie przewyższa wymagania norm europejskich serii PN-EN 54 w zakresie funkcjonalności oraz niezawodności działania. Należy zwrócić tu szczególną uwagę na pełną redundancję komponentów sprzętowych oraz oprogramowania central Integral IP MXF/MXE. Ze względu na swoje unikalne parametry techniczne system znalazł zastosowanie w wielu skomplikowanych obiektach przemysłowych. Należą do nich: Elektrownia Kozienice, Elektrownia Opole, Rafineria LOTOS Gdańsk, Elektrociepłownia Wrocław, Ikea Jarosty, Azoty Tarnów i wiele innych.

Najważniejsze funkcje systemu, dzięki którym rozwiązanie idealnie wpisuje się w standardy obiektów przemysłowych:

1	100% redundancja systemu (sprzęt + oprogramowanie) – najbezpieczniejsze rozwiązanie dostępne na polskim rynku, zapewniające ciągłość działania w krytycznych sytuacjach dla obiektu w ruchu.
2	Gwarancja kompatybilności „w przód" i „wstecz" – brak konieczności wymiany całego systemu przy rozbudowie czy modernizacji obiektu. Dotyczy to zarówno elementów peryferyjnych (czujki, ROP-y, moduły we/wy), jak i CSP/CSG.
3	Pełna współpraca z każdym typem SUG: systemy gaszenia gazem, instalacje mgły wodnej, tryskaczowe, zraszaczowe, pianowe, aerozole gaśnicze itp.
4	CSP/CSG o modułowej budowie i elastycznym oprogramowaniu – możliwość stworzenia dowolnej konfiguracji systemu spełniającego obowiązujące normy i wytyczne ubezpieczycieli.
5	CSP/CSG standardowo wyposażone w rozszerzoną pamięć zdarzeń dla 65 000 rekordów, co zapewnia weryfikację stanu pracy i analizę stanów systemowych w bardzo długim horyzoncie czasowym,
6	Możliwość budowy sieci central CSP/CSG o strukturze równorzędnej i hierarchicznej na bazie sieci Integral LAN i Integral WAN - dostosowanie konfiguracji do wymagań technicznych i organizacyjnych inwestora.
7	Możliwość połączenia CSP/CSG w sieć za pomocą przewodów miedzianych i światłowodowych o różnych topologiach: pierścień, drzewo i sieć kratowa. Odporność na 3 uszkodzenia w sieci (pierścień redundantny) lub 7 (sieć kratowa).
8	Pełna współpraca z systemem integrującym urządzenia przeciwpożarowe (SIUP) SIS-FIRE – sterowanie, wizualizacja i zarządzanie bezpieczeństwem pożarowym obiektu.
9	Możliwość integracji z różnymi systemami zewnętrznymi zgodnie ze standardami BACnet, MODBUS, OPC.
10	Wyniesione redundantne panele obsługi dla CSP/CSG posiadające czytelny interfejs użytkownika i programowalne klawisze funkcyjne umożliwiające intuicyjną obsługę i dostosowanie funkcji do operatora - do zastosowania w pomieszczeniach służb ochrony i nadzoru (brak konieczności stosowania dodatkowych central).
11	Elastyczne oprogramowanie z możliwością definiowania blokad międzystrefowych z selektywną obsługą 2, 3 i więcej alarmów pożarowych w SSP/SSG –selektywne sterowania automatyką ppoż.
12	Wysoka odporność systemu na zakłócenia elektromagnetyczne i odporność na fałszywe alarmy – zapewnienie ciągłości działania procesu produkcyjnego.
13	Bezpieczna weryfikacja algorytmów sterowań i testowanie instalacji SSP/SSG dzięki zintegrowanym funkcjom oprogramowania i specjalnego trybu serwisowego.
14	Dedykowany pakiet narzędzi do zdalnego dostępu „Remote Integral" – szybsze rozpoznanie zagrożenia, oszczędność na serwisie, szybsza wymiana informacji między właścicielem (operatorem) obiektu a służbami technicznymi.
15	Aplikacje do nadzorowania stanu systemu do zastosowania na urządzeniach mobilnych – wspomaganie operatora zwłaszcza w rozległych obiektach przemysłowych.
16	Linie pętlowe X-LINE o długości do 3500 m, z możliwością podłączenia do 250 elementów peryferyjnych – nadzorowanie rozległych obszarów i łatwa rozbudowa.
17	Interaktywne czujki wielokryteryjne (dymu, ciepła, CO) serii CUBUS – możliwość detekcji pełnego spektrum pożarów TF1-TF9.
18	Elastyczne dostosowanie parametrów detekcji czujek punktowych (klasa czułości i wybór sensorów) w przypadku zmiany przeznaczenia pomieszczeń.
19	Specjalne wykonania czujek punktowych: lakierowana elektronika, pierścienie uszczelniające, dedykowane gniazda do różnych sposobów montażu (strop betonowy, sufit podwieszany, podłoga techniczna).
20	Pełna gama specjalnych czujek pożarowych, które umożliwiają zabezpieczenie każdego obszaru w przemyśle: czujki zasysające dymu, liniowe czujki ciepła, liniowe czujki dymu, czujki płomienia, wielosensorowe czujki gazu itp.
21	Czujki zasysające ASD 535 zintegrowane bezpośrednio z linią pętlową - możliwość odczytu parametrów i programowania, z wykorzystaniem oprogramowania systemu Integral IP.
22	Czujki zasysające ASD 535 z dedykowanym osprzętem do zabezpieczenia pomieszczeń mroźni i chłodni oraz obszarów zagrożonych wybuchem.
23	Zastosowanie czujki zasysającej ASD 535 do sterowania urządzeń SUG - koincydencja międzyczujnikowa (między układami orurowania).
24	Czujki liniowe ciepła do stosowania w bardzo ciężkich warunkach otoczenia, np. tunele drogowe i kablowe, systemy taśmociągowe, lakiernie, rampy załadunkowe itp.
25	Urządzenia spełniające wymagania norm serii PN-EN 54, dyrektywy ATEX i wytycznych ubezpieczycieli, np. VdS, FM. Możliwość uzyskania zniżki u niektórych ubezpieczycieli.
26	Duża sieć partnerów, którzy przechodzą obowiązkowe szkolenia z zakresu systemów sygnalizacji pożarowej dzięki wyjątkowemu programowi partnerskiemu Schrack Seconet.
27	Stała opieka działu handlowego i technicznego dająca pewność funkcjonowania systemu SSP w każdych warunkach środowiskowych.
28	Bardzo duża liczba obiektów referencyjnych zrealizowanych wspólnie z partnerami Schrack Seconet.

Johnson Controls
Fire Detection Poland
pawel.jozwik@jci.com
www.johnsoncontrols.com

Centrale Zettler Profile Flexible

Co nowego? 10 powodów, dlaczego...

Współczesne systemy sygnalizacji pożarowej, niezależnie od producenta, marki, miejsca produkcji czy wykorzystywanej technologii, zawsze spełniają pewne wymagania stawiane przez lokalne przepisy. Niekiedy jednak spełnienie tych minimalnych wymagań dyktowanych przez prawo jest dla klienta niewystarczające.

Paweł Józwik

W takich wypadkach poszukuje on produktu, który ma do zaoferowania coś więcej – coś unikalnego, co pozwoli dopasować system idealnie do budynku, ułatwi instalację czy obsługę oraz w dłuższej perspektywie zapewni wieloletnie wsparcie, kompatybilność ze starszymi i nowszymi rozwiązaniami oraz przyniesie oszczędności w jego eksploatacji.

Zettler jako producent systemów sygnalizacji pożarowej od wielu lat stara się wychodzić naprzeciw oczekiwaniom klientów, którzy poszukują najbardziej zaawansowanych rozwiązań. Najnowsza rodzina central sygnalizacji pożarowej Zettler PROFILE Flexible oferuje szereg cech i funkcji, które stawiają poprzeczkę jeszcze wyżej niż do tej pory:

1 Zwiększona pojemność pętli

Projekt systemu sygnalizacji pożarowej zawsze musi uwzględniać takie kwestie praktyczne, jak: układ budynku, lokalizacja szachtów oraz tras kablowych czy liczba urządzeń alarmowych pobierających duże ilości energii. Te zmienne często decydują o użytecznym rozmiarze pętli dozorowej, co może skutkować nieefektywnym wykorzystaniem jej pojemności. Aby zoptymalizować wykorzystanie pojemności pętli, PROFILE Flexible oferuje możliwość wyboru, jak zostanie ona zaprojektowana: czy jako pętla dużej mocy (HP) o dużej obciążalności prądowej (do 1 A) i pojemności 250 adresów, czy jako para pętli współdzielonych (SP), która korzysta z elastycznego przydzielania zasobów (250 adresów, prąd 1 A) pomiędzy dwiema fizycznymi pętlami dozorowymi w budynku. Tego rodzaju optymalizacja może znacznie obniżyć koszty instalacji systemu.

2 Parametry przewyższające wymagania przepisów

Parametry systemu PROFILE Flexible przewyższają wymagania stawiane przez przepisy. System jest zgodny z normą EN 54-13 dotyczącą kompatybilności poszczególnych jego elementów. Certyfikat potwierdza, że zgodne z normami są nie tylko poszczególne elementy systemu, takie jak centrale, czujki, moduły – czego wymagają przepisy – ale zapewnia również, że poszczególne podzespoły systemu współpracują ze sobą spójnie i bez zakłóceń. Spełnienie wymienionej normy europejskiej daje poczucie bezpieczeństwa oraz pewność ochrony życia i mienia.

3 Szerokie możliwości rozbudowy systemu

Rozbudowa systemu sygnalizacji pożarowej jest często konieczna wraz z rozwojem zabezpieczanego budynku. PROFILE Flexible zapewnia pojemność nawet do 4000 adresów w jednej centrali, a sieć współpracujących ze sobą węzłów aż do 99 central. System PROFILE Flexible jest zdolny nie tylko do rozbudowy w miarę rozwoju firmy, ale może być także dostosowywany do zmieniających się potrzeb dzięki możliwości łatwego dodawania kart rozszerzeń czy paneli wyniesionych z ekranami dotykowymi.

4 Obniżenie kosztów instalacji dzięki konstrukcji modułowej

W nowej rodzinie central zastosowano konstrukcję modułową wykorzystującą nowe wtykowe karty rozszerzeń. Istnieje około 50 różnych opcji projektowych, co oznacza dostępność bardzo wielu kombinacji pasujących do zróżnicowanych obiektów. Daje to możliwość stworzenia najbardziej ekonomicznego projektu, dostosowanego do konkretnych potrzeb w danej aplikacji, bez potrzeby inwestowania od razu we w pełni wyposażony system. Dodatkowo możliwość łatwego dodawania kart rozszerzeń czy wyświetlaczy strefowych pozwala zbudować system przyjazny kieszeni użytkownika końcowego.

5 Łatwy montaż

Centrale PROFILE Flexible są dostarczane z łatwą w instalacji ramą, dzięki czemu montaż centrali na ścianie może przeprowadzić nawet jedna osoba. Instalacja ramy montażowej i przygotowanie okablowania mogą być przeprowadzone przed powieszeniem samego urządzenia, co pozwala na bezproblemową i bezpieczniejszą niż kiedykolwiek instalację central.

6 Kompatybilność wstecz i w przód

Technologia PROFILE Flexible może zastąpić istniejące systemy sygnalizacji pożarowej Zettler, wykorzystując okablowanie, czujki i inne istniejące urządzenia pętlowe. Co więcej – dzięki możliwości współpracy różnych generacji central Zettler we wspólnej sieci – nawet systemy zbudowane na początku XX w. mogą być stale rozbudowywane o nowe urządzenia. Dzięki temu klienci mają również możliwość uaktualnienia tradycyjnego interfejsu obsługi do zaawansowanego wyświetlacza PROFILE z kolorowym ekranem dotykowym, co znacznie wydłuża okres użytkowania istniejących systemów klienta, przy jednoczesnej minimalizacji kosztów.

7 Graficzny interfejs użytkownika (GUI) z ekranem dotykowym

Graficzny interfejs z ekranem dotykowym centrali PROFILE Flexible został zaprojektowany z myślą o ergonomii i wygodzie obsługi przez użytkowników końcowych. Przycisk informacyjny zapewnia pomoc kontekstową oraz instrukcje ekranowe dla operatora. Gwarantuje to szybkie i niezawodne wsparcie, zwłaszcza dla użytkowników, którzy rzadko korzystają ze wszystkich funkcji centrali. W pełni konfigurowalny ekran główny pozwala wkomponować centralę w wygląd otoczenia i dopasować ją do wystroju każdego wnętrza.

8 Wygodny dostęp

Użytkownicy mogą wybrać metodę dostępu do systemu: z wykorzystaniem tradycyjnego klucza, hasła lub karty RFID. Dzięki kartom RFID nie ma potrzeby pamiętania haseł, a zalogowanie do centrali staje się proste i szybkie, co jest szczególnie istotne w sytuacjach awaryjnych. Identyfikatory oraz poziomy dostępu użytkowników są kontrolowane i rejestrowane, co jest szczególnie użyteczne w obiektach o podwyższonym ryzyku, gdzie istotne jest śledzenie, kto wykonuje operacje o znaczeniu krytycznym.

9 Ekranowe mapy obiektu

Interfejs użytkownika centrali PROFILE Flexible (GUI) może wykorzystywać pliki graficzne do pokazywania lokalizacji zdarzeń. Ekranowe mapy obiektu pozwalają na szybki dostęp do informacji, takich jak rzuty pięter oraz rozszerzone informacje o urządzeniach czy warunkach panujących w danej strefie dozorowej. Załadowane do wyświetlacza grafiki można w łatwy i szybki sposób zmieniać przy wykorzystaniu pamięci flash USB, co pozwala na bezproblemowe dostosowanie do zmian zachodzących w budynku. Mapy prezentowane w wersji elektronicznej na wyświetlaczu GUI pozwalają również oszczędzić czas, bardzo cenny w przypadku wystąpienia pożaru, gdyż informacje o jego lokalizacji są łatwo dostępne – za jednym dotknięciem palca.

10 Zaawansowana konfiguracja i diagnostyka

Oprogramowanie konfiguracyjne można z łatwością wczytać do centrali również za pomocą klucza USB, co pozwala na oszczędność czasu i pieniędzy podczas instalacji. Na klucz USB można zapisać do 10 tys. zdarzeń z rejestru pamięci centrali, w celu dalszego przetwarzania, np. w aplikacji Excel. Dodatkowo dostępne są szczegółowe raporty dotyczące testów krokowych, stanu systemu czy postępów w konserwacji, a szerokie opcje ich filtrowania pozwalają na dogłębną diagnostykę wszystkich zdarzeń.

Wymienione cechy stanowią tylko wycinek szerokich możliwości, które dają najnowsze centrale z rodziny Zettler PROFILE Flexible. Na pewno jednak pozwalają się wyróżnić i dać klientowi coś „ekstra", co pozwala spełnić jego oczekiwania w stosunku do systemu, który ma chronić jego mienie i życie ludzi.

Więcej informacji o firmie ZETTLER i linii produktów PROFILE Flexible na stronie **http://tycofpp.com/ZETTLER-profile-flexible/**

Przemysłowy Internet Rzeczy

W obliczu agresywnej konkurencji w sektorze przemysłowym fabryki i zakłady produkcyjne starają się podnieść wydajność i ograniczyć przestoje do minimum. Zarządzający produkcją mogą dziś korzystać z Przemysłowego Internetu Rzeczy (IIoT – *Industrial Internet of Things*) i danych generowanych przez połączone z siecią urządzenia, zwiększając „inteligencję" linii produkcyjnych.

Choć dane najczęściej są przetwarzane przez pracujące w *data center* serwery, to coraz więcej dzieje się w urządzeniach brzegowych sieci.

a&s International

W ostatnich stuleciach przemysł doświadczał kolejnych rewolucji, a każda wpływała na sposób wytwarzania produktów. W wyniku pierwszej w XVIII w. ludzi zaczęły zastępować maszyny. Do drugiego przełomu doszło na początku XX w., kiedy to powstała koncepcja linii produkcyjnej. Wraz z upowszechnieniem się komputerów, sieci i robotów przemysł jeszcze bardziej zmienił swoje oblicze.

Niedawno rozpoczęła się era Przemysłowego Internetu Rzeczy (IIoT – Industrial Internet of Things), zwana także Przemysłem 4.0, w wyniku czego doświadczamy następnej rewolucji, polegającej na wykorzystaniu połączonych z siecią urządzeń i czujników w celu zwiększenia wydajności i efektywności. Przykładowo czujniki mogą generować dane dotyczące stanu urządzeń i procesów, czyszczenia bez dekompletacji maszyny (CIP – *Clean-In-Place*), bezpieczeństwa i planowania produkcji oraz śledzenia zasobów. W rezultacie staje się łatwiejsze przechodzenie do podejścia proaktywnego wykonywanych operacji oraz zwiększania wydajności. Gdy ważna jest jakość, można zastosować dodatkowe czujniki, które wspomogą kontrolę jakości procesów.

– *Pomiary dokonywane przez czujniki dotyczą różnych parametrów, użycie konkretnych sensorów zależy od tego, jakie dane są kluczowe z biznesowego punktu widzenia. Mogą być np. związane z warunkami środowiskowymi (temperatura, wilgoć, ciśnienie). Mogą także dotyczyć bezpieczeństwa i ochrony, wtedy zostaną użyte czujniki zbliżeniowe albo wizyjne, monitorujące dany obszar. Są także sensory, które sprawdzają stan produkcji i maszyn, mierząc przyspieszenie i wibracje* – tłumaczy Eric Ehlers, Vertical Marketing Manager w Cisco. – *Otrzymywane w rezultacie ich zastosowania dane dają pełniejszy wgląd, zwiększając efektywność i automatyzację procesów, bezpieczeństwo i ochronę oraz monitorowanie i optymalizację zużycia zasobów. Uzyskiwane informacje mogą służyć do usprawniania łańcucha dostaw oraz projektowania nowych produktów.*

Potencjału wykorzystania IIoT nie można zignorować. Według szacunków analityków z firmy MarketsandMarkets wartość rynku IIoT ma się zwiększyć z 113,7 mld USD w roku 2015 do 195,5 mld USD w 2022 r., przy średnim rocznym wzroście w latach 2016–2022 obliczanym na 7,9 proc. W raporcie napisano: „Branża przemysłowa przeżywa transformację wynikającą z wprowadzania koncepcji inteligentnej fabryki oraz technologii automatyzacji produkcji. Rządowe inicjatywy, np. Industrie 4.0 w Niemczech oraz Plan Industriel we Francji, mają wspierać wdrażanie rozwiązań IIoT w Europie. Można się też spodziewać, że kraje o największych wzrostach w sektorze przemysłowym, takie jak USA, Chiny i Indie, będą – wprowadzając technologie inteligentnej produkcji – w dalszym ciągu rozwijać tę branżę, co zwiększy jej udział w tamtejszym PKB".

Znaczenie danych

Podstawą IIoT są dane, które szefom produkcji dają większy wgląd w linie produkcyjne. Tradycyjnie przez dekady dane z czujników były zbierane w trzech celach: jako wejściowa informacja do sterowania procesami kontroli maszyn, fabryki w czasie rzeczywistym; do wyświetlania ich w pomieszczeniach kontrolnych, by można było je kontrolować i reagować na zmiany lub alarmy wyzwalane zgodnie z prostymi, ustalonymi regułami; do przechowywania lokalnie z myślą o działaniach *post factum* i wykorzystania ich po awarii do analizy oraz usprawnienia procesów kontroli. W szczególności dane mogą być przydatne w serwisowaniu predykcyjnym, które staje się wyjątkowo ważne dla producentów próbujących zminimalizować przestoje w fabrykach. »

JAK SPRAWDZAJĄ SIĘ ROZWIĄZANIA SECURITY W PRZEMYŚLE

Oprócz czujników przemysłowych szefowie produkcji mogą także wykorzystywać rozwiązania security, takie jak monitoring wizyjny i kontrola dostępu, których podstawową funkcją jest stałe zapewnianie bezpieczeństwa i ochrony w obiektach produkcyjnych.

– *W ramach tworzenia ochrony fizycznej w fabryce na początku często wdraża się kamery, co wyraźnie poprawia bezpieczeństwo w obiekcie. Dane z systemów kontroli dostępu w połączeniu z obrazami z kamer mogą zagwarantować, że dostęp do obiektu będą miały jedynie uprawnione do tego osoby. Mogą w konsekwencji ułatwić dostosowywanie się do standardów, a także pomóc w likwidowaniu przyszłych zagrożeń, które mogłyby wpływać na produkcję* – twierdzi Eric Ehlers, Vertical Marketing Manager w Cisco.

W coraz większym stopniu wizja jako medium zaczyna być wykorzystywana w fabrykach także do innych zadań. Przykładem może być widzenie maszynowe, w którym obraz rejestrowany przez kamery jest wykorzystywany do wykrywania defektów, prowadzenia ramion robotów albo automatycznego kierowania pojazdami w fabryce. W raporcie MarketsandMarkets analitycy tej firmy przewidują, że wartość globalnego rynku widzenia maszynowego w 2022 r. osiągnie 14,4 mld USD, co oznacza średni roczny wzrost na poziomie 8,4 proc. w latach 2016–2022.

– *Do najważniejszych czynników stymulujących wzrost rynku widzenia maszynowego należą: rosnąca potrzeba kontroli jakości i automatyzacji produkcji, zwiększające się wykorzystanie wizyjnie sterowanych robotów w branżach samochodowej, farmaceutycznej, spożywczej i opakowaniowej oraz innych sektorach przemysłowych, a także coraz większe wymagania dotyczące systemów widzenia maszynowego znajdujące zastosowanie w specyficznych aplikacjach* – twierdzą autorzy raportu.

Jednocześnie kamery są używane do uzyskiwania większego wglądu w procesy. – *Przykładowo czujniki wykrywające ruch mogą być łączone z kamerami w celu rejestracji zdarzeń oraz tworzenia gorących miejsc na mapach obiektu, pomagając poznać wzorce przepływu ruchu. Czujniki mogą być wykorzystywane także do monitorowania procesu i wyzwalania alarmów w trudno dostępnych rejonach instalacji przemysłowych. Ułatwiają także zdalne naprawy, są pomocne w ograniczaniu strat w produkcji – mogą monitorować jakość produktów, wyszukując odchylenia od wzorców* – wyjaśnia Eric Ehlers z Cisco.

» Mikrowzorce ukryte w terabajtach danych wygenerowanych przez czujniki mogą ostrzegać przed awariami maszyn, które jeszcze kilka lat temu nie były wykrywane nawet przez najbardziej zaawansowane systemy monitorowania. Analitykom danych brakowało narzędzi do przewidywania awarii, a zakłady przemysłowe nie zatrudniały badaczy danych, by podejmować takie próby. Wraz z nastaniem czasów Przemysłu 4.0 zainteresowanie rozwiązaniami predykcyjnego serwisowania w szybkim tempie rośnie, coraz więcej tego rodzaju rozwiązań trafia też na rynek.

Urządzenia brzegowe kontra chmura

Kluczową sprawą staje się analiza generowanych i gromadzonych danych. Najczęściej są one wysyłane do serwera w centrum danych w celu ich przeanalizowania. Ale obecnie w coraz większym stopniu ich przetwarzanie zaczyna być przeprowadzane w urządzeniach brzegowych sieci, co ma zalety.

Analiza krytycznych danych, wrażliwych na opóźnienia, której trzeba dokonać w czasie od milisekundy do poniżej sekundy, powinna być przeprowadzona w urządzeniu brzegowym. Dzięki temu, jeśli pojawi się błąd, jego korekcji można dokonać natychmiast, bez zbędnej zwłoki. W przetwarzaniu na brzegu sieci nie ma problemu z pasmem i opóźnieniami, a podejmowanie decyzji odbywa się w pobliżu miejsca zdarzenia. W ten sposób optymalizuje się także przesył danych do sieci. Można ustalić reguły tak, by właściwe dane docierały do właściwych ludzi we właściwym czasie, co zapewni pełen obraz sytuacji.

> Im można szybciej przetwarzać informacje z czujników na linii produkcyjnej, podejmować decyzje albo wprowadzać korekty, tym szybciej są likwidowane problemy wpływające na jakość i produkcję. Oszczędza się czas, zwiększa wydajność, podnosi jakość i optymalizuje proces produkcji.

Analityka wykonywana na serwerach w centrach danych czy chmurze nie przestała być potrzebna. Jest niezbędna do długoterminowych analiz, które nie są tak uzależnione od czasu. Będzie odpowiednia przy obliczeniach, które wymagają dużo czasu i są przeprowadzane na wielkich zbiorach danych, zwanych *big data*. Przykładami takiego zastosowania są przeglądy predykcyjne i optymalizacja procesów. Okazuje się, że najlepszym podejściem do optymalizacji IIoT w środowisku produkcyjnym jest połączenie obu koncepcji. Przy kompleksowej analizie danych kombinacja analityki w urządzeniach brzegowych z wykonywaną przez serwery przynosi najlepsze rezultaty. Urządzenia brzegowe wyposażone w sztuczną inteligencję (AI) mogą przechwytywać i analizować krytyczne dane, a do serwerów są przesyłane tylko dane przetworzone. W efekcie dalsza analiza na serwerach lokalnych bądź w chmurze staje się bardziej efektywna, ogranicza się opóźnienie danych oraz sprawia, że dane z czujników są bezproblemowo obsługiwane przez system sterowania. Kombinacja analityki brzegowej z dokonywaną na serwerach zapobiega tworzeniu się zatorów w sieci, ponieważ do serwerów są przekazywane jedynie dane przetworzone. O alarmach i zdarzeniach bezpośrednio wychwytywanych przez urządzenia brzegowe są informowani pracownicy i personel zajmujący się utrzymaniem maszyn.

– *Krytyczne aplikacje, które wymagają małych opóźnień oraz szybkich pomiarów, są lepiej obsługiwane w urządzeniach brzegowych. Z kolei aplikacje o dużych woluminach danych, które potrzebują znacznie większych zasobów obliczeniowych, będą lepiej działać w środowisku data center i chmury. Łącząc analitykę danych w czasie rzeczywistym na brzegu sieci z analityką big data, dotyczącą danych historycznych, można określać warunki, które pozwolą podnieść jakość, zwiększyć wydajność oraz całkowitą efektywność sprzętu. Dane te mogą być następnie integrowane z systemami planowania zasobów przedsiębiorstwa (ERP – Enterprise Resource Planning) oraz realizacji produkcji (MES – Manufacturing Execution System) w celu uzyskania lepszego wykorzystania zasobów, wglądu w środowisko oraz większej kontroli jakości w trakcie produkcji* – podkreśla E. Ehlers.

Wykorzystanie sztucznej inteligencji w IIoT

W IIoT najważniejsze dane są generowane przez połączone urządzenia przemysłowe. Dzięki nim możliwe jest dalsze poszukiwanie, wydobywanie i analizowanie informacji przez specjalistów. Przedsiębiorstwa mają jednak ograniczone budżety i często nie są w stanie pozwolić sobie na zatrudnienie właściwych ekspertów. Na rynku brakuje wykwalifikowanych analityków *big data* i inżynierów. Zakłady przemysłowe nie są też na tyle elastyczne, by tworzyć własne centra kompetencji, a technicy z hal produkcyjnych nie staną się nagle ekspertami od uczenia maszynowego. W związku z tym dostawcy IIoT będą zmuszeni dostarczać rozwiązania, które nie wymagają wielkiego wkładu pracy od personelu zakładu produkcyjnego. Z pomocą przychodzą AI i uczenie maszynowe. Na rynku są już dostępne systemy predykcyjnego serwisowania zasobów oparte na IIoT, wykorzystujące wspomniane technologie. Taki system automatycznie przeprowadza ekstrakcję cech charakterystycznych, kalibrację modelu (w uczeniu maszynowym znaną także pod hasłami *meta-parameter search* lub *hyper-parameter optimization*) oraz selekcję modelu w celu wybrania najbardziej odpowiedniego rodzaju detekcji anomalii dla każdego czujnika, który będzie analizowany. Krótko mówiąc, wykonuje pracę ekspercką na zbiorze danych.

Nie można zaniedbać cyberbezpieczeństwa

Przemysłowy Internet Rzeczy generuje mnóstwo danych, dlatego kluczowe staje się zagwarantowanie, by były bezpiecznie przesyłane i przechowywane. W efekcie, korzystając z IIoT, trzeba zadbać o cyberbezpieczeństwo. Użycie analityki *big data* do optymalizacji procesu produkcji nie spełni swojej funkcji, gdy te same połączenia czujników z chmurą wykorzystają cyberprzestępcy do przechwycenia kontroli nad produkcją, wstrzymania jej oraz wymuszenia okupu za ponowne uruchomienie. Systemy wcześniej niedostępne przez Internet stają się nagle widoczne w całej światowej sieci. Od tego, czy zdołamy zabezpieczyć IIoT przed atakami, będzie zależało, czy spełnią się obietnice Przemysłowego Internetu Rzeczy, czy też okaże się on porażką. Bezpieczeństwo cybernetyczne i zabezpieczenia techniczne są ze sobą ściśle powiązane.

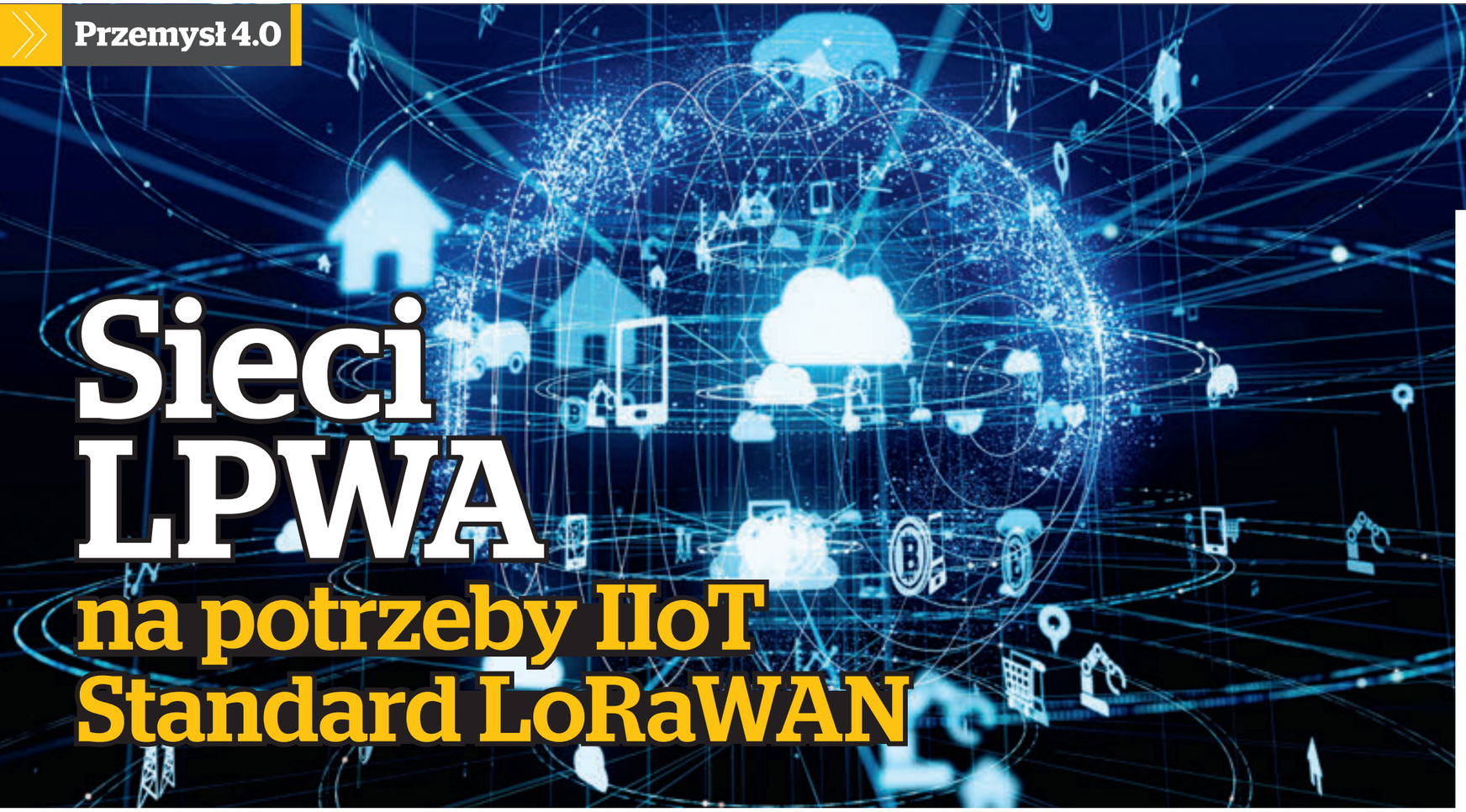
TROCHĘ O KONWERGENCJI OT-IT

Przez długi czas technologie operacyjne (OT – *Operational Technology*), czyli sterowania przemysłowego, oraz technologie informatyczne (IT) funkcjonowały w zakładach produkcyjnych oddzielnie. Wraz z pojawieniem się IIoT stała się możliwa konwergencja OT i IT oferująca użytkownikom wiele korzyści.

– *W OT chodzi przede wszystkim o zapewnianie ciągłości działania, z kolei w IT ważne są standardy, które gwarantują integralność i poufność danych. Obecnie od obu obszarów oczekuje się, by biznes stał się bardziej elastyczny, efektywny i przynosi więcej korzyści z poczynionych w nowe technologie inwestycji* – mówi Eric Ehlers, Vertical Marketing Manager w Cisco.

IT i OT były oddzielnymi silosami w różnych ekosystemach, skupionymi na różnych celach. Przepaść pomiędzy nimi powstrzymywała przedsiębiorstwa w ich dążeniach do osiągnięcia efektywności operacyjnej. Sytuacja zmienia się wraz z pojawieniem się w sektorze przemysłowym IIoT, *big data* i inteligentnych maszyn, a przedsiębiorcy dostrzegają korzyści z łączenia IT z OT. Dane wygenerowane przez systemy OT mogą być korelowane przez systemy IT, co umożliwia optymalizowanie procesów biznesowych, ograniczanie kosztów operacyjnych, pozyskiwanie informacji w celu doskonalenia procesu decyzyjnego, poprawa planowania produkcji i logistyki.

Podstawowym problemem przy konwergencji OT-IT pozostaje interoperacyjność pomiędzy różnymi formatami danych. Potrzebna jest wydajna, oparta na standardach komunikacyjnych struktura wykorzystywana jako znormalizowana szyna danych, w której liczne protokoły peryferii (często o firmowej, niestandardowej naturze) mogą być tłumaczone przez tzw. bramy. W ten sposób będzie możliwe skomunikowanie systemów, które nie były do tego stworzone, szybka ich integracja i osiągnięcie korzyści, jakie przynosi IIoT. Przykładami takich schematów są: DDS (*Data Distribution Service*) opracowany przez OMG oraz OPC UA przygotowany przez OPC Foundation.



Sieci LPWA na potrzeby IIoT Standard LoRaWAN

Dostępne na rynku kamery czy elementy kontroli dostępu działające w ramach IoT najczęściej łączą się między sobą za pomocą sieci Wi-Fi lub Bluetooth. Takie rozwiązanie sprawdza się na niewielkim obszarze (np. firma) oraz – ze względu na relatywnie duże zapotrzebowanie na prąd – tylko w przypadku urządzeń na stałe podłączonych do źródła zasilania. A co z sieciami IoT na dużych obszarach (fabryki czy miasta), z wieloma autonomicznymi czujnikami, do których doprowadzenie kabli jest trudne i kosztowne? Na potrzeby tych zastosowań (nazwanych *Industrial IoT,* IIoT) opracowano specjalny rodzaj sieci – LPWAN (*Low Power, Wide Area Network*)[1].

Jan T. Grusznic

Ogólna definicja branżowa IoT mówi o technologii łączenia wszystkiego ze wszystkim. Ponieważ wielokrotnie stanowiło to fundament różnych nieporozumień, przypomnę, że Internet Rzeczy (IoT) to zbiór połączonych bezprzewodowo obiektów – specjalizowanych układów scalonych, oprogramowania, czujników, urządzeń wykonawczych – i protokołów łączności bezprzewodowej, które umożliwiają gromadzenie i wymianę informacji z aplikacjami za pośrednictwem sieci bezprzewodowych podłączonych do Internetu. IoT zapewnia podłączonym obiektom zdalną komunikację i sterowanie z poziomu aplikacji za pomocą istniejącej infrastruktury internetowej i standardów komunikacji bezprzewodowej. Innymi słowy umożliwia bezpośrednią integrację i komunikację między światem realnym a jego cyfrowym opisem. Na podstawie prognoz Gartnera, wiodącej globalnej firmy badawczo-doradczej na świecie, przewiduje się, że IoT wygeneruje ogromne ilości informacji, które zostaną wykorzystane do optymalizacji zużycia wszelkiego rodzaju zasobów i poprawy wydajności coraz bardziej połączonych systemów. Internet Rzeczy będzie również wzmacniać istniejące lub tworzyć nowe usługi, zapewniając trwałą wartość dla użytkowników, konsumentów i całego środowiska.

Według prognoz Machina Research[2] liczba połączonych urządzeń w ramach Internetu Rzeczy do 2025 r. przekro-

[1] http://ccnews.pl/2018/04/11/rodzimy-operator-uczyni-polskie-miasta-bardziej-smart/

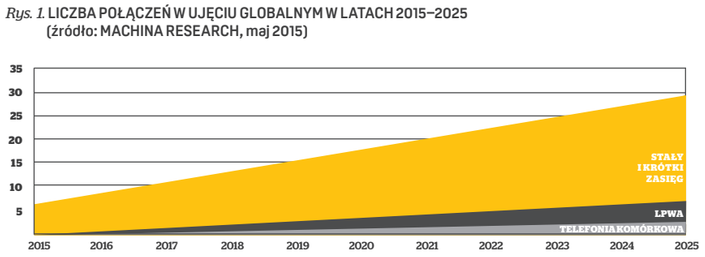
[2] *IoT Global Forecast & Analysis 2015-2025*, Machina Research, 2016

ROZLEGŁE SIECI O NISKIM POBORZE MOCY (LPWA) - SŁOWNICZEK -

ADR	**Adaptive Data Rate** Adaptacyjna szybkość transmisji danych
AS Serwer aplikacji	**Application Server** Informacje o routingu określające sposób kierowania danych z czujników do aplikacji połączonej z platformą rdzenia sieci
EUI ID	**Extended Unique Identifier** Unikalny 64-bitowy identyfikator przypisany zgodnie z wytycznymi IEEE EUI-64
ISM	**Industrial, Scientific and Medical** Nielicencjonowane spektrum częstotliwości dedykowane do zastosowań przemysłowych, naukowych i medycznych
LoRa	**Long Range** Technologia radiowa RF o dalekim zasięgu i niskiej energii opracowana przez firmę Semtech. LoRa® jest zarejestrowanym znakiem handlowym firmy Semtech Corporation
LPWA	**Low Power Wide Area** Rozległe sieci o niskim poborze mocy
LRC Kontroler dalekiego zasięgu	**Long Range Controller** Komponent rdzenia sieci LPWA implementujący warstwę MAC opartą na chmurze i działający jako funkcja mediacji między podłączonymi urządzeniami a serwerami aplikacji
LRR Odbiornik dalekiego zasięgu; Stacja bazowa	**Long Range Router** Sprzęt implementujący jedno lub więcej nadajników radiowych zgodnych ze specyfikacją warstwy MAC sieci LoRaWAN. LRR działa pod kontrolą LRC.
MAC	**Media Access Control** Kontrola dostępu do medium lub warstwa kontroli dostępu do nośnika (MAC) stanowi dolną podwarstwę warstwy łącza danych (warstwa 2) siedmiowarstwowego modelu OSI
MQTT	**Message Queue Telemetry Transport** Standard ISO (ISO / IEC PRF 20922) subskrypcji oparty na „lekkim" protokole przesyłania komunikatów przez protokół TCP/IP
NwkSKey	**Network Session Key** 128-bitowy klucz używany przez sieć LPWA do weryfikacji autentyczności i integralności każdej wiadomości przesyłanej przez system
Plan łączności	Plan łączności określa funkcje sieciowe (np. potwierdzone komunikaty, ruch w dół łącza), parametry polityki ruchu (regulatory tokena dla ruchu w górę i dół łącza) i powiązaną z nimi aktywację i opłatą cykliczną związana z danym urządzeniem
RSSI	**Receive Signal Strength Indication** – wskaźnik siły odbieranego sygnału
SNR	**Signal to Noise Ratio** – stosunek sygnał/szum
TDoA	**Time Difference on Arrival** (różnica w czasie przybycia) Technologia lokalizacji bezprzewodowej, opierająca się na wrażliwych odbiornikach, które zwykle znajdują się w stacjach bazowych, w celu ustalenia lokalizacji urządzenia
Urządzenie	Urządzenie zidentyfikowane przez unikatowy na świecie identyfikator IEEE EUI-64, który jest w stanie zainicjować ruch w górę łącza lub pobierać informacje z jednego lub więcej serwerów aplikacji za pośrednictwem infrastruktury sieciowej LPWA

czy 27 mld, z czego 11% połączeń będzie używało technologii LPWA. Na podstawie wykonanej analizy duża ich część będzie pochodzić z połączeń stacjonarnych i krótkiego zasięgu, takich jak Wi-Fi, Bluetooth, ZigBee, Z-Wave itp. Technologie te są dobrze dostosowane do zastosowań krótkiego zasięgu, w których zużycie energii i żywotność baterii nie stanowią poważnego problemu. Większe zasięgi są obecnie obsługiwane przez dostępne rozwiązania mobilnej transmisji danych.
Obecne generacje technologii komórkowych będą jednak musiały być uzupełnione o technologie LPWA, aby obsługiwać wiele nowych zastosowań IoT ze względu na wymagania dotyczące niskiego zużycia energii przez urządzenia wysyłające i odbierające stosunkowo niewielkie ilości danych.

Rys. 1. LICZBA POŁĄCZEŃ W UJĘCIU GLOBALNYM W LATACH 2015–2025 (źródło: MACHINA RESEARCH, maj 2015)



Rys. 2. SEGMENTACJA TECHNOLOGII KOMUNIKACYJNYCH DLA INTERNETU RZECZY

LPWA – technologia radiowa (RF) o dalekim zasięgu i niskiej mocy energetycznej

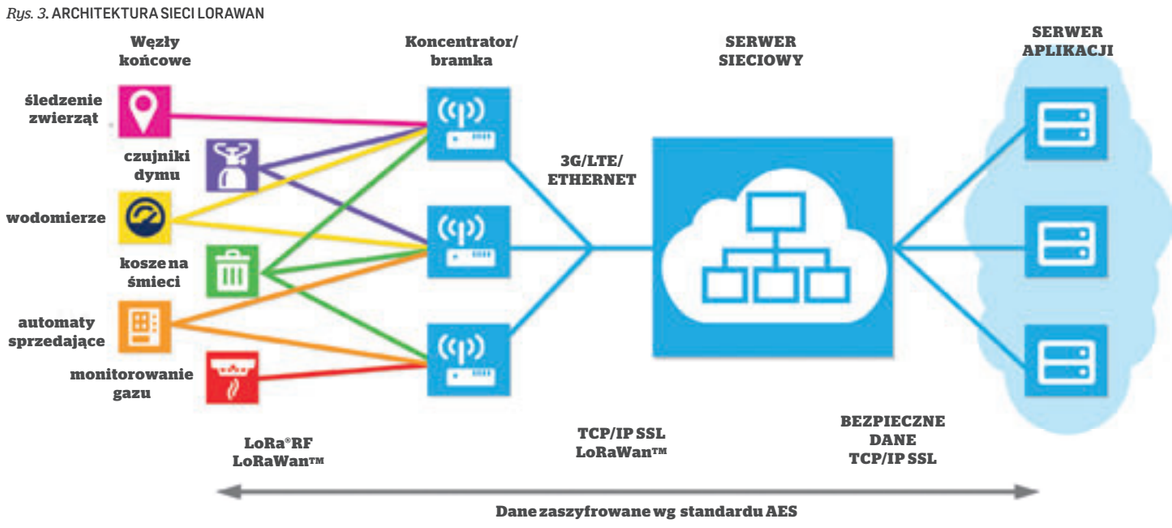
LPWA to rodzaj sieci połączonych ze sobą na dużych obszarach urządzeń, które charakteryzują się niskim zapotrzebowaniem na energię elektryczną. To nowa rodzina łączy bezprzewodowych IoT, doskonale wspierająca usługi wymagające pokonania dużych odległości (dziesiątki kilometrów), by dotrzeć do urządzeń pomiarowych lub wykonawczych, charakteryzujących się niskim poborem mocy i mogących pracować przez wiele lat na jednym komplecie baterii. Kompromisem takiego rozwiązania jest niska przepustowość łącza, od 300 b/s do 5 Kb/s (w kanale 125 kHz).
Kluczowe zastosowania sieci LPWA obejmują aplikacje dla inteligentnych miast, takie jak inteligentny parking, inteligentne oświetlenie ulic, zarządzanie łańcuchem dostaw (ze śledzeniem aktywów i monitorowaniem ich stanu), inteligentne sieci dystrybucji energii elektrycznej, pomiary wody i gazu, inteligentne rolnictwo (z monitorowaniem stanu terenu lub śledzenia zwierząt) oraz *geofencing*[3]. To tylko kilka przykładów istniejących aplikacji. Rosnąca świadomość na temat możliwości LPWA i pojawiające się informacje o nowych wdrożeniach kreują nowe potrzeby rynkowe. Tak jak w każdym rodzaju technologii, tak i w przypadku LPWA niezbędny jest wspólny standard gwarantujący kompatybilność. Najczęściej wykorzystywany jest obecnie o nazwie LoRa, dlatego też bardzo często mówi się o tworzeniu sieci IoT opartych na LoRaWAN.

LoRa? LoRaWAN?

LoRa to technologia komunikacji bezprzewodowej, podobnie jak bardziej popularne standardy typu Wi-Fi, Bluetooth, LTE i ZigBee. Żaden z nich nie jest w stanie samodzielnie spełnić potrzeb wszystkich użytkowników i w wielu przypadkach wybór konkretnego standardu wymaga kompromisu. LoRa wypełnia lukę pomiędzy nimi jako tania, energooszczędna metoda przesyłania danych na duże odległości, przeznaczona do urządzeń zasilanych bateryjnie lub energią odnawialną. Została opracowana w 2010 r. przez francuski start-up Cycleo na bazie techniki modulacji fal elektromagnetycznych określanej mianem CSS (*Chirp Spread Spectrum*), przez dekady stosowanej w aplikacjach wojskowych i astronautyce. Jej kluczową zaletą jest możliwość uzyskania dużego zasięgu transmisji i odporność na interferencje.

[3] *Geofencing* to termin, który na razie nie doczekał się polskiego odpowiednika. Próbując go przetłumaczyć, otrzymalibyśmy „geograficzną siatkę" – miejsce o ściśle wyznaczonych granicach. Obecnie termin *geofencing* jest używany dla wielu aplikacji. Rodzice lub szkoły mogą dzięki tej technologii być informowane o tym, że ich dziecko wyszło poza teren placówki edukacyjnej. Firmy świadczące usługi ochrony korzystają z tej technologii do zarządzania powierzonymi pojazdami. Auta wyposażone w odpowiednie urządzenie mogą zostać unieruchomione w przypadku kradzieży lub wyjazdu poza pewien obszar. Dzięki *geofencingowi* można także wyznaczać obszary, w których użytkownik lub urządzenie mobilne mają dostęp do wybranej sieci lokalnej czy zasobów znajdujących się na serwerze.

Rys. 3. ARCHITEKTURA SIECI LORAWAN



LoRaWAN natomiast to protokół MAC (*Medium Access Control* – protokół sterowania dostępem do łącza) dodany przez firmę Semtech, która w 2012 r. kupiła Cycleo, by ustandaryzować i rozszerzyć warstwę fizyczną komunikacji LoRa do Internetu. Protokół dostępu LoRaWAN opracowany przez Semtech pod kątem dużej wydajności, dalekiego zasięgu i małego poboru mocy dla urządzeń Internetu Rzeczy korzysta z zalet technologii LoRa oraz optymalizuje zużycie energii i obsługuje mechanizmy optymalizacji ruchu pomiędzy węzłami. Jest w pełni dwukierunkowy, co pozwala na niezawodny przesył informacji. Zawiera również kilka kluczowych funkcji sieci bezprzewodowej, takich jak szyfrowanie (kluczem 128-bitowym) i bezpieczeństwo E2E (*end-to-end*), adaptacyjną optymalizację szybkości przesyłania danych, jakość usług i inne zaawansowane aplikacje komunikacyjne. Ponadto definicja LoRaWAN obejmuje bezprzewodową rejestrację nowych urządzeń w sieci i nadawanie w trybie multicast (komunikacja jeden-do-wielu)[4].
LoRaWAN to standard otwarty. Korzysta z niewymagającego ponoszenia opłat licencyjnych pasma radiowego ISM (*Industrial, Scientific, Medical* – zastosowania przemysłowe, naukowe i medyczne). W Europie LoRaWAN działa na częstotliwości 868 MHz, a w USA na 915 MHz. Użycie nielicencjonowanego pasma sprawia, że każdy może łatwo utworzyć własną tego typu sieć. Wielu operatorów telekomunikacyjnych zainteresowało się LoRaWAN i zaczęło tworzyć infrastrukturę w tym standardzie, dostarczając usługi na niej oparte w różnych krajach na całym świecie. Holenderski KPN, francuski Orange, koreański SK Telecom, amerykański Comcast i wielu innych operatorów jest aktywnie zaangażowanych we wdrażanie takich rozwiązań w dużej skali. To sprawia, że LoRaWAN staje się coraz bardziej interesującą technologią, gdyż jest kompatybilna z sieciami zbudowanymi przez różnych operatorów, zarówno małych, jak i obejmujących bardzo duży obszar.

Standardem LoRaWAN opiekuje się LoRa Alliance, organizacja złożona z ponad 500 firm członkowskich – m.in. IBM, Microchip, ST, Cisco, Softbank i ARM – które wspierają protokół oraz opracowują zgodne z nim komponenty, produkty i usługi.

Architektura LoRaWAN

Architektura sieci LoRaWAN jest oparta na topologii gwiazdy, w której bramki (stacje bazowe) przekazują dane między urządzeniami końcowymi (węzłami) a centralnym serwerem sieciowym (*rys. 3*). Wszystkie bramki łączą się z serwerem sieci szkieletowej za pośrednictwem standardowych połączeń IP, natomiast urządzenia końcowe wykorzystują komunikację LoRa z pojedynczym skokiem do jednej lub wielu bramek (nie obsługują protokołu IP). Cała komunikacja jest natywnie dwukierunkowa, chociaż komunikacja w górę łącza – od urządzenia końcowego do serwera sieciowego – jest dominująca.
Topologia gwiazdy to najlepszy kompromis między komunikacją dalekiego zasięgu, liczbą anten (stacjami bazowymi) i żywotnością baterii urządzeń. Wymiana informacji między urządzeniami końcowymi a bramkami jest rozłożona na różne kanały częstotliwości i szybkości transmisji danych. Wybór optymalnej prędkości transmisji danych jest kompromisem między zasięgiem komunikacji a czasem potrzebnym na przesłanie wiadomości. Kluczową cechą LoRaWAN jest automatyczna optymalizacja prędkości, z jaką urządzenie przesyła dane. Funkcja ADR – adaptacyjna szybkość przesyłu danych (*Adaptive Data Rate*) jest kluczowa dla zwiększania sumarycznej przepustowości sieci LoRaWAN. ADR pozwala na łatwe skalowanie sieci, umożliwiając zwiększanie liczby bramek. Dzięki temu wiele urządzeń automatycznie zmienia swój współczynnik rozproszenia (SF), a zatem skraca czas potrzebny na przesłanie pakietu, w efekcie pozostawiając więcej wolnego pasma dla innych urządzeń.

[4] https://pl.farnell.com/podstawy-lorawan

ADR to prosty mechanizm, który prowadzi do zmiany prędkości transmisji, kierując się następującymi zasadami:
- jeśli moc sygnału radiowego (nazywanego budżetem łącza) jest duża, szybkość transmisji może być zwiększona,
- jeśli budżet łącza jest mały, szybkość transmisji może zostać obniżona.

W *tabeli 1* zilustrowano szybkość transmisji danych w funkcji zasięgu i współczynnika rozproszenia. Protokół LoRaWAN optymalizuje szybkość transmisji danych w celu zminimalizowania czasu antenowego (czasu transmisji) i zużycia energii przez urządzenia. W porównaniu ze stałą prędkością transmisji danych w technologii LPWA ta optymalizacja może stukrotnie zmniejszyć średnie zużycie energii przez podłączony obiekt.

LoRaWAN używa pasma nielicencjonowanego ISM przeznaczonego do zastosowań przemysłowych, naukowych i medycznych. W Europie dostęp do pasma ISM (do częstotliwości 868 MHz i 433 MHz) reguluje ETSI (Europejski Instytut Norm Telekomunikacyjnych). Ich wykorzystanie podlega ograniczeniom: moc wyjściowa (EIRP) nadajnika nie przekracza 14 dBm lub 25 mW, a cykl roboczy jest ograniczony do 1% (dla urządzeń) lub 10% (dla bramek) w zależności od użytego podpasma[5]. Urządzenia końcowe mogą nadawać w dowolnym dostępnym kanale, w dowolnym czasie, z każdą dostępną szybkością transmisji danych, o ile przestrzegane są poniższe zasady:
- urządzenie końcowe zmienia kanał w sposób pseudolosowy dla każdej transmisji. Wynikowa różnorodność częstotliwości sprawia, że system jest bardziej odporny na zakłócenia;
- w pasmie EU 868 ISM urządzenie końcowe musi przestrzegać maksymalnego cyklu pracy nadawania w stosunku do zastosowanego podpasma i przepisów lokalnych (1% w przypadku urządzeń końcowych).

Tab 1. **PROTOKÓŁ LORAWAN I WSPÓŁCZYNNIK ROZPROSZENIA ZESTAWIONY Z PRZEPUSTOWOŚCIĄ ŁĄCZA I CZASEM NADAWANIA (PRZY ZAŁOŻENIACH: WSPÓŁCZYNNIK KODOWANIA 4/5, PASMO 125 KHZ, WSPÓŁCZYNNIK BŁĘDÓW PAKIETÓW 1%)**

Współczynnik rozproszenia	Przepustowość	Zasięg (wartość orientacyjna, zależna od warunków propagacji)	Czas antenowy (transmisji węzłów) dla danych użytecznych (10 bajtów) – węzły wzbudzają się tylko na czas transmisji
SF7	5470 b/s	2 km	56 ms
SF8	3125 b/s	4 km	100 ms
SF9	1760 b/s	6 km	200 ms
SF10	980 b/s	8 km	370 ms
SF11	440 b/s	11 km	740 ms
SF12	290 b/s	14 km	1400 ms

Tab 2. **KLASY KOMUNIKACYJNE LORAWAN**

Nazwa klasy	Przeznaczenie
A (muszą ją spełnić wszystkie urządzenia)	**Czujniki zasilane bateryjnie lub urządzenia wykonawcze** niewrażliwe na opóźnienia. Najbardziej energooszczędna klasa komunikacyjna. Na jednej baterii urządzenia mogą pracować nawet 10 lat! Urządzenia klasy A pobierają najmniej energii w porównaniu z urządzeniami pozostałych klas, ponieważ mogą odbierać informacje (*downlink*) tylko po wysłaniu własnych danych (*uplink*). Nadają się do przesyłania danych z określonym interwałem, np. co 15 minut, lub do przesyłania informacji opartych na zdarzeniu, np. gdy mierzona temperatura przekroczy zadane 21°C lub spadnie poniżej 19°C
B (sygnalizacja zmian)	**Urządzenia wykonawcze zasilane bateryjnie** Energooszczędna klasa komunikacji dla urządzeń końcowych, których czas opóźnienia ruchu w dół sieci wymaga kontroli. Oparta na komunikacji podzielonej na części (tzw. sloty) synchronizowanej z sygnalizacją sieci. Węzły klasy B mogą otrzymywać więcej wiadomości niż urządzenia wykonawcze klasy A. To pozwala zmniejszyć opóźnienia przesyłanych wiadomości kosztem obniżenia efektywności energetycznej urządzenia
C (pracujące w otwartym kanale komunikacyjnym, ciągle nasłuchując)	**Urządzenia wykonawcze zasilane z sieci** Urządzenia, które mogą sobie pozwolić na ciągłe nasłuchiwanie. Brak opóźnień dla komunikacji w dół sieci. Urządzenia klasy C mogą ciągle odbierać wiadomości, z wyjątkiem momentów, gdy same wysyłają dane. Z tego powodu to najmniej energooszczędna klasa i zazwyczaj wymaga zastosowania stałego źródła zasilania do pracy

Klasy profili komunikacyjnych

W sieciach LoRa są dostępne trzy różne klasy (A, B, C) profili komunikacyjnych. Każda klasa spełnia różne potrzeby aplikacji i ma zoptymalizowane wymagania do określonych celów. Podstawową różnicą między profilami A, B i C jest kompromis między czasem oczekiwania a zużyciem energii.
Technologia LoRaWAN została zaprojektowana do tych zastosowań, kiedy czujnik przesyła niewielkie ilości danych kilka razy dziennie, a przez większość czasu pozostaje nieaktywny. Jest dobrze przystosowana do inteligentnych liczników, urządzeń śledzących, czujników itp. Nie jest przeznaczona do obsługi aplikacji wymagających dużych szybkości transmisji danych, takich jak audio lub wideo. Protokół LoRaWAN można jednak wykorzystać do sterowania innymi funkcjami urządzeń bezprzewodowych – np. zadać parametr kamerze, aby rozpoczęła pracę wbudowanych grzałek i wentylatorów, i pozostawała w trybie niskiego poboru mocy, gdy parametry środowiskowe tego nie wymagają.

Społeczność LoRa i rozwiązania biznesowe

Wszystkie wiadomości z urządzeń końcowych przesyłane przez bramki są przekazywane do serwera sieciowego. To w nim zachodzą bardziej skomplikowane procesy, związane z przetwarzaniem danych. Jest on odpowiedzialny przede wszystkim za:
– przekierowywanie i przekazywanie danych do odpowiednich aplikacji;
– określanie, która z bramek jest najlepsza do skierowania wiadomości przesyłanej do wybranego węzła. Zazwyczaj operacja ta bazuje na porównaniu parametru jakości łącza, który jest obliczany na podstawie współczynników RSSI (*Receive Signal Strength Indication;*
– wskaźnik siły odbieranego sygnału oraz SNR (*Signal to Noise Ratio* – stosunek sygnał/szum) poprzednio otrzymanych pakietów, usuwanie zduplikowanych wiadomości, jeśli zdarzyło się, że dane z węzła zostały przekazane do serwera przez więcej niż jedną bramkę, deszyfrowanie wiadomości przesyłanych z węzłów końcowych i szyfrowanie informacji przesyłanych do węzłów.

Bramki zazwyczaj łączą się z serwerem sieciowym za pomocą szyfrowanego połączenia IP. Sieć zawiera interfejs do nadzorowania pracy i instalacji nowych bramek, pozwalając kontrolerowi sieci na zarządzanie nimi, rozwiązywanie problemów, wykrywanie usterek, monitorowanie pojawiających się alarmów itp.
Sieci LoRaWAN działają już w wielu miejscach na świecie. We Francji firma Orange tworzy w 17 największych miastach publiczną sieć opartą na tym protokole, która będzie się składać ze 1200 bramek LoRa, firma Leroy Merlin natomiast ogłosiła, że będzie korzystać z technologii LoRa w swoich produktach automatyki domowej w celu poprawy ich funkcjonalności.
Innym przykładem zastosowania technologii LoRa jest produkt firmy Enevo – niezwykle skuteczny system usprawnienia gospodarki odpadami, monitorujący ilości śmieci w koszach i wykorzystujący te informacje do optymalizacji trasy przejazdu śmieciarki i planu odbioru odpadów.

W Polsce także działają sieci oparte na tym standardzie. We Wrocławiu utworzyła ją firma Espotel, należąca do LoRa Alliance. Antena wraz z odpowiednim urządzeniem firmy Multitech, pełniącym rolę koordynatora sieci i bramki internetowej, została umieszczona na jednym z budynków Wrocławskiego Parku Technologicznego, w którym Espotel ma swoje biura. Dane transmitowane z urządzeń zalogowanych do sieci trafiają do chmury, gdzie mogą być dowolnie przechowywane, przetwarzane bądź przekierowywane na odpowiednie serwery. Sieć jest w fazie testów, udało się przeprowadzić transmisję na dystansie 4–5 km.
W Gdyni również działa podobna sieć zarządzana przez firmy MpicoSys i WiRan z Pomorskiego Parku Naukowo-Technologicznego. Pokrywa ona obszar 30 km^2 w terenie zabudowanym oraz 450 km^2 w terenie otwartym. Planowane jest powiększenie zasięgu na całe Trójmiasto.
Interesującym pomysłem jest też inicjatywa *The Things Network*, która pojawiła się w Amsterdamie. W krótkim czasie kilka firm stworzyło tam wspólnie sieć LoRa, którą stale rozbudowują – początkowo było 10 bramek, w grudniu 2016 r. natomiast działało już 26. Dzięki zbiórce pieniędzy w Internecie do akcji przyłączyli się mieszkańcy 170 miast i regionów z 60 krajów, które u siebie rozpoczęły budowę sieci LoRa. W Polsce, oprócz Wrocławia i Gdyni, są to Poznań i Warszawa.

Podsumowanie

Wielu dostawców rozwiązań z zakresu systemów zabezpieczeń technicznych upatruje w technologii LPWA możliwości świadczenia nowych usług. Na rynku dostępnych jest kilka protokołów LPWA, z których dwa przyczyniają się do szybkiego rozwoju rynków technologii LPWA IoT – są to LoRaWAN i Ultra-Narrowband (UNB), ze wskazaniem protokołu LoRaWAN jako przyszłościowego. Ma on kilka zalet w porównaniu z innymi technologiami LPWA:
- szybkość przesyłania danych wynosi od 300 b/s i aż do 5 Kb/s (przy przepustowości 125 kHz) i 11 Kb/s (z przepustowością 250 kHz), co pozwala na lepszy czas antenowy i wydłuża czas pracy baterii;
- komunikacja jest natywnie dwukierunkowa i nieograniczona (w aspekcie lokalnych przepisów dotyczących pasma ISM);
- natywne szyfrowanie komunikacji;
- lokalizacja bez GPS z TDoA;
- bogata oferta bramek: bramki makro, bramki wewnętrzne, bramki pico do użytku domowego;
- możliwość tworzenia sieci publicznych i/lub prywatnych;
- ADR (*Adaptive Data Rate*) ułatwia tworzenie sieci skalowalnej, ponieważ dodanie stacji bazowej obniża średnią ADR i czas antenowy, a to pozwala na komunikację większej liczby węzłów końcowych.

Protokół LoRa w sensie technologicznym nie jest niczym odkrywczym, ale dzięki swoim zaletom oraz prężnie działającym popularyzatorom ma szansę stać jednym z najlepszych rozwiązań komunikacyjnych do realizacji niskoprzepustowej transmisji danych dla aplikacji Internetu Rzeczy[6].

BIO

Jan T. Grusznic
z-ca red. naczelnego „a&s Polska". Z branżą wizyjnych systemów zabezpieczeń związany od 2004 r. Ma bogate doświadczenie w zakresie projektowania i wdrażania rozwiązań dozoru wizyjnego w aplikacjach o rozproszonej strukturze i skomplikowanej dystrybucji sygnałów. Ceniony diagnosta zintegrowanych systemów wspomagających bezpieczeństwo.

[5] Gdy jedno urządzenie transmituje w jednym kanale w okresie 2 jednostek co 10 jednostek czasu, to urządzenie ma cykl roboczy wynoszący 20%. Jeśli weźmiemy pod uwagę więcej niż 1 kanał, sprawa się nieco komplikuje. Kiedy mamy urządzenie, które transmituje na 3 kanałach zamiast na jednym, każdy kanał jest nadal zajęty przez 2 jednostki co 10 jednostek czasu (czyli 20%). Jednak urządzenie przesyła 6 jednostek czasu co 10 jednostek czasu, co daje 60% czasu pracy.

[6] www.magazynprzemyslowy.pl/produkcja/LoRa-energooszczedna-dlugodystansowa-siec-w-natarciu

Duże obiekty przemysłowe

Systemy zarządzania bezpieczeństwem

Zapewnienie ochrony osób i mienia w dużych obiektach przemysłowych jest zadaniem trudnym i złożonym. Mają na to wpływ czynniki związane nie tylko z lokalizacją obiektów, ich rozległością, specyfiką zabudowy, rodzajem wytwarzanego produktu, ale także ze spełnieniem wymagań formalnoprawnych oraz postępem cywilizacyjnym.

Andrzej Kozłowski
PGNiG TERMIKA SA

Stosowane dotychczas standardowo zabezpieczenia, wewnętrzne procedury postępowania oraz profesjonalna ochrona fizyczna obiektów bez odpowiedniego wsparcia technicznego mogą być już niewystarczające dla zapewnienia bezpieczeństwa na oczekiwanym poziomie. Dzieje się tak, ponieważ wraz z postępem cywilizacyjnym rosną również nasze wymagania dotyczące spełnienia potrzeb związanych z poczuciem wewnętrznego spokoju, pewności, stabilności, niezależności, a także poziomu i jakości życia oraz zapewnienia swobód i praw wolności obywatelskich. Ogólnie mówiąc, chcemy czuć się coraz bezpieczniej i swobodniej. Dlatego wchodząc do chronionego obiektu, trudno nam się pogodzić z sytuacją, gdy zostajemy poddani procedurze identyfikacji, a nasze poczynania są rejestrowane przez system monitoringu wizyjnego czy kontroli dostępu. Od wejścia 25 maja br. unijnego rozporządzenia o ochronie danych (RODO) coraz więcej osób nieznających zapisów tego dokumentu uważa, że są naruszane ich podstawowe prawa wolności.

Nie należy się temu dziwić, ponieważ na sposób odczuwania i postrzegania niekorzystnych dla nas zjawisk olbrzymi wpływ ma sfera naszego umysłu, która jest odzwierciedleniem świadomości na dany temat. Stąd pojawia się konieczność uświadamiania, że są to prawnie usprawiedliwione działania, mające na celu zapewnienie bezpieczeństwa w danym obiekcie.

Oczywiście należy również poinformować o przysługujących prawach i konsekwencjach wynikających z niepodporządkowania się do obowiązujących w obiekcie procedur.

Ważnym elementem jest więc edukacja, aby wszyscy pracownicy i kontrahenci rozumieli istotę podejmowanych przez przedsiębiorstwa działań związanych z zapewnieniem bezpieczeństwa.

Przedsiębiorcy zaczynają dostrzegać, że samo uświadamianie to za mało. Oprócz nakładów finansowych na wdrażanie nowych technologii produkcyjnych niezbędne są też inwestycje w nowoczesne systemy zarządzania bezpieczeństwem dopasowane do potencjalnych zagrożeń i rodzajów ryzyka. Rozumieją też, że postępu technicznego nie da się zahamować, a nowoczesne dzisiaj rozwiązania za kilka lat mogą stać się bezużyteczne. Stąd konieczność właściwego dopasowania funkcjonalności systemów do potrzeb przedsiębiorstw stała się jednym z wyzwań dla osób odpowiedzialnych za bezpieczeństwo.

Trudność polega na tym, że rynek systemów zabezpieczeń oferuje szereg rozwiązań technicznych z ogromną liczbą funkcjonalności, które mają zapewne wpływ na podnoszenie poziomu bezpieczeństwa w obiektach, ale w przypadku konkretnego przedsiębiorstwa niekoniecznie znajdą zastosowanie.

> Rynek zabezpieczeń oferuje rozwiązania techniczne o ogromnej liczbie funkcjonalności, które generalnie mają wpływ na podniesienie poziomu bezpieczeństwa w obiektach, ale w przypadku konkretnego przedsiębiorstwa nie wszystkie znajdą zastosowanie.

Czym zatem kierować się przy wyborze systemu? Na pewno nie należy sugerować się ceną produktu ani mnogością oferowanych funkcji.

Proponowałbym rozważyć możliwość wyboru systemu opartego na otwartej platformie zarządzania bezpieczeństwem klasy PSIM *(Physical Security Information Management)* na podstawie wcześniej przygotowanej analizy potrzeb przedsiębiorstwa. Zadaniem platformy jest zarządzanie na wspólnym interfejsie informacjami pochodzącymi z różnych systemów zabezpieczeń.

Istotną zaletą tego rozwiązania jest możliwość interakcji pomiędzy urządzeniami i systemami różnych producentów. Zaletą jest również to, że PSIM prowadzi człowieka „krok po kroku" (automatycznie) przez zdarzenia na podstawie opracowanych wcześniej procedur postępowania (logicznie uporządkowane czynności sposobu reagowania). Ma to niebagatelny wpływ na poprawę efektywności pracy operatora systemu, ogranicza możliwość popełnienia przez niego błędu w procedurze oraz poprawia szybkość jego reakcji.

Przed podjęciem decyzji o zakupie warto jednak zapoznać się z działaniem takiego systemu w warunkach obiektowych. Mówiąc wprost, należy zwrócić się do oferentów z prośbą o umożliwienie przeprowadzenia wizji lokalnych w obiektach, w których już wdrożono podobne projekty.

To bardzo ważny etap postępowania, który umożliwia przyszłemu inwestorowi zapoznanie się z działaniem systemów w warunkach rzeczywistych i opiniami bezpośrednich użytkowników. Takie podejście zwiększa prawdopodobieństwo, że oferowany produkt został już przetestowany, a przedsiębiorstwo nie stanie się poligonem doświadczalnym.

Kiedy kierownictwo przedsiębiorstwa podejmie ostateczną decyzję o zakupie i wdrożeniu systemu zarządzania bezpieczeństwem, pojawia się kolejne wyzwanie. Tym razem jest ono związane z przygotowaniem precyzyjnych wymagań technicznych dotyczących przyszłego systemu. Na tym etapie należy precyzyjnie określić m.in. wymagania w zakresie zapewnienia międzynarodowych standardów technicznych oraz spełnienia norm państwowych i branżowych, a także wymagania sprzętowe i funkcjonalne oraz wszelkie możliwe zależności pomiędzy poszczególnymi elementami.

Spełnienie przez wykonawcę opisanych wymagań stanowi dla inwestora pewnego rodzaju zabezpieczenie, że otrzyma on oczekiwany produkt (skrojony na miarę). Ma również zabezpieczyć właściwą jakość wykonania systemu, jego poszczególnych elementów oraz ich integrację. Wdrożenie systemu zarządzania bezpieczeństwem wymaga od przedsiębiorstw również poniesienia niemałych nakładów finansowych, które niekoniecznie znajdą swoje odzwierciedlenie w redukcji kosztów zarządzania bezpieczeństwem. Najczęściej są one technicznym narzędziem wspierającym procesy organizacyjne związane z zapewnieniem bezpieczeństwa w obiektach, którego podstawowym celem jest ułatwienie pracy służbie ochrony, a nie ograniczenie stanu etatowego.

Oczywiście szybka identyfikacja przez system sytuacji czy zdarzenia alarmowego pozwala na podjęcie niemal natychmiast reakcji zapobiegającej powstaniu zagrożenia, ale nie byłaby ona możliwa bez udziału człowieka.

Należy pamiętać, że tylko dzięki zapewnieniu synergii działań wszystkich pracowników związanych z dążeniem przedsiębiorstwa do poprawy stanu bezpieczeństwa możliwe jest osiągnięcie oczekiwanego celu.

BIO

Andrzej Kozłowski Specjalista ds. bezpieczeństwa w Biurze Bezpieczeństwa PGNiG TERMIKA SA. Ekspert od zarządzania kryzysowego i organizacji ochrony w obiektach energetycznych. Autor książki „Zarządzanie bezpieczeństwem w obiektach energetycznych" i publikacji o zagrożeniach bezpieczeństwa energetycznego.

Bezpieczeństwo przemysłowe

paradygmat tradycyjny kontra nowoczesny

Koncesjonowane firmy ochrony, zabezpieczając obiekty przemysłowe, z założenia chronią osoby i mienie. Tak stanowi prawo, w szczególności Ustawa o ochronie osób i mienia. **Praktyka jest jednak inna, gdyż chroniąc obiekty przemysłowe, firmy stawiają czoła licznym zagrożeniom odległym od wspomnianego celu, choć oczywiście „osoby i mienie” także są tu obecne.**

Jacek Grzechowiak

Zasadniczą potrzebą operacyjną obiektów przemysłowych jest produkcja. Jest ona jednak cechą zakładu, a nie jego potrzebą. Potrzebą jest ciągłość działania produkcji, rozumiana jako zapewnienie nieprzerwanego i niezakłóconego funkcjonowania podstawowych funkcji biznesowych. W tym obszarze swoje zadania wykonują firmy ochrony.

Zarządzanie ciągłością działania, popularnie zwane BCM od pochodzącego z języka angielskiego odpowiednika tego określenia, jest procesem skomplikowanym i dotyczącym całej organizacji, a co ważniejsze realizowanym nie w czasie kryzysu, ale w codziennej działalności właśnie po to, aby nie doprowadzić do kryzysu. Przyjrzyjmy się temu przez pryzmat kilku nietypowych incydentów.

Jak ochronić przed kradzieżą towar, którego nigdy nie było w magazynie?

Pytanie sugeruje typowo teoretyczny przykład akademicki, ale zdarzenie rzeczywiście miało miejsce. Dotyczyło produkcji tkaniny o nazwie flizelina. Ochrona obiektu jest skupiona na kontroli pojazdów wyjeżdżających z gotowymi wyrobami. Proces ten jest także bardzo skrupulatnie realizowany i dokumentowany, z zachowaniem weryfikacji dokumentów, wielopoziomowego zatwierdzania oraz okresowej weryfikacji załadunków, poprzez rozładunki kontrolne. Flizelina, jak każda tkanina, może mieć różną grubość, a więc w rolce może być różna długość tkaniny. Z tego punktu widzenia proces kontroli wydaje się efektywny… do czasu, gdy inwentaryzacja roczna wykazała braki magazynowe.

Analiza procesu wskazała, że wszystko jest w porządku – dane magazynowe i dane dystrybucji są spójne, wszystko to, co znajdowało się na stanie magazynu, albo wyjechało, albo jest na miejscu. Skąd więc braki? I tu właśnie z pomocą przyszła ochrona, która zastosowała te same zasady, co przyjęte do komponentów produkcyjnych. Porównanie danych ochrony przyniosło nieoczekiwane odkrycie – ilość surowca przyjętego przez zakład była niższa, niż wynikało z dokumentacji logistycznej. Wniosek był oczywisty: część

> Zarządzanie ciągłością działania jest procesem skomplikowanym i dotyczącym całej organizacji, realizowanym nie w czasie kryzysu, ale w codziennej działalności właśnie po to, aby do kryzysu nie doprowadzić.

surowca wjechała wyłącznie „na papierze”. To było właśnie to mienie, którego nigdy nie było w magazynie.

Pojawia się drugi, dość oczywisty wniosek, że oba kanały przepływu mienia – tzn. surowiec i wyroby gotowe – powinny być nadzorowane przez jeden ośrodek zarządzający i kontrolny, a ochrona nie powinna zaczynać się na ogrodzeniu, ale znacznie wcześniej, już na etapie zamawiania surowca i jego dostawy do zakładu.

Co to ma wspólnego z ciągłością działania? Apetyt rośnie w miarę jedzenia – tak było i w tym przypadku. Na początku kradzieże surowca były niewielkie, dokonywane sporadycznie, jakby w celu przetestowania szczelności systemu, ale z czasem zbyt był już spory i co najważniejsze, regularny. Analiza tego trendu wykazała, że po upływie 3-4 miesięcy mogłyby wystąpić okresowe braki surowca, a tym samym zaburzenie ciągłości produkcji.

Sabotaż - zagrożenie z przeszłości czy współczesne?

Wyobraźmy sobie zakład produkujący elementy szklane, np. półki do lodówek. Taki produkt jest bardzo delikatny, łatwy do zniszczenia, łatwo tłukący się. Zakład produkujący te wyroby jest do tego przystosowany. Problem wydarzył się gdzie indziej… Firma ma dużego odbiorcę, dobrego, ale wymagającego. Odbiorca sprawdza każdą dostawę, szczegółowo kontrolując próbę badawczą, np. wybraną paletę. W przypadku stwierdzenia wad jakościowych odsyła całą dostawę, a firma w trybie awaryjnym produkuje kolejną dostawę. W zakładzie zaczęły pojawiać się problemy jakościowe, z czasem na tyle poważne, że został zagrożony kontrakt nie tylko z kluczowym klientem, ale także innymi, gdyż awaryjna produkcja dla klienta kluczowego dezorganizuje pozostałą pracę.

Analiza produkcji i kontroli jakości nie rozwiązała problemu. Z pomocą pospieszyli pracownicy ochrony, którzy przeanalizowali sprawę z punktu widzenia bezpieczeństwa, ujawniając przesłanki do rozważenia sabotażu. Na podstawie tego ryzyka wyciągnięto następujący wniosek: ochrona powinna uczestniczyć w planowaniu produkcji i włączać się w monitorowanie projektów o szczególnym znaczeniu dla firmy lub narażonych na nietypowe ryzyko, np. sabotaż. Zespół ochronny powinien uczestniczyć w spotkaniach cyklicznych osób zarządzających, by już na wczesnym etapie poznać problem. Czujność ochrony powinna być skierowana także na ryzyko jakościowe.

Zagrożenia non security

RUCH DROGOWY WEWNĄTRZ ZAKŁADU

Zakłady produkcyjne, zwłaszcza rozległe, są narażone na wiele rodzajów ryzyka związanych z naruszaniem przepisów ruchu drogowego. Jednym z powszechniejszych jest nadmierna prędkość. Nie tyle wielkość przekroczenia prędkości, ile potencjalne skutki dla ciągłości działania. Istotnym elementem tego typu incydentów jest masa przewożonego ładunku – im większa, tym problem potencjalnie także większy. W takich przypadkach przepis na problem przypomina sumę małych liczb:

PROBLEM = POŚPIECH + NIEUWAGA + LEKCEWAŻENIE PROCEDUR

Przy czym lekceważenie procedur nie dotyczy tylko zbyt szybkiej jazdy, ale np. przekładania poprawnego zabezpieczenia ładunku na czas postoju w miejscu wyczekiwania przed zważeniem na tzw. pauzę itd. Tego typu postępowanie zazwyczaj kończy się przesunięciem ładunku na skrzyni ładunkowej. Mniejszy problem, jeśli nie nastąpi uszkodzenie pojazdu, a w zakładzie można pojazd przeładować. Zdarzają się jednak przypadki uszkodzenia kabiny kierowcy i związane z tym uszkodzenie układu hamulcowego powodujące zablokowanie pojazdu. Zadaniem służb ochrony jest wówczas szybkie zorganizowanie objazdu i kierowanie ruchem w celu niedopuszczenia do zablokowania zakładu. Działanie to ma bezpośredni wpływ na

ciągłość procesów dystrybucji zarówno wyrobów gotowych, jak i surowców.
W zarządzaniu ciągłością działania najważniejsza jest profilaktyka. Pracownicy ochrony mają tu swoją rolę do odegrania w postaci całego dużego kompleksu kształtowania świadomości, poczynając od przypominania kierowcom zasad poruszana się po zakładzie, kończąc na prewencyjnym stosowaniu urządzeń do kontroli prędkości.

http://tir.arbiter.pl

BLACK BOX, CZYLI TO, CZEGO OCHRONA NIE WIDZI

W wielu zakładach produkcyjnych zespoły ochronne nie są wtajemniczane w procesy logistyczne, a tym bardziej informatyczne. Bez wątpienia ma to wpływ na ciągłość działania i wyniki finansowe zakładu. Brak znajomości procesów logistycznych powoduje, że ochrona działa „w ciemno", tym samym jej skuteczność może być mniejsza. Przykładem jest procedura postępowania w przypadku awarii systemu IT zarządzającego logistyką. Wdraża się wtedy rozwiązania zastępcze; ochrona powinna wiedzieć, iż wystąpiła szczególna sytuacja, a odpowiednie procedury powinny być przygotowane i sprawdzone. Znane są przypadki, gdy podczas awarii takich systemów dokumenty magazynowe są sporządzane w edytorze tekstu czy arkuszu kalkulacyjnym, co może spowodować zarówno omyłki, jak i celowe podwójne przygotowanie dokumentów wywozowych, sporządzenie ich bez numeracji czy z numeracją podwójną.
Utrudnia to, a niekiedy wręcz uniemożliwia efektywne zarządzanie procesem czy wyjaśnianie ewentualnych incydentów. Może dojść do kradzieży i braku wyrobów gotowych dla jednego lub kilku klientów, czyli typowego zaburzenia ciągłości działania w obszarze dystrybucji wyrobów gotowych. Wspierająca i kontrolna rola pracowników ochrony jest podstawą uniknięcia tego ryzyka. Jak wszędzie niezbędne są jasne procedury, wykwalifikowani i czujni pracownicy oraz testowanie systemu.

WYSOKOWARTOŚCIOWE MIENIE NISKOCENNE

Sprzeczność w tytule jest tylko pozorna. Wyobraźmy sobie duży młyn, np. do mielenia kamienia. W takich młynach często stosuje się kule żeliwne, które wprawdzie nie są drogie, ale często padają łupem złodziei. Ze względu na ich niską cenę nierzadko nie podlegają żadnej ochronie, z reguły do czasu aż ich zabraknie, a tym samym zostanie zatrzymana praca młyna i w konsekwencji wstrzymana produkcja. To klasyczny przykład zaburzenia ciągłości działania w obszarze produkcyjnym. Duże znaczenie ma w tym przypadku wiedza zespołu ochronnego na temat mienia krytycznego i miejsc jego przechowywania, jak również procedur związanych z dystrybucją. Może to też dotyczyć np. elektrod zgrzewarek, opakowań aluminiowych czy elementów automatyki przemysłowej starszej generacji, mających znikomą wartość rynkową, lecz krytyczną dla ciągłości działania zakładu. Przykłady można by mnożyć. Jak widać, bezpieczeństwo przemysłowe niekoniecznie musi dotyczyć bezpośrednio osób i mienia, a mimo to istotnie wpływać na ciągłość produkcji.
Tak pojmowana ochrona wymaga ścisłego współdziałania struktur wewnętrznych zakładu produkcyjnego z zespołem ochronnym. Współdziałania precyzyjnie zorganizowanego i obejmującego również procesy IT. Wymaga jasno zdefiniowanej struktury zespołu ochronnego oraz kompetencji potrzebnych na poszczególnych stanowiskach. To obszar, który obecnie jest eksploatowany przez działy badawczo-rozwojowe firm ochrony. W Polsce nie jest to jeszcze widoczne, ale ten trend już się na świecie ugruntował.
Zakłady produkcyjne to także miejsca, w których mienie istotne, niekiedy wręcz krytycznie ważne dla ciągłości działania, wcale nie musi mieć dużej wartości materialnej. Liczy się znaczenie dla zakładu, a wiedza o tym jest zespołowi ochrony niezbędna. Tym samym powinien on współpracować np. z działem utrzymania ruchu, jednak podobnie jak w przypadku działów IT, współpraca ta nie jest jeszcze zbyt widoczna.
Dla ochrony nie ma nieważnego działu w chronionym obiekcie, a to wymaga bliskiej współpracy z każdym działem. Gdy w zakładzie jest osoba zarządzająca bezpieczeństwem, współpraca ta jest z reguły naturalna. Tam, gdzie takiej osoby nie ma, wiele zależy od kreatywności firmy ochrony. Oba modele współpracy są w praktyce spotykane, oba mogą być efektywne. Niezależnie od wybranego modelu niezbędne jest rozważenie wszelkich rodzajów ryzyka, łącznie z tymi z pozoru nieadekwatnymi do profilu i charakteru chronionego obiektu.
Patrząc na przykłady innych branż, a także branży ochrony, funkcje zarządzające ochroną będą coraz częściej kupowane od firm specjalistycznych. W każdym przypadku niezbędne będzie zastosowanie odpowiednich procedur, uwzględniających mienie i zasoby niematerialne o znaczeniu krytycznym oraz odpowiednie wsparcie systemami zabezpieczeń technicznych.

Przykładów przedstawionych w artykule nie należy wiązać ani z obecnym, ani z poprzednimi miejscami pracy autora.

BIO

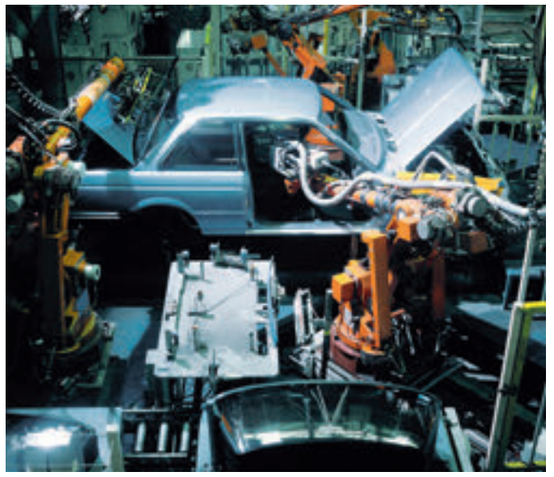
Jacek Grzechowiak
Menedżer ryzyka i bezpieczeństwa. Przez kilkanaście lat związany z grupą Securitas, obecnie w grupie Celsa. Absolwent WAT, studiów podyplomowych w SGH i Akademii L. Koźmińskiego. Gościnnie wykłada na uczelniach wyższych.

Zabezpiecz firmę według potrzeb

Cenne surowce i towary znajdujące się w fabrykach, magazynach i zakładach przetwórstwa należy monitorować i chronić przez całą dobę.

Połączenie technologii kamer IP i detektorów ruchu z technologią radarową pozwala zaprojektować rozwiązanie dozorowe na miarę potrzeb, zapewniające:
- dokładną, niezawodną detekcję i śledzenie na wybranym obszarze z identyfikacją wzrokową,
- automatyczne powiadomienia w czasie rzeczywistym o wtargnięciu na obszar lub do stref zastrzeżonych z potwierdzeniem wzrokowym i lokalizacją obiektu,
- elastyczne i łatwe w zastosowaniu rozwiązanie obejmujące solidne, wytrzymałe na wandalizm kamery i detektory ruchu do montażu na zewnątrz pomieszczeń.

Ochrona obiektów przemysłowych wiąże się z pokryciem rozległych obszarów oraz patrolowaniem i zabezpieczaniem długich ogrodzeń. Istotne jest wykrywanie, lokalizacja i identyfikacja intruzów zarówno przy bramach, wzdłuż ogrodzeń, jak i na trasach prowadzących do obiektów przemysłowych. Kamery muszą objąć zasięgiem ogromne przestrzenie w celu wykrycia obiektu, zlokalizowania go i zweryfikowania, czy jest nim zwierzę, osoba uprawniona, czy intruz. Rozwiązania do ochrony obwodowej firmy Axis opierają się na kamerach termowizyjnych z wbudowanym oprogramowaniem do analizy obrazu.



Sprawdzają się w ciemności, automatycznie wysyłając alarm, gdy ktoś wejdzie na określony obszar. Przykładem może być seria kamer AXIS Q19, które na monitorowanym obszarze wykrywają ludzi i przedmioty o temperaturze wyższej od otoczenia. Można je łatwo zintegrować z innymi kamerami IP, reflektorami, głośnikami, radarem i zainstalowanymi systemami zabezpieczeń, zapewniając optymalne działanie systemu. Kamery wizyjne są niezbędnym uzupełnieniem kamer termowizyjnych. Szybkoobrotowe kamery PTZ Axis, które zapewniają szeroki widok monitorowanego obszaru i możliwość zbliżenia każdego detalu, podnoszą bezpieczeństwo chronionego mienia. Patrolowanie z wykorzystaniem sterowania PTZ może być obsługiwane przez operatora lub odbywać się automatycznie (kamera samoistnie śledzi poruszające się osoby bądź podąża wyznaczoną trasą dozorową, przyjmując automatycznie ustawione prepozycje). Przykładem może być kopułkowa kamera sieciowa AXIS Q6155-E PTZ z zaawansowaną technologią laserową. To idealna propozycja do zastosowań wymagających natychmiastowego ustawiania ostrości przy obserwacji poruszających się obiektów i szybko zmieniających się scen.
Ciekawym rozwiązaniem jest seria stałopozycyjnych kamer sieciowych AXIS Q16 do montażu wewnątrz i na zewnątrz pomieszczeń, które zapewniają doskonałą jakość obrazu w trudnych warunkach, np. przy słabym lub zmiennym oświetleniu.

Sieciowy detektor radarowy AXIS D2050-VE doskonale nadaje się do monitorowania niewielkich obszarów zewnętrznych. Wraz z kamerami sieciowymi Axis i głośnikami tubowymi Axis lub innymi urządzeniami sieciowymi stanowi uzupełnienie systemów dozoru wizyjnego. Wykorzystuje zaawansowaną technologię radarową i inteligentne algorytmy wykrywania osób, które weszły na teren posesji, przełamując pierwszą linię zabezpieczeń. Jest precyzyjny i pozwala zminimalizować liczbę fałszywych alarmów w każdych warunkach atmosferycznych i o dowolnej porze.
Kamery sieciowe nie tylko pomagają zachować bezpieczeństwo obiektu, ale są także cennym narzędziem pozwalającym zwiększyć wydajność i bezpieczeństwo środowiska pracy. Zintegrowanie systemu kamer z systemem produkcji zapewnia dostęp do obrazów na żywo z dowolnego miejsca w sieci, umożliwiając:
– zdalne monitorowanie linii produkcyjnych, inspekcję wzrokową oraz potwierdzenie prawidłowości procesów i ich przebiegu,
– kontrolę przestrzegania zasad i procedur BHP oraz właściwego zarządzania narzędziami i sprzętem,
– zdalne rozwiązywanie problemów i wsparcie w zakresie konserwacji i pomocy.

Securitas Polska Sp. z o.o.
ul. Cybernetyki 21,
02-677 Warszawa
www.securitas.pl

Nowoczesne technologie wspierają biznes w wielu sektorach rynku. Branża security nie jest wyjątkiem. To właśnie innowacyjne technologie oparte na mobilności, inteligentnej analizie danych i sztucznej inteligencji stały się w branży security inwestycją pozwalającą ograniczyć wzrost kosztów usług ochrony i jednocześnie nadać bezpieczeństwu nowy wymiar.

Biznes lubi technologie

Małgorzata Rejman
Securitas Polska

W branży security rozwiązania oparte na nowoczesnych technologiach podnoszą poziom bezpieczeństwa, zapewniają komfort użytkowania, są mobilne, pozwalają na automatyzację i robotyzację, a ponadto wbrew pozorom ich wdrożenie nie generuje niebotycznych kosztów.

Skutecznie, nowocześnie i jednocześnie tanio. Gdzie tkwi haczyk?

To proste. Rozwiązania te pozwalają na znaczną optymalizację zasobów i zwiększenie efektowności. Jakość usług jest nieporównywalnie wyższa niż w rozwiązaniach konwencjonalnych. Haczykiem jest jedynie bariera psychologiczna i przeświadczenie o wyższości człowieka nad techniką.

Tymczasem dobrze wdrożona technologia pozwala osiągnąć efekt synergii maszyny i potencjału ludzkiego. Dla przykładu operator monitoringu potrzebuje przerw w pracy, gdyż jego koncentracja z czasem maleje, a pracownik wykonujący obchód nie zauważa wszystkiego. Powodów tego może być wiele. Pracownik może być w danym momencie tylko w jednym miejscu, coś lub ktoś może odwrócić jego uwagę, może być ciemno, a warunki pogodowe niesprzyjające. O ileż skuteczniejszy jest zdalny system monitoringu wizyjnego z zaawansowaną detekcją ruchu, analizą zawartości obrazu i kamerami termowizyjnymi.

Mobilność

Rozwiązaniem wpisującym się w nowe technologie jest RVS (*Remote Video Solutions*), czyli zdalny monitoring wizyjny wspierany inteligentną analizą danych. System może działać w pełni autonomicznie lub wspomagać pracę operatora. Wyposażony w technologię wykrywania i klasyfikacji obiektów wykrywa zdarzenie niepożądane już na etapie naruszenia wirtualnych stref lub linii perymetrycznych ustawionych w bezpiecznej odległości od chronionego obszaru. System ocenia, czy zdarzenie stanowi zagrożenie, wydaje automatyczny komunikat głosowy, uruchamia oświetlenie i powiadamia najbliższy patrol. W drugiej opcji to operator po weryfikacji sygnału alarmowego ocenia zagrożenie, korzystając z systemu audio, wydaje komunikat głosowy i podejmuje decyzję o interwencji. Securitas korzysta z możliwości zdalnego monitoringu, świadcząc usługi klientom z różnych sektorów rynku. Jedną z nich jest wirtualny patrol. Operator Securitas na podstawie obrazu z kamer dokonuje zewnętrznej i wewnętrznej wirtualnej kontroli obiektu. Wirtualny patrol może odbywać się zgodnie z ustalonym harmonogramem czasowym lub wyrywkowo. Operator monitoruje wyznaczone miejsca przez określony czas, a jego praca jest dokumentowana w formie nagrań i logów. To ekonomiczna i skuteczna alternatywa dla tradycyjnej formy obchodu.

Innym przykładem zastosowania przez Securitas zdalnego monitoringu jest obserwacja ujęć wody do zakładów produkcyjnych, często będących punktami krytycznymi infrastruktury warunkującymi ciągłość produkcji. Są one zlokalizowane zazwyczaj w trudno dostępnych miejscach i poza obszarem zabudowanym. Ze względu na ukształtowanie terenu i warunki atmosferyczne dojazd patrolu zajmuje dużo czasu. Zdalny dozór i wizyjna weryfikacja sygnałów alarmowych minimalizują konieczność interwencji do faktycznych sytuacji stanowiących zagrożenie, a punkty krytyczne są objęte stałym monitoringiem. W branży logistycznej Securitas oferuje kompleksowe zarządzanie i nadzór nad flotą oraz automatyzację procesu *self-checking* kierowców i przyjmowania dostaw aut w branży motoryzacyjnej. W obiektach biurowych i bankowych zdalny system KD pozwala nie tylko na wyznaczenie stref i zarządzanie nimi, ale także na wprowadzenie usługi *door-lock* (zdalnego uzbrajania i rozbrajania systemu alarmowego, bez konieczności zamykania placówek przy użyciu kluczy).

Pseudonimizacja

Podczas świadczenia usług monitoringu wizyjnego możemy zastosować technologię tzw. dynamicznego maskowania osób lub wyznaczonych stref, czyli pseudonimizację, zapewniając ochronę prywatności podczas przetwarzania danych osobowych. Zainteresowanie tymi rozwiązaniami zwiększyło się po wprowadzeniu RODO. W przypadku wystąpienia incydentu wymagającego analizy pełnego nagrania system pozwala osobom posiadającym odpowiednie uprawnienia na wyłączenie funkcji maskowania.

Automatyzacja i robotyzacja

Szacuje się, że w ciągu ostatnich dwóch lat zostało wygenerowanych około 90% wszystkich zgromadzonych dotychczas danych. Spadek kosztów ich przechowywania oraz przetwarzania wpłynął na rozwój AI i masowego wykorzystania sztucznych sieci neuronowych, a ciągle uczące się algorytmy poprawiają swoją skuteczność w oparciu o stale dostarczane nowe dane.

Z tych osiągnięć korzysta Securitas, współpracując z amerykańską firmą Knightscope produkującą autonomiczne roboty na potrzeby sektora security. Ich zadaniem jest patrolowanie otoczenia i przekazywanie informacji do stacji monitorowania. Roboty potrafią skanować tablice rejestracyjne, rozpoznają ludzki krzyk, reagują na dźwięk tłuczonego szkła, są wyposażone w czujniki zbliżeniowe, radary, kamery panoramiczne, termowizyjne i *Time of Flight*, które działają na zasadzie pomiaru czasu przemieszczania się światła. Niedawno zaprezentowano stacjonarny model robota, który, stosując technologię milimetrowych fal radiowych, skanuje obiekt w poszukiwaniu broni i metalowych przedmiotów. Robot zastąpi tradycyjne bramki na lotniskach i w szpitalach.

Microsoft Hololens

Inną formą wykorzystywania przez systemy Securitas petabajtów danych gromadzonych w postaci obrazów, tekstów, sygnałów zerojedynkowych, komunikatów dźwiękowych i głosowych są gogle Hololens. Rozwiązanie jest przeznaczone głównie do obiektów handlowych. Świadczenie usług ochrony wymaga przetworzenia ogromu napływających informacji i przygotowania odpowiednich scenariuszy reakcji. Dane połączone z realną przestrzenią w ramach tzw. rozszerzonej rzeczywistości (AR – *Augmented Reality*) pozwalają pracownikom Securitas na szybsze podejmowanie właściwych działań (a w sytuacji zagrożenia czas reakcji jest krytyczny). Hololens nanosi informacje z systemów bezpieczeństwa na przezroczysty ekran w goglach, wyznacza najszybszą trasę, wyświetla ją i nawiguje do celu.

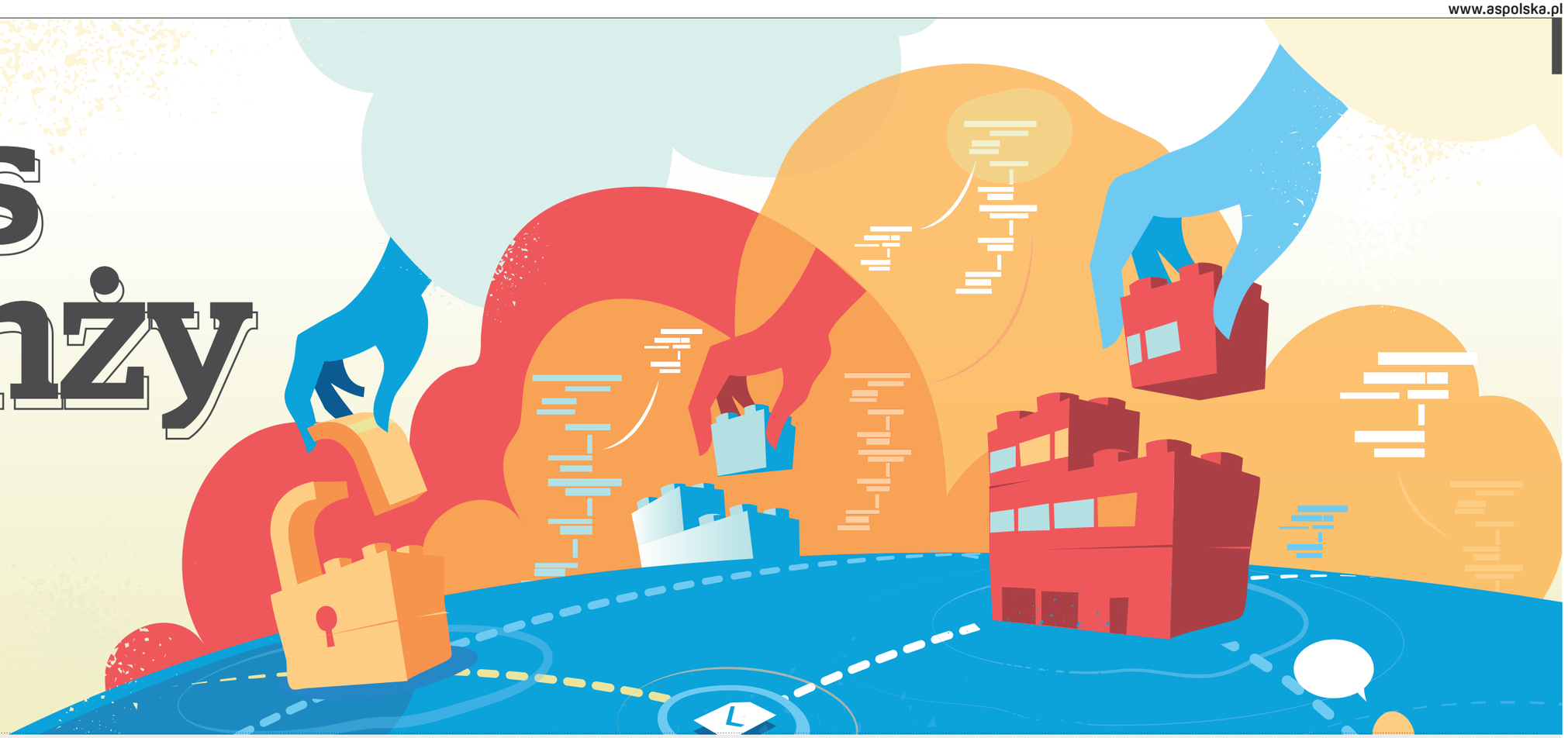
Oszczędza to cenny czas potrzebny do podjęcia decyzji. Prezentacja danych w ramach AR umożliwia pracownikom Securitas otrzymywanie informacji o takich zmianach jak przestawiona gaśnica, niedomknięte drzwi czy pozostawiony bagaż.

Rozpoznawanie twarzy

Technologia identyfikacji twarzy znajduje zastosowanie najczęściej w obiektach biurowych, handlowych czy podczas dużych eventów. System kamer dozorowych, identyfikując twarz na podstawie bazy zdjęć, może uruchomić alarm, śledzić osobę lub nadać jej odpowiedni poziom dostępu. Technologia rozpoznawania twarzy może być też używana w celach biznesowych. Może klasyfikować klientów z podziałem na wiek, płeć, a nawet szacować preferencje zakupowe. W przypadku połączenia tych danych z *heat mappingiem*, czyli systemem monitorującym ruch pojedynczych osób lub grup o określonym profilu, zarządca obiektu handlowego poznaje preferowane trasy klientów, wie, ile czasu spędzają w określonym miejscu, gdzie najchętniej się zbierają w ciągu dnia lub w ciągu miesiąca. Securitas wykorzystuje te informacje do optymalizacji systemu ochrony i alokacji środków w strategiczne miejsca, a klient buduje na ich podstawie strategię marketingową.

Nowe technologie stawiają przed branżą security nowe wyzwania i szanse na rozwój. Postępująca automatyzacja wiąże się wprawdzie z zagrożeniem bezrobociem technologicznym, ale jednocześnie tworzy popyt na pracowników o specjalistycznych kwalifikacjach. Warto pamiętać, że za każdym rozwiązaniem technologicznym stoi człowiek.

Głos branży



Kluczowe decyzje podejmuje człowiek

Karol Radzajewski
Hikvision Poland

Bezpieczeństwo pracy w obiektach przemysłowych w dużej mierze zależy od pracowników i przestrzegania przez nich określonych zasad. Szczególnie trudne jest zarządzanie bezpieczeństwem w dużych przedsiębiorstwach, zatrudniających kilkaset lub nawet kilka tysięcy osób. Przy tak dużej liczbie osób znajdujących się w jednej lub rozproszonej lokalizacji niezwykle istotną rolę odgrywają systemy zabezpieczeń.

Obiekty przemysłowe wymagają szczególnego podejścia oraz przeanalizowania wielkich możliwych scenariuszy działania w sytuacjach kryzysowych, począwszy od podstawowych, które są niezbędne do odbioru budynku, czyli np. zapewnienia dróg ewakuacyjnych. W zależności od specyfiki obiektu nacisk może być położony na inny system.

Nawet w najbardziej zaawansowanych systemach decyzję o kluczowych działaniach musi podjąć człowiek. Systemy zabezpieczeń mogą jedynie wspierać zarządzanie bezpieczeństwem. Wyszkolona, wyspecjalizowana obsługa powinna mieć pełną wiedzę odnośnie do całego obiektu oraz systemów zabezpieczeń w nim zainstalowanych. W rzeczywistości często jest inaczej.

Wizualizacja poszczególnych systemów pozwoli użytkownikom szybciej kontrolować i zarządzać ryzykiem. Gdy przedsiębiorstwo ma kilka obiektów, wizualizacja np. schodzącego alarmu pożarowego, przekroczenia linii lub sforsowanych drzwi umożliwia natychmiastowe zlokalizowanie na mapie miejsca tego alarmu. Mając opracowane scenariusze na wypadek wystąpienia ryzyka bezpieczeństwa, dzięki integracji systemów można wesprzeć obsługę obiektu poprzez automatyzację określonych reakcji różnych systemów na akcję innego. Największym wyzwaniem powinno być świadome zarządzanie oraz integrowanie systemów bezpieczeństwa, a także szkolenie personelu.

Automatyzacja procesów

Każdy nieco inaczej definiuje pojęcie bezpieczeństwa funkcjonalnego. Istnieją jednak międzynarodowe standardy, które szczegółowo opisują tę kwestię. Każda z norm reguluje inne obszary, m.in. bezpieczeństwo procesu przemysłowego, maszyn czy elektrowni jądrowych. Istotne, aby w danym przedsiębiorstwie programowalne systemy zabezpieczenia technicznego zadziałały w odpowiednim momencie.

To właśnie szybkie wykrycie awarii lub uszkodzenia jednego z elementów pozwala uchronić przedsiębiorstwo przed niepożądanymi sytuacjami i wypadkami. Uszkodzenia maszyn wytwórczych mogą doprowadzić np. do całkowitego zatrzymania na pewien czas produkcji, co dla przedsiębiorstwa stanowi realną stratę. W przypadku bardziej poważnych uszkodzeń może dojść do pożaru i zniszczeń na dużą skalę. Do tego dochodzi zagrożenie zdrowia i życia ludzkiego.

Jako że świadomość tych zagrożeń ciągle rośnie, zwiększa się też zapotrzebowanie na systemy wczesnego ostrzegania o awariach lub zapobiegania im. W ostatnich latach w wielu przedsiębiorstwach stosuje się w tym celu kamery termowizyjne. Wcześniej termowizja była używana jedynie w obszarach produkcyjnych w tzw. widzeniu maszynowym w celu weryfikacji jakości produkowanych elementów lub całych produktów. Obecnie kamery są również używane do monitorowania m.in. hal magazynowych lub produkcyjnych.

Funkcja pomiaru temperatury pozwala na zweryfikowanie, czy któraś z maszyn np. nie przegrzewa się, co umożliwia zaalarmowanie, zanim zostanie zauważony płomień.

Integracja takich rozwiązań w nowoczesnych przedsiębiorstwach będzie w przyszłości bardzo istotnym elementem ciągłości ich pracy. Rozwiązania termowizyjne pozwalają bowiem na automatyzację procesów, która jest tak istotna w przemyśle 4.0.

Jakub Sobek
certyfikowany trener techniczny, Linc Polska

Zapewnienie ciągłości działania systemu bezpieczeństwa pożarowego

Krzysztof Kunecki
dyrektor ds. technicznych,
Schrack Seconet Polska

Na etapie budowania koncepcji ochrony przeciwpożarowej obiektu przemysłowego należy mieć na względzie cel nadrzędny, jakim jest dobór takich rozwiązań, urządzeń technicznych i warunków organizacyjnych, które zapewnią bezpieczeństwo ludzi, mienia oraz ciągłość działania całej organizacji. Zgodnie z przepisami urządzenia przeciwpożarowe muszą spełniać konkretne wymagania – w zakresie parametrów technicznych, funkcjonalności i odporności na warunki środowiskowe (w tym dotyczące kompatybilności elektromagnetycznej) – które są weryfikowane na etapie badań atestacyjnych i certyfikacji przed wprowadzeniem wyrobów do obrotu i użytkowania.
Posiadanie wymaganego dokumentu atestacyjnego potwierdza zgodność z normami, jednak nie oznacza, że urządzenia będą spełniały wszystkie specjalne wymagania dotyczące funkcjonalności i niezawodności charakterystyczne dla obiektu przemysłowego.
Przy doborze urządzeń i rozwiązań technicznych systemu sygnalizacji pożarowej należy spojrzeć na temat szerzej i przeanalizować odporność pojedynczych urządzeń i całego systemu na możliwość wystąpienia uszkodzenia (awarii), które może spowodować, że alarm pożarowy nie zostanie wykryty lub nie zostaną wykonane wszystkie funkcje systemu (sterowania) zgodnie z przyjętym scenariuszem pożarowym.
Powinno się przeprowadzić podobną analizę do tej, jaką często wykonuje się w automatyce przemysłowej w związku z oceną potencjalnych zagrożeń, prawdopodobieństwa ich wystąpienia i doboru rozwiązań zabezpieczających, minimalizujących ryzyko – w celu zapewnienia ciągłości działania całej instalacji wg kryterium oceny poziomu nienaruszalności bezpieczeństwa (SIL).
W systemach sygnalizacji pożarowej jest kilka podstawowych metod, które pozwalają znacznie zwiększyć niezawodność działania. Pierwszym krokiem jest dobór urządzeń i rozwiązań o architekturze w pełni redundantnej, niezależnie od liczby elementów w systemie. Dotyczy to przede wszystkim urządzeń zarządzających i centralnych, takich jak centrala sygnalizacji pożarowej czy system zarządzania bezpieczeństwem pożarowym, które w przypadku uszkodzenia nawet pojedynczego komponentu powinny realizować w sposób niezakłócony wszystkie funkcje detekcji, sygnalizacji, sterowania i zarządzania.
Redundancja powinna dotyczyć zarówno komponentów sprzętowych, jak i oprogramowania.
W dalszej kolejności powinny zostać zdublowane krytyczne tory komunikacyjne poprzez zastosowanie bezpiecznych topologii sieci (pierścień lub sieć kratowa) zapewniających pracę nawet przy trzech uszkodzeniach.
Kolejnym elementem bezpieczeństwa jest zastosowanie urządzeń sterujących z funkcją *fail-safe*, które przełączają się w pozycję bezpieczną w momencie wystąpienia uszkodzenia – tę funkcję należy zapewnić wszystkim obwodom wyjść sterujących.
Dopełnieniem zabezpieczeń sprzętowych jest odpowiednie oprogramowanie systemu, które przy tworzeniu procedur sterujących powinno uwzględniać zabezpieczenia w postaci alternatywnej procedury w przypadku awarii czy posiadać zabezpieczenia przed niewłaściwą obsługą systemu.

Business Resilience Director

Jacek Tyburek
zastępca dyrektora
Biura Bezpieczeństwa,
Polski Holding Obronny

W wyjątkowo pozwolę sobie na głos w tonacji rewolucyjnej. Na pytanie o „szeroko rozumiane bezpieczeństwo" w obiektach przemysłowych reagują alergicznie. Szerokość i głębokość tegoż bezpieczeństwa są uzależnione od wielu zmiennych, w przemyśle zbyt wielu, by termin „bezpieczeństwo" był wystarczająco wyczerpujący.
Zupełnie inaczej bezpieczeństwo jest rozumiane w przemyśle motoryzacyjnym, inaczej w spożywczym i FMCG.
A świat produkcji wrażliwej to zupełnie inny świat. Na te zastrzeżenia nakładają się filtry właścicielskie i jakościowe.
Korporacja brytyjska, niemiecka, francuska czy polska spółka Skarbu Państwa to bardzo często różne światy. Różne wymagania, różne agendy, różne oczekiwania.
Truizmem jest mówienie o różnicach w zarządzaniu bezpieczeństwem w firmach przemysłowych, w których pracuje nie więcej niż 1000 osób, a tymi, które zatrudniają 10 tys. i więcej, w dodatku w rozproszonych lokalizacjach. Przed zarządzającym bezpieczeństwem stoją wówczas inne wyzwania.
Pogłębiająca się specjalizacja i profesjonalizacja serwisów obiektów, poczynając od usług ochrony fizycznej, przez możliwości techniczne systemów zabezpieczeń, kończąc na usługach utrzymania technicznego obiektów mające wpływ na ciągłość działania, wymaga zmiany. Przede wszystkim zmiany postrzegania roli osoby lub funkcji zarządzającej bezpieczeństwem.
Reasumując, moim zdaniem nie można mówić o „szeroko rozumianym bezpieczeństwie", tylko raczej o „niezwykle bogatej teczce z narzędziami do zapewnienia bezpieczeństwa".
Jeśli zrobimy „wycieczkę" po ofertach pracy z opisem „security", zobaczymy, że 80% ofert na rynku pracy dotyczy dziś osób zajmujących się cyberbezpieczeństwem lub bezpieczeństwem informacji.
Funkcja specjalistów zarządzania ryzykiem, incydentami i ciągłością działania nie rozwinęła się tak powszechnie, jak wielu z nas w branży przewidywało. Istnieją w niektórych organizacjach, ale na pewno nie jest to model dominujący. Wiele organizacji ciągle jeszcze nie „odkryło" zarządzania ryzykiem operacyjnym. Zaskakujące, ale prawdziwe.
Czego więc zarządy firm przemysłowych mogą oczekiwać od Security Managera?
Moim zdaniem są dwie agendy: jawna i ukryta, ale jakże pożądana… Pierwsza, żeby był on klasycznym Security Managerem w ujęciu korporacyjnym – żeby dbał o majątek, ludzi procesy itp. Natomiast ta prawdziwa potrzeba to posiadanie w zespole zarządzającym człowieka, który zapewni tzw. święty spokój, a w razie kryzysu będzie filarem działań. Taka osoba powinna mieć maksymalnie szeroką wiedzę o organizacji, doświadczenie zawodowe w zakresie security, zrozumienie bezpieczeństwa informacji i cyberbezpieczeństwa, a przy tym posiadać ten dar, który można nazwać „radarem na ryzyka".
To są główne wyzwania. Jak im sprostać? Uważam, że należy jak najszybciej zrzucić trykot superbohatera z napisem „Security Manager" i włożyć nowy, piękny, nowoczesnie zaprojektowany i uszyty z nowoczesnych materiałów trykot z napisem „Business Resilience Director". Co to znaczy? Proszę poszukać w źródłach. Warto.

Machine Vision przyszłością rynku security

Robert Sienkiewicz
Project Manager
Dahua Technology Poland

Machine vision (widzenie maszynowe) to dla branży security pojęcie zaczerpnięte jakby z innego świata, znane z filmów *science fiction,* dotyczące stricte rozwiązań przemysłowych. Obie technologie oparte na obrazie *(television* i *machine vision)* podążały dotychczas osobnymi ścieżkami, realizując tylko swoje funkcje. Ale to się zmienia. Każdego roku widać ogromny postęp – kamery przemysłowe *machine vision* są stosowane w inteligentnych systemach ruchu, systemach nadzoru miejskiego czy ochronie obszarów o podwyższonym poziomie zagrożeń.
Technologia *machine vision* leży u podstaw nowej generacji systemów specjalizowanych, np. do egzekwowania i poboru opłat na autostradach (firmy Q-Free ASA w Norwegii). Taki system składa się z dwóch kamer CCTV rejestrujących obraz przedniej i tylnej tablicy rejestracyjnej samochodu oraz z dwóch przemysłowych kamer matrycowych *(area-scan)* śledzących do strefy wjazd i wyjazd z niej, łącznie z informacją o zmianie pasa. W przyszłości system mógłby realizować wiele innych funkcji, takich jak odczyt tablic ADR (informacje o towarach niebezpiecznych), identyfikacja kontenerów oparta na kamerach ze skanowaniem liniowym *(line-scan),* śledzenie trasy przejazdu samochodu w ruchu przygranicznym w celu zapobieganiu przemytowi (Projekt Krajowej Izby Skarbowej – Cyfrowa Granica).
To rozwiązanie o wiele bardziej użyteczne niż obecnie działający system poboru opłat drogowych viaToll. Ministerstwo Infrastruktury analizuje możliwość wprowadzenia radykalnej zmiany sposobu naliczania płatności za korzystanie z autostrad. Być może wspomniany system będzie dobrym wyborem.
Kamery *machine vision* znakomicie radzą sobie również w systemach wykrywania skradzionych pojazdów. Tradycyjny system monitoringu wizyjnego miasta może dać wiele cennych wskazówek, gdzie należy szukać interesującego auta, ale kamery CCTV swoim zasięgiem nie pokrywają wszystkich ulic, nie zawsze też przekazany obraz ma pożądaną rozdzielczość ze względu na znaczne odległości. Obecnie, znając numery rejestracyjne, patrol policji wyposażony w system wykrywania pojazdów z technologią *machine vision* jest w stanie zidentyfikować 8 tys. pojazdów na dobę. Wskaźniki wykrywania są bliskie 95%, a system nie wymaga żadnych działań zespołu patrolującego. Dla porównania poprzednie rozwiązania oparte na patrolach tradycyjnych angażowały 30 osób przez 12 miesięcy w celu osiągnięcia tej samej wydajności.
W systemach ochrony obszarów o podwyższonym poziomie ryzyka można spotkać nowe urządzenia do skanowania podwozia pojazdów, które ułatwiają kontrolę wjazdu na teren obiektu chronionego. Uzyskujemy w tym przypadku kompleksową informację o czasie wjazdu i wyjazdu, numerze rejestracyjnym i marce samochodu oraz czy pod autem nie zainstalowano przedmiotów niebezpiecznych. Można zeskanować pojazd o szerokości do 4,5 m poruszający się z prędkością do 80 km/godz. i wadze 50 t. Sercem tego systemu jest kamera *machine vision* ze skanowaniem liniowym.
Machine vision w połączeniu z innymi dostępnymi na rynku security technologiami tworzy nową generację zaawansowanych systemów nadzoru, które dają wymierne korzyści w postaci mniejszej liczby potrzebnego personelu, generowania niższych kosztów czy wspomagania operatora w podejmowaniu kluczowych decyzji.

Podane przykłady zastosowania tylko w niewielkim stopniu pokazują możliwości zastosowania technologii widzenia maszynowego, która dzięki rozwojowi (kamery smart i 3D) sukcesywnie uwalnia drzemiący w niej ogromny potencjał.

Nieustająca ochrona

Bogumił Szymanek
Axis Communications

Zabezpieczenie i kontrola obiektów przemysłowych oraz zarządzanie nimi stanowi duże wyzwanie. Odpowiedzialność za bezpieczeństwo i ciągłość funkcjonowania obiektów to kluczowe zadania stawiane przed osobami dokonującymi wyboru właściwych rozwiązań zapewniających takie bezpieczeństwo. Trzeba widzieć wszystko, co się dzieje na terenie obiektu, bez względu na lokalizację, otoczenie czy panujące warunki środowiskowe.

W obiektach przemysłowych należy skupić się na zagrożeniach bezpieczeństwa ludzi i mienia, ale też ciągłości produkcji i zyskowności. Rozwiązania Axis przeznaczone do ochrony obiektów przemysłowych pozwalają uporać się ze wszystkimi zagrożeniami za pomocą jednego efektywnego kosztowo systemu.

Rozwiązania proponowane przez Axis zapobiegające wtargnięciom na teren obiektu to przede wszystkim niezawodne urządzenia ochrony obwodowej. Kamery optyczne i termowizyjne oraz detektory z funkcjami analizy obrazu i śledzenia obiektów przesyłają sygnały alarmowe do centrum sterowania. Ostrzeżenia audio są odtwarzane za pomocą głośników sieciowych, a intruzów można zidentyfikować dzięki obrazom z kamer dozorowych. Ze względu na ogromne koszty związane z potencjalnymi stratami wynikającymi z uszkodzeń urządzeń czy infrastruktury oraz ze wstrzymaniem produkcji bardzo ważne jest, by na najwcześniejszym etapie przeciwdziałać zagrożeniom. Zapewniają to systemy Axis wczesnego automatycznego wykrywania i odstraszania potencjalnych intruzów.

Rozwiązania Axis umożliwiają integrację systemu wizyjnego z systemami analityki oraz innymi systemami wspomagającymi pracę przedsiębiorstwa, np. monitorującymi działania pracowników, przyczyniając się w ten sposób do poprawy efektywności działania całej firmy.

Bezpieczeństwo pod profesjonalnym dozorem

Jestem przekonany, że czasy, gdy do zapewnienia bezpieczeństwa wystarczało zatrudnienie pracowników ochrony, którzy w imieniu zleceniodawcy weryfikowali uprawnienia do wejścia czy wjazdu na teren obiektu, przeszły już do historii. Taki poziom organizacji według mnie nie zapewni dziś bezpieczeństwa obiektu.

Rozważmy zatem, jak rozumiemy bezpieczeństwo obiektu przemysłowego? Jakie rodzaje ryzyka chcemy eliminować? Przed czym chronić te obiekty?

W ochronie majątku (towary i majątek ruchomy) istotne ryzyko mogą stanowić zagrożenia płynące z wnętrza firmy. Powiedzmy szczerze, włamywacz nie stanowi istotnego problemu. Ryzyko powstania wysokich strat finansowych prawie zawsze powstaje wewnątrz zakładu. Dopiero znajomość stosowanych mechanizmów kontroli i bezpieczeństwa uwidacznia kreatywność osób, które nie chcą zadowolić się tylko wynagrodzeniem. To w tym obszarze w mojej praktyce najczęściej odkrywałem zaawansowane metody maskowania oszustwa na dużą skalę, w którego funkcjonowanie byli zaangażowani pracownicy zakładu, firm transportowych oraz nieuczciwych klientów (odbiorców dużych partii towaru).

Projektując rozwiązania bezpieczeństwa, ochronę należy zacząć znacznie wcześniej niż na bramach obiektów. Skuteczne zapewnienie bezpieczeństwa towarom i mieniu spółki powinno się rozpoczynać od wplatania „genu" bezpieczeństwa w cały proces funkcjonujących w obiekcie procesów i operacji. Procesy te, wzajemnie się zazębiając, powinny płynnie przekazywać sobie zarówno towar, jak i jasno określoną za niego odpowiedzialność. Ważne, by na każdym etapie blokować potencjalne możliwości manipulacji danymi w systemach i rozliczeniach, np. poprzez ponowny wpis, bez historii poprzednich zapisów.

W dobie rosnącego zagrożenia aktami terrorystycznymi nie wolno zapominać o groźbie użycia niebezpiecznych substancji i instalacji znajdujących się na terenie zakładu przemysłowego i spowodowania wysokiego zagrożenia czy też wymuszenia okupu pod groźbą spowodowania katastrofy. Tu należy położyć nacisk na kwestie skutecznej kontroli dostępu do takich miejsc połączonej z zaawansowanymi systemami detekcji intruza.

Jacek Tobiasz
Security Manager
Grupa Żywiec

Szybka weryfikacja alarmu i sprawna reakcja ze strony wskazanej komórki interwencji czy ochrony może zapobiec katastrofie ogromnych rozmiarów.

Aby system bezpieczeństwa był w takim przedsiębiorstwie sprawnie i efektywnie wdrożony, powinien znajdować się pod nadzorem profesjonalnego Security Managera.

Bezpieczeństwo fizyczne i cyfrowe

Produkcja przemysłowa wraz z całą swoją infrastrukturą jest ciągle poddawana presji rynkowej, sprowadzającej się do nieustannego usprawniania efektywności. Metodą na sprostanie tym oczekiwaniom jest technologia.

Cyfryzacja i automatyzacja procesów produkcyjnych stała się faktem. Oprócz oczywistych korzyści nowe rozwiązania przynoszą także nowe zagrożenia. Uważam, że największym problemem jest obecnie niedoszacowanie tej „ciemnej" strony nowych technologii. Pozytywny efekt finansowy może tworzyć atmosferę sukcesu, w której świadomie lub nieświadomie ignoruje się możliwe niebezpieczeństwa.

Używając terminu „niedoszacowanie", miałem na myśli przede wszystkim skalkulowanie ryzyka. To oczywiście w dalszej perspektywie prowadzi do kalkulacji kosztów bezpieczeństwa, jednak dzisiaj problem jest raczej związany z brakiem zarówno należytej uwagi, jak i czasu poświęcanemu na zastanowienie się, co oznacza termin „bezpieczeństwo".

Czy w dalszym ciągu miarą dobrego zabezpieczenia obiektu przemysłowego jest zastosowanie wszystkich tradycyjnych atrybutów, takich jak ogrodzenia, bramy, strażnicy, kamery itp.? Może jednak środek ciężkości przesuwa się w stronę zachowania ciągłości działania i zdolności do jak najszybszego odtworzenia działalności po wystąpieniu zdarzenia?

Wszystko wskazuje na to, że zdarzenia te będą miały charakter incydentów związanych z bezpieczeństwem cyfrowym. Cyberbezpieczeństwo w oderwaniu od bezpieczeństwa fizycznego jest pustym określeniem.

Znalezienie właściwej równowagi pomiędzy tymi dwoma światami będzie największym wyzwaniem nie tylko w obiektach przemysłowych. Będzie wymagać nowego spojrzenia i w pewnym sensie odrzucenia wcześniejszych wyobrażeń o bezpieczeństwie. Przeszkodą będzie wypracowanie nowych rozwiązań, głównie organizacyjnych.

Janusz Syrówka
Dział Bezpieczeństwa/Country Security Chair
innogy Polska SA

Największe zagrożenie tkwi według mnie w mentalnym zakorzenieniu się w przeszłości – zarówno u ludzi związanych z IT, jak i z bezpieczeństwem.

Bezbłędna ochrona

Monitoring wizyjny dużych obiektów przemysłowych ma z założenia uzupełniać i wspierać ochronę fizyczną w obiekcie.

Algorytmy inteligentnej analizy obrazu coraz częściej są implementowane nawet w modelach kamer ze średniej półki cenowej. Pozwala to na bardziej precyzyjne prowadzenie ochrony obiektu i reakcję na zaistniałe zdarzenia wg przyjętych schematów.

Przykładem ciekawego użycia funkcji IVA jest droga pożarowa i wytyczenie obszaru, na którym nic nie powinno przebywać dłużej niż przez zadany czas. Kamera analizująca obraz wyśle sygnał alarmu ochronie obiektu, która nie musi obserwować obrazów z danej kamery. Inteligentne funkcje mogą jednak powodować spore zamieszanie, jeśli zostaną źle skonfigurowane.

Dobrym tego przykładem może być próba zapewnienia ochrony perymetrycznej poprzez konfigurację funkcji przekroczenia linii w kamerach zewnętrznych z wbudowanym promiennikiem. Standardowo zainstalowana kamera z właściwie skonfigurowaną funkcją przekroczenia linii będzie działała poprawnie, dając prawidłowe alarmy tylko w ciągu dnia. W nocy system wygeneruje wiele fałszywych alarmów, których powodem będą owady gromadzące się przy promienniku. Aby temu zapobiec, najlepiej zastosować zewnętrzne promienniki lub doświetlenie światłem białym.

Najodpowiedniejszym narzędziem dozorującym w ochronie obwodowej są kamery termowizyjne. Ich odporność na fałszywe alarmy, możliwość prowadzenia obserwacji i wykrywania obiektów na dużym obszarze dają ogromną przewagę nad obrazem z kamer światła widzialnego.

Błędy w konfiguracji lub zbyt duża liczba fałszywych alarmów mogą doprowadzić do zignorowania właściwego alarmu i w efekcie braku reakcji ochrony fizycznej. Poprawne skonfigurowanie systemu wymaga od instalatora wielu rozmów z inwestorem, poznania specyfiki zabezpieczanego obiektu.

Marcin Morzyk
BCS

Tylko wówczas, gdy wszystkie elementy systemu – wymagania, sprzęt i konfiguracja – są odpowiednio dopracowane, zminimalizujemy możliwość niedostrzeżenia zagrożenia. Urządzenia i systemy inteligentnej analizy obrazu mają za zadanie jak najszybciej przekazać alarm, sygnalizując możliwość zagrożenia, na które ochrona fizyczna powinna zareagować.

Deloitte – Biuro w Warszawie
al. Jana Pawła II 22
00-133 Warszawa
www.deloitte.com/pl

Polska musi się przygotować na czwartą rewolucję przemysłową

Zmiany związane z komercyjnym wykorzystywaniem najnowszych zdobyczy technologii, cyfryzacja, sztuczna inteligencja, sensory, biomateriały, możliwości analizy gigantycznych ilości danych – to wszystko istotnie wpływa na sposoby wytwarzania. **Nie omija to również Polski.**

Julia Patorska
lider zespołu ds. analiz ekonomicznych
Deloitte

Jesteśmy świadkami początku czwartej rewolucji przemysłowej i to najwyższy czas dla menedżerów, by znaleźć odpowiedź – jak skutecznie wprowadzić swoją firmę na poziom Przemysłu 4.0.
O Przemyśle 4.0 mówi i pisze się coraz więcej. W Davos zagadnienia związane z *czwartą rewolucją przemysłową* były jednym z głównych tematów, nie pomijając jednak kluczowych kwestii społecznych czy środowiskowych, które również wybrzmiały podczas tegorocznego forum ekonomicznego. Czy rzeczywiście zmiany, które aktualnie obserwujemy, są tak duże i istotne, jak wcześniejsze rewolucje – maszyna parowa, elektryfikacja czy informatyzacja? Moim zdaniem nie bez powodu mówimy o kolejnym przełomie, który nie jest już tylko futurologią, a dzieje się na naszych oczach. Warto zatem mieć je szeroko otwarte i potrafić umiejętnie wykorzystać ten moment.

Czym jest Przemysł 4.0

Sformułowanie definicji tego, co można rozumieć pod pojęciem *czwartej rewolucji przemysłowej*, nie jest łatwe. Dotykamy tutaj szeregu zagadnień, które w sumie dają istotną i ogromną zarazem zmianę w procesach wytwórczych. **Tak jak we wcześniejszych rewolucjach, i tym razem celem jest zwiększanie produktywności i lepsze dostosowywanie produktu do potrzeb odbiorców.** To wszystko ma odbywać się z poszanowaniem otoczenia, wypracowując wartość dla szerszego grona odbiorców przy minimalizacji kosztów zewnętrznych. Wydaje mi się, że wcześniejsze rewolucje były jednak łatwiejsze do zrozumienia – jeden impuls zmieniał cały łańcuch wartości. Tym razem jest nieco inaczej. Nakłada się równolegle szereg technologii i odmiennych zachowań, które zintegrowane prowadzą do nowego spojrzenia na produkcję dóbr i usług. Jednym zdaniem **Przemysł 4.0 tym różni się od wcześniejszych rewolucji, że łącząc istniejące technologie, równocześnie zaciera granice między sferami fizyczną, cyfrową i biologiczną procesów wytwórczych**.

Czwarta rewolucja przemysłowa w praktyce

Nic lepiej nie zobrazuje zmian, jak żywy przykład. Dla mnie najłatwiejsze do uchwycenia i tym samym wytłumaczenia są zmiany zachodzące w motoryzacji, gdzie podnoszenie efektywności produkcji wpływa istotnie na pozycję konkurencyjną producentów i odbywa się z myślą o poszanowaniu środowiska. Jest to widoczne w wytwarzaniu na coraz większą skalę bezemisyjnych samochodów, czy w wykorzystaniu coraz bardziej zaawansowanych materiałów, w tym także pochodzenia biologicznego (wyściółki tapicerki z owczej wełny, elementy z biopolimerów). Następnie wymienić można prace nad pojazdami autonomicznymi oraz szerokim zastosowaniem sztucznej inteligencji oraz *big data* już podczas użytkowania pojazdu. Na końcu łańcucha dodatkowo włączane są także roboty do rozbiórki zużytych pojazdów po to, by efektywniej wydobyć materiały i zachować ich wartość. Dzieje się to za pomocą wsparcia regulacyjnego, ale choćby projekt ICARRE 95 (w którym udowodniono możliwość recyklingu i odzysku energetycznego 95 proc. pojazdu, mierząc to jego masą) pozwala dostrzec istotną pozycję samego producenta w zachodzącej zmianie.
Czy przykład branży motoryzacyjnej możemy uznać za zwiastun i pewnik dziejącej się rewolucji? Przytoczone przeze mnie przykłady dotyczą różnych wytwórców, często nie są ze sobą jeszcze powiązane w spójną całość. Rozdźwięk pomiędzy możliwościami a rzeczywistością potwierdza także badanie Industry 4.0, które Deloitte przeprowadził na kadrze kierowniczej firm i agencji rządowych w 19 liczących się gospodarkach z całego świata.

> Przemysł 4.0 tym różni się od wersji poprzedniej, że łącząc istniejące technologie, zaciera granice między sferami fizyczną, cyfrową i biologiczną procesów wytwórczych.

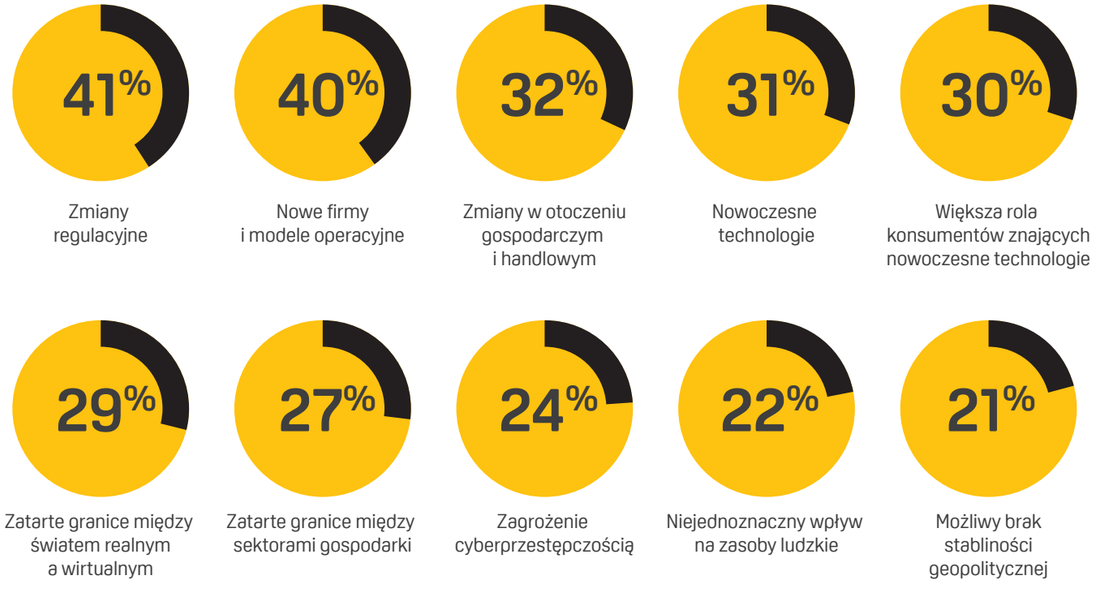
Respondenci rozumieją zachodzące zmiany w ich otoczeniu, ale niekoniecznie potrafią je wykorzystać. Oceny są niejednoznaczne. Zdaniem aż 87 proc. respondentów Przemysł 4.0 może doprowadzić do zmniejszenia różnic społecznych i ekonomicznych, ale równocześnie pojawiają się obawy, czy kadra jest odpowiednio przygotowana i czy generalnie społeczeństwo posiada oczekiwane kompetencje (tylko jedna czwarta ankietowanych uważa, że posiada odpowiednie zasoby osobowe do sprostania wyzwaniom przyszłości). Kadra kierownicza nie jest przekonana kto ma tę zmianę wdrażać. Podobnie w obszarze technologii. Respondenci, choć dostrzegali jej znaczącą rolę w zachodzących zmianach, to nie zawsze potrafili biznesowo uzasadnić inwestycje w technologie, które w ich otoczeniu były realizowane. Sprzeczności, które wykazało cytowane badanie, da się łatwo uzasadnić jeszcze niewielkim zintegrowaniem zachodzących zmian i częstym brakiem synergii pomiędzy ulepszeniami. Wskazuje to raczej na początek drogi do ugruntowanej pozycji Przemysłu 4.0, choć niewątpliwie kierunku jej zmienić się już nie da.

> Im więcej człowieczeństwa zachowamy, tym większej liczbie ludzi pomogą w życiu zdobycze Przemysłu 4.0.

Polski Przemysł 4.0

Warto zatem zadać pytanie o przygotowanie Polski do czwartej rewolucji przemysłowej. Myślę, że aby dana gospodarka mogła wykorzystać najlepiej możliwości Przemysłu 4.0, konieczne są następujące czynniki: istotny udział przemysłu w generowaniu PKB, zaawansowanie technologiczne kraju oraz wysoki kapitał społeczny, który umożliwi integrację innowacji i sieciowe wykorzystanie osiągnięć w poszczególnych sferach. Ważne jest zatem, aby przyjrzeć się, gdzie na tej mapie znajduje się Polska, oraz czy jest gotowa stanąć do wyścigu o ważną międzynarodową pozycję.
Jedną z cech ostatnich dwóch dekad w wielu krajach był malejący udział przemysłu przetwórczego w wartości dodanej wytwarzanej przez całą gospodarkę. Mogliśmy to zaobserwować w USA czy ogółem w strefie euro. Polsce jednak udało się zachować poziom industrializacji z końca XX w., ale działo się to także dzięki bezpośrednim inwestycjom zagranicznym. Nasze przewagi w tym zakresie wynikały przede wszystkim z niższych kosztów osobowych, przy relatywnie ich wysokiej jakości. Dodatkowo polski przemysł jest rozdrobniony. Brakuje nam dużych przedsiębiorstw ze znacznym kapitałem, gdzie więcej wydaje się na badania i rozwój, a efekty skali istotnie podnoszą produktywność.
W efekcie dzisiejszy przemysł może mieć problem z utrzymaniem wysokiego poziomu generowanej wartości dodanej w PKB. Kwestie zaawansowania technologicznego mogą być kolejną barierą.

Czynniki, które wywrą największy wpływ na Państwa organizację w ciągu nadchodzących 5 lat



Uwaga: ankietowani mogli wybrać do trzech odpowiedzi

Przemysł 4.0 dopiero raczkuje. Czwarta rewolucja przemysłowa zmieni świat, ale tylko 14 proc. zarządzających jest na nią gotowych.

W szeregu różnorodnych rankingów mierzących naszą pozycję globalną w zakresie stosowanych technologii, gotowości adaptacji nowych rozwiązań IT czy też ogólnego środowiska sprzyjającego kreacji i zmianom **w ramach czwartej rewolucji przemysłowej plasujemy się w czwartej/piątej dziesiątce świata (38. miejsce na 127 w Global Innovation Index 2017, 42. miejsce na 139 w Networked Readiness Index 2016, 23. miejsce na 28 krajów UE w Digital Economy and Society Index 2017).** Badanie Deloitte w zakresie dojrzałości ekosystemu start-upów także potwierdza dystans, jaki dzieli nas od czołówki gospodarek w tym zakresie.

Jako społeczeństwu czasem trudno nam się porozumieć, cechujemy się dużą nieufnością wobec innych, nie zawsze potrafimy współpracować, widząc możliwość osiągnięcia celu w sytuacji „win-win". O niskim i wręcz spadającym kapitale społecznym nie zawsze mówi się w kontekście biznesu, ale w mojej opinii to jeden z większych hamulców zmian.

Biorąc pod uwagę powyższe uwarunkowania, Polska nie jest jeszcze gotowa na czwartą rewolucję przemysłową. Pocieszające jest to, że na wielu innych rynkach Przemysł 4.0 też dopiero raczkuje.

– *Czwarta rewolucja przemysłowa zmieni świat, ale tylko 14 proc. zarządzających jest na nią gotowych* – powiedział Punit Renjen, CEO Deloitte Global, w Davos, cytując przeprowadzone przez firmę badanie.

Zatem szansa czy gwóźdź do trumny?

Wyzwania powinniśmy próbować przekuwać w sukcesy, mimo że poruszone struny mogą nie brzmieć optymistycznie. Problemy demograficzne i obecnie obserwowane perturbacje na rynku pracy w Polsce mogą prowadzić do zwiększenia inwestycji w technologie, które będą zastępowały człowieka i tym samym podnosiły produktywność. Rozdrobnienie przemysłu może wpływać na większą elastyczność i szybsze dostosowywanie się do koniecznych zmian. A technologie informatyczne, które wykorzystujemy m.in. do komunikacji, będą wymuszać współpracę. Na końcu bowiem wszyscy pozostajemy ludźmi i im więcej człowieczeństwa zachowamy, tym większej liczbie ludzi pomogą w życiu zdobycze czwartej rewolucji przemysłowej.

Bardzo ważną rolę w zmianie może także odgrywać świadomy konsument. To w końcu on dokonuje wyborów na rynku. Nowoczesne metody komunikowania pomagają konsumentom zdobywać informacje, stwarzając możliwość dialogu pomiędzy dostawcą produktów czy usług oraz tymi, którzy je kupują. Jeśli dostrzegalny będzie rozdźwięk między deklaracjami firmy a rzeczywistością, którą oferuje, sukces tego podmiotu jest wątpliwy.

ŚWIAT PRZEMYSŁU ZMIENIA SIĘ NA NASZYCH OCZACH

Dominika Bettman,
prezeska Siemens Polska

Świat przemysłu zmienia się na naszych oczach. Wraz z postępem technologicznym większość „analogowych" narzędzi, takich jak młotek czy spawarka zastępowanych jest przez urządzenia ery cyfrowej, czyli komputery, elektroniczne urządzenia diagnostyczne i panele do obsługi robotów.

W tak zmienionym otoczeniu to wiedza pracowników decyduje o przewadze konkurencyjnej przedsiębiorstw i właśnie wiedza oraz kompetencje cyfrowe są kluczem do rozwoju zakładów w XXI wieku. Zmiany w sposobie produkcji, które dokonują się na naszych oczach określamy mianem nowej, czwartej rewolucji przemysłowej. Cyfrowość obejmuje nie tylko produkty, z których korzystamy – „inteligentne" pralki, ekspresy do kawy czy samochody. Samo wytwarzanie wspomagane jest najnowszymi cyfrowymi technologiami – sztuczną inteligencją, komunikacją urządzeń w tzw. Internecie Rzeczy, przetwarzaniem dużej ilości danych *(Big Data)* z czujników umieszczanych na liniach produkcyjnych i w działających produktach, pozwalających monitorować ich zachowanie. Dzięki tym technologiom możemy doskonalić produkcję, wykrywać wady na wczesnym etapie i korzystać z potrzebnych nam rzeczy w sposób bardziej ekonomiczny.

Gospodarka w dobie czwartej rewolucji przemysłowej potrzebuje kadr, które sprostają wyzwaniom związanym z jej modernizacją oraz cyfryzacją. Współczesnego, a jeszcze bardziej przyszłego inżyniera charakteryzować będzie specyficzny zestaw umiejętności, łączący takie dziedziny jak mechatronika czy informatyka przy jednoczesnej zdolności do rozumienia całości procesów technologicznych specyficznych dla poszczególnych branż produkcyjnych.

Przemysł polski potrzebuje zatem nowych kadr o kompetencjach interdyscyplinarnych. Siemens dąży to tego, by wśród nich znalazły się także kobiety. Grupą, zasługująca w naszej opinii na szczególną uwagę, zwłaszcza w kontekście potrzeby łączenia różnych obszarów wiedzy, są studentki, czyli przyszłe inżynierki. Siemens stara się w sposób szczególny docierać do młodych kobiet studiujących na polskich uczelniach technicznych i przedstawiać im nowe perspektywy kariery zawodowej, zachęcając jednocześnie do rozwijania kompetencji zwłaszcza w obszarze łączącym umiejętności tzw. miękkie ze znajomością nowych technologii Industry 4.0.

BIO

Julia Patorska
Ekspert w obszarze analiz ekonomicznych i społecznych w Deloitte. Doradza w zakresie prognozowania wpływu planowanych regulacji i zmian realizowanych polityk na gospodarkę i społeczeństwo, prowadzi badania nad rozwojem branż i rynków. Jest przewodniczącą Rady Towarzystwa Ekonomistów Polskich (TEP) i ekspertem Centrum Badań i Analiz Pracodawców RP.

DŻUNGLA MIASTA

Rozpoczynamy serię artykułów o bezpieczeństwie. Inspiracji do powstania cyklu dostarczył poradnik Jacka Pałkiewicza „Dżungla miasta. Klucz do bezpieczeństwa". Na łamach „a&s Polska" partneruje mu wieloletni praktyk zarządzania bezpieczeństwiem Jacek Tyburek. Wspólnie przedstawią swój punkt widzenia na bezpieczeństwo w jego różnych aspektach.

Jacek Pałkiewicz, Jacek Tyburek

Myśląc o współczesnych miastach, zwłaszcza metropoliach, trudno o lepszą nazwę niż „dżungla". Określenia typu „betonowa dżungla" zazwyczaj sugerują siłę, dynamikę, czasami drapieżność i tempo życia w mieście. W tym kontekście porównanie do dżungli jest trafne, z jednym wszak zastrzeżeniem. Duże miasto, szczególnie metropolia, to organizm bardziej skomplikowany i wystawiający swoich mieszkańców na zagrożenia znacznie bardziej różnorodne. W tropikalnym lesie zabłąkany wędrowiec może stracić życie, bo się zgubi, coś go pożre, utopi się czy coś go śmiertelnie ukąsi. Lista zagrożeń jest spora, ale nie aż tak różnorodna jak w dzisiejszym mieście, które jest dżunglą do potęgi. Tak też chcemy na nie spojrzeć, bez opisywania możliwości urządzeń, systemów czy rozwiązań organizacyjnych. Tę pracę wykonują profesjonalnie eksperci. Autorski duet Jacek&Jacek ma ambicję spojrzeć na bezpieczeństwo życia miejskiego z innej perspektywy.

Bezpieczeństwo w przemyśle

Praktyka wskazuje, że elementami, które są warunkiem koniecznym zapewnienia bezpieczeństwa w zakładzie przemysłowym i jego otoczeniu, są: właściwe rozpoznanie zagrożeń (analiza ryzyka), system narzędzi prewencyjnych oraz umiejętność skutecznego reagowania na materializujące się zagrożenia.

Truizmem jest twierdzenie, że system jest tak skuteczny, jak jego najsłabsze ogniwo. Truizmy mają jednak coś z mądrości ludowych, tzn. mogą wywoływać uśmiech politowania, lekkie zdenerwowanie u osobowości bardziej wymagających albo zadumę u mniej skłonnych do zbytniego zgłębiania materii. Jedno natomiast jest bezdyskusyjne – zarówno z mądrości ludowych, jak i truizmów przebija doświadczenie z trudnym do zmierzenia stażem i trudną do policzenia powtarzalnością.

Doświadczenie w temacie skuteczności reakcji na zdarzenia niepożądane w przemyśle podpowiada, że kluczowych jest kilka kwestii: czas reakcji, właściwe skoordynowanie działań, niepopadanie w panikę oraz umiejętna i adekwatna komunikacja na temat zdarzenia. Co może być trudnego w takim zgraniu działań służb zakładowych, żeby sprawnie zarządzić incydentem? Dlaczego jakieś zdarzenie miałoby wywoływać nerwowość czy wręcz panikę i po co w to mieszać komunikację zakładów lub grupy zakładów?

W dobrze zorganizowanym przedsiębiorstwie przemysłowym, zwłaszcza gdy jest to firma o bogatej historii i wysokiej kulturze organizacyjnej, tego rodzaju kwestie nie powinny stanowić jakiegokolwiek problemu. Działają tu różne służby, zarówno porządkowe, jak i ratownicze, które mają struktury, dyżury, telefony kontaktowe, kamery, czytniki, czujniki, ekrany, aplikacje itd. Każda z tych służb odbywa szkolenia, w newsletterach pojawiają się „przypominacze", a niektóre muszą nawet raportować służbom państwowym, bo taki jest wymóg prawny.

Rzeczywistość zakładów przemysłowych jest dużo bardziej złożona niż wyłaniająca się z prezentacji w PowerPoincie na temat bezpieczeństwa. Obiekty przemysłowe są organizmami niezwykle skomplikowanymi. Poziom skomplikowania zwiększa się wraz z ich wielkością, skalą działania, zaawansowaniem technologicznym produktów czy wreszcie branży, w której działają, lub sektora gospodarki. Należy więc przyjąć zasadę, że w obiektach przemysłowych „im bardziej, tym bardziej i trudniej". Zasada ta dotyczy szczególnie bezpieczeństwa i reagowania na incydenty.

Bo czym są incydenty w takim obiekcie? Czy będą je tak samo rozumieli zakładowy strażak, szef bezpieczeństwa, szef służby BHP, szef zakładowej służby zdrowia, prawnik, specjalista IT czy wreszcie szef HR, zakładowy specjalista środowiskowy i rzecznik prasowy? Doświadczenie podpowiada, że zdecydowanie nie. Każda z tych służb czy osób na to samo zdarzenie spojrzy z innej perspektywy – innych przepisów, regulacji, procedur. Dla jednych to samo zdarzenie będzie ogromne i krytyczne, inni odnotują je bez emocji.

Czy incydent, zdarzenie, wypadek, sytuacja kryzysowa to synonimy opisujące to samo zdarzenie przez wszystkich interesariuszy? Czy wymienione wcześniej służby zareagują tak samo, czy zastosują podobne działania? Czy wreszcie powiadomią siebie nawzajem o zdarzeniu i w jakiej kolejności?

Są zapewne zakłady przemysłowe, które na wszystkie z tych pytań mogą udzielić pozytywnych i właściwych odpowiedzi. W pozostałych – środowisko osób odpowiedzialnych za bezpieczeństwo przemysłowe powinna „zjeść" profesjonalna zazdrość, która wywoła jednocześnie ambicję zbudowania podobnego systemu u siebie w firmie. Można jednak mieć obawy, że nie istnieje wiele takich obiektów...

Powiadamianie służb

Przygotowanie sprawnego systemu jest nie lada sztuką i proces budowy go napotyka wiele raf. Jednym z podstawowych czynników krytycznych jest skuteczność powiadomienia służb o zdarzeniu. Rzadko to służby same z siebie lokalizują incydent lub inne poważniejsze zdarzenie. Zazwyczaj to osoby znajdujące się najbliżej problemu są naocznymi świadkami lub pierwszymi odkrywcami trudnej sytuacji. Taka osoba musi powiadomić odpowiednie służby.

Pytanie pierwsze – czy wie, jak to zrobić? Każdy z nas zna numer 112. Nie wchodźmy w dyskusję na temat sposobu działania 112. Jego niewątpliwą zaletą jest to, że jest powszechnie znany, co ważne – łatwo z niego skorzystać. Nie potrzebujemy prefiksów, instrukcji, po prostu wybieramy 112 i czekamy na reakcję operatora. Czy mamy pewność, że w zakładach przemysłowych, które znamy, są takie numery telefonów alarmowych?

Kolejne pytanie, jakie należy zadać, to czy świadomość istnienia takiego telefonu jest

powszechna wśród pracowników i podwykonawców? Często problemem jest zapewnienie różnych możliwości dodzwonienia się na telefon alarmowy, szczególnie gdy firma jest zakładem wieloobiektowym, rozproszonym w terenie. Jeden numer telefonu, bez skomplikowanych prefiksów, identyczny dla telefonów służbowych i prywatnych, zarówno komórkowych, jak i tradycyjnych, stojących na biurkach, jest wyzwaniem technicznym. Wyzwaniem organizacyjnym jest z kolei takie komunikowanie ścieżki powiadamiania o incydentach, aby była ona utrwalona w pamięci pracowników i gości na terenie zakładu, by nie stanowiła problemu w sytuacji stresu.

Specyfika telefonu 112 jest taka, że rozmowa jest kierowana do operatora, który po krótkim wywiadzie na temat zdarzenia właściwie je adresuje. Zdarzenie zgodnie ze specyfiką otrzymuje swojego „opiekuna", który rozwiązuje problem. Identycznie jest w zakładzie przemysłowym. W każdym razie tak być powinno. Oznacza to ni mniej, ni więcej, że właściwie zorganizowany system bezpieczeństwa zakładu powinien mieć centrum nadzoru i monitoringu. Powinno ono multidyscyplinarne, a ludzi w nim pracujących należy bardzo starannie dobierać i regularnie szkolić. Na polskim rynku działają już firmy, które profesjonalnie przygotowują pracowników centrum monitoringu.

Rozwiązanie operacyjne oparte na zautomatyzowanych procesach IT, ze sprawnym procesem komunikacji, dostosowanym do procedur przekazywania zadań i korzystania z systemów bezpieczeństwa mogłoby być hitem sprzedaży.

Usługi takie, czyli centrum monitoringu z *hot line* można również zorganizować na zasadach *outsourcingu*, ale jest to niezwykle trudne do skutecznego przeprowadzenia. Wymaga znacznie dokładniejszego procesu przejęcia usługi i jej zorganizowania. Podjęcie takiej decyzji wymaga wielkiej rozwagi i związania się ze sprawdzonym partnerem.

Centrum monitoringu i nadzoru musi mieć stały personel pracujący w trybie ciągłym 24/7/365. Jego budowa to proces również bardzo skomplikowany, gdyż wymaga współpracy wielu służb, zbudowania zaufania do działania centrum, któremu de facto najbliżej jest z podległością firmowemu Działowi Bezpieczeństwa. Pracownicy centrum muszą więc przyjąć informacje o zdarzeniu w sposób kompleksowy i gwarantujący zdobycie o nim możliwie dużo wiadomości. Muszą takiej informacji nadać bieg, uruchomić właściwe służby. To od tych ludzi może zależeć życie i zdrowie, ale też dzięki ich właściwemu działaniu incydent ma szansę nie rozwinąć się do poziomu sytuacji kryzysowej.

Nigdy nie wiadomo, czy dany przypadek jest jeszcze incydentem, czy już zdarzeniem, a może wręcz wypadkiem. A może jednocześnie nosić cechy zdarzenia, wypadku BHP, uszczerbku na zdrowiu i mieć charakter kryminalny. Które służby wtedy uruchomić, kto ma priorytet? Kogo powiadomić? W działaniach pracowników centrum nie ma przypadkowości. Jest głębokie przeszkolenie, często odnawiane, znajomość organizacji i umiejętność pracy w sytuacji stresu. Przygotowania organizacyjne w postaci posiadania własnego lub w *outsourcingu* centrum nadzoru i monitoringu musi być wsparte niezawodnymi technologiami.

Ściana ekranów, pracownicy maksymalnie skupieni nad obrazem z kamer lub/i innych systemów, w tym systemów operacyjnych, integrujących pozostałe systemy bezpieczeństwa i zarządzanie obiektem w wysokiej jakości operacyjnej platformy integrującej jest typowym obrazem, ale w żadnym stopniu nie przesadzonym. Dobrze funkcjonujące centrum monitoringu i nadzoru musi być wyposażone w systemy telewizji przemysłowej, system alarmowy, wizualizacje systemu ppoż. i innych krytycznych dla obiektu przemysłowego systemów.

Brak pełnej integracji systemów w jednej platformie sterującej jest natomiast czynnikiem kosztotwórczym. Powiadamianie o zdarzeniach niekorzystnych, możliwość prowadzenia komunikacji z osobami decyzyjnymi oraz pracownikami uczestniczącymi w usuwaniu skutków incydentu znacząco poprawia sprawność operacyjną i niesie korzyści synergii.

Rynek proponuje narzędzia, które do tego typu zdarzeń mogą być użyte. Praktyk wskazuje jednak, że w większości przypadków wymagają one dostosowania, szycia na miarę. Czasami problemem jest struktura aplikacji, jej strony prawna i własnościowa. Duże firmy korporacyjne niechętnie zgadzają się na wprowadzenie w swój krwiobieg systemów IT obcych rozwiązań. Występowanie o tego typu zgody, badania zgodności oraz mierzenie ryzyka przekazywania danych do nie swoich rozwiązań IT często na tyle zniechęca do przechodzenia przez proces, że w końcu takie projekty upadają.

A rozwiązanie operacyjne oparte na zautomatyzowanych procesach IT, ze sprawnym procesem komunikacji, dostosowanym do procedur przekazywania zadań, korzystania z systemów bezpieczeństwa mogłoby być hitem sprzedaży.

Zarządzanie incydentem

Zarządzanie incydentem w zakładzie przemysłowym to przede wszystkim sprawna komunikacja, podział kompetencji i wypracowane procedury działania. Przy czym komunikacja stanowi nerw całej operacji.

Z jednej strony zawsze w sytuacji trudnej naturalnym mechanizmem ludzkim ujawniającym się jest ciekawość. Ludzie chcą wiedzieć, co się stało. Dlaczego na teren zakładu wjeżdża na sygnale karetka pogotowia, straż pożarna lub widać umundurowanych policjantów?

Zmorą służb ratunkowych i odpowiadających za bezpieczeństwo są telefony od wielu osób. Problem pojawia się, gdy członkowie zarządu o incydencie dowiadują się nie od szefa bezpieczeństwa czy BHP, ale od przypadkowych osób, z plotek, e-maili i innych komunikatorów. Nigdy nie pomogą akcji ratunkowej zdenerwowany prezes i jeszcze bardziej zdenerwowany członek zarządu, który nie wie, co odpowiedzieć prezesowi, bo jeszcze nie uzyskał informacji od szefa bezpieczeństwa.

Sytuacja staje się jeszcze trudniejsza, gdy informacje o incydencie zaczynają wypływać poza firmę w niekontrolowany sposób przez media społecznościowe, udzielanie informacji mediom w wywiadach itp. Duży obiekt przemysłowy może być źródłem niepoliczalnych ilości oraz charakterystyk incydentów i wypadków. Bardzo łatwo mogą się one przerodzić w kryzys zarówno wewnętrzny, zagrażający ciągłości produkcji, jak i zewnętrzny (np. w sytuacjach opisywanych przez Jacka Pałkiewicza w „Dżungli miasta…"). Zanieczyszczenie środowiska, skażenie terenu czy stworzenie zagrożenia życia ludzi w mieście, w którym funkcjonuje zakład, lub ekosystemu, jeśli firma prowadzi swoją produkcję na obrzeżach miasta, to potencjalne zdarzenia z długiej listy.

Budowanie sprawnego systemu reagowania na incydenty i inne zdarzenia wymaga inwestycji w rozwiązania techniczne, ale również zgrywania procedur wszystkich służb z terenu zakładu przemysłowego. Każda z nich ma swoich szefów, bywa, że raportują oni do różnych dyrektorów strukturalnych i członków zarządów. Przekonanie tych osób do tego, żeby dopasować wzajemnie procedury działania, swoje przyzwyczajenia i przekonania o wyższości własnej służby, zazwyczaj jest trudne.

Oddanie części władzy operacyjnej nad służbą na rzecz centrum monitoringu i nadzoru, które musi podlegać jednej ze służb (np. ochronie zakładu, rozumianej jako dział bezpieczeństwa, a nie firmą ochrony osób i mienia), może stanowić problem, głównie mentalny i organizacyjny. Nie są to jednak trudności, których nie da się rozwiązać.

Pomocne jest stałe i konsekwentne analizowanie każdego przypadku i incydentu na terenie zakładu przemysłowego. Gdy zaczyna się liczyć wszystkie zdarzenia, badać ich źródła i zaangażowane siły oraz uruchomione procedury, okazuje się, że wachlarz zdarzeń jest bardzo szeroki, ich liczba niemała, a zakład przemysłowy jest stale narażony na zagrożenia integralności i ciągłości produkcji. Odporność organizacji jest funkcją przygotowania do reagowania na zdarzenia, umiejętności rozpoznania, czy incydent ma potencjał do rozwinięcia się w poważny kryzys, czy jest łatwy do zażegnania.

W przemyśle zdolność do wychwycenia nieprawidłowości w fazie incydentu, który nie eskalował do poziomu zdarzenia, wypadku czy kryzysu, stanowi test jakości polityki bezpieczeństwa.

System reagowania na incydenty i zdarzenia jest jednym z podstawowych zadań polityki bezpieczeństwa i odporności przedsiębiorstwa produkcyjnego. Spina inne podsystemy – techniczne (telewizji przemysłowej, kontroli dostępu, różne systemy alarmowe) i powiadamiania o nieprawidłowościach w działaniu infrastruktury obiektu, a także proceduralne.

W przemyśle zdolność do wychwycenia nieprawidłowości w fazie incydentu, który nie eskalował do poziomu zdarzenia, wypadku czy kryzysu, stanowi test jakości polityki bezpieczeństwa.

Budowanie sprawnych służb wyspecjalizowanych w obsłudze obiektu, które w przypadku sytuacji trudnej przeistaczają się w zespół reagowania, jest zadaniem logicznym i oczywistym. Dlaczego jednak ciągle tak rzadkim? W gronie specjalistów warto podjąć dyskusję nad stworzeniem modelu zarządzania bezpieczeństwem i odpornością zakładów przemysłowych.

BIO

Jacek Pałkiewicz
Reporter, jeden z najbardziej aktywnych podróżników i eksploratorów naszych czasów. Trener i twórca pierwszej szkoły survivalu w Europie. Członek rzeczywisty Królewskiego Towarzystwa Geograficznego w Londynie.
Na swoim koncie ma wiele osiągnięć i wyróżnień, m.in. odkrycie źródła Amazonki, szkolenia kosmonautów i jednostek antyterrorystycznych.
Autor ponad 40 książek i wielu publikacji w prasie międzynarodowej.

BIO

Jacek Tyburek
Menedżer bezpieczeństwa organizacji. Doświadczenie zdobywał w różnych obszarach bezpieczeństwa; od przemysłu i logistyki, przez BPO, po bezpieczeństwo w rzeczywistości wirtualnej. Promotor pojęcia *Organisational Resilience*. Entuzjasta bezpieczeństwa miast, realizujący swoją pasję w powstającej pracy doktorskiej.

JAK SKUTECZNIE CENTRALIZOWAĆ

ZARZĄDZANIE BEZPIECZEŃSTWEM ORGANIZACJI

Co oznacza centralne zarządzanie bezpieczeństwem organizacji? **Przygotowując firmę do tego procesu, trzeba brać pod uwagę wiele czynników, by czerpać korzyści z takiej formy funkcjonowania, unikając przy tym jej negatywnych aspektów.**

Rafał Łupkowski

W swojej dotychczasowej karierze zawodowej miałem przyjemność budować bezpieczeństwo w korporacjach o strukturze wielooddziałowej i do tego najchętniej z racji doświadczenia się odnoszę. Naturalną konsekwencją była także bardzo podobna specyfika oddziałów, choć nie zawsze forma prawna (np. franczyza) umożliwiała bezproblemową centralizację.

Pierwszy, najbardziej wymowny przykład zarządzania bezpieczeństwem, który wzbudził we mnie bezwzględną konieczność wprowadzenia standardów zunifikowanego zarządzania, sięga kilkunastu lat wstecz. W ówczesnej strukturze instytucji finansowej funkcjonowało na terenie kraju ok. 50 oddziałów i każdy z nich był swego rodzaju „księstwem" samodzielnie radzącym sobie z wszelkimi usługami i systemami w zakresie bezpieczeństwa.

Zarząd, chcąc budować scentralizowaną formułę zarządzania organizacją, zalecił wytypowanie jednego dostawcy usług w obszarze bezpieczeństwa fizycznego. I tak też się stało. Jakież było moje zdziwienie, gdy tuż po przetargu, obejmując obszar bezpieczeństwa fizycznego, odkryłem, że co prawda jeden dostawca świadczy określony zakres usług, ale każdy oddział ma co najmniej trzy usługi, a każdą z nich określa odrębna umowa z rzeczonym dostawcą. Dawało to łącznie, jak łatwo policzyć, około 150 umów! Co więcej, w zależności od regionu, ceny usług się różniły.

Nie zapomnę pierwszego miesięcznego rozliczania kosztów bezpieczeństwa – pamiętam, że chciałem uciec jak najdalej (czytaj: zmienić czym prędzej pracę). Na szczęście proces ten w takim wydaniu już się nie powtórzył.

WNIOSEK NR 1:

Planując centralizację, należy wziąć pod uwagę stronę formalną, a nie tylko kosztową i operacyjną przedsięwzięcia.

Oczywiście strona formalna została „wyprostowana" dość szybko i stałem się jednym z pierwszych szczęśliwych zarządzających – trzech umów sieciowych dla 50 oddziałów w pełni kontrolowanych przez centralę organizacji, w tym mój zespół.

Jak łatwo się domyśleć, proces taki (zwłaszcza że owa instytucja dorobiła się docelowo struktury 440 oddziałów) cyklicznie powtarzał się przez lata. Jednak raz osiągnięte efekty skali i skuteczności procesu zarządzania były tylko udoskonalane, a ja dla określonego wzoru postępowania stałem się zagorzałym zwolennikiem wprowadzania strategii i jej realizacji na poziomie centrali, co dawało określone korzyści:

– synergie kosztowe dzięki efektowi skali,
– łatwość i przejrzystość w kreowaniu budżetu i zarządzaniu nim,
– możliwość korzystania z szerszej palety różnorakich rozwiązań,
– bezpośrednie przełożenie na zarządzany obszar poprzez nadzór umów i kosztów,
– łatwiejsze badanie i egzekwowanie jakości usługi,
– bardziej skuteczna reakcja na incydenty,
– lepsze wsparcie.

Przedstawiona lista stanowi tylko część z licznych zalet centralnego zarządzania obszarem bezpieczeństwa. Są także aspekty negatywne, które stanowią tzw. drugą stronę medalu, nie przysłaniają one jednak wielu zalet z tym związanych. Nie mniej ciekawie termin centralizacja odnosi się do aspektów systemowo-sprzętowych, lecz w tym przypadku dobra umowa i jej wdrożenie raczej nie wystarczą.

W dobie rozwoju systemów zabezpieczeń, mając sporą swobodę w wyborze i rekomendacji rozwiązań, zdarzyło mi się wdrożyć swoistego „mercedesa" w zakresie systemów sygnalizacji włamania i napadu (SSWiN). Centrala alarmowa miała niesamowite możliwości, z powodzeniem mogła obsługiwać inteligentne budynki – świetnie zatem sprawdziła się w budynku centrali, nie mniej dobrze działała w małym oddziale. W miarę rozwoju sieci oddziałów okazało się, że ten „mercedes" wymaga zupełnie innego rodzaju serwisu, a co za tym idzie koszty niewspółmiernie rosły. Ponadto potrzebował specjalnie oddelegowanego serwisanta, a wiedza, ponieważ okazała się rzadka, była niezwykle pożądana i cenna. Na szczęście każdy system kiedyś się amortyzuje, a jego wymiana pozwala wyciągnąć wnioski pod warunkiem zarządzania obszarem przez tę samą jednostkę i dokonanie autorefleksji.

WNIOSEK NR 2:

Centralizując i unifikując systemy, należy brać pod uwagę własne potrzeby w odniesieniu do specyfiki zabezpieczanego obszaru, a także uwzględniać łatwość i dostępność komponentów do późniejszej eksploatacji, w tym możliwości integracji.

Najciekawsze doświadczenia płynęły z centralizacji systemów telewizji dozorowej, ponieważ wraz z rozwojem sieci teleinformatycznych obszar ten można określić terminem *Sky is the limit* – dzisiejsze możliwości integracji na poziomie zarówno sprzętowym, jak i programowym są nieograniczone. Ze względu na specyfikę bezpieczeństwa biznesu warto przytoczyć pewne wydarzenie.

Ponad dziesięć lat temu z kilkoma uznanymi na rynku ekspertami miałem przyjemność opracować na potrzeby swojej organizacji oraz wdrożyć system wideoweryfikacji alarmów na skalę krajową. Jak się później okazało, byliśmy w tym obszarze prekursorami, jednak kluczowym elementem było to, że unifikacja sprzętu i oprogramowania była wypadkową do realizacji dodatkowej usługi przez firmy świadczące usługi w zakresie ochrony mienia, wraz z usługami powiązanymi.

Podzielenie się wiedzą i doświadczeniem w zakresie przeprowadzonego projektu pozwoliło na wdrożenie go w identycznej niemal formie w innej organizacji o tożsamej specyfice. Prawdziwy sukces projektu przyszedł po kilku latach, gdy obie organizacje przeprowadziły fuzję, o której na etapie wymiany doświadczeń nikt nawet nie myślał. W rezultacie połączenie dwóch instytucji finansowych na poziomie sprzętowym odbyło się płynnie, bez konieczności wymiany kluczowych urządzeń, co stanowiło istotną synergię kosztową.

WNIOSEK NR 3:

Dobierając rozwiązania techniczne zarządzane centralnie, warto myśleć o uniwersalnej formule platformy, a także korzystać z doświadczeń innych.

Centralizacja zarządzania obszarem bezpieczeństwa w ujęciu korporacyjnym stała się faktem.

Trzeba jednak wymienić kilka głównych aspektów mogących niejako negatywnie wpływać na proces po jego centralizacji.

- Wydłużenie procesu decyzyjnego w zakresie projektu (nie może dotyczyć sytuacji kryzysowych przy prawidłowo prowadzonym procesie zarządzania sytuacją kryzysową czy incydentem bezpieczeństwa).
- Brak bezpośredniego wpływu na koszty na poziomie lokalnym (koszty przy centralizacji powinny być zarządzane centralnie – można jednak delegować uprawnienia kosztowe do pewnego poziomu, przy zachowaniu zasady stopniowania kontroli).
- Nienależyte rozpoznanie potrzeb danej jednostki (błąd dotyczy badania przed fazą wdrożenia projektu – warto słuchać głosu oddziału oraz testować i konsultować rozwiązania, jednak w ściśle określonym zakresie).
- Zaburzenia w procesie zgłaszania nieprawidłowości w systemie czy usłudze zarządzanymi centralnie (prawidłowy, cykliczny proces badania jakości).

Im więcej przykładów negatywnych, tym gorzej opracowany projekt i samo wdrożenie, co negatywnie wpływa na zarządzającego – a przecież nie ma wątpliwości, że właściwie wdrożony i zarządzany na poziomie centrali proces bezpieczeństwa ma służyć organizacji i wspierać, a nie utrudniać jej podstawową działalność operacyjną.

Aby skutecznie centralizować lub wprowadzać procesy w obszarze bezpieczeństwa, należy zacząć przede wszystkim od potrzeb, a następnie tworzyć strategię adekwatną do potrzeb, z założeniem zrównoważonego rozwoju danej usługi czy systemu w organizacji.

Ostatnio zetknąłem się z kilkoma przypadkami wdrażania systemów zabezpieczeń bez jakichkolwiek kryteriów i ich korelacji ze specyfiką działalności i usługami, w myśl zasady „ginie... więc załóżmy kamery". A może wystarczy zamknąć drzwi? Co powoduje, że centralne zarządzanie usługami i systemami w zakresie bezpieczeństwa przynosi wartość dodaną dla organizacji? Co decyduje o skuteczności takich działań?

Moim zdaniem wpływa na to kilka istotnych czynników:

- Centralizacja zarządzania obszarem bezpieczeństwa musi być wpisana w strategię organizacji.
- Zakres centralizacji musi odpowiadać poziomowi rozwoju organizacji.
- Prawidłowo przeprowadzona i zorganizowana centralizacja odbywa się na poziomach: formalnym, zarządczym i operacyjnym (wykonawczym).
- Kluczowym narzędziem w centralnym zarządzaniu obszarem jest odpowiednia komunikacja na wszystkich wymienionych poziomach.
- Narzędziem niezbędnym, wspierającym procesy są właścicielstwo biznesowe lub kluczowy wpływ na regulacje, budżet i umowy.
- Centralizacja zarządzania musi cyklicznie badać i uwzględniać zmiany specyfiki organizacji, w tym zakładać delegowanie uprawnień i ich kontrolowanie.
- Centralizacja „za wszelką cenę" przez pryzmat jednej zmiennej, np. kosztów, jest nieskuteczna.

Nawet najlepiej zarządzane przedsiębiorstwo realizujące swoją strategię na podstawie metodologii SIX SIGMA nie byłoby prawie doskonałe, gdyby nie przystosowywało się do zachodzących zmian. A zatem każdy, nawet najlepiej przygotowany proces musi być cyklicznie weryfikowany, a jego właściciel biznesowy powinien o każdej porze dnia i nocy wiedzieć, po czym poznać skuteczność wprowadzanych zmian. Autorefleksja i zdolności adaptacyjne wydają się kluczem do sukcesu każdego, kto zdecyduje się szybko podjąć takie wyzwanie, w przeciwnym razie skala zaniedbań będzie rosła.

BIO

Rafał Łupkowski
Pasjonat i wieloletni praktyk zarządzania bezpieczeństwem biznesu w korporacjach międzynarodowych, współtwórca Kongresu Security. Niezależny doradca w obszarze bezpieczeństwa biznesu – właściciel firmy SecurityBroker.

CYBERBEZPIECZEŃSTWO FIRMY i ORGANIZACJI

UWARUNKOWANIA I WYMOGI[1]

Cyberprzestrzeń stała się obszarem działania organizacji sektora prywatnego równie ważnym, jak płaszczyzna materialna. Równolegle podejmowane działania w rzeczywistości materialnej i wirtualnej są traktowane jako powiązane i niezbędne obszary działania podmiotów z sektorów prywatnego i publicznego.

Krzysztof Liedel,
Paulina Piasecka

Ta konstatacja wpływa na sposób postrzegania zagrożeń w cyberprzestrzeni i warunkuje potrzebę analizy istniejących i prognozowanych zagrożeń bezpieczeństwa jednostek biorących udział w życiu gospodarczym i społecznym. Cyberprzestrzeń stała się obszarem właściwej działalności organizacji, dla których informacja jest przedmiotem podejmowanych działań (np. firmy analityczne zajmujące się brokeringiem informacji) oraz firm i organizacji, które narzędzia informacyjne traktują jako niezbędny element zarządzania operacyjnego i wsparcia realizowanych działań na poziomie sterowania, komunikacji, gromadzenia informacji – budowania świadomości sytuacyjnej, zarządzania procesami logistycznymi i innych.

Zapewnienie cyberbezpieczeństwa powinno znajdować się na początku listy priorytetów nie tylko firm prywatnych. Stabilność gospodarcza państwa zależy m.in. od zdolności podmiotów gospodarczych do dostosowywania się do nowych wyzwań ekonomicznych i technologicznych oraz od tworzenia skutecznych rozwiązań organizacyjnych, aby im sprostać. Ekonomiczne wspieranie przez państwo inicjatyw związanych z cyberbezpieczeństwem w poszczególnych organizacjach, m.in. w ramach współpracy publiczno-prywatnej, polegające choćby na systemie zachęt związanych z szybkim reagowaniem na problemy cyberbezpieczeństwa i kar za nieadekwatne do skali problemu podejście (np. ulgi podatkowe lub ubezpieczenia na preferencyjnych warunkach), to ważne narzędzie budowania wspólnego bezpieczeństwa. Podobną rolę może odgrywać zwiększony nacisk państwa na właściwe projektowanie systemów cyberbezpieczeństwa, realizowany z uwzględnieniem roli rządu jako kluczowego odbiorcy cybertechnologii.

Do szerokiego wachlarza zagrożeń związanych z funkcjonowaniem w cyberprzestrzeni należą: dezinformacja, trolling, działania mające na celu naruszenie dobrego imienia firmy czy podważenie jej wiarygodności, zakłócające realizację istotnych zadań; ataki powodujące zakłócenia funkcjonowania sieci teleinformatycznych w organizacjach o podwyższonym stopniu wrażliwości, w tym tworzących infrastrukturę krytyczną; występowanie luk technologicznych, które pozwalają wywierać wpływ na zdolności do działania w cyberprzestrzeni. Do najważniejszych działań na rzecz cyberbezpieczeństwa organizacji należą:

- ocena warunków cyberbezpieczeństwa, w tym rozpoznawanie zagrożeń, szacowanie rodzajów ryzyka i identyfikowanie szans,
- zapobieganie (przeciwdziałanie) zagrożeniom, redukowanie różnych rodzajów ryzyka i wykorzystywanie szans,
- obrona oraz ochrona własnych systemów i zgromadzonych w nich zasobów,
- po ewentualnym ataku odtworzenie sprawności i funkcjonalności systemów tworzących cyberprzestrzeń.

Wśród praktycznych przedsięwzięć na rzecz zapewnienia efektywności działań w cyberprzestrzeni można wskazać m.in. posiadanie zdolności obrony oraz ochrony własnych systemów teleinformatycznych i zgromadzonych w nich zasobów, tworzenie i wzmacnianie struktur przeznaczonych do realizacji zadań w cyberprzestrzeni, bieżące monitorowanie i wzmacnianie bezpieczeństwa sieci stosowanych do dystrybucji i przechowywania informacji oraz wzmacnianie działań edukacyjnych zwiększających świadomość pracowników, członków organizacji o ich roli w zapewnieniu bezpieczeństwa w cyberprzestrzeni.

Większa zależność tempa i sposobu prowadzenia operacji bezpieczeństwa w środowisku sieciowym ma jednocześnie wiele negatywnych aspektów. Najważniejsze warunki brzegowe, które muszą być spełnione, aby w pełni wykorzystać potencjał systemów bezpieczeństwa w otoczeniu sieciowym, to: bezpieczeństwo transmisji danych, trwałość sygnału transmisji, przepustowość kanałów transmisyjnych, zdolność do właściwego ukierunkowania wiadomości i transmisji, kompatybilność sygnałów i protokołów[2].

Epoka informacji wymaga zmian nie tylko w sposobie działania, ale także w sposobie organizowania się – wymaga ewolucji starych lub powstania nowych struktur, które będą efektywnie odpowiadać na wyzwania współczesnego środowiska bezpieczeństwa. Dostosowanie struktur bezpieczeństwa do wymogów usieciowionego środowiska bezpieczeństwa to szczególne wyzwanie. Możliwość funkcjonowania w środowisku sieciocentrycznym wymaga budowy organizacji, które swoje cele osiągają poprzez elastyczność ról i działań oraz szybkość procesów sterowania[3]. Takie organizacje, wykorzystując zaawansowane technologie informacyjne, swoje działania opierają przede wszystkim na innowacyjnych strukturach kierowania, dążąc do jak najszybszego reagowania na pojawiające się wyzwania, zagrożenia i zmiany w zakresie świadomości sytuacyjnej.

Aby efektywnie funkcjonować w usieciowionym środowisku, organizacja musi mieć cechy samoprojektowania w trybie ciągłego dostosowywania się do nowych warunków. Teoria organizacji zawiera dwie koncepcje, które mogą posłużyć za bazę do rozważań nad powstaniem tego rodzaju organizacji – koncepcję modyfikowanych form organizacyjnych opartych na technologiach informacyjnych oraz koncepcję organizacji zdolnych do gwałtownej zmiany i innowacji[4]. Koncepcja modyfikowanych form organizacyjnych obejmuje takie podejścia, jak organizacje wirtualne, alianse strategiczne, partnerstwa i organizacje usieciowione.

Choć elastyczność i wielozadaniowość organizacji wirtualnej, jaką mogą być połączone siły zadaniowe, mają liczne zalety, nie można pominąć problemów związanych z ich użyciem. Wśród najważniejszych należałoby wskazać zależność efektywności wykonywanych działań od skuteczności komunikacji, która w organizacji nieprzetestowanej pod względem koordynacji może w kluczowym momencie zawieść. Problemy z określeniem statusu, autorytetu i zakresu kompetencji poszczególnych komponentów również mogą stanowić przeszkodę skutecznego działania. Odpowiedzią na te wyzwania może stać się dopracowana i szczegółowa doktryna działania, jednak i ona musiałaby być przez pewien czas wdrażana, aż do momentu wzajemnego rozpoznania się elementów takiego systemu[5]. Koncepcja organizacji zdolnych do innowacji i gwałtownej zmiany, by efektywnie dostosować się do nowych wyzwań, jest oparta na założeniu, że takie organizacje zmieniają się w trybie ciągłym, co jest warunkowane trudnymi warunkami (zasada „dostosowania się, aby przetrwać").

Wśród zaleceń dotyczących kształtowania skutecznych systemów cyberbezpieczeństwa warto zatem wskazać najważniejsze:

- postrzeganie zobowiązania do realizacji zadań w cyberprzestrzeni w taki sam sposób, jak w innych istotnych obszarach zapewniających bezpieczeństwo organizacji i firmy,
- przygotowanie „mapy drogowej" barier w obszarze cyberbezpieczeństwa wraz z planem wyeliminowania tych barier, harmonogramem i prognozami finansowymi,
- opracowanie i wdrożenie algorytmów działania, określających dobre praktyki i zasady działania na rzecz cyberbezpieczeństwa organizacji.

Choć uzależnienie od sieci i jej ciągłego wykorzystania na każdej niemal płaszczyźnie funkcjonowania organizacji, firmy czy jednostki stało się rzeczywistością, sporo jeszcze brakuje do realnego dostosowania struktur odpowiedzialnych za bezpieczeństwo do wymogów tego nowego środowiska. Jest to szczególnie prawdziwe dla struktur bezpieczeństwa. Ze względu na tradycyjne podejście do organizowania się oraz przywiązanie – także pod względem kultury organizacyjnej – do sztywnych hierarchicznych struktur ewolucja do postaci elastycznej, sieciowej organizacji może okazać się wyzwaniem nie na poziomie technologicznym, ale na poziomie możliwości mentalnego i psychicznego przystosowania zarówno kierownictwa organizacji, jak i jej poszczególnych członków.

Artykuł powstał na podstawie „Doktryny cyberbezpieczeństwa RP", wyd. BBN, Warszawa 2015, źródło: http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf

1) Analizy i wnioski powstały w toku badań prowadzonych podczas prac nad raportem „Cyberbezpieczeństwo. Piąte pole walki Diagnoza i rekomendacje", K. Liedel, P. Piasecka, IBK 2016.
2) Carlo Kopp: *Understanding Network Centric Warfare*, www.ausairpower.net/TE-NCW-Jan-Feb-05.html
3) Kishore Sengupta, Carl R. Jones, *Creating Structures for Network-Centric Warfare: Perspectives from Organization Theory*, Naval Postgraduate School, Monterey 1999, źródło: www.dtic.mil/dtic/tr/fulltext/u2/a458996.pdf, s. 1.
4) Ibidem, s. 3.
5) Ibidem, s. 3.

BIO

dr Krzysztof Liedel
Prawnik, specjalista w zakresie zwalczania międzynarodowego terroryzmu, ekspert w zakresie analizy informacji. Wiceprezes Instytutu Bezpieczeństwa RESCON. Dyrektor Centrum Badań nad Terroryzmem i kierownik Instytutu Analizy Informacji Collegium Civitas. Ekspert Sekcji ds. Zapobiegania Terroryzmowi Rady Bezpieczeństwa ONZ, International Association of Crime Analysts oraz International Association for Counterterrorism & Security Professionals.

dr Paulina Piasecka
Specjalistka ds. terroryzmu międzynarodowego i walki informacyjnej. Dyrektor ds. projektów strategicznych Instytutu Bezpieczeństwa RESCON. Wykładowca Collegium Civitas. Były główny specjalista w Wydziale ds. Przeciwdziałania Terroryzmowi w Departamencie Bezpieczeństwa Publicznego MSWiA.

G Data Software
ul. Warcisława IV 2
78-400 Szczecinek
www.gdata.pl

STATYSTYKI ZAGROŻEŃ W PIERWSZEJ POŁOWIE 2018 ROKU:

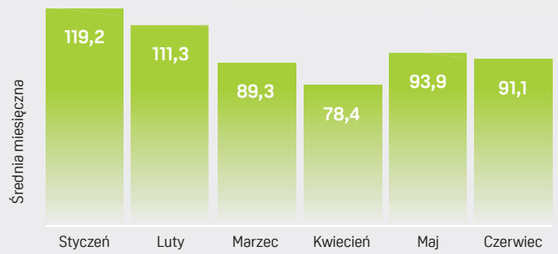
NIEBEZPIECZEŃSTWO CZAI SIĘ W SIECI

W obecnych czasach w większości przypadków złośliwe oprogramowanie rozprzestrzenia się w sieci – pliki wykonywalne stają się coraz mniej powszechnym problemem. Już w pierwszej połowie roku eksperci ds. zabezpieczeń firmy G DATA zauważyli specyficzną tendencję zagrożeń, które mogłyby okazać się niebezpieczne dla urządzeń.

Podobnie jak ma to miejsce w kontekście przemysłu IT, rozwój obecnie występujących grup złośliwego oprogramowania podlega znacznym zmianom. Pokazują to najnowsze analizy laboratorium zabezpieczeń G DATA Security Labs: dziewięć na dziesięć najszerzej rozpowszechnionych zagrożeń czyhających na użytkowników komputerów w poprzednich latach nie znalazło się w pierwszej połowie 2018 roku w grupie dziesięciu najczęściej wykrywanych zagrożeń. 70% z nich stanowią oprogramowania PUP, a 30% - *malware*. Poza tym ataki coraz częściej są przeprowadzane za pośrednictwem stron internetowych, a nie jak to miało miejsce w przeszłości, wyłącznie poprzez pliki wykonywalne.

– *Zgodnie z tradycyjnym podejściem złośliwe oprogramowanie rozprzestrzenia się głównie za pośrednictwem plików wykonywalnych. Obserwujemy jednak wyraźny wzrost liczby ataków przeprowadzanych za pośrednictwem stron internetowych, a niektóre z nich w ogóle nie wykorzystują plików* – mówi Ralf Benzmüller, główny przedstawiciel G DATA Security Labs – *Ataki za pośrednictwem makr w dokumentach biurowych również są powszechne i skłaniają użytkowników do interakcji. Najkrótszy w historii cykl rozwoju złośliwego oprogramowania pokazuje, że użytkownicy zyskają kompletną ochronę wyłącznie dzięki proaktywnym technologiom od G DATA Security Labs.*

Liczba ataków wykrywanych codziennie na 1000 użytkowników



Przedstawione dane liczbowe oparte są na statystykach zebranych przez G DATA Security Labs. Informacje zbiera inicjatywa informowania o złośliwym oprogramowaniu Malware Information Initiative (MII), w ramach której klienci G DATA mogą dobrowolnie przesyłać do firmy dane statystyczne na temat zidentyfikowanych oraz udaremnionych zagrożeń, co umożliwia przeprowadzenie dokładniejszej analizy bieżących próbek pod kątem obecnie panujących zagrożeń.

Rok 2018 do tej pory pod znakiem Cryptojackingu

Cryptojacking – tajemnicze kopanie kryptowalut, z reguły Monero – zyskał szczególne znaczenie w pierwszej połowie roku. Zwłaszcza w pierwszym kwartale, na wielu stronach internetowych ukrywano *Cryptominer* pobierający skrypty na komputer użytkownika i prowadzący do przeciążenia procesora. Jednak w niektórych przypadkach funkcje kopania walut można odkryć także w takich plikach wykonywalnych, jak gra Abstractionism dostarczana za pośrednictwem platformy Steam. Nie zawsze pozostaje jasne, czy użytkownicy wyrazili wcześniej zgodę na tego typu działanie. Z tego powodu G DATA klasyfikuje kopanie kryptowalut po części jako złośliwe oprogramowanie – w przypadku, gdy działaniu jednoznacznie przyświecają niecne zamiary – a w niektórych przypadkach jako „Potencjalnie Niechciany Program" (PUP). Trzy narzędzia do kopania kryptowalut znajdują się pośród dziesięciu najpowszechniejszych zagrożeń w formie złośliwego oprogramowania, a aż cztery takie narzędzia pośród dziesięciu najczęściej wykrywanych PUP-ów. Nowością jest to, iż Web Assembly w postaci kodu bajtowego jest wykorzystywany nie tylko w narzędziach do kopania kryptowalut działających za pośrednictwem stron internetowych, ale także w złośliwym oprogramowaniu. Web Assembly to dodatek do JavaScript, obecnie obsługiwany przez wszystkie popularne przeglądarki. Przy pomocy Web Assembly web developerzy są w stanie osiągnąć znacznie krótszy czas ładowania oraz szybsze wykonanie kodu – w ten sposób standard webowy staje się idealną technologią dla kopania monet.

Co istotne z technicznego punktu widzenia, coraz częściej złośliwe oprogramowanie wykorzystuje mniej znane funkcje systemu Windows w celu wykonywania złośliwych poleceń przy pomocy skryptów wierszy poleceń. Dla przykładu: eksperci z firmy G DATA z powodzeniem wykorzystali heurystyczne wykrywanie próbek złośliwego oprogramowania Voiv do blokowania licznych ataków wykorzystujących „zaplanowane zadania" w systemie Windows w celu wprowadzania zmian do systemu. Złośliwe oprogramowanie ukrywa się, podając się za proces związany z działaniem przeglądarki. W zależności od wersji wykonuje różne rodzaje kodu za pośrednictwem różnych silników skryptujących, które np. same aktualizują złośliwe oprogramowanie bądź ładują jego dodatkowe moduły.

TOP 10 – złośliwe oprogramowanie w Polsce

Rzekome wsparcie techniczne umarło. Niech żyje rzekome wsparcie techniczne

Zwłaszcza w miesiącach letnich eksperci firmy G DATA zauważyli powrót do dobrze już znanej metody oszustwa – opartego na rzekomym wsparciu technicznym. Użytkownik widzi zajmujące cały ekran wyskakujące okienko z informacją, że jego komputer został zainfekowany przez złośliwe oprogramowanie i konieczne jest jego odpłatne naprawienie. W tym celu należy zadzwonić pod numer rzekomej infolinii. Rozmówcy zazwyczaj podają się za pracowników firmy Microsoft i wywierają presję psychiczną na użytkowniku. Płatności zazwyczaj należy dokonać za pośrednictwem karty przedpłaconej iTunes. Tim Berghoff, specjalista ds. zabezpieczeń w firmie G DATA, skorzystał w zeszłym roku z okazji i odbył tego typu rozmowę z oszustem. Berghoff przedstawia bieżące doniesienia oraz wskazówki od G DATA o tym, jak radzić sobie z oszustami.

Wtyczki Adobe Flash to kolejny powszechny problem w kontekście zabezpieczeń. Luka z 2017 roku (CVE-2017-3077) uplasowała się na siódmej pozycji w rankingu udaremnionych zagrożeń wykrytych wśród klientów G DATA. W tym wypadku zmodyfikowany obraz w formacie PNG jest wykorzystywany po to, by wprowadzić złośliwy kod do komputera użytkownika i wykorzystać istniejące luki. Po utworzeniu tego rodzaju punktu wyjścia dla ataku powstaje możliwość załadowania kolejnych porcji złośliwego kodu. G DATA zaleca, by przestać korzystać z Adobe Flash Playera i odinstalować go. Jeśli nie wyobrażasz sobie takiego rozwiązania, pamiętaj, by zawsze niezwłocznie instalować aktualizacje.

Gracze, miejcie się na baczności!

Czwartą i ósmą pozycję w rankingu zajmują przypadki wykrycia generycznego złośliwego oprogramowania ukrywające się pod postacią scrackowanych wersji gier. Twórcy złośliwego oprogramowania często ukrywają swoje „dzieła" w grach, nie tylko na komputerach z systemem Windows, jako że wiele dzieci nie zdaje sobie sprawy z potencjalnych zagrożeń. W szczególności jeśli chodzi o system Android, gry dedykowane dla dzieci znajdują się na celowniku oszustów. Firma G DATA niedawno ostrzegała o pojawiających się fałszywych wersjach gry Fortnite na system Android.

Jeśli chodzi o wykrywanie Potencjalnie Niechcianych Programów (PUP), poza Monero Miners, nadal istnieją programy, które modyfikują ustawienia przeglądarki bez zgody użytkownika, – np. zmieniają stronę startową lub domyślną przeglądarkę bądź instalują irytujące paski narzędzi. „Open Candy" i „Mindspark"-Framework, ukryte głównie w instalatorach darmowego oprogramowania, które są w tym kontekście znane od lat. Nadal krążą po sieci, a rozwiązania od G DATA skutecznie je wykrywają. Co interesujące, oprogramowanie sklasyfikowane jako PUP, takie jak Win32. Application.DownloadGuide.T, które obecnie rozpoznaje również maszyny wirtualne, stara się w tym wypadku uniknąć wykrycia przez programy antywirusowe poprzez przyjęcie mniej agresywnej strategii działania.

Liczba odpartych ataków nieznacznie spada

Informacje o atakach udaremnionych w minionym półroczu docierają do nas odrobinę rzadziej niż w roku ubiegłym. Było to szczególnie widoczne w drugim kwartale 2018 roku.

Dane statystyczne pokazują również, że w zakresie złośliwego oprogramowania sytuacja znacząco różni się w poszczególnych krajach. Większość udaremnionych ataków złośliwego oprogramowania i PUP-ów została w pierwszej połowie 2018 roku odnotowana w Turcji, zostawiając daleko w tyle Izrael, który uplasował się na drugiej pozycji. W Turcji rozwiązania zabezpieczające od G DATA powstrzymały zwłaszcza ataki za pomocą dobrze znanych narzędzi do crackowania oprogramowania systemu Windows.

Liczba nowo powstających przykładów złośliwego oprogramowania również nieznacznie zmalała w pierwszej połowie roku w porównaniu z rokiem ubiegłym. Łącznie laboratoria G DATA wykryły 2 396 830 nowych przykładów złośliwego oprogramowania. Średnio wykrywano dziennie 13 000 nowych próbek złośliwego oprogramowania, co daje 9 na minutę. Benzmüller w ten sposób komentuje dane liczbowe: – *Przewidujemy, że w drugiej połowie roku liczba nowych przykładów złośliwego oprogramowania znów wzrośnie. W tym roku rekord prawdopodobnie nie zostanie pobity, chociaż indywidualne ataki stają się coraz bardziej wyrafinowane i ściśle ukierunkowane.*

Axis Partners' Day

W odrestaurowanych historycznych wnętrzach Hotelu Europejskiego odbyła się kolejna edycja dorocznej konferencji Axis Partners' Day. Axis Communications zgromadził 2 października liczne grono partnerów oraz ekspertów z branży. Podczas spotkania zostały przedstawione ciekawe rozwiązania oraz najnowsze trendy w zakresie dozoru wizyjnego.

Sukces Axis Communications na polskim rynku opiera się na ścisłej i rozległej współpracy z lokalnymi partnerami, dzięki którym firma odnotowała w pierwszym półroczu 2018 roku wzrost sprzedaży w Polsce o rekordowe 60% w porównaniu do roku minionego. Do zintegrowanej sieci należy ponad 2500 partnerów ADP *(application development partners*), którzy korzystając z otwartych kamer i enkoderów, tworzą szyte na miarę aplikacje dla użytkowników końcowych. Podstawą jest otwarta platforma Axis, która w prosty sposób daje możliwość rozszerzenia podstawowej funkcjonalności kamer. Jak co roku, firma Axis przyznała swoim partnerom nagrody w poszczególnych kategoriach. Tytułem Najlepszego Partnera Roku 2018 uhonorowano firmę mvb ze Szczecina. Najlepszym dystrybutorem z najbardziej dynamicznym wzrostem ogłoszono firmę Anixter, za najlepszy debiut roku uznano wyniki firmy Electrum, zaś wyróżnienie za dynamiczny wzrost otrzymała firma S-NOVA Security, a najciekawszy projekt przygotowała firma Instom.

Dużo uwagi poświęcono tematyce *smart city*. Dalibor Smažinka, Enterprise Solutions Manager na Europę Wschodnią w Axis Communications, na ciekawych przykładach potwierdził kierunek rozwoju monitoringu wizyjnego: *Punktem wyjścia dla władz lokalnych jest zapewnienie mieszkańcom poczucia bezpieczeństwa. Następny krok to usprawnienie zarządzania ruchem ulicznym, a wisienką na torcie jest stworzenie kompleksowych rozwiązań dla inteligentnego środowiska miejskiego, gdzie komfort życia mieszkańców powinien być wartością nadrzędną.*

Targi ADI expo 2018

Prawie 200 osób odwiedziło targi ADI expo 4 października w hotelu DoubleTree by Hilton w Warszawie. Dystrybutor zaprosił do prezentacji 25 czołowych producentów branży security, z których każdy zorganizował stoisko firmowe i poprowadził seminarium.

Podczas seminariów prelegenci poruszali istotne dla użytkowników kwestie związane z wykorzystaniem produktów i systemów security. Przedstawiciele producentów wiele uwagi poświęcili na omówienie nowości w ofercie swoich firm.

Bardzo nas cieszy frekwencja. W ubiegłym roku zanotowaliśmy wzrost o 50 proc., w tym roku odwiedziło nas o 30 proc. więcej uczestników – podsumowuje Maciej Skalski, prezes ADI Global Distribution w Polsce. Oryginalna formuła spotkania łączy dwie konwencje: konferencyjną i targową. Równolegle odbywa się część merytoryczna (seminaria firmowe) i networkingowa (odwiedzanie stoisk producentów i rozmowy w części targowej).

Na stoiskach targowych oraz podczas seminariów prezentowali się przedstawiciele 25 firm, których produkty są dystrybuowane przez ADI. Na targi zaproszono firmy: 2N, Alarmtech, Axis Communications, CDVI, CQR, Dahua Technology, Detector Tester, Ewimar, Elmdene, Hanwha Techwin, GJD, HID, Hikvision, Honeywell, IDESCO, IFTER, Labor Strauss, Milestone, Nedap, OPTEX, Seagate, TRENDnet, Vanderbilt, Western Digital, Winland.

Nedap Security Day

Czy automatyczna wymiana danych pomiędzy systemami telewizji dozorowej, kontroli dostępu oraz sygnalizacji włamania i napadu to już standard? Jakie wymagania integracyjne odnośnie do systemów kontroli dostępu mają klienci nowoczesnych organizacji? Nad tymi zagadnieniami zastanawiali się uczestnicy spotkania Nedap Security Day, które odbyło się pod koniec września w Klubie Mila Zegrzynek.

Podczas dwudniowego spotkania przedstawiciele organizatora – firmy Nedap Security Management – oraz partnerów technologicznych: Hikvision, Indoorway, Milestone i TBS zaprezentowali najnowsze rozwiązania oraz korzyści płynące ze wzajemnej współpracy. Zarówno w prezentacjach, jak i w rozmowach kuluarowych zastanawiano się, czy jesteśmy gotowi na wdrażanie technologii mobilnych, korzystanie z usług geolokalizacji czy biometrii w zastosowaniach security.
W spotkaniu nad Zalewem Zegrzyńskim wzięli udział partnerzy biznesowi oraz klienci i użytkownicy rozwiązań firmy Nedap.

VIII Smart City Forum

Jesienna edycja Smart City Forum odbyła się 19–20 września w Warszawie. To najważniejszy w Polsce kongres poświęcony funkcjonowaniu i rozwojowi inteligentnych miast. Redakcja „a&s Polska" była partnerem medialnym wydarzenia.

W kongresie wzięło udział ponad 500 uczestników i 60 prelegentów. Podczas dwóch dni debat i prezentacji rozmawiano o przyszłości inteligentnych miast – jak ją widzą samorządy, czego oczekują mieszkańcy i co do zaproponowania mają firmy czy start-upy?
W gorącym okresie przed wyborami samorządowymi przedstawiciele polskich miast opowiadali o swoich osiągnięciach, planach oraz wizji rozwoju. Podczas uroczystego otwarcia na scenie stanęli Maciej Bluj, wiceprezydent Wrocławia, Jacek Jaśkowiak, prezydent Poznania, i Krzysztof Żuk, prezydent Lublina.
W programie Smart City Forum pojawiła się także nowość, która z dużym prawdopodobieństwem przerodzi się w osobny Kongres o rozwoju sektora nieruchomości. Blok tematyczny „PropTech w praktyce" opowiadał o *cross-sektorowych* technologiach, które zmieniają podejście do badania, wynajmu, kupna i zarządzania nieruchomościami.
Sesja *round tables* była idealną okazją do wymiany wiedzy i doświadczeń, a także do interakcji między uczestnikami kongresu a gospodarzami stołów. W tej innowacyjnej formule odbyły się 4 sesje, którym kierunek wyznaczali eksperci z poszczególnych dziedzin:

- Stacje ładowania – elektromobilność
- Zarządzenie danymi miejskimi, bezpieczeństwo
- Strategie komunikacji z mieszkańcami ułatwiające wprowadzenie innowacji
- Zagospodarowanie przestrzeni miejskiej w ramach udogodnień dla mieszkańców, turystów

Zgodnie z hasłem wydarzenia, podczas dwóch dni udowadniano, że *smart city* to nie tylko technologie, ale w głównej mierze jakość życia i poczucie szczęścia jego mieszkańców.

Zaproszenie do Jachranki: Ogólnopolskie Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego

Spotkanie organizowane przez firmę Schrack Seconet Polska we współpracy z Partnerami na stałe wpisało się w kalendarz wydarzeń branżowych. W tym roku odbędzie się 25-26 października, tradycyjnie w Jachrance.

Dwa dni merytorycznych spotkań będą doskonałą okazją do wzięcia udziału w kilku różnych studiach przypadków, na które będą składały się bloki eksperckie z zakresu takich zagadnień, jak projektowanie, realizacja i eksploatacja systemów bezpieczeństwa.
Całość wystąpień będzie uzupełnieniem i komentarzem do pokazu zadziałania zintegrowanych ze sobą urządzeń, a podsumowaniem każdego studium przypadku będzie dyskusja ekspertów.
Udział w dwudniowych warsztatach zostanie potwierdzony wspólnym certyfikatem, wystawionym przez Schrack Seconet Polska oraz wszystkich Partnerów spotkania. Otrzymanie dokumentu z kompletem podpisów wszystkich producentów uzależnione będzie od udziału uczestnika w poszczególnych sesjach szkolenia.
Rejestracja uczestników odbywa się wyłącznie online – wszystkie szczegóły dotyczące spotkania (zaproszenie, plan merytoryczny, plan warsztatów poszczególnych producentów oraz link do rejestracji online) są dostępne na stronie: www.schrack-seconet.pl oraz na stronach Partnerów spotkania.

AXIS T8129-E Outdoor PoE Extender – wyczekiwana premiera

Superwytrzymały przedłużacz AXIS T8129-E PoE Extender to łatwe w instalacji rozwiązanie pozwalające zwiększyć zasięg połączeń kamer i innych urządzeń sieciowych Axis Communications do kilkuset metrów.
AXIS T8129-E Outdoor PoE Extender nie wymaga dodatkowego zasilania, a podłączona kamera sieciowa jest zasilana przez jeden przełącznik PoE lub midspan. Urządzenie może być instalowane wewnątrz i na zewnątrz obiektów. Jest odporne na deszcz, kurz i wysokie amplitudy temperatury od -40 do 60ºC, utrzymuje stałą, pełną wydajność w każdych warunkach atmosferycznych (IP66/IP67). Jest kompatybilne ze standardem zasilania IEEE 802.3af, IEEE 802.3at oraz Axis 60 W High PoE, obsługując kamery w odległości przekraczającej 100 m bez potrzeby inwestowania w kosztowną infrastrukturę.
Połączenia Ethernet i PoE ograniczają maksymalną długość kabla do 100 m. Przy większych zasięgach stosuje się inny przełącznik lub router, które wymagają zewnętrznego źródła zasilania. AXIS T8129 PoE Extender-E instaluje się jako łącznik między kablami bez konieczności stosowania zewnętrznego zasilacza. Jego dwa porty Ethernet są automatycznie konfigurowane pod kątem pełnej przepustowości sieci w połączeniu *duplex* lub *crossover*. Zasięg zależy od wymaganej mocy zasilacza midspan i typu kamery. Przykładowo 25-watową kopułkę PTZ można zainstalować w odległości 200 m, stosując jeden przedłużacz AXIS T8129-E. Zainstalowanie kamery na dystansie 400 m wymaga użycia trzech przedłużaczy (po jednym na każde 100 m).
Nowe urządzenie jest dostępne na rynku od września 2018 r. za pośrednictwem kanałów dystrybucyjnych Axis.

Dahua Technology: Kamery Fullcolor

Dahua Technology Poland wprowadziła do sprzedaży nowe kamery Fullcolor oparte na nowoczesnych przetwornikach obrazu. Zastosowane matryce generują sygnał o prawie dwa razy wyższym napięciu wyjściowym. Osiągana dzięki temu doskonała czułość pozwala na ogląd kolorowych obrazów bardzo zaciemnionych scen. Kamery te nie mają promiennika podczerwieni, ponieważ jego zastosowanie mijałoby się z celem (obraz czarno-biały). Mają służyć do poprawnego rozpoznania kolorów nawet przy minimalnym oświetleniu zewnętrznym.
W ofercie pojawiły się kamery w obudowie kopułowej IPC-HFW4239T-ASE oraz tubowej IPC-HDBW4239R--ASE. Oba modele są zgodne ze standardem ePoE, czyli mogą być zasilane ze switcha lub rejestratora w tym systemie na odległość do 800 m. Poza tymi właściwościami produkty te mają funkcjonalności znane z serii Pro (Ecosavvy3.0) urządzeń Dahua (np. analityka IVS, 3 strumienie, możliwość zapisu na karcie, szeroki zakres dynamiki WDR itp.).

Nowa sieciowa kamera dzień/noc serii Wisenet

Hanwha Techwin poszerza ofertę kamer serii Wisenet T o nowy, dwumegapikselowy model sieciowy P/T. Wisenet TNU-6320
Kamery Wisenet T są projektowane do pracy w trudnych warunkach otoczenia. Najnowszy model w obudowie ze wzmocnionego aluminium może pracować w zakresie temperatury od -40°C do 55°C.
Model Wisenet TNU-6320 jest wyposażony w mechanicznie usuwany filtr IR. Sterowanie ułatwiają obroty wokół osi pionowej bez punktu krańcowego (n x 360°) oraz możliwość korzystania z 255 pozycji presetów (maks.) ustawianych automatycznie zgodnie z harmonogramem czasowym. Wyposażona w przetwornik obrazu ze skanowaniem progresywnym kamera generuje ostre obrazy poruszających się obiektów i pojazdów. W Wisenet TNU-6320 zaimplementowano funkcje: WDR 120 dB, Defog i cyfrową stabilizację obrazu, dzięki którym kamera dostarcza optymalne jakościowo obrazy w każdych warunkach środowiskowych.
W kamerze zastosowano kodeki H.264 i MJPEG. Gniazdo na kartę pamięci SD/SDHC/SDXC pozwala na nieprzerwaną rejestrację obrazów wideo nawet w przypadku awarii połączenia sieciowego. Zaimplementowano detekcję ruchu oraz algorytm analizy treści obrazu, m.in. wykrywanie przekroczenia wirtualnej linii, pojawienia się/zniknięcia obiektu, wykrycia twarzy oraz dokonania próby sabotażu obrazu z kamery.

Światłowodowy system ochrony obwodowej

OPTEX Security wprowadza do oferty system ochrony obwodowej Fiber Defender® produkowany przez amerykańską firmę Fiber SenSys Inc. należącą do OPTEX CO. LTD.

Koncepcja systemu została oparta na aktywnym światłowodzie mocowanym do ogrodzenia. Drgania ogrodzenia wywołane ingerencją intruza (wspinanie, cięcie, podnoszenie) są analizowane w procesorze wysyłającym sygnał alarmowy. W zależności od modelu jeden procesor może obsłużyć nawet 25 stref detekcji, każda o maksymalnej długości 2,3 km. Dopasowanie do wymogów instalacji ułatwia zastosowanie dodatkowego kabla nieaktywnego, pozwalającego na zamontowanie procesora sterującego w odległości do 20 km od ochranianego fragmentu ogrodzenia. Do strojenia systemu służą dedykowane aplikacje komputerowe.
W odróżnieniu od rozwiązań opartych na detektorach mechanicznych światłowód jest odporny na działanie czynników środowiskowych, takich jak promieniowanie UV, promieniowanie elektromagnetyczne, wilgoć, sól czy wyładowania atmosferyczne. System Fiber Defender pracuje stabilnie we mgle, przy zapyleniu czy w ciemności. Może być stosowany w strefach zagrożenia wybuchem. Parametry techniczne i niezawodność rozwiązania potwierdza certyfikat najwyższej klasy ochrony armii USA, zezwalający na jego instalację w obiektach, w których przechowuje się materiały nuklearne. System jest rekomendowany przez brytyjski urząd ochrony infrastruktury krytycznej (CPNI).
Więcej informacji na: www.fibersensys.com.

Centrum usługowe RBEI w Warszawie

Dział Robert Bosch Engineering and Business Solutions (RBEI) otworzył w Warszawie centrum usług (*nearshoring*). Jego celem jest wsparcie globalnej działalności Grupy Bosch w regionie Europy Środkowej i Wschodniej, a także rozwój oferty usług w takich obszarach, jak testy oprogramowania czy budowa maszyn. Planuje się, że do końca 2020 r. będzie w nim pracować około 50 pracowników.

Fot. Bosch

Dzięki powstaniu nowego centrum dział RBEI będzie miał przedstawicielstwo w Europie Środkowej i Wschodniej, a także zyska dostęp do lokalnej bazy talentów. Warszawa dysponuje specjalistami o szerokich kompetencjach w dziedzinie IT, jest także ważnym hubem technologicznym w takich obszarach, jak sztuczna inteligencja, analityka danych czy robotyka. Będziemy mogli to wykorzystać w rozwoju naszego biznesu – powiedział Sandeep Mulbagal Gururaj, szef centrum.

Robert Bosch Engineering and Business Solutions z siedzibą w Indiach jest spółką należącą w całości do koncernu Robert Bosch GmbH. Oferuje kompleksowe rozwiązania z zakresu inżynierii, IT oraz biznesu. Zatrudnia ponad 19 tys. pracowników i jest największym centrum rozwoju oprogramowania Bosch poza granicami Niemiec. Swoją działalność prowadzi za pośrednictwem centrów w Indiach, Meksyku, Wietnamie oraz Polsce, obejmując zasięgiem USA, Europę oraz region Azji i Pacyfiku.

Zadaniem warszawskiego centrum jest opracowanie kluczowych ról i kompetencji, takich jak *Functional Consultant* oraz *Solution Architect* przy wsparciu ze strony zespołu RBEI w Indiach. RBEI jest ściśle związany z regionami, w których prowadzi działalność, i z tego względu zamierza zatrudnić głównie pracowników z rynku lokalnego. Ponadto w globalnej działalności biznesowej klienci wymagają zwykle bliskości kulturowej i geograficznej, a Warszawa świetnie odpowiada na te potrzeby.

Polska lokalizacja okazała się najbardziej atrakcyjna, spełniając wysokie wymagania kolegów z Indii dotyczące rozwoju IT i usług cyfrowych. Cieszymy się, że to właśnie w Warszawie zaczęło funkcjonować centrum pracujące nad rozwiązaniami dla IoT i smart living i będziemy mogli aktywnie wspierać jego rozwój w obszarach dedykowanych klientom w Europie – powiedziała Krystyna Boczkowska, prezes zarządu spółki Robert Bosch w Polsce.

Centrum kompetencyjne IT w Warszawie

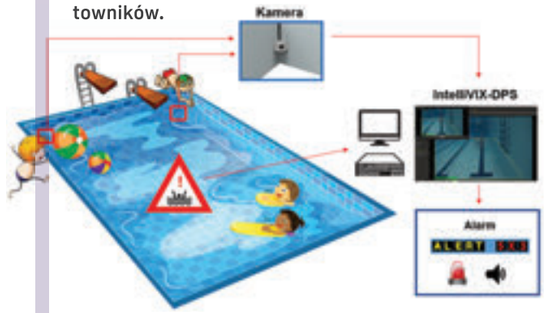
Od kilku lat Grupa Bosch intensywnie rozwija w Warszawie swoje Centrum Kompetencyjne IT. W ciągu ostatnich 12 miesięcy zatrudnienie w centrum zwiększyło się dwukrotnie: ponad 200 osób pracuje tutaj nad nowymi technologiami, które mają kluczowe znaczenie dla działalności biznesowej i produkcyjnej oddziałów Bosch na całym świecie. Obejmują one takie obszary, jak Przemysł 4.0, handel elektroniczny, zarządzanie cyklem życia produktów i systemy *Enterprise Resource Planning* (SAP).

Otwarcie centrum RBEI jest kolejnym, bardzo ważnym krokiem w rozwoju kompetencji Grupy Bosch w Warszawie w obszarach inżynierii oraz IT.

Moduł analizy obrazu IntelliVIX-DPS

Firma IntelliVIX opracowała moduł analizy obrazu, wchodzący w skład pakietu IntelliVIX-DPS, który ma na celu poprawę bezpieczeństwa osób pływających w basenach.

Przypadki tonięcia i śmierci w wodzie zdarzają się niestety bardzo często, również w obiektach strzeżonych przez wysoko wykwalifikowanych ratowników.



IntelliVIX-DPS to wyjątkowe rozwiązanie inteligentnej analizy obrazu w czasie rzeczywistym. Pakiet IntelliVIX-DPS, oprócz modułu analizy obrazu, składa się z wodoodpornych kamer, tablicy elektronicznej oraz lampy ostrzegawczej z wbudowanym głośnikiem alarmowym.

Moduł IntelliVIX-DPS w czasie rzeczywistym wykrywa tonięcie obiektu i w ciągu kilku sekund powiadamia ratownika o potencjalnym zagrożeniu.

Dzięki integracji z lampą oraz dźwiękowym systemem ostrzegawczym pracownicy basenu oraz pozostałe osoby przebywające tam zauważą ostrzeżenie.

Instalacja systemu IntelliVIX-DPS znacząco zwiększa szansę na szybkie zlokalizowanie osoby tonącej oraz skuteczne udzielenie jej pomocy. Rozwiązanie to znakomicie ułatwia pracę ratownikom oraz poprawia bezpieczeństwo w tego typu obiektach sportowych.

Więcej o IntelliVIX-DPS oraz pozostałych produktach IntelliVIX:
www.intellivixeu.com
intellivixeu@intellivix.com

Koza na sznurku

Przechodnia zadziwił człowiek z białą laską prowadzący kozę. – Jak pan nie zgubi tej kozy? – zapytał go. – **To prosta technologia, jestem do niej podłączony sznurkiem** – usłyszał.

Im więcej czytam o tym, kogo i co prowadzi przez życie, myślę, że z kozą mamy wspólny temat – chociaż sznurek się unowocześnił i rozgałęził na pęki widocznych i niewidocznych transmisyjnych sznureczków. Zupełnie jak trzymający nas na „sznurkowej" smyczy telefon/smartfon, wspaniałe narzędzie komunikacji oraz inwigilacji, nie do końca negatywnej.
Technologie zmieniają nas i świat wokół. Nawet humaniści – zwykle antytechniczni – biorą się do ich oceny. Umberto Eco w książce „Pape Satan aleppe", nad którą pracował do śmierci, zacytował myśli z publikacji Maurizia Ferrarisa „Dove sei? Ontologia del telefonino" poświęconej filozofii telefonu komórkowego. Widać, że humanistyka próbuje nadążać za sprinterskim tempem rozwoju techniki. Zanotowałem z niej proste, ale ciekawe spostrzeżenia. – Różnica pomiędzy rozmową przez telefon stacjonarny a komórkowy jest taka, że przy urządzeniach stacjonarnych pytaliśmy, czy zastaliśmy człowieka, z którym chcemy rozmawiać, zaś w drugim zawsze wiemy, kto odbierze (pomijając sytuacje kradzieży aparatu lub jego użyczenia).
W przypadku telefonu stacjonarnego zawsze wiedzieliśmy, gdzie znajduje się odbiorca.
Z komórką już nie jest tak prosto. Rozmówca może stać kilkanaście metrów za nami, ale gdy korzysta z zagranicznej sieci, jego słowa mogą docierać do nas z drugiej części globu.
Zaplątanie jest większe. Rozmówca nie wie, gdzie znajduje się dzwoniący do niego, ale operator sieci telekomunikacyjnej zna położenie obu. Ich działania nie są tak ściśle kontrolowane, jak w orwellowskiej wizji Wielkiego Brata, ale są jawne (moim zdaniem tylko dla „wybrańców").
Hulaj dusza, piekła nie ma – tak złośliwie można by przedstawić sprawę bezpieczeństwa w cyberprzestrzeni. Może coś się poprawi. 28 sierpnia weszła w życie Ustawa o krajowym systemie cyberbezpieczeństwa (KSC) – finalizowane są prace nad ośmioma rozporządzeniami wykonawczymi do niej. To wdrożenie do polskiego systemu prawnego unijnej Dyrektywy NIS dotyczącej bezpieczeństwa sieciowego, przyjętej w ub. roku przez Parlament Europejski. Państwa zostały zobowiązane do przyjęcia krajowych strategii NIS – w Ministerstwie Cyfryzacji pracują nad taką.
Ustawa o KSC porządkuje strukturę ochrony cyberprzestrzeni, tworząc spójny system zarządzania ryzykiem, z przydziałem zadań i obowiązków. Ma on zapewnić sprawność w zakresie wykrywania, zapobiegania i minimalizowania skutków ataków naruszających bezpieczeństwo państwa, być spójny i pozwalać na współpracę.
W skład KSC wchodzą instytucje administracji państwowej i samorządowej oraz najwięksi przedsiębiorcy z kluczowych sektorów gospodarki. Chodzi o banki, energetykę, przewoźników lotniczych, kolejowych i armatorów, szpitale, dostawców usług kluczowych (np. internetowe platformy handlowe), także instytucje publiczne i podmioty telekomunikacyjne. Mowa o zespołach reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) z lokalizacją w ABW, NASK i MON. Przy Ministrze Cyfryzacji powstanie pojedynczy punkt kontaktowy do wymiany informacji i ostrzeżeń w przypadku poważnych incydentów, które dotknęły co najmniej dwa państwa unijne.
W ciągu trzech pierwszych miesięcy obowiązywania RODO do UODO wpłynęło 2,4 tys. skarg na przypadki łamania rozporządzenia (w 2017 r. było wszystkich 3 tysiące). Prezes UODO zapowiedziała kontrole, m.in. sektorowe, dotyczące rejestrów publicznych, kontroli monitoringu wizyjnego, giełdy długów i inne.
Na początku września otworzono oferty przetargowe na zamówienie przez KG Policji 2110 małych kamer mundurowych (tzw. nasobnych) wraz z urządzeniami i oprogramowaniem. Pilotaż pracy systemu w trzech garnizonach wypadł dobrze. Mniej było agresji uczestników interwencji i skarg na policjantów prewencji i drogówki. Aby można było nagrywać sytuacje m.in. w interwencjach domowych, konieczna jest również implementacja tzw. europejskiego DODO (takie „RODO" dla organów ścigania i wymiaru sprawiedliwości – trwa proces legislacyjny). Wśród wymogów funkcjonalnych i technicznych na zamawiane kamery znalazłem w SIWZ dotyczące zdolności oznaczania nagrania jako „dowód", nanoszenia znaków wodnych, a po wyczerpaniu pojemności pamięci – braku możliwości nadpisywania nagrań wcześniejszych. I o to w budowaniu zaufania chodzi.

BIO

Andrzej Popielski
Dziennikarz, fotograf. Autor felietonów o bezpieczeństwie w „Systemach Alarmowych" (w latach 2005–2015).

MIEJ WSZYSTKO POD KONTROLĄ

Zintegrowany system zarządzania HDCVI - IoT do pomiaru temperatury, wilgotności z obrazem wizyjnym i alarmem

HDCVI 4.0 IoT

HDCVI- IoT zwiększa wszechstronność systemu. Po przekroczeniu ustalonych wartości temperatury i wilgotności powietrza wyzwalany zostaje alarm.

- Kamera do pomiaru temperatury i wilgotności powietrza, która w czasie rzeczywistym zbiera informacje, zwiększając wszechstronność systemu.
- Punkt dostępowy w kamerze: odbiór sygnału z czujników bezprzewodowych, transmisja po przewodzie koncentrycznycm do rejestratora XVR.
- Kamera MotionEye, która wyposażona została w detekcję ruchu i czujnik PIR. Rozdzielczość kamery do 4 Mpx.
- Rejestrator HDCVI- IoT, zapewnia zintegrowany system zarządzania z przyjaznym interfejsem użytkownika i dostępnymi raportami danych.
- Łatwe wdrożenie systemu HDCVI bez dodatkowego okablowania.

Polecane modele

HAC-LC1220T-TH
Kamera HDCVI do pomiaru temperatury i wilgotności, 2 Mpx

HAC-LC1200SL-W
Kamera Gateway HDCVI, 2 Mpx

HAC-ME1400B/ME1200B
Kamera MotionEye, HDCVI 2 Mpx / 4 Mpx

XVR7000-4KL
Rejestrator IoT HDCVI

PFM871A-N1
Identyfikator USB IoT HDCVI

CE FC RoHS ISO 9001:2000

www.dahuasecurity.com/pl

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