CZASOPISMO RYNKU SECURITY

a&s POLSKA

05 (29) 09/10 2021

PRZEMYSŁ 4.0

GAMBIT ROBOTÓW

KONFERENCJA

WARSAW SECURITY SUMMIT

Podejście do bezpieczeństwa wraz z nadejściem pandemii bardzo się zmieniło. O lekcjach z COVID-19 i nowej rzeczywistości prelegenci konferencji mówili najwięcej. Wysłuchało ich ponad 300 osób stacjonarnie i niemal 500 na żywo online.

PRZEMYSŁ 4.0

OCHRONA OBIEKTÓW ROZPROSZONYCH

Stworzenie skutecznej ochrony przemysłowych obiektów rozproszonych wymaga gruntownego przygotowania. Musi być realizowana w bezpośrednim związku z koncepcją funkcjonowania całej firmy, łącząc czynnik ludzki z technicznym.

CYBERBEZPIECZEŃSTWO

HARDENING SYSTEMÓW ZABEZPIECZEŃ

Proces hardeningu zabezpieczeń elektronicznych powinien być jednym z elementów szeroko rozumianej polityki bezpieczeństwa. Ponieważ jest zmienny, utwardzony system po pewnym czasie może być podatny na nowe zagrożenia.

APLIKACJA MOBILNA

www.aspolska.pl

ISSN 2451-5175

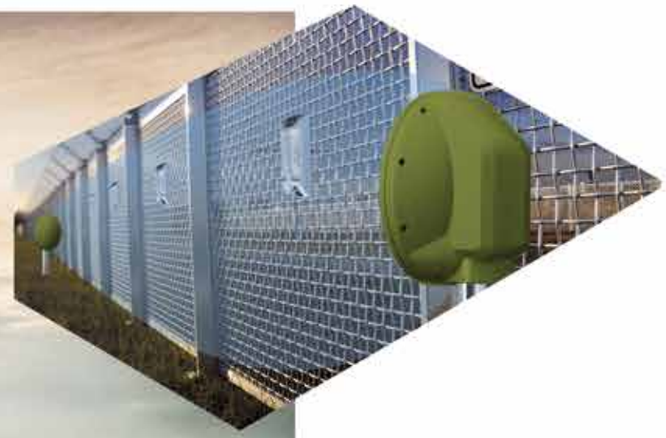
9 772451 517703 05

15 zł (w tym 8% VAT)

BARIERY MIKROFALOWE SERII BM

Nowoczesne, sprawdzone na światowych rynkach bariery mikrofalowe włoskiego producenta AVS Electronics stanowią skuteczne rozwiązanie ochrony perymetrycznej. Rozwiązanie zaprojektowane i certyfikowane z myślą o obiektach wojskowych oraz infrastrukturze krytycznej.

Robust Concepts for Security



System ochrony obwodowej oparty o bezprzewodowe detektory RFID montowane bezpośrednio na ogrodzeniach, bramach i furtkach. Niezawodne czujniki akcelerometryczne oraz szyfrowana komunikacja gwarantują najwyższy poziom bezpieczeństwa - GRADE 4.

OCHRONA NAPŁOTOWA VARYA PERIMETER

Ekosystem autonomicznych dronów, stacji dokujących oraz oprogramowania opartego o działanie sztucznej inteligencji. Dronehub® został stworzony do optymalizacji procesów monitoringu oraz wspomagania systemów ochrony obwodowej.

AUTOMATYCZNA STACJA DOKUJĄCA DRONEHUB

Drodzy Czytelnicy

Za nami 5. edycja konferencji Warsaw Security Summit. Po pandemicznej przerwie w warszawskim hotelu Sheraton zgromadziło się blisko 300 osób, niemal 500 oglądało transmisję na żywo online. Długo oczekiwane spotkanie *face to face* było okazją do ożywionych rozmów i komentarzy nt. ciekawych prelekcji, a także dyskusji o obecnej i przyszłej sytuacji na branżowym rynku (s. 16). Zapis konferencji jest dostępny na portalu aspolska.pl oraz na stronie WarsawSecuritySummit.online

Branża IT żartuje, że IoT to skrót, w którym „B" oznacza bezpieczeństwo... Rzeczywiście, w naszych cyfrowych czasach nie można mieć pewności, że firma jest dobrze zabezpieczona. Urządzenia IoT można zaprojektować i skonfigurować z myślą o bezpieczeństwie albo zająć się tylko ich stroną funkcjonalną. Wdrażając mechanizmy ochrony, należy wymodelować mogące wystąpić zagrożenia z uwzględnieniem czynnika ludzkiego. Na co jeszcze zwracać uwagę – przeczytacie w wywiadzie na s. 22.

W czasie pandemii służby ochrony obiektów realizowały zadania, które wcześniej nie należały do ich obowiązków. Przestrzeganie przepisów sanitarnych czy kontrola dystansu społecznego to nie są klasyczne zadania pracownika ochrony, a typowe raczej dla służb BHP. Czy biznes jest dziś gotowy na wdrożenie koncepcji przeorganizowania działania służb obiektowych w kierunku stewardingu obiektowego? (s. 44)

Negatywny wpływ COVID-19 na przemysł nadal jest duży, ale widać optymizm co do perspektyw wzrostu gospodarczego. Sektor na całym świecie zaczął już akceptować stosowanie robotyki w niemal każdym procesie produkcyjnym. Rynek przemysłu 4.0 dostosowuje się do aktualnej sytuacji, wdrażając przełomowe technologie i techniki automatyzacji oraz łącząc siły z innymi przedsiębiorstwami. Jednak podatność IIoT na cyberataki może hamować rozwój tego rynku. O prognozach dla tego sektora gospodarki piszemy na s. 52.

Kontynuując wątek zadań ochrony – rozproszone wielowymiarowe zakłady produkcyjne są najtrudniejsze do ochrony. Tutaj od pracowników ochrony są wymagane kompetencje w zakresie obsługi systemów miejscowych i reagowania na zdarzenia poza obiektem głównym, nawet za granicą. Skuteczna ochrona musi być realizowana w bezpośrednim związku z koncepcją funkcjonowania całej firmy. Jak krok po kroku stworzyć taki system, podpowiadamy na s. 58. Zaprosiliśmy też ekspertów, aby podzielili się swoimi doświadczeniami, jak sobie radzić z zapewnieniem bezpieczeństwa w trudnych czasach pandemicznej huśtawki zachorowań i nastrojów mających wpływ na gospodarkę (s. 70).

W każdym wydaniu podejmujemy teraz tematykę cyberbezpieczeństwa. W kolejnym artykule z tej serii poruszamy kwestię hardeningu systemów (s. 86) z nadzieją na zaktywizowanie naszej branży do podnoszenia kwalifikacji. Proces hardeningu powinien być jednym z elementów szeroko rozumianej polityki bezpieczeństwa. W procesie inwestycyjnym warto zwracać uwagę na to zagadnienie jako ważny aspekt odbioru, modernizacji lub uszczelniania elektronicznych systemów zabezpieczeń technicznych.

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznic
Z-CA REDAKTORA NACZELNEGO

Mariusz Kucharski
DYREKTOR ZARZĄDZAJĄCY

a&S POLSKA REDAKCJA

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

Dyrektor zarządzający
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Z-ca redaktora naczelnego
Jan T. Grusznic

Dział reklamy i marketingu
Iwona Krawiec

Dział projektów specjalnych
Jolanta A. Kucharska
Aleksandra Czapska

Kolegium redakcyjne
Norbert Bartkowiak
Sebastian Błażkiewicz
Marek Domański
Jacek Grzechowiak
Rafał Łupkowski
Przemysław Pierzchała
Janusz Sawicki
Stefan Jerzy Siudalski
Jerzy Sobstel
Jacek Tyburek
Paweł Wittich
Waldemar Wnęk
Aleksander M. Woronow

Korekta
Jolanta Kucharska

Projekt graficzny i skład
Kalwala Studio

Adres redakcji
Aura Sky Offices
ul. M. Rodziewiczówny 1 lok. 801
04-187 Warszawa
e-mail: info@aspolska.pl
www.aspolska.pl

Prenumerata
www.aspolska.pl/prenumerata

Redakcja zastrzega sobie prawo skracania i adiustacji zamówionych tekstów. Artykułów niezamówionych i niezatwierdzonych do druku nie zwracamy. Opinie autorów nie muszą być tożsame z poglądami redakcji. Za treść reklam redakcja nie odpowiada. Przedruki tekstów bez zgody redakcji są niedozwolone.

A&S Polska jest częścią grupy wydawniczej A&S International.

© Copyright by A&S Polska

A&S POLSKA
ZŁOTY PARTNER

AXIS COMMUNICATIONS · BCS · Linc Polska Sp. z o.o. · nedap · SCHRACK SECONET · smart-i

A&S POLSKA
SREBRNY PARTNER

HIKVISION

A&S POLSKA
WYDANIE ONLINE

www.aspolska.pl/czasopismo

BCS MOBILCAM

NIEZAWODNA
MOBILNA
OCHRONA

CHROŃ LUDZI, MIEJSCA
I ZASOBY Z WIEŻĄ BCS
MOBILCAM

MOBILCAM ZWIĘKSZY
BEZPIECZEŃSTWO
OBSZARU LUB OBIEKTU

» WIĘCEJ PRZECZYTASZ NA STRONIE 10

POLSKA MARKA BCS

www.bcs.pl
www.facebook.com/bcscctvpl

a&S POLSKA

05

29

09/10

2021

SPIS TREŚCI

RYNEK SECURITY

axxonsoft
EXPERIENCE THE NEXT®

Światowy lider w dziedzinie inteligentnego oprogramowania VMS i PSIM

Sztuczna Inteligencja i Sieci Neuronowe

AxxonSoft proponuje rozwiązania analityki wideo zapewniające wiele korzyści dla biznesu i bezpieczeństwa dzięki sieciom neuronowym zasilanym przez AI (sztuczną inteligencję) i algorytmy głębokiego uczenia. Inteligentna Analiza Obrazu AxxonSoft otwiera drogę do aktywnego, zautomatyzowanego nadzoru, który pomaga chronić własność poprzez wykrywanie i powstrzymywanie przestępstw. Aplikacje mogą wykrywać ludzi / pojazdy, ogień / dym lub nieprawidłowe zachowanie / warunki i automatycznie o tym powiadamiać.

- Analityka Behawioralna
- Identyfikacja Obiektów
- Rozpoznawanie Tablic Rejestracyjnych
- Rozpoznawanie Twarzy
- Detekcja Dymu i Ognia

www.axxonsoft.com/pl

SPIS TREŚCI

PRZEMYSŁ 4.0

BEZPIECZEŃSTWO POŻAROWE

BEZPIECZEŃSTWO BIZNESU

CYBERBEZPIECZEŃSTWO

SERWIS INFORMACYJNY

GEMOS
advanced PSIM

Od 29 lat integrujemy systemy
i aplikacje bezpieczeństwa w obiektach

HOTELE
GALERIE HANDLOWE
MUZEA
BIUROWCE
LOTNISKA
FABRYKI
SZPITALE
ELEKTROWNIE

ela.pl
facebook.com/BuildingManagementSystems
linkedin.com/company/elacompil

AXIS COMMUNICATIONS

www.axis.com/pl

Profesjonalne transmisje strumieniowe od Axis

AXIS COMMUNICATIONS WPROWADZA NA RYNEK KAMERĘ AXIS V5938 PTZ PRZEZNACZONĄ DO PROFESJONALNYCH TRANSMISJI STRUMIENIOWYCH NA ŻYWO. URZĄDZENIE CHARAKTERYZUJE SIĘ DOSKONAŁĄ JAKOŚCIĄ I PŁYNNOŚCIĄ OBRAZU I DŹWIĘKU, ŚWIETNIE SPRAWDZI SIĘ W REJESTRACJI HALOWYCH WYDARZEŃ SPORTOWYCH, LEKCJI, WYKŁADÓW CZY OBRZĘDÓW RELIGIJNYCH.

Kamera PTZ AXIS V5938 zapewnia doskonałą jakość obrazu w rozdzielczości 4K przy 30 kl./s. Obiektyw z 20-krotnym zoomem optycznym pozwala zarejestrować nawet najdrobniejsze szczegóły. Oprogramowanie oparte na VISCA RS-232 umożliwia łatwą konfigurację kamery z innymi urządzeniami, a poprzez IP można zdalnie sterować wieloma kamerami.
Tryb pracy sceniczny lub sportowy pozwala operatorowi na lepszą kontrolę przekazywanego obrazu z różnych okoliczności. Do urządzenia dołączona jest 3-miesięczna licencja próbna programu Camstreamer, który umożliwia bezpośrednie transmisje na żywo na takich platformach, jak YouTube czy Facebook.
Zastosowana w kamerze technologia Axis Zipstream z kodowaniem H.264 i H.265 znacznie zmniejsza wymagania dotyczące przepustowości sieci i pamięci masowej, bez pogorszenia jakości obrazu. Studyjna jakość dźwięku jest zapewniana przez wejścia XLR, kamera ma też wyjścia 3G-SDI oraz HDMI.

Ulepszone funkcje bezpieczeństwa chronią system przed niepożądanym dostępem osób trzecich i próbami zainstalowania na urządzeniu niechcianego oprogramowania. Funkcja bezpiecznego uruchamiania zabezpiecza sterowniki kamery przed plikami *malware*.

BCS

www.bcscctv.pl

Wieże BCS MOBILCAM

NOWOŚCIĄ, KTÓRĄ BCS PRZYGOTOWAŁ DLA SWOICH KLIENTÓW, SĄ MOBILNE SYSTEMY MONITORINGU WIZYJNEGO OPARTE NA AUTORSKIM PROJEKCIE WIEŻ. WIEŻA Z 6-METROWYM RĘCZNIE WYSUWANYM MASZTEM STANOWI IDEALNĄ PLATFORMĘ DLA URZĄDZEŃ MONITORINGU, KTÓRE MOŻNA WYBRAĆ Z JEDNEJ Z PRZYGOTOWANYCH PRZEZ NAS OPCJI LUB DOSTOSOWAĆ WEDŁUG WŁASNYCH POTRZEB, WYKORZYSTUJĄC URZĄDZENIA BCS.

Bazę MOBILCAM stanowi ocynkowana konstrukcja wyposażona w podpory stabilizujące, zamykana od góry po wysunięciu masztu. Wieża ma osprzęt niezbędny do uruchomienia systemu monitoringu, w tym dwa akumulatory do zasilania buforowego o pojemności 220 Ah każdy. Zasilanie systemu może być realizowane z sieci elektrycznej 230 V lub, gdy nie ma takiej możliwości, zestaw można doposażyć w jeden lub dwa panele fotowoltaiczne o mocy 305 W każdy. Zastosowana w kamerze technologia Axis Zipstream z kodowaniem H.264 i H.265 znacznie zmniejsza wymagania dotyczące przepustowości sieci i pamięci masowej, bez pogorszenia jakości obrazu. Studyjna jakość dźwięku jest zapewniana przez wejścia XLR, kamera ma też wyjścia 3G-SDI oraz HDMI.
Wieże są dostępne w dwóch wersjach: wieża w pierwszej wersji jest na stałe zintegrowana z przyczepą bez hamulców o masie 750 kg, w drugiej wersji jest na przyczepie z hamulcami o masie 1200 kg, wyposażonej w podnośnik hydrauliczny, dzięki któremu można ją bezpiecznie postawić w miejscu, gdzie konieczne jest wykorzystanie monitoringu wizyjnego.
Tego typu rozwiązanie sprawdzi się wyśmienicie wszędzie tam, gdzie nie ma możliwości zainstalowania skomplikowanego systemu monitoringu lub monitoring jest potrzebny doraźnie. Plac budowy, zabezpieczenie imprezy masowej czy trudno dostępne tereny to miejsca, gdzie wieża BCS MOBILCAM stworzy bezpieczną strefę ochrony.

HIKVISION

www.hikvision.com/pl

Hik-ProConnect – platforma do zarządzania systemami zabezpieczeń

HIK-PROCONNECT TO KONWERGENTNE, OPARTE NA CHMURZE ROZWIĄZANIE DO ZARZĄDZANIA SYSTEMAMI ZABEZPIECZEŃ. PLATFORMA OFERUJE OBSŁUGĘ Z URZĄDZEŃ STACJONARNYCH I MOBILNYCH M.IN. W ZAKRESIE: PODGLĄDU OBRAZÓW W CZASIE RZECZYWISTYM, ODTWARZANIA MATERIAŁU NAGRANEGO, MONITOROWANIA STANU URZĄDZEŃ („HEALTHCHECK"), ICH ZDALNEJ KONFIGURACJI, ZARZĄDZANIA UŻYTKOWNIKAMI I UPRAWNIENIAMI, NATYCHMIASTOWYCH POWIADOMIEŃ W SYSTEMIE PUSH DO APLIKACJI MOBILNYCH, INFORMUJĄCYCH NP. O UTRACIE POŁĄCZENIA Z URZĄDZENIEM, JEGO NIEPRAWIDŁOWEJ PRACY, NISKIM POZIOMIE NAŁADOWANIA AKUMULATORA ITP. ZDALNIE SĄ TEŻ DOSTĘPNE DZIENNIKI ZDARZEŃ URZĄDZEŃ.

Hik-ProConnect jest dostępny w modelu subskrypcyjnym i jest o wiele bogatszy od znanej już platformy Hik-Connect. Użytkownik sam decyduje, czy korzysta z wersji bezpłatnej, czy dokupuje poszczególne pakiety. Nowa platforma umożliwia personalizację logotypu firmowego – klientom można oferować aplikację mobilną ze znakami firmowymi.
Architektura platformy przewiduje możliwość profilowanej obsługi – innej dla instalatora, innej dla administratora czy klienta końcowego. Hik-ProConnect to także komfortowa współpraca z centrami monitorowania alarmów (CMA). Systemy SSWiN, CCTV, wideodomofony, kontrola dostępu i inne urządzenia Hikvision można łatwo zintegrować dzięki innowacyjnemu pakietowi SDK, obejmującemu technologię HPNetSDK i HIKIP Receiver Pro, uzupełnioną wtyczkami do obsługi różnych formatów wideo.

ALNET SYSTEMS

Polskie profesjonalne zintegrowane rozwiązania VMS
Ponad 200 000 instalacji na całym świecie
Jesteśmy z Wami od 2003 roku

Z naszych rozwiązań korzysta

Eurocast

Producent
wielowarstwowych innowacyjnych
folii giętkich

www.alnetsystems.com

LINC POLSKA

www.linc.pl

EVO² – najnowsza technologia termowizyjna w kamerach SilentSentinel

W NOWEJ SERII KAMER EVO² WYKORZYSTANO NAJNOWOCZEŚNIEJSZE ROZWIĄZANIA TECHNOLOGICZNE DO PRODUKCJI PRZETWORNIKA TERMOWIZYJNEGO I STOSOWANEJ OPTYKI. NOWE KAMERY ZAPEWNIAJĄ W TEN SPOSÓB ZAAWANSOWANE MOŻLIWOŚCI DETEKCJI W NAJBARDZIEJ EKSTREMALNYCH WARUNKACH PRACY. TECHNOLOGIA EVO² WYKORZYSTUJE NIECHŁODZONE PRZETWORNIKI TERMOWIZYJNE (PASMO LWIR), Z OBIEKTYWAMI O STAŁEJ LUB ZMIENNEJ OGNISKOWEJ. NAJNOWSZA TECHNOLOGIA DOSTĘPNA JEST DLA KAMER Z SERII OCULUS, AERON, OSIRIS I JAEGAR.

Najważniejsze cechy nowej technologii:
- parametr Pixel Pitch 12 µm pozwala na osiągnięcie znacznie większych dystansów pracy kamer marki SilentSentinel,
- Seria EVO² jest standardowo dostarczana z przetwornikiem termowizyjnym w rozdzielczości 640 × 512. Dostępna jest również rozdzielczość 1024 × 768 (XGA),
- Seria EVO² oferuje funkcję autofocus jako standardową dla niemal wszystkich obiektywów zmiennoogniskowych.

Najnowsze kamery SilentSentinel zapewniają najwyższą jakość obrazu i wyjątkową łatwość ich obsługi. Szukając odpowiedniej kamery termowizyjnej, warto o nich pomyśleć.
Więcej informacji na:
www.linc.pl/termowizja-do-ochrony/

NEDAP SECURITY MANAGEMENT

www.nedapsecurity.com/pl/

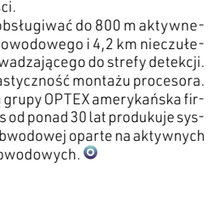
Rozwiązania Nedap uzyskały najwyższy poziom certyfikacji EN60839

SPRZĘT, TAKI JAK CZYTNIKI I KONTROLERY, MOŻE BYĆ SŁABYM OGNIWEM SYSTEMU KONTROLI DOSTĘPU. DLATEGO ZAWSZE DĄŻYMY DO ZAPEWNIENIA NAJWYŻSZEGO POZIOMU BEZPIECZEŃSTWA. SPRZĘT FIRMY NEDAP WYMIENIONY PONIŻEJ UZYSKAŁ NAJBARDZIEJ RYGORYSTYCZNY POZIOM (GRADE 4) CERTYFIKATU BEZPIECZEŃSTWA EN60839.

Daje to nie tylko pewność, że Nedap zapewnia najwyższej jakości rozwiązania. Jeśli zabezpieczasz miejsca takie jak obiekty publiczne, wojskowe lub miejsca związane z infrastrukturą krytyczną, taki certyfikat jest często niezbędny.
Nasze produkty z certyfikatem EN60839:

Kontroler AEOS Blue (AP7803) – zaawansowany kontroler drzwi. Adekwatna moc obliczeniowa w połączeniu z inteligentnymi komponentami oprogramowania umożliwia korzystanie ze wszystkich funkcji systemu AEOS w pojedynczym module. Działa autonomicznie oraz w trybie online. Wyposażony w moduł SAM *(Secure Access Module)* do bezpiecznego przechowywania kluczy i certyfikatów w celu zapewnienia wyższego poziomu bezpieczeństwa.

Moduł kontroli dostępu AEOS Blue (AP7003) – urządzenie peryferyjne dedykowane do kontrolera AP7803. Moduł obsługi przejść wykorzystuje inteligencję AP7803, posługując się magistralą RS-485. Zapewnia to maksymalną swobodę projektowania i możliwość wykorzystania istniejącego okablowania.
Czytnik Invexs MD190 i czytnik Invexs MDK190 – czytniki zaprojektowane do pracy w ekstremalnych warunkach pogodowych.



OPTEX SECURITY

www.optex-europe.com/pl

FD7104 – inteligentny system ochrony obwodowej FiberSenSys

FIBERSENSYS, ŚWIATOWY LIDER ŚWIATŁOWODOWYCH SYSTEMÓW OCHRONY OBWODOWEJ, WYKORZYSTAŁ SWOJE 30-LETNIE DOŚWIADCZENIE DO STWORZENIA INTELIGENTNEGO SYSTEMU FD7104. JEGO KONCEPCJĘ OPARTO NA AKTYWNYM ŚWIATŁOWODZIE MOCOWANYM DO OGRODZENIA. WSZELKIE DRGANIA OGRODZENIA SĄ WYKRYWANE I ANALIZOWANE PRZEZ ALGORYTMY AI W PROCESORZE, Z ODRÓŻNIENIEM DRGAŃ WYWOŁANYCH PRZEZ INTRUZA OD FAŁSZYWYCH POBUDZEŃ.

Oprócz inteligentnego algorytmu detekcji procesor FD7104 wyróżnia się łatwością konfiguracji. Po raz pierwszy software został wbudowany w procesor sterujący systemu dostępny przez przeglądarkę. Eliminuje to potrzebę dodatkowego oprogramowania oraz umożliwia lokalny lub sieciowy dostęp do urządzenia. FD7104 może być zasilany przez PoE lub tradycyjnie, co zapewnia elastyczność instalacji i ułatwia integrację z PSIM i VMS dzięki komunikacji ethernetowej.
System FD7104 z łatwością dostosowuje się do warunków panujących w konkretnej lokalizacji – operator może zakwalifikować poprzednie zdarzenia jako fałszywy alarm. Wówczas parametry detekcji zmieniają się automatycznie, co pozwala wyeliminować podobne fałszywe alarmy w przyszłości.
FD7104 może obsługiwać do 800 m aktywnego kabla światłowodowego i 4,2 km nieczułego kabla doprowadzającego do strefy detekcji. Zapewnia to elastyczność montażu procesora. Będąca częścią grupy OPTEX amerykańska firma Fiber SenSys od ponad 30 lat produkuje systemy ochrony obwodowej oparte na aktywnych kablach światłowodowych.

OPTEX SECURITY

www.optex-europe.com/pl

Czujki laserowe OPTEX do zadań specjalnych

REDSCAN PRO, NAJNOWSZA CZUJKA LASEROWA Z NAGRADZANEJ SERII REDSCAN LIDAR, POTRAFI Z NIEZWYKŁĄ DOKŁADNOŚCIĄ WYKRYWAĆ INTRUZÓW NA OBSZARZE AŻ 50 X 100 M BEZ JAKICHKOLWIEK LUK I UTRATY SKUTECZNOŚCI DETEKCJI ZE WZROSTEM ODLEGŁOŚCI. ZASTOSOWANIE PÓL DETEKCJI W KSZTAŁCIE PROSTOKĄTA A NIE WACHLARZA ELIMINUJE ICH NAKŁADANIE SIĘ, DZIĘKI CZEMU CZUJKI DOSKONALE NADAJĄ SIĘ DO OCHRONY ELEWACJI I OGRODZEŃ PRZY UŻYCIU WIRTUALNYCH ŚCIAN I PŁASZCZYZN OBEJMUJĄCYCH OTWARTE PRZESTRZENIE, SUFITY I DACHY.

Czujka REDSCAN PRO bazuje na inteligentnych algorytmach wielostrefowych, by spełnić wymagania danej lokalizacji. Oznacza to, że dla każdej strefy detekcji można niezależnie określić czułość, rozmiar obiektu i sygnał wyjściowy, co pozwala na dostosowanie urządzenia do zagrożeń i specyfiki lokalizacji, gwarantuje maks. częstotliwość przechwytywania i ogranicza fałszywe alarmy. Moduł kamery zapewnia wizualne wspomaganie na potrzeby konfiguracji i analizy zdarzenia, które wywołało alarm. W razie wystąpienia alarmu zapisywany jest plik dziennika zdarzeń i obraz wideo. Ułatwia to pracownikom ochrony analizę przyczyn alarmu.
Czujka charakteryzuje się nowym eleganckim wzornictwem, elastycznością opcji montażu (można ją pochylić pod kątem od +5 do -95∞), łatwością ustawień i prostotą konfiguracji za pomocą przeglądarki sieciowej. Seria REDSCAN Pro obejmuje dwa modele: RLS-3060V o maks. zasięgu 30 x 60 m oraz RLS-50100V o zasięgu do 50 x 100 m, zgodne z protokołem ONVIF S.

SCHRACK-SECONET

www.schrack-seconet.pl

Nowa seria wzmacniaczy BO-CD-200-4-EV|-AX w systemie APS®-APROSYS

WYCHODZĄC NAPRZECIW OCZEKIWANIOM RYNKU, SCHRACK SECONET WPROWADZIŁ DO OFERTY JUŻ DRUGĄ ODSŁONĘ UZNANYCH NA CAŁYM ŚWIECIE, CZTEROKANAŁOWYCH WZMACNIACZY SERII BO-CD-XXX-4-EV|-AX Z WBUDOWANĄ FUNKCJĄ CYFROWEJ OBRÓBKI SYGNAŁU – DSP *(DIGITAL SIGNAL PROCESSING)*. TYM RAZEM ICH MOC W ODNIESIENIU DO PIERWSZEJ SERII ZOSTAŁA ZWIĘKSZONA DWUKROTNIE, ZE 100 W DO 200 W NA KANAŁ.

Wzmacniacze BO-CD-200-4-EV|-AX klasy „D" świetnie sprawdzają się wszędzie tam, gdzie jest potrzebna selektywność rozgłaszania i możliwość zastosowania DSP indywidulanie dla każdego z 4 dostępnych kanałów. Niezależna regulacja poziomu głośności sygnału lub zastosowanie np. funkcji *shadow volume* (automatycznego ściszania tła muzycznego w momencie rozgłaszania komunikatu na żywo, np. z poziomu pulpitu mikrofonowego), bez konieczności używania do tego komputera daje dużą swobodę w obsłudze systemu przez uprawniony personel / autoryzowany serwis w zakresie szybkiej regulacji poziomów głośności sygnałów.
Wzmacniacze serii BO-CD-XXX-4-EV|-AX produkowane w szwajcarskiej fabryce g+m elektronik ag doskonale się sprawdzają nawet w najtrudniejszych warunkach środowiskowych. Już pierwsza ich wersja BO-CD-100-4-EV znalazła zastosowanie w instalacji dźwiękowego systemu ostrzegawczego w najdłuższym na świecie tunelu kolejowym „The NEAT / Gotthard Base Tunnel" o imponującej długości 57 km, gdzie głównym celem instalacji było zapewnienie wysokiej wartości wskaźnika zrozumiałości mowy w tak trudnej akustycznie przestrzeni, który udało się z powodzeniem spełnić.

TP-LINK

www.tp-link.com.pl

TP-Link TL-SG1210MPE – kompaktowy przełącznik PoE do systemów monitoringu CCTV

PRZEŁĄCZNIK TP-LINK TL-SG1210MPE IDEALNIE SPRAWDZI SIĘ PRZY INSTALACJACH KAMER CCTV. SWITCH MOŻNA RÓWNIEŻ WYKORZYSTAĆ DO ROZBUDOWY INFRASTRUKTURY SIECIOWEJ W MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTWACH. JEST W PEŁNI ZGODNY Z PUNKTAMI DOSTĘPOWYMI, KAMERAMI, TELEFONAMI IP I WIELOMA INNYMI URZĄDZENIAMI ZASILANYMI PRZEZ STANDARD POE.

TL-SG1210MPE wyposażono w 8 Gb portów RJ45 PoE+ oraz dodatkowo w 2 Gb porty uplink do integracji z resztą sieci: gigabitowy RJ45 i gigabitowy port combo RJ45/SFP. Całkowity budżet mocy PoE wynosi 123 W (na każdym porcie maks. 30 W). Switch wyposażono też w funkcje IGMP Snooping (optymalizacji ruchu multimediów, np. aplikacji IPTV) i PoE Auto Recovery (samoczynna naprawa połączenia), gwarantujące stabilne działanie urządzeń PoE. Dzięki możliwości konfiguracji VLAN sieć jest dzielona na segmenty, zapewniając jej wydajniejsze działanie i wyższy poziom bezpieczeństwa zasobów. Z kolei dzięki funkcji QoS ruch sieciowy w zastosowaniach czułych na opóźnienia (połączenia głosowe i wideo) przebiega płynnie i bez zakłóceń. W trybie Extend zasięg transmisji PoE sięga nawet 250 m – przełącznik jest doskonałym rozwiązaniem w przypadku rozmieszczania kamer IP na dużym obszarze.
Switchem TL-SG1210MPE można zarządzać przez intuicyjny interfejs przeglądarkowy lub dedykowane oprogramowanie na PC. Bezwentylatorowa konstrukcja zapewnia cichą pracę urządzenia.
Switch jest już dostępny w sprzedaży i objęty 5-letnią gwarancją.

RACS 5 v2

Skalowalny system kontroli dostępu, bezpieczeństwa i automatyki klasy *Enterprise*

- Obsługa systemów rozproszonych
- Obsługa wind serwerowych KONE i Schindler
- Integracje PSIM, SMS, VMS, OFFICE
- Globalny anti-passback

roger
Intelligence for Building

Warsaw Security Summit 2021

a&S POLSKA

Długo wyczekiwana konferencja Warsaw Security Summit 2021 odbyła się 6 września – dokładnie po 27 miesiącach od poprzedniej edycji. Po pandemicznej przerwie wydarzenie (w formie hybrydowej: stacjonarnej i online) zgromadziło prawie 300 osób w warszawskim hotelu Sheraton i niemal 500 oglądających transmisję na żywo.

Z COVID-19 wszyscy wyciągnęliśmy lekcje. O nich i nowej rzeczywistości prelegenci Warsaw Security Summit 2021 mówili najwięcej. Podejście do bezpieczeństwa wraz z nadejściem pandemii bardzo się zmieniło. Do segmentu security doszło wiele obowiązków z zakresu safety. Nowe zadania trafiły do działów bezpieczeństwa w dużych korporacjach, przemyśle, handlu czy obiektach infrastruktury krytycznej. Zmiany objęły też zabezpieczenia techniczne. System telewizji dozorowej zaczął służyć także do pomiaru temperatury ciała pracowników i użytkowników, noszenia maseczek czy zachowywania dystansu.
W czasie Warsaw Security Summit 2021 skupiliśmy się na pokazaniu rozwiązań wdrożonych i działających z powodzeniem w referencyjnych realizacjach. Obok wystąpień ekspertów widzowie obejrzeli case study z rozwiązań z różnych sektorów gospodarki z całej Polski. Prelegenci i partnerzy omówili najnowsze trendy w zabezpieczeniach technicznych, kontroli dostępu, telewizji dozorowej czy smart city.

PARTNERZY KONFERENCJI: • Nedap Security Management • Genetec • Axis Communications • Securitas Polska • Sicco • Milestone Systems • Ela-compil • 2N • Gunnebo • Reconeyez/TVPrzemysłowa • TP Link

PARTNERZY TECHNOLOGICZNI: • Hyder Tech • Polfa Tarchomin

PATRONI BRANŻOWI: • Business Center Club • Krajowa Izba Gospodarcza • Polska Rada Centrów Handlowych • Stowarzyszenie Polalarm • Polski Związek Pracodawców Ochrona • Polska Izba Systemów Alarmowych

Mariusz Kucharski

a&s Polska

Organizując tegoroczną edycję konferencji, wykorzystaliśmy wszystkie trzy koła ratunkowe. Po pierwsze: pół na pół. Będzie lockdown czy go nie będzie… Tu się udało. Po drugie: telefon do przyjaciela – tutaj konsultowaliśmy się z naszymi przyjaciółmi z branży. I ostatnie koło ratunkowe: pomoc publiczności, czyli pomoc Państwa, naszych czytelników, uczestników wydarzeń, które organizujemy. No i Państwo w zasadzie jednogłośnie wypowiedzieli się: tak, chcemy się spotkać. Zapadła decyzja: spotykamy się na początku września. Udało się!

Hubert Urbański

prowadzący konferencję

Piotr Sitko

Polska Wytwórnia Papierów Wartościowych

Opowiedziałem o realizacji inwestycji związanej z unifikacją systemu kontroli dostępu w obiektach PWPW. Opowiadałem o systemie, o tym, jak on się integruje, jak jest otwarty na inne systemy. Mówiłem o tym, z jakimi trudnościami się spotykaliśmy i jak je rozwiązywaliśmy, jak to wszystko się udało...

Anna Twardowska

Nedap Security Management

Panel, który prowadzałam wraz z kolegą, Grzegorzem Kosikiem i dwoma naszymi klientami: Grupą Polpharma i Polską Wytwórnią Papierów Wartościowych, dotyczył wprowadzenia systemu kontroli dostępu w obiektach o podwyższonym ryzyku.
Konferencja była pozytywnym zastrzykiem energii. Możliwość rozmowy z klientami i partnerami to jest coś, na co długo czekałam, i bardzo się cieszę, że mogłam tu być.

Jakub Kozak

Genetec

Miałem przyjemność opowiadać o unifikacji systemów zabezpieczeń, o porównaniu unifikacji i integracji oraz o różnicach, które pomiędzy tymi dwoma podejściami można wskazać. I przez chwilę opowiadałem o bardzo dużym wdrożeniu firmy Genetec w Chicago, które opiera się na naszym produkcie Citigraf.
Bardzo dobrze, że Warsaw Security Summit trzyma poziom i jest platformą do wymiany doświadczeń z klientami, z użytkownikami końcowymi i z integratorami systemów zabezpieczeń.

Tomasz Guzikowski

Grupa CIECH

Mówiłem o elementach, które organizacja wdrożyła w trakcie pandemii. Wskazałem na aspekty bezpieczeństwa, które pozwoliły na to, że nasi pracownicy pracowali w sposób bezpieczny. To nam pozwoliło uniknąć nawet jednego dnia przerwy w produkcji.

Krzysztof Poznański

Polska Rada Centrów Handlowych

Mnie osobiście najbardziej zainteresowała prezentacja dotycząca smart city oraz rozwiązań dotyczących bezpieczeństwa i inteligentnych rozwiązań w miastach.
Potrzebujemy więcej takich rozmów o tym, jak powinien wyglądać handel, bezpieczeństwo w handlu w czasie pandemii i po pandemii. Potrzebujemy jak najbardziej więcej tego typu spotkań, więcej tego typu debat.

Konrad Badowski

Axis Communications

Rozmawialiśmy na temat roli dostawcy i integratora w dostarczaniu rozwiązań w obszarze infrastruktury krytycznej.

Tomasz Kępa

UM Katowice

Staraliśmy się przedstawić katowicki system, jako system bardzo oryginalny, otwarty na nowe technologie, który jest nie tylko, jak już na początku XXI w., systemem monitoringu, ale również systemem selektywnego poboru danych. To jest niezwykle istotne w realizacji polityki zrównoważonego rozwoju miasta ze szczególnym uwzględnieniem warunków klimatycznych.

Ewa Oldenburg

Ela-Compil

Rozmawialiśmy o integracji systemów bezpieczeństwa w obiektach. Prezentowaliśmy nasz system GEMOS, który jest wdrażany w Polsce od 1997 roku.

Jacek Tobiasz

Eurocasta

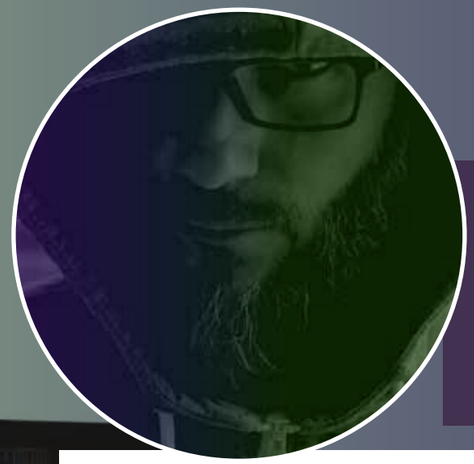
Spotkaliśmy się w takim gronie, że myślę, że wszyscy mamy wspólne spojrzenie na to, jak każdy z nas odczuwa i postrzega ryzyka, jak sobie z nimi radzić, jak możemy iść w przyszłość, jak możemy zabezpieczyć nasze biznesy przed tymi ryzykami w kolejnych okresach...

Paula Siekierska

SICCO

Bardzo się cieszę, że mogłam wystąpić z moim współprelegentem Janem Grusznicem i opowiedzieć o usprawnianiu procesów logistycznych – o tym, jak budować przewagę konkurencyjną, jak cyfryzować mądrze, czyli jak korzystać z dóbr technologii, żebyśmy mieli faktycznie dużą wartość dodaną.

Być mądrzejszym przed włamaniem



Z PIOTREM KONIECZNYM, INFORMATYKIEM, EKSPERTEM DS. BEZPIECZEŃSTWA KOMPUTEROWEGO ORAZ PENTESTEREM, ZAŁOŻYCIELEM POLSKIEGO SERWISU O BEZPIECZEŃSTWIE TELEINFORMATYCZNYM NIEBEZPIECZNIK.PL, ROZMAWIAMY O BŁĘDACH W PODEJŚCIU DO BEZPIECZEŃSTWA I ZABEZPIECZEŃ, KTÓRE MOGĄ NARAZIĆ NAS NA WŁAMANIA.

Jako pentesterzy testujecie systemy zabezpieczeń obiektów, próbując dostać się do środka bez uprawnień i wykraść ważne dla firmy dane. Na ile nieuprawnione wejście i pozyskanie danych ograniczają elektroniczne systemy zabezpieczeń, a na ile ułatwiają je sami pracownicy firmy?

Odpowiem typowym dla ludzi pracujących w bezpieczeństwie stwierdzeniem: TO ZALEŻY. Trzeba by było rozpatrywać te zdarzenia w odniesieniu do konkretnego przypadku. Przypominam sobie sytuację, kiedy udało nam się przeniknąć do biura w siedzibie klienta w ogóle bez zastanawiania się, czy jakieś elementy elektronicznego systemu zabezpieczeń istnieją i funkcjonują, bo po drodze ich nie widzieliśmy. Nasza taktyka polegała na manipulacji strażnikami bądź pracownikami firmy. Ale były też przypadki, gdy z pracownikami w ogóle nie mieliśmy do czynienia, ponieważ wchodziliśmy do obiektu, który był odizolowany od części pracowniczej. Był monitorowany tylko za pomocą kamer, odpowiednich czujników, miał też zabezpieczenia fizyczne w postaci ogrodzenia, mat naciskowych i innych tego typu urządzeń, czyli był zabezpieczony techniką i z nią się zmagaliśmy. Prawdopodobnie do tej techniki gdzieś na końcu był podpięty człowiek, który albo spał, albo tak dobrze udało nam się ominąć różnego rodzaju czujniki, że nie wywołały alertów i żaden patrol nie przyjechał, żeby nas z tego obiektu wyprowadzić.

To znaczy, że udało się wejść do środka pomimo tych zabezpieczeń?

Tak, udało się. W każdym przypadku, który do tej pory realizowaliśmy, udało nam się osiągnąć wyznaczony przez klienta cel lub nawet kilka celów. Nie zawsze jest to np. wyniesienie serwera lub zdobycie konkretnych danych. Często chodzi o wykonanie dokumentacji fotograficznej, np. danego spotkania czy osoby, która o danej godzinie będzie w gabinecie prezesa. Firmy określają pewne scenariusze zagrożeń, których najbardziej się obawiają. Czasem jest to przeniknięcie nieznanej osoby, np. z konkurencji lub agencji detektywistycznej, która zbiera informacje o tym, jak funkcjonuje firma, jak przebiegają u niej różne procesy, a czasem brutalne przeniknięcie do serwerowni kończące się wyniesieniem konkretnego serwera. Oczywiście takie kontrolowane wejścia siłowe, bo mają one z siłą wiele wspólnego, w przełamywaniu zabezpieczeń praktycznie zawsze realizujemy w taki sposób, żeby minimalizować straty klienta. Naszym celem nie jest przecięcie kabli czy kradzież serwera, co unieruchomi firmę, narażając ją na straty finansowe z powodu przerwy w działalności czy utraty klientów. My, będąc na wyciągnięcie ręki od serwera, np. wiążemy kokardkę na odpowiednim kablu sieciowym, i to jest wiadomość dla firmy: byliśmy tutaj, mogliśmy ten kabel przeciąć, mogliśmy ten serwer wynieść itp., ale nie robimy tego. I na tym polega różnica pomiędzy osobami chcącymi zaszkodzić a tymi, które tylko takie zabezpieczenia testują.

Przykładów tego, co interesuje klienta, jest dużo, chociażby zostawienie tzw. implantu (czyli urządzenia podsłuchowego) w sali konferencyjnej, gdzie odbywa się wiele ważnych spotkań. Podsłuch może być klasyczny, np. w postaci długopisu kupionego na AliExpress za kilka dolarów. My stosujemy implanty sieciowe. Podpinając taki implant do gniazdka sieciowego w sali konferencyjnej, zbieramy wszystko, co audiowizualnie dzieje się w danym pomieszczeniu, ale też jesteśmy w stanie w trakcie takiego spotkania próbować się włamywać na laptopy podpięte do tej sieci, a często poprzez nią do całej sieci firmowej, np. do działu finansowego lub HR. Możemy też połączyć się z najbliższą drukarką i pobrać ostatnio drukowane dokumenty nie tylko osób będących w tej sali, ale także z całej firmy.

Nasze zadanie polega głównie na tym, aby taki implant niepostrzeżenie podpiąć. To nie wymaga zbyt wiele czasu, tu krytyczne jest bycie niezauważonym. Wiele wysiłku wkładamy w zamaskowanie tego implantu, by nie został usunięty. Często stosujemy następujący trik: przyklejamy żółtą kartkę z napisem: *Nie odpinać!* I zadziwiająco dobrze to działa, bo sporo pracowników z *upper managementu* to nie są osoby techniczne. Chcą w sali konferencyjnej podpiąć laptop i puścić prezentację. I jeśli widzą karteczkę z napisem: *nie odpinać*, to myślą, że jest to polecenie ich działu IT, i stosują się do tych instrukcji.

W swoich działaniach nadużywamy zaufania ludzi, bo jest to jednak atak socjotechniczny. Mówimy komuś nie dotykaj – i on się do tego stosuje. Ale jednocześnie jest to metoda oszukania pewnych zabezpieczeń, ponieważ podpięcie nieznanego urządzenia pod port sieciowy powinno zostać wychwycone przez dział techniczny i wiązać się z odpowiednią reakcją. Zakładam, że w idealnym świecie taka czynność wywołuje odpowiedni komunikat w dziale IT. Pracownik tego działu sprawdza, co się dzieje w sali konferencyjnej, i jeśli zobaczy karteczkę z komunikatem, o którego istnieniu nie wie, to ją usunie, słusznie przypuszczając, że nie zostawili jej koledzy i nie powinno jej tu być. Praktyka jest taka, że wiele osób na tego typu monity nie reaguje, jeśli w ogóle takie zdarzenia monitoruje. Większość zakłada, że jeżeli ktoś jest w biurze, jest to zaufana osoba.

Na podstawie swojego doświadczenia możesz wskazać, na ile zabezpieczenia techniczne, a na ile sami pracownicy ułatwiają penetracje?

Przy wejściach fizycznych zawsze jesteśmy przygotowani na zabezpieczenia techniczne, które w jakiś sposób można ominąć. Inaczej jest z zabezpieczeniami natury informatycznej. Nie bawimy się we wspinanie po drabinie i zasłanianie pola widzenia kamery zdjęciem z polaroidu, jak to pokazują w filmach amerykańskich. Godzimy się z faktem, że tego typu zabezpieczenia funkcjonują, i liczymy na to, że osoba patrząca na ekran w danej chwili po prostu nie zauważy w naszym zachowaniu albo w wyglądzie czegoś podejrzanego. Biorąc pod uwagę czynnik ludzki, duże znaczenie ma element wiarygodności. Gdy wchodzimy do obiektu, staramy się mieć identyfikatory, które – przynajmniej z daleka – wyglądają jak autentyczne. Obrazy tych identyfikatorów bardzo łatwo można zdobyć, czy to przeglądając zdjęcia pracowników, które sami umieszczają w mediach społecznościowych, czy też np. w kantynie podczas przerwy obiadowej. Tam można zobaczyć, co mają na swoich bagdach. Nasze wejście do firmy zawsze jest poprzedzone zwiadem, który ma na celu maksymalne rozpoznanie mechanizmów bezpieczeństwa firmy na płaszczyźnie ochrony zarówno fizycznej, jak i technicznej.

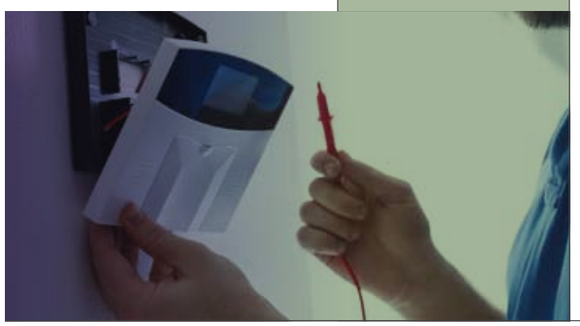
Oczywiście nie zawsze udaje nam się oszukać system. Czasem ktoś zauważy, że w naszym etui na identyfikator jest zwykła folia śniadaniowa, która tylko symuluje hologram. Wtedy musimy wykazać się umiejętnością manipulacji, żeby takiego pracownika przekonać, że jesteśmy wiarygodni i możemy iść dalej, lub żeby zająć go czymś innym, aby mieć czas na szybkie opuszczenie obiektu czy nawet ucieczkę.

Jak rozumiem, jeszcze nie uciekaliście, bo mówiłeś, w każdym przypadku udało się wam zrealizować cel?

Oczywiście to, że zrealizowaliśmy cele, które do tej pory przed nami postawiono, nie oznacza, że nie uciekaliśmy z obiektu. Cel może być wieloetapowy i mamy pięć czy sześć podejść, by dostać się do środka. Kiedy nas raz złapią, to staramy się powtórzyć próbę za jakiś czas, licząc np. na inną zmianę pracowników. Nie zawsze schwytanie oznacza, że wzywana jest policja, czasami jest to po prostu interwencja ochrony. Jeśli nie uda nam się metoda

na tzw. pałę, to opracowujemy bardziej finezyjny plan. Mieliśmy też sytuację, że pracownik zidentyfikował nas jako nieproszonych gości. Wtedy gratulowaliśmy czujności i przyznawaliśmy się, że jesteśmy na specjalnym zleceniu, na dowód wyciągaliśmy dokument nazywany przez nas *free-of-jail-card,* podpisany przez zleceniodawcę. Pracownik, widząc znajome nazwisko, puszczał nas wolno. Oczywiście było to złamanie przez niego procedury, ponieważ powinien potwierdzić autentyczność dokumentu, dzwoniąc do tego szefa. Tu często brakuje wyszkolenia pracowników.

Na co więc powinni zwracać uwagę security menedżerowie przy zabezpieczaniu obiektu?
Należy brać pod uwagę dwie sprawy. Po pierwsze, nie ma idealnych zabezpieczeń, każde można ominąć. To kwestia budżetu, jakim dysponuje atakujący, jak dobrze będzie przygotowany i jak bardzo zdeterminowany i czy będzie mu sprzyjał los. Bo raz na jakiś czas może pojawić się nieprzewidziane wydarzenie, które ułatwi wejście do budynku. Przykładowo mogą to być ćwiczenia związane z ewakuacją. Wtedy drzwi są otwarte, wszyscy wychodzą i nikt nie zwraca uwagi na nieznajomych. Często o takich akcjach informują nas sami pracownicy, zapowiadając to na Snap Chacie lub wrzucając zdjęcia z takiego wydarzenia na social media.
Po drugie – jeśli mówimy o security menedżerach – trzeba zwrócić uwagę na procesy, czyli wymodelowanie zagrożeń, które dla firmy są najistotniejsze. Gdy to będzie nieproszony gość, to które piętro jest newralgiczne i czy są strefy wydzielone w obiekcie. Bo w przypadku hali produkcyjnej zakładu farmaceutycznego lub produkującego żywność, gdyby tam pojawił się intruz, ryzyko jest ogromne – może dojść np. do skażenia produktów i w efekcie ogromnych strat dla firmy. Nie mam tu uniwersalnej rady, ale jest pewien proces, który nazywamy w bezpieczeństwie analizą ryzyka. Zdefiniuj, co jest dla ciebie priorytetowe, czy



to jest właśnie hala produkcyjna, czy może dane pracowników, a może dane klientów, które mogą znajdować się w chmurze lub na serwerze. Kiedy masz zdefiniowane najważniejsze rzeczy, to tak zbuduj ochronę tego obszaru, żeby był on w odpowiednim stopniu zabezpieczony. Wdrażając mechanizmy ochrony, czy to na warstwie fizycznej, czy informatycznej, należy wymodelować mogące nastąpić zagrożenia. Oczywiście nie da się przewidzieć wszystkich, ale można bazować na incydentach, które już się u nas pojawiały.
Te wszystkie działania należy dostosować do specyfiki danej firmy, jej celów biznesowych i posiadanego budżetu przeznaczonego na bezpieczeństwo.

Oprócz wymienionych przez ciebie czynników dochodzą ogólnoświatowe, np. pandemia, która przyczyniła się do wzrostu popularności rozwiązań w chmurze. Jednak zwiększona aktywność cyberprzestępców spowodowała, że nie wszyscy są przekonani do tego typu metod. Czym się kierować przy wyborze rozwiązań opartych na chmurze?
To temat, który spędza sen z powiek wielu specjalistom ds. bezpieczeństwa. Po godzinach rozważań dochodzimy do tej samej co poprzednio odpowiedzi – TO ZALEŻY. Zależy od specyfiki firmy, od tego, jak zbudowana jest infrastruktura, bo nie każdą łatwo można przenieść do chmury, zależy od tego, ile ktoś ma czasu na ten projekt, ile środków może na niego przeznaczyć. Na kanale Niebezpiecznika na YouTubie mamy ponadgodzinny wywiad z ekspertem z Polskiej Chmury Krajowej, w którego ramach przechodzimy przez te wszystkie dylematy, zastanawiamy się, która konstrukcja chmury jest najlepsza, kiedy się opłaca, ile kosztuje u poszczególnych dostawców. Zauważamy, że dziś coraz popularniejsze jest podejście hybrydowe, kiedy to część rozwiązań możemy zostawić u siebie. Koszty mogą być niższe niż w przypadku abonamentu za usługi chmurowe w całości. Nie odważyłbym się odpowiedzieć na pytanie, które rozwiązanie jest lepsze, bez wnikliwej analizy, a ta może zająć nawet kilka miesięcy, ponieważ trzeba poznać procesy funkcjonujące w danej firmie, jej potrzeby, spodziewany kierunek rozwoju, poziom merytoryczności kadry i chęci do podnoszenia kwalifikacji.
Z mojego doświadczenia wynika, że wiele firm podejmuje decyzję o wyborze rozwiązania bez głębszej analizy tych danych. To zawsze należy dokładnie przemyśleć, ponieważ w niektórych przypadkach lepiej sprawdzi się korzystanie z usług w chmurze, a w innych nie.

Trochę zweryfikowałeś mój pogląd, bo sądziłam, że chmura jest absolutnie bezpieczna...
Nie ma rozwiązań absolutnie bezpiecznych. W naszej branży mówi się, że chmura to tak naprawdę czyjś komputer. Nie patrzymy na to, czyj on jest i gdzie się znajduje, sprawdzamy go pod kątem metod ataku. Tak jak w przypadku komputera przeciętnego użytkownika.

Z naszych obserwacji wynika, że w branży zabezpieczeń technicznych jest silny trend do korzystania z rozwiązań w chmurze. Mamy przeświadczenie, że dostawca tych rozwiązań zadbał o to, żeby ktoś tam siedział i na bieżąco aktualizował system. W przeciwieństwie do serwerów lokalnych, które nie będąc na bieżąco aktualizowane, są gorzej chronione. Czy zgadzasz się z tym?
Nie do końca. Są plusy i minusy każdego rozwiązania. Faktem jest, że mówiąc o chmurze, mówimy o cudzej in-

ŻART, KTÓRY KRĄŻY W NASZEJ BRANŻY: „IoT JEST SKRÓTEM, W KTÓRYM B OZNACZA BEZPIECZEŃSTWO"

frastrukturze, która zazwyczaj ma własny zespół monitorujący jej bezpieczeństwo. Jeśli monitorują takie zagrożenia, jak ataki DDoS czy nowe błędy w protokołach, o których ze względu na ich duży udział w sieci zostają poinformowani przez producentów oprogramowania jako jedni z pierwszych, to jak najbardziej jesteśmy bezpieczni. Lecz nie jest tak, że jeśli mamy serwer w chmurze, to nas nikt nie zhakuje. Dostawcy usługi oczywiście o nas dbają, patrzą dokładnie na naszą aplikację, analizują ją pod kątem bezpieczeństwa, będą robić wszystko, aby nas zabezpieczać. Ale są mechanizmy w chmurze zbierające np. logi i za ich analizę odpowiedzialność spoczywa na nas. Czyli dalej firmowy zespół bezpieczeństwa musi zabezpieczać nasz system, tylko teraz może to robić za pomocą zdalnych narzędzi w wirtualnym środowisku, a nie lokalnie, na urządzeniach, do których musi się podpiąć fizycznie.
Wszystko zależy od tego, jak wygląda konfiguracja systemu, o jakich typach ataków mówimy. Nie ma jednego rodzaju ataku i nie ma jednego mechanizmu obrony. Chmura ma zalety, ale i wady. Trzeba odpowiedzieć sobie na pytanie, na czym nam bardziej zależy. Jeśli na mniejszej awaryjności, to prawdopodobnie chmura w większości przypadków może być lepszym rozwiązaniem.
Oczywiście mogą się zdarzyć sytuacje nieprzewidziane, takie jak pożar serwerowni jednego z większych dostawców usług chmurowych, który spowodował, że nagle część świata na kilka godzin przestała funkcjonować. Jest to jednak nieporównywalne z konsekwencjami incydentów, jakie mogą się zdarzyć lokalnie, np. gdy zostaniemy pozbawieni prądu w wyniku awarii sieci, a jej usuwanie potrwa dłużej niż kilka dni, lub brak zasilania uszkodzi dyski i utracimy dane na nich zapisane.
Dla tych, którzy mają obawy, nie wiedzą, jakie podejście wybrać, dobrym rozwiązaniem będzie przenieść część zasobów do chmury, a pozostałą część pozostawić u siebie lokalnie. A potem porównać, gdzie i jakie mamy problemy. Które z nich są dla nas bardziej kosztowne? Bo nawet zostawiając rozwiązania lokalnie, można zatrudnić profesjonalną firmę zajmującą się świadczeniem usług security, która będzie sprawowała pieczę nad bezpieczeństwem naszego systemu, czyli będzie lokalnie monitorowała, sprawdzała i reagowała na zagrożenia dokładnie tak samo, jak robią to specjaliści dostawców chmury. Jeśli oprogramowanie jest zaktualizowane, ryzyko ataku hakerskiego jest niewielkie. Zazwyczaj to ryzyko jest związane z nieznanym atakiem, do którego nie mamy jeszcze łatki.

A czy Niebezpiecznik.pl korzysta z rozwiązań w chmurze?
Tak.

OK, to nam wystarczy. Wróćmy do tematu elektronicznych systemów zabezpieczeń, które – w większości realizacji – stają się już częścią większej infrastruktury sieciowej. Co muszą wiedzieć administratorzy sieci, a co specjaliści „od kamer", aby system dozorowy działał poprawnie i jednocześnie nie był zagrożeniem dla pozostałych elementów infrastruktury?
Nie patrzmy, czy to jest kamera, czy czujka dymu lub inne urządzenie inteligentne. Generalnie urządzenia IoT, czy tzw. *smart devices,* z punktu widzenia osób zajmujących się bezpieczeństwem sieci nie są niczym innym, jak rodzajem komputera. Można je skonfigurować w dobry sposób, czyli poddać tzw. *hardeningowi*, zaprojektować z myślą o bezpieczeństwie albo zostawić w domyślnej konfiguracji. Z punku widzenia sieci niezależnie, czy podpinamy komputer pracownika, czy kamerę CCTV, administrator musi na to patrzeć dokładnie tak sa-

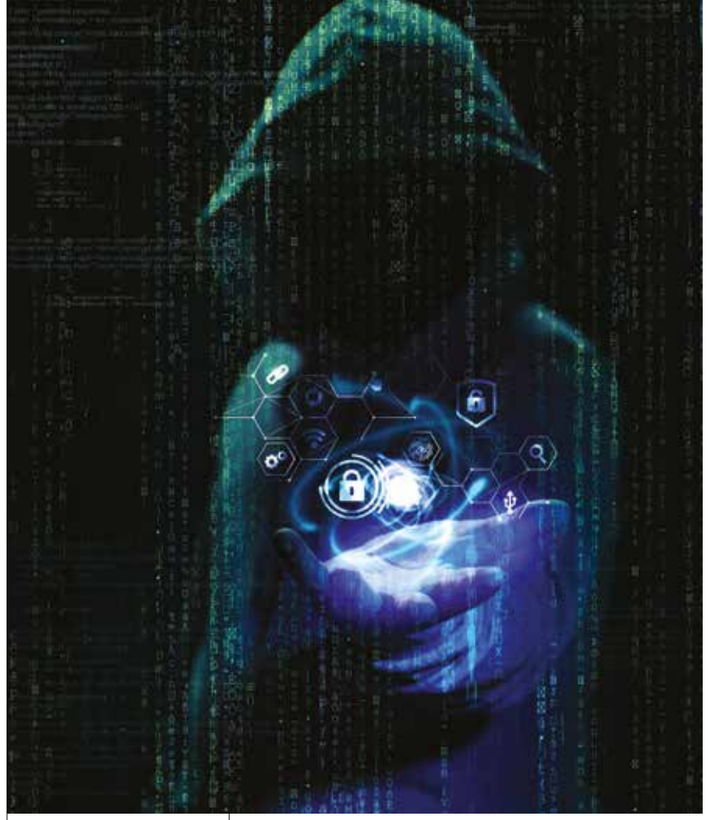
mo. Bo do kamery sieciowej również można się włamać i wgrać złośliwe oprogramowanie. Ten aspekt znakomicie odzwierciedla żart, który krąży w naszej branży, że „IoT jest skrótem, w którym B oznacza bezpieczeństwo". Jest jeszcze jedna kwestia: system monitoringu wizyjnego można przecież skonfigurować w sposób, który utrudnia działania atakującym. Podam przykład. Jeśli są przeprowadzane audyty, czyli sprawdzamy: kamery – są, *hardening* – jest, hasło – jest itd., czyli wszystko zgodnie z najlepszymi praktykami, to w wielu przypadkach jest to wystarczające. Tylko jeśli nie przeskanuje się portów danego urządzenia, to nie będzie się wiedzieć, że na jednym z nich bez żadnego uwierzytelnienia da się podpiąć pod strumień wideo. Po wybraniu odpowiedniego kanału można oglądać obrazy z kamery, mimo że nie ma się hasła do niej. Zmierzam do tego, że nie muszę mieć loginu i hasła, żeby widzieć to, co pokazuje się po zalogowaniu do panelu administratora.

W takim razie, jakie błędy obserwujecie po stronie branży elektronicznych systemów zabezpieczeń, zaczynając od producentów, przez dystrybutorów, instalatorów i wreszcie użytkowników?

W skrócie – wszystkie. Po pierwsze producenci tworzą urządzenia nie zawsze przygotowane do pracy w Internecie. Część systemów była przewidziana tylko do pracy w sieci wewnętrznej. Ale dziś, nawet jeśli wydzielimy zamknięty system monitoringu wizyjnego, wystarczy tylko jedno urządzenie, np. stacja robocza pracownika ochrony, które ma dostęp do Internetu. Gdy pracownik kliknie w to, w co chcemy, żeby kliknął, mamy dostęp do jego komputera, a poprzez to do całej sieci firmowej. Jeśli w sieci jest przynajmniej jedno urządzenie z dostępem do Internetu, to cała sieć, mimo że jest wewnętrzna, może być narażona na ataki.

Drugą kwestią jest brak odpowiedniej konfiguracji niektórych urządzeń. Oczywiście są urządzenia, które mają zmieniane hasła domyślne, pozmieniane porty, włączone dodatkowe zabezpieczenia wymagane przez producenta, ale często są też takie, które zostawiono na domyślnych ustawieniach. Spotkaliśmy się też z sytuacją, kiedy urządzenia konfigurował pracownik firmy XYZ. Dla ułatwienia konfiguracji do wielu urządzeń stosował jedno hasło serwisowe. Mogliśmy więc z dużym prawdopodobieństwem przewidzieć, że takie samo hasło, co u klienta X, zastosuje też u klienta Y. Często się to zdarza. Tu również potrzebne jest wdrożenie dobrych praktyk.

Ostatnią rzeczą, która jest chyba najsłabszym ogniwem w łańcuchu bezpieczeństwa, jest „interfejs białkowy", czyli człowiek, który powinien monitorować, nadzorować i reagować, a tego nie robi, bo np. patrzy w smartfon, ogląda Facebooka albo filmik na YouTubie.



Tu pojawia się też brak zrozumienia niektórych producentów, na jakie ataki mogą być narażone ich urządzenia. Zwracają uwagę na bezpieczeństwo całego systemu, ale pomijają jego małe elementy. Przykładowo karty kontroli dostępu można łatwo sklonować, stając za pracownikiem firmy, np. w kolejce po lunch.

Czy klonujecie takie karty?

Staramy się tego nie robić, bo to jednak zajmuje czas. A są prostsze i szybsze metody. Mówiąc obrazowo: jeśli u klienta widzimy drzwi z kartonu, to po prostu je wyważamy. Ale jeśli klient ma dobre drzwi antywłamaniowe, to zamiast je forsować, wybieramy wejście przez okno, czyli poszukujemy innej, najłatwiejszej ścieżki.

Na zakończenie poprosimy, żebyś podzielił się swoimi radami, na co powinniśmy zwracać baczną uwagę, aby nasze obiekty i firmy były bezpieczne

Z perspektywy atakującego często spotykamy sytuacje, że osoby inwestują w wysoko zaawansowane i bardzo drogie urządzenia, przechodzą szkolenia, a potem my stajemy za ich plecami i widzimy, jaki kod wpisują na pinpadzie. Mógłbym podać wiele takich przykładów. Inwestujemy dużo w zabezpieczenia, myślimy, że jesteśmy bezpieczni, ale dalej nie zwracamy uwagi na to, co dzieje się wokół nas. Nie zdajemy sobie sprawy z tego, że będąc uprzejmym i przytrzymując drzwi osobie, która ma zajęte ręce wielką przesyłką lub tacą z napojami, wpuszczamy do środka intruza. Często głównym czynnikiem stwarzającym zagrożenie jesteśmy my sami. Dbając o bezpieczeństwo, musimy przestrzegać procedur, a to nie zawsze wiąże się z przestrzeganiem reguł savoir vivre'u czy pójściem na kompromisy. W dobrym bezpieczeństwie kompromisów po prostu nie ma.

Rozmawiali
Iwona Krawiec i Jan T. Grusznic (a&s Polska)

Innowacyjne rozwiązania integracji systemów bezpieczeństwa
Światowa nowość na polskim rynku klasy PSIM-CSIM

Venom PSIM PLATFORM

Skontaktuj się z nami w sprawie dedykowanej prezentacji

MEGAVISION TECHNOLOGY Sp. z o. o.
Heliotropów 1
04-796 Warszawa
tel. +48 22 292 3 292
psim@psim.pl

MEGAVISION technology

Czy inteligentna analiza wizyjna zapobiegnie samobójstwom w celi więziennej

Cz. 2. Technologie informatyczne wspierające operatora systemu monitoringu

W części pierwszej artykułu (A&S 4/2021) autorzy wskazali na wyniki przeprowadzonych badań operatorów systemu dozoru wizyjnego w polskiej Służbie Więziennej oraz potrzebę ich wsparcia w stałej obserwacji zachowania osadzonych, szczególnie w celu zapobiegania samobójstwom.

Cezary Mecwaldowski

Robert Poklek

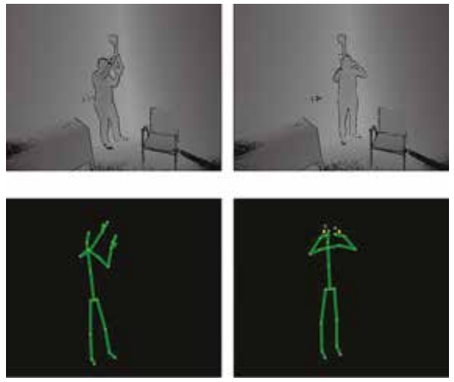
Za rozwiązanie najbardziej obiecujące uznano inteligentną analizę treści wizyjnej *(intelligent video analytics* – IVA, *video content analysis* – VCA*)*. Nie jest to nowość w więziennictwie. Na świecie prowadzi się wiele badań w tym zakresie – od Korei Płd., Chin, przez Niemcy, Wlk. Brytanię, USA, po badania autorów w Polsce. Odpowiedź na jedno pytanie rodzi dwa kolejne, dlatego badania są kontynuowane i świadomie nie zdecydowano się na wdrożenia. Od dawna trwają próby zaadaptowania tej technologii w zakresie wykrywania zachowań ludzkich – od łatwo dostrzegalnych, np. pozostawienie przedmiotu, przekroczenie linii, kierunek i prędkość poruszania, błądzenie, odległość pomiędzy osobami, postać leżąca, stojąca itp., po te, które trudniej zaobserwować, np. zmiana stanu emocjonalnego, sposobu chodzenia czy zachowania wynikające z długiego czasu obserwacji.

Autorzy przestrzegają przed stosowaniem technologii IVA bez ich wcześniejszych badań i adaptacji przy rozróżnieniu stanowisk i ich celów w więzieniach. Należy rozróżnić stosowanie dozoru wizyjnego (monitoringu) w zakresie zachowania osadzonych i bezpieczeństwa (bójki, ucieczki, niszczenie mienia itp.) od zapobiegania samobójstwom w celi więziennej. Prowadzone na świecie badania, które mogą znaleźć zastosowanie w zapobieganiu samobójstwom w więzieniach, bazują z reguły na dwóch rozwiązaniach: rozpoznawaniu postawy osoby, dynamiki obrazu *(fot. 1)* oraz rozpoznawaniu emocji z obrazu twarzy *(fot. 2)*. Zdaniem autorów najsłabszą ich stroną są sytuacje samobójstw w łóżku, gdyż poza osoby nie jest jednoznaczna, a kamera nie może zapewnić odpowiedniego obrazu twarzy. Niestety rozwiązania bazujące wyłącznie na postawie osoby i dynamice obrazu w najlepszym przypadku pozwolą uzyskać alarm z systemu, gdy do próby samobójczej już dojdzie. Nie należy sugerować się przykładami spoza więzień, np. opisywanym w literaturze przypadkiem zapobiegania samobójstwom na mostach w Seulu[1]. Występują tam zupełnie inne uwarunkowania zachowań samobójczych, przestrzeni i miejsca. Na moście, dzięki możliwości zastosowania detekcji przekroczenia linii lub obszaru, uzyskuje się dodatkowy parametr, który wraz z detekcją „szwendania-błądzenia" pozwala ustalić kryterium i wygenerować alarm z wysokim prawdopodobieństwem zdarzenia suicydalnego. Takich jednoznacznych kryteriów w celi więziennej nie da się ustalić.

Koncepcja autorów opiera się na rozwiązaniu, którego wynik pozwoli na alarmowanie presuicydalne, suicydalne i postsuicydalne. Jej istotą jest połączenie różnych technologii uczenia maszynowego z rozpoznawaniem postawy, emocji i behawioralnych reakcji osadzonego w celi w długim wymiarze czasowym. Uczenie maszynowe pozwoli na generowanie alarmu nie tylko w sytuacji niedostrzegalnych dla obserwatora zmian obrazu (np. na poziomie pojedynczych pikseli), ale także przy wystąpieniu subtelnych zmian zachowania, poruszania się, gestów, emocji z mimiki lub głosu *(fot. 3)*, ruchów manipulacyjnych dłoni, postawy ciała itp. w długim okresie.
Kolejną niezwykle istotną kwestią jest operator systemu dozoru wizyjnego. Mimo zastosowania algorytmów automatycznej detekcji nadal pełni on nadrzędną decyzyjną funkcję. Analizy przeprowadzone przez autorów doprowadziły do następujących konkluzji: należy jednoznacznie wybrać typ operatora[2].

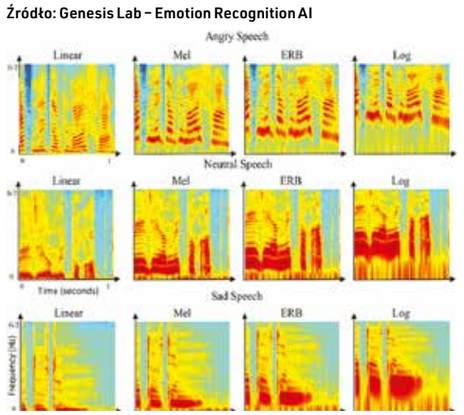
Typ 1 to klasyczny operator monitoringu, który wyłącznie obserwuje obrazy i podejmuje decyzje o wykryciu zdarzenia. Technologia IVA w przypadku implementacji algorytmów do zadań typu 1 będzie takiego operatora rozpraszała, a po czasie stwierdzi, że nie musi obserwować, skoro system za niego weryfikuje zdarzenia (pojawi się naturalny efekt minimalizacji zużycia energii). Jednak niezadziałanie automatycznych algorytmów pozostawia szansę zaobserwowania zdarzenia przez operatora zaangażowanego w obserwację. Typ 2 z kolei to operator, który oczekuje na alarm z innych systemów. Dopiero sygnał uaktywnia operatora, który przyczynę alarmu z systemu IVA weryfikuje z sytuacją na obrazie z kamer. Jego obowiązkiem nie jest ciągła obserwacja i wyszukiwanie zdarzeń w obrazie. Istnieje poważne ryzyko, że gdy algorytm nie zadziała, operator nie zareaguje na zdarzenie. W obszarze przestrzegania prawa do prywatności osadzonego wybór operatora typu 2 jest właściwszy – mimo mniejszej skuteczności (operator nie obserwuje stale osadzonego, robi to wyłącznie w sytuacji detekcji i alarmu zdarzenia wygenerowanego przez IVA).

1 Seul, *Sztuczna inteligencja wykrywa i zapobiega próbom samobójczym na mostach*, „Rzeczpospolita", 30.06.2021 r.
2 C. Mecwaldowski, R. Poklek, *Przygotowanie stanowiska operatora systemu dozoru wizyjnego. Aspekty psychologiczne i techniczne*, OMil 6/2019.



Fot. 1. Technologia rozpoznawania pozycji ciała w przypadku próby samobójczej
Źródło: W. Bouachir, R. Noumeir, Automated video surveillance for preventing suicide attempts

Fot. 2. Rozpoznawanie emocji na podstawie analizy mimiki twarzy
Źródło: Genesis Lab – Emotion Recognition AI



Fot. 3. Rozpoznawanie emocji na podstawie analizy głosu
Źródło: M. Lech, M. Stolar, Ch. Best, R. Bolia, Real-Time Speech Emotion Recognition Using a Pre-trained Image Classification Network: Effects of Bandwith Reduction and Companding. Frontiers in Computer Science, 26.05.2020

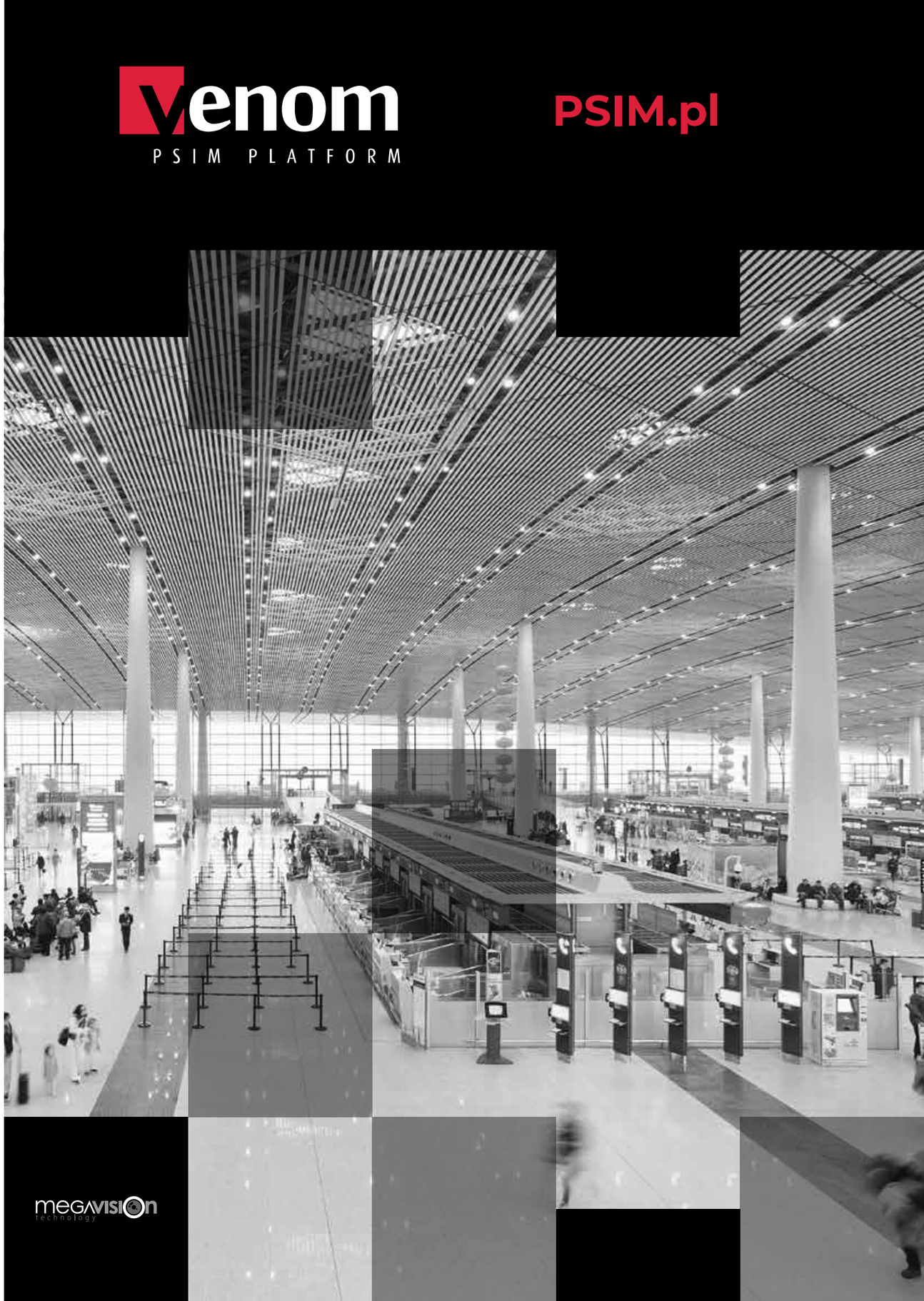
Zastosowanie technologii do rozpoznawania prób samobójczych za pomocą pozycji ciała osadzonego ma słabe strony. Ograniczona przestrzeń celi utrudnia rozpoznanie pozycji ciała, a tym bardziej innych metod samobójstwa. W razie pocięcia, połknięcia leków, trucizny, przedmiotów, podpalenia, porażenia prądem czy uduszenia workiem (w łóżku, i to pod przykryciem) zastosowanie wyłącznie detekcji pozycji ciała jest mało lub w ogóle nieskuteczne w przeciwdziałaniu takim zdarzeniom. Operator otrzyma informację, że do próby samobójczej już doszło.
Analiza zachowań zarejestrowanych bezpośrednio przed dokonaniem czynu samobójczego wykazała, że większość z nich jest typowa i nie odbiega zbytnio od codziennych czynności – osadzony spokojnie realizuje swój plan, jest zdeterminowany, co często nadaje pewność jego ruchom. Jednak cały plan odebrania sobie życia układany jest zdecydowanie wcześniej i wiąże się ze zmianami behawioralnymi (zamyślenie, zmiany stanu emocjonalnego zauważalne na twarzy i w gestach, początkowa nerwowość, próby ukrycia swoich zamiarów, a na końcu pozorna poprawa samopoczucia), które są na tyle subtelne, że obserwator nie jest w stanie ich ze sobą powiązać i skojarzyć jako przygotowanie do samobójstwa. Stąd zaproponowane wprowadzenie przez autorów uczenia maszynowego zachowań osadzonych w celi, poddawane analizie w długich okresach. System uczy się zachowania osadzonych i tworzy wzorzec niezauważalny dla operatora, ale system wykryje nawet subtelne zmiany we wzorcowym zachowaniu. Jak zakładają autorzy, pozwoli to na rzeczywiste alarmowanie presuicydalne i zapobieganie, a nie tylko działanie *post factum*.
Skuteczność proponowanego połączenia technologii może być mniejsza w sytuacji, kiedy osadzony przebywa krótko w więzieniu, ale rośnie z czasem pobytu i wraz z gromadzonymi danymi w systemie uczącym się zachowań i emocji osadzonego. Mocną stroną koncepcji jest zastosowanie trzech technologii uczenia maszynowego, rozpoznawania pozycji ciała (postawy) osoby i emocji z mimiki twarzy (lub w wariancie głosu, pozwalając także rozpoznawać stan zdrowia, zbliżający się atak serca lub zdrowie psychiczne). Wykorzystanie mimiki i rozpoznania stanu emocjonalnego osadzonego może być alarmowane bezpośrednio do funkcjonariuszy pracujących z osadzonym w oddziale – ochronie, wychowawcy czy psychologom. Taki funkcjonariusz po otrzymaniu informacji (SMS lub na dedykowany komunikator), że dany osadzony ma obniżony nastrój, depresję lub jest pobudzony, mógłby niemal natychmiast się nim zainteresować.
Rozwiązania rozpoznające stan zdrowia i emocje drastycznie ingerują w sferę prywatności. Istnieje uzasadnione zagrożenie nadużyć w tym zakresie, więc przed wdrożeniem takiej technologii niezbędne są odpowiednie regulacje ustawowe i procedury gwarantujące praworządne stosowanie.

Natura ludzka ma cechę dążenia do osiągnięcia celu, więc jeżeli celem tym będzie samobójstwo, osadzony z pewnością go dokona mimo trudności. Będzie usiłował „przechytrzyć" system, np. rozbierze się ze specjalnej odzieży, uszkodzi stosowane środki techniczne, przemyci przedmioty itp. Skutek może być dwojaki – dokonanie samobójstwa lub spowodowanie alarmu inteligentnej analizy obrazu, który często generowany, osłabi czujność operatora i wywoła rutynę.
Oprócz opisanego przykładu przeciwdziałania samobójstwom analityka obrazu może wspierać zadania operatora monitoringu oraz pełnić funkcję automatycznego alarmowania w systemach bez operatora. Istotnym argumentem jest kwestia ochrony prywatności, kiedy za bezpieczeństwo odpowiada automatyczny system i nie ma stałej obserwacji przez operatora.
Autorzy już w 2015 r. w Centralnym Ośrodku Szkolenia Służby Więziennej w Kaliszu, w ramach zadań Zespołu Rozwojowo-Badawczego, rozpoczęli projekt badań nt. zastosowania IVA/VCA w zakładach karnych. Założenia koncepcyjne zostały opisane w artykule w 2015 r. Przeprowadzili analizy zarejestrowanych nagrań ze zdarzeń prób samobójczych i samobójstw oraz innych zdarzeń z udziałem osadzonych. Badali literaturę tematu oraz możliwości zastosowania istniejących rozwiązań IVA, przygotowali też nagrania symulowanych scen sytuacyjnych w celach więziennych do prac nad dedykowanym oprogramowaniem jako materiał wejściowy do opracowania analizy wizyjnej.
Koncepcja obejmowała zastosowanie IVA oraz uczenia maszynowego *(Machine learning – ML)*. Materiały zostały przygotowane w laboratorium Centralnego Ośrodka Szkolenia SW w Kaliszu. Opracowane zostały założenia koncepcyjne do programu badawczo-rozwojowego. Koncepcja obejmuje szereg zagadnień i wykorzystuje wieloletnie doświadczenie autorów w zakresie psychologii i systemów dozoru wizyjnego.

Fot. 4. Przykład materiałów do badania zastosowania IVA – bójka w celi
Źródło: opracowanie własne

Fot. 5. Przykład materiałów do badania zastosowania IVA – postawa siedząca przy łóżku
Źródło: opracowanie własne

3 J. McCormick, *What AI Can Tell from Listening to You*, "The Wall Street Journal", 1.04.2019.



Fot. 6. Przykład materiałów do badania zastosowania IVA – postawa leżąca w łóżku

Źródło: opracowanie własne

Początkowe założenia koncepcyjne objęły szerokie zastosowanie analizy wizyjnej. Poniżej przykład obszarów dozorowania, z przyporządkowanymi automatycznie alarmami generowanymi po zebraniu wystarczającego materiału behawioralnego do stworzenia maszynowego wzorca zachowań:

- **W celach mieszkalnych, celi izolacyjnej, przejściowej, celi dla tzw. niebezpiecznych, celi szpitalnej, ambulatoryjnej. Alarm uruchamia się, gdy:**
  - osadzony nie porusza się w łóżku w określonym czasie,
  - zakrywa się kołdrą, kocem,
  - osadzony przebywa „długo" w kąciku sanitarnym,
  - zbyt długo stoi nieruchomo przy oknie lub przy zamkniętych drzwiach,
  - w celi pojawia się dynamiczny ruch,
  - nastąpiło omdlenie lub upadek osadzonego,
  - pojawiły się niepokojące stany emocjonalne u osadzonego.
- **W celi zabezpieczającej. Alarm uruchamia się, gdy:**
  - osadzony nie porusza się w celi w określonym czasie,
  - pojawia się dynamiczny ruch w celi,
  - osadzony przebywa „długo" przy zamkniętych drzwiach,
  - nastąpiło omdlenie, upadek osadzonego,
  - wystąpiły niepokojące stany emocjonalne u osadzonego.
- **W świetlicach, na placach spacerowych. Alarm uruchamia się, gdy:**
  - występuje dynamiczny ruch w wyznaczonej przestrzeni,
  - dwóch, trzech osadzonych znajdzie się w odległości mniejszej niż dozwolona, np. 30 cm,
  - pojawia się osoba, która nie powinna znajdować się w wyznaczonej przestrzeni,
  - wystąpiły wyraźne sygnały napięcia emocjonalnego w grupie osadzonych.
- **W przejściach, wejściach, łącznikach budynków. Alarm uruchamia się, gdy:**
  - system identyfikacji nie rozpoznaje twarzy,
  - pojawia się dynamiczny ruch w wyznaczonej przestrzeni,
  - pojawią się osoby, które nie powinny w tym czasie znajdować się w wyznaczonej przestrzeni, np. grupy izolacyjne w areszcie.
- **Pasy ochronne, teren więzienia. Alarm uruchamia się, gdy:**
  - nastąpi przekroczenie wirtualnych granic lub zmiana kierunku ruchu osób,
  - w polu obserwacji znajdą się pozostawione lub przerzucone przez wygrodzenia przedmioty,
  - pojawią się poruszające się obiekty – drony.

Ponadto inteligentna analiza obrazów obejmowałaby obraz ścian budynków, pawilonów mieszkalnych czy innych i reagowała alarmem na nielegalne kontakty między osadzonymi, pojawienie się obiektu (np. liny, dronu) lub człowieka (np. uciekiniera). Jednak podstawowym celem wieloletnich badań i analiz prowadzonych przez autorów jest sytuacja przeciwdziałania samobójstwom, szczególnie w celach poddanych stałemu dozorowi wizyjnemu – stale obserwowanemu zachowaniu osadzonych przez funkcjonariusza, tzw. monitorowego.

Wnioski autorów o niezbędnej ostrożności wdrażania technologii analizy wizyjnej potwierdzają także wyniki badania NW Systems Group z Wielkiej Brytanii – 9 na 10 użytkowników tej technologii zgłasza zbyt dużą liczbę fałszywych alarmów przez nią generowanych. Wynika to przede wszystkim ze złej jakości wykonania, eksploatacji i konfiguracji systemów dozoru wizyjnego. Aż 27% badanych stwierdziło, że te alarmy wynikały z błędnego doboru i konfiguracji analityki wizyjnej, a 41% wskazało na owady i zabrudzenie optyki kamer[4].

Istnieje niebezpieczeństwo wykorzystania medialnego wrażenia, jakie robi funkcjonowanie analizy wizyjnej do pozornego działania, mającego pomóc w przeciwdziałaniu samobójstwom, czyli wdrożenie niezbadanej i niewłaściwie skonfigurowanej technologii. Podobnie wygląda sytuacja ze szkoleniami operatorów w zakresie przeciwdziałania samobójstwom, których metodyka nie jest wypracowana. Najpierw należy opracować koncepcję, następnie zgromadzić wiedzę, aby stworzyć teorię. Kolejny etap to sprawdzenie empiryczne, czyli przeprowadzenie serii badań weryfikujących teorię. Dopiero na tej podstawie można wypracować metodykę szkolenia czy wdrażać rozwiązania tak zaawansowanych technologii. Skoro jest potrzeba, pojawiają się szkolenia, które w tytule mają operatora lub dotyczą monitoringu wizyjnego. Nie oznacza to jednak, że przygotowują one merytorycznie do realizacji zadań na tym stanowisku. Autorzy wskazują na ryzyko pochopnych i pozornych działań, zwłaszcza gdy chodzi o tak delikatną materię, jak życie ludzkie i samobójstwo. Należy także przywołać odmienne podejście do opisanego wyżej, polegające na ograniczeniu kontroli i dozoru osadzonych. To sukces systemu penitencjarnego w Norwegii i Niemczech, który przyniósł oczekiwany efekt zmniejszenia liczby antyspołecznych zachowań i zdarzeń. Wystarczyło otoczyć osadzonych opieką, z poszanowaniem godności człowieka i humanitaryzmem. Opisane w artykule zaawansowane prace badawczo-projektowe zostały przerwane w COSSW w Kaliszu w związku z likwidacją tej jednostki, ale są kontynuowane przez autorów w ramach własnej aktywności naukowej i publikacyjnej.

MGR INŻ. CEZARY MECWALDOWSKI

Starszy wykładowca zajmujący się szkoleniami zawodowymi i specjalistycznymi z zakresu zabezpieczeń elektronicznych, urządzeń do kontroli. Projektant z praktyką zagraniczną. Absolwent Politechniki Łódzkiej o specjalizacjach: energetyka przemysłowa i informatyka stosowana. Wykładowca Centralnego Ośrodka Szkolenia Służby Więziennej oraz Ośrodka Szkolenia Polskiej Izby Systemów Alarmowych

DR ROBERT POKLEK

Psycholog, adiunkt na Wydziale Pedagogiczno-Artystycznym w Kaliszu Uniwersytetu im. Adama Mickiewicza w Poznaniu. Członek Polskiego Towarzystwa Zapobiegania Samobójstwom

4 IFSEC Global: 93% of firms reporting excess of CCTV false alarms linked to poor installation or maintenance (https://www.ifsecglobal.com/author/ifsecglobal/ (dostęp: 15.08.2021)

Monitoring wizyjny

nieskończone możliwości metadanych

Wanda Nijholt

Panasonic Business Europe

Według ostatnich badań dotyczących najbardziej monitorowanych miast w użyciu jest 770 mln kamer, do końca 2021 r. na całym świecie będzie ich ponad miliard. Kamera dozoru wizyjnego jest powszechnie stosowanym narzędziem, obecnie obserwujemy ważny okres transformacji technologicznej na tym rynku. Coraz częstsze zastosowanie sztucznej inteligencji i dostępność metadanych z analizy obrazu zmieniają układ sił w zakresie dozoru wizyjnego. Rozwój jest stymulowany pod względem technologicznym i etycznym.

EWOLUCJA KAMER CCTV

Rynek kamer dozorowych rozwija się od wielu lat i przeszedł już kilka małych rewolucji. Przełomem było pojawienie się kamery sieciowej IP, która połączona przez sieć Ethernet przeszła transformację od prostego czujnika do pełnoprawnego narzędzia komputerowego. Po 2000 r., kiedy rynek monitoringu wizyjnego przeżywał rozkwit, opracowano i wdrożono pierwsze algorytmy AI, które umożliwiły analizę strumieni danych wizyjnych i dały początek branży analizy obrazu z kamer.

Dzisiaj systemy te mogą np. wykrywać nietypowy ruch na danych obszarze, rozpoznać obecność osób lub obiektów i przekazać te informacje dalej. Jednak dokładność analizy zależy od warunków środowiskowych, w jakich pracuje kamera. Ulewny deszcz lub silny wiatr utrudniają detekcję, powodując fałszywe alarmy lub przyczyniając się do przeoczenia incydentu. Kolejną przeszkodą jest koszt infrastruktury: aby przeanalizować nagrania wideo i uzyskać odpowiednie wyniki, konieczne jest zainstalowanie serwerów dużej mocy obliczeniowej.
Kamery dozorowe są też często krytykowane za kolejny problem operacyjny: zebrane materiały muszą zostać przetworzone, co wymaga znacznych zasobów ludzkich, zwłaszcza w miejskich centrach bezpieczeństwa. Jednak to nie powstrzymało ich ewolucji, a dzięki postępowi w dziedzinie AI są coraz bardziej wydajne i autonomiczne.

GŁĘBOKIE UCZENIE I METADANE: SKOK NAPRZÓD W MONITORINGU WIZYJNYM

Bardziej precyzyjne algorytmy AI nowej generacji pozwalają dokonywać poprawniejszych wstępnych analiz sytuacji. W przypadku przestrzeni miejskiej mogą zwrócić uwagę operatora na gromadzący się tłum czy nietypowe zachowania ludzi. Umożliwia to zastosowanie *deep learning*, metody pozwalającej na wykorzystanie dużych ilości danych, na podstawie których algorytmy AI „uczą się" rozpoznawać charakterystyczne wzorce. Na tej podstawie są w stanie rozróżnić nie tylko kształty obiektu (mężczyzna, kobieta, kot), ale też kolory czy cechy szczególne – np. mężczyznę w czerwonej koszulce i z wąsami, dziecko na hulajnodze. Do tego dochodzi postęp w zakresie procesorów o dużo większej mocy obliczeniowej, które są teraz zintegrowane bezpośrednio z kamerami dozorowymi, co sprawia, że koszty wdrożenia tych technologii są bardziej przystępne dla użytkowników końcowych.
Dzisiejsze systemy dozoru wizyjnego stały się zatem „ekspertami" w wykrywaniu i rozpoznawaniu wzorców na obrazie. Na podstawie tego, co wykryły, tworzą bazę metadanych, która sama się zasila i coraz dokładniej analizuje obraz. Kamera jest teraz podstawowym narzędziem biometrycznym rozpoznawania twarzy. A ochrona danych osobowych?
Z punktu widzenia bezpieczeństwa celem metadanych nie jest identyfikacja obywateli (w Europie niedozwolona ze względu na RODO), ale optymalizacja wykorzystania dozoru wizyjnego, a także uczynienie go proaktywnym i predykcyjnym. Podłączone kamery samochodowe pozwalające uniknąć wypadków, inteligentne miasta optymalizujące ruch drogowy i ograniczające liczbę incydentów – perspektywy są nieograniczone, a niektóre z nich stały się już rzeczywistością.
Dzisiejsze systemy zabezpieczeń wykraczają poza funkcje ochrony. Szacuje się, że do 2024 r. 30% kamer sprzedawanych na rynku będzie wykorzystywało głębokie uczenie. Analiza obrazu oparta na AI przeżywa rozkwit. Teraz to tylko kwestia czasu potrzebnego na wdrożenie infrastruktury i stworzenie aplikacji AI, które pozytywnie wpłyną na nasze życie.

PANASONIC MARKETING EUROPE

ul. Wołoska 9a,
02-583 Warszawa
https://business.panasonic.pl/

Innowacyjny system do weryfikacji paszportów covidowych

przyszłość firm i instytucji w czasach pandemii

Żyjemy w czasach, kiedy wymóg weryfikacji statusu epidemicznego obywateli może stać się faktem. Coraz więcej instytucji staje przed dylematem, czy i jak sprawdzać ważność tzw. paszportów covidowych osób chcących wejść do obiektu, by było to szybkie i zarazem ekonomiczne. Jak zwykle z pomocą w takich sytuacjach przychodzi nowoczesna zaawansowana technologia.

Nowatorski system weryfikacji paszportów covidowych od DFE Security to innowacyjne rozwiązanie umożliwiające weryfikację kodów QR z zapisaną informacją o statusie zdrowotnym danej osoby.
System, który jest autorskim rozwiązaniem DFE Security, składa się z bezobsługowych (bezdotykowych) multiczytników oraz zainstalowanej na nich specjalnej aplikacji. To rozwiązanie, w połączeniu z drzwiami automatycznymi lub bramkami kontroli dostępu, pozwala na automatyczne weryfikowanie kodów QR certyfikatów szczepionkowych oraz automatyczne przydzielanie dostępu do strefy bądź obiektu osobie zaszczepionej.
System działa bez konieczności obsługi przez osobę z personelu czy pracownika ochrony. Wystarczy zbliżyć kod QR do ekranu urządzenia. Czytnik zeskanuje kod i wyświetli komunikat – zielony o przydzieleniu dostępu, gdy szczepienie jest ważne, lub czerwony o braku możliwości wejścia w przypadku, gdy szczepienie straciło ważność.

Niewątpliwą zaletą tego innowacyjnego rozwiązania jest jego szybkość oraz automatyczność działania. System jest samoobsługowy, nie wymaga obecności personelu ochrony. Istotną korzyścią jest również bezdotykowość weryfikacji. Opracowane rozwiązanie jest prostym sposobem na spełnienie wymogów służb epidemiologicznych w pandemicznej rzeczywistości.
Opcją może być pomiar temperatury ciała osoby chcącej uzyskać dostęp do obiektu bądź strefy. Dzięki wbudowanej kamerze podczerwieni czytnik bezkontaktowo i automatycznie mierzy temperaturę osoby. Urządzenie wyświetla na ekranie wynik pomiaru i gdy jest w normie, przydziela dostęp. Jeśli natomiast jest podwyższona, wejście pozostaje zablokowane.
System znajduje zastosowanie w placówkach medycznych, na uczelniach, w zakładach produkcyjnych, podczas imprez masowych oraz w miejscach związanych z transportem, takich jak lotniska czy dworce kolejowe. Bardzo dobrze sprawdza się też w sklepach, restauracjach, klubach fitness, kinach, bankach hotelach czy biurowcach.
Rozwiązanie zostało oparte na technologii wielofunkcyjnych czytników MK Mini oraz MK Midi Android i może stanowić część oferowanych przez DFE Security rozwiązań na czas pandemii – EPIDEMIA SECURITY. Mają one na celu jak najlepsze i efektywne zabezpieczenie przedsiębiorstw i obiektów przed skutkami pandemii oraz umożliwienie dalszego bezpiecznego funkcjonowania. Wspomagają działania prewencyjne, pozwalając na dostosowanie do wymogów i limitów wprowadzanych przez władze i służby epidemiologiczne.
EPIDEMIA SECURITY to, oprócz systemów kontroli paszportów covidowych, systemy do pomiaru temperatury ciała, system liczenia osób 3D oraz kompleksowe rozwiązania z bramkami kontroli dostępu.
Wszystkie rozwiązania z zakresu kontroli wejścia i sterowania dostępem do obiektów są dostosowane do indywidualnych potrzeb klientów. Firma DFE Security zapewnia doradztwo i pomoc wykwalifikowanej i doświadczonej kadry na każdym etapie. Oferuje wysoką jakość i niezawodność urządzeń, a także niestandardowe designerskie rozwiązania.

DFE SECURITY

ul. Polska 25
00-703 Warszawa
tel. 22 622 22 73
www.dfes.pl

Nowość w sterowaniu systemami alarmowymi INTEGRA i VERSA

Poznaj nowe manipulatory z ekranem dotykowym

Wraz z postępującym rozwojem technologii zmieniają się oczekiwania inwestorów. Coraz częściej wybierają sprzęt umożliwiający wygodniejsze sterowanie wieloma funkcjami – zarówno bezpieczeństwa, jak i automatyki. Tak powstały manipulatory INT-TSH2 i INT-TSG2 z ekranami dotykowymi dla systemów INTEGRA oraz VERSA.

MOCNE WNĘTRZE

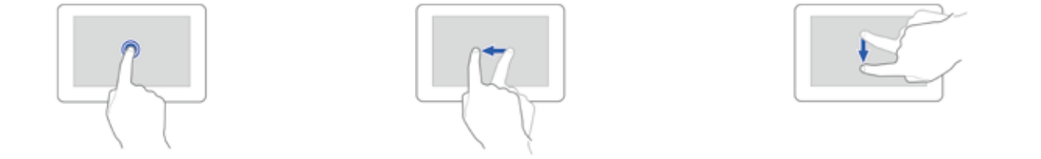
Szklany panel frontowy nie tylko nadaje manipulatorom elegancki wygląd. Chroni on pojemnościowy ekran przed zarysowaniem i innymi uszkodzeniami, by zachować precyzję dotyku, jaką daje nowy wyświetlacz. Dzięki niemu (a także nowemu oprogramowaniu) możliwe było wdrożenie funkcji obsługi gestów. By zapewnić płynność pracy urządzeń, zastosowany został procesor nowej generacji. Procesor INT-TSH2 jest ponad 2-krotnie szybszy w porównaniu z poprzednikiem (INT-TSH), a w przypadku INT-TSG2 nawet 4-krotnie szybszy (w porównaniu z INT-TSG). Slot karty pamięci microSD umożliwia wgranie własnych zdjęć (do fotoramki i motywów użytkownika), dźwięków powiadomień (tylko w przypadku INT-TSH2) oraz aktualizacji programowania. Pracując w systemie INTEGRA, manipulator obsługuje dodatkowe dwa programowalne wejścia przewodowe. Zastosowane w urządzeniach mechanizmy chronią je przed próbami sabotażu i sprawiają, że manipulatory spełniają wymogi branżowe na poziomie Grade 3.

PROSTE PROJEKTOWANIE INTERFEJSU

Interfejs manipulatorów INT-TSH2 oraz INT-TSG2 został zaprojektowany całkowicie na nowo, by zapewniać prostą obsługę systemów alarmowych i zintegrowanych z nimi instalacji automatyki budynkowej. Do projektowania nowego, trzypoziomowego interfejsu służy niezmiennie znany instalatorom program DLOADX. Do dyspozycji instalator ma aż 24 ekrany, na których łącznie może umieścić do 64 makropoleceń. Funkcje można rozmieścić tematycznie (np. sterowanie czy ogrzewanie razem) albo według pomieszczeń (wszystkie urządzenia działające w jednym pokoju, na jednym ekranie).
Na poziomie górnym znajduje się wygaszacz ekranu. Można na nim wyświetlić zegar cyfrowy, fotoramkę albo go wyłączyć. Wygaszacz można uzupełnić o ikony statusu poszczególnych wejść i wyjść czy o informacje o odczytywanych przez czujniki temperaturach.

Po przesunięciu ekranu wyświetlany jest „ekran główny", wybierany dowolnie spośród wszystkich utworzonych ekranów. Funkcja prowadnic ułatwia równe rozmieszczenie ikon – do wyboru spośród 100. Każde makropolecenie czy ekran można zaznaczyć jako wymagający dodatkowej weryfikacji, czyli ponownego wpisania hasła użytkownika. Po zmianie stanu ikona może zmienić wygląd, dając użytkownikowi lepszy obraz aktualnego statusu danego urządzeń.

Manipulatory INT-TSH2 i INT-TSG2 są dostępne w dwóch wersjach kolorystycznych: nowoczesnym białym i klasycznym czarnym.



Nowym interfejsem użytkownik może sterować za pomocą gestów, co znacznie ułatwia nawigację po menu

Nową funkcją jest widżet „Odsyłacz". Po jego kliknięciu użytkownik zostaje przeniesiony na dowolny ekran wskazany przez niego i przypisany przez instalatora. Ułatwia to znacznie nawigację po menu, bez konieczności przewijania wielu ekranów. Nowością jest także możliwość wgrania (poprzez kartę SD) mapy obiektu. Zamiast projektować tradycyjne menu, ikony można rozmieścić na przygotowanej grafice – znacznie ułatwia to inwestorom sterowanie systemem.

Ikony odpowiadające funkcjom systemu możesz dowolnie umieścić na wgranej mapie. Pamiętaj, by na każdym ekranie dodać funkcję „Wstecz" – inaczej użytkownik nie będzie mógł powrócić do poprzedniego ekranu!

Program DLOADX służy także do prostej konfiguracji motywu graficznego interfejsu. Instalator może wybrać jeden z ponad 20 gotowych już motywów, różniących się tapetą, kolorem czcionki, ikon czy podświetlenia elementu. Może też zaprojektować autorski motyw na życzenie inwestora. Ekran manipulatorów wyświetla ponad 16 mln kolorów, dzięki temu barwy są niezwykle żywe i wyraziste, zapewniając dobrą jakość tapetom czy zdjęciom fotoramki.

UNOWOCZEŚNIONY TRYB SERWISOWY

Nowy interfejs nie pominął trybu serwisowego. Urządzenia i ich stan są wyświetlane w postaci przewijanej listy, dla wygody podzielonej na kategorie. Z tego miejsca można też wygodnie zaprogramować przyciski działającego w systemie pilota SATEL. Instalator może też wywołać tradycyjną klawiaturę, by zaprogramować system w znany już sobie sposób.

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

DualCurtain Outdoor:

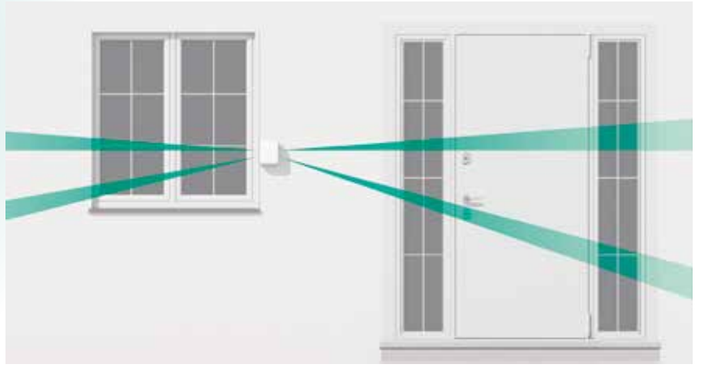
Wiedza w zakresie ochrony obwodowej

Linia czujek zewnętrznych Ajax obejmuje obecnie dwukierunkową kurtynową czujkę ruchu, która może monitorować obszar w odległości do 30 metrów (zasięg detekcji), skutecznie chroniąc dostęp do okien, drzwi, bram, ogrodzeń i witryn okiennych.

DWIE CZUJKI W JEDNEJ OBUDOWIE

Każdy element czujki DualCurtain Outdoor stanowi potwierdzenie idei technicznej precyzji. Opływowe kształty z głęboko osadzonymi soczewkami i dwoma czujnikami (sensorami) tworzą nowoczesną, odporną na deszcz obudowę. Panel montażowy SmartBracket pozwala w prosty i bezpieczny sposób zamocować czujkę powierzchniowo, jednocześnie zamykając panel konfiguracyjny.

Parametry czujki są regulowane niezależnie dla każdego kierunku obserwacji (obszaru detekcji po lewej i prawej stronie obudowy). Elementy sterujące na tylnej ściance umożliwiają ustawienie zasięgu wykrywania dla każdej strony detekcji dalekiej, aktywację detekcji w pobliżu czujki oraz przesunięcie sektora obserwacji w pionie o 3°, aby wystające fragmenty elewacji nie zasłaniały pola obserwacji czujki.



W aplikacji mobilnej Ajax można sterować każdym kanałem czujki osobno: włączać/wyłączać czujniki podczerwieni i antymaskingu, uaktywniać je na stałe niezależnie od trybu czuwania oraz regulować czułość. Aplikacja pozwala na elastyczne dostosowanie interakcji z czujką – ustawienie opóźnień wejścia/wyjścia, powiązanie aktywacji syren z określoną stroną detekcji oraz tworzenie scenariusza automatycznego generowania alarmu.

Detektor DualCurtain Outdoor chroni nawet najbardziej oddalone obszary dzięki zasięgowi połączenia (transmisji podczerwieni) do 1700 metrów od huba. W gęstej zabudowie podwajacze zasięgu ReX mogą pomóc w zbudowaniu solidnej ochrony obwodowej, niezależnie od wielkości obiektu.

PODWÓJNE FILTROWANIE FAŁSZYWYCH ALARMÓW

Dzięki dwóm czujnikom podczerwieni umieszczonym po obu stronach czujki DualCurtain Outdoor skutecznie eliminuje fałszywe alarmy. Czujka nie zareaguje, jeśli tylko jeden jej czujnik wykryje ruch. Gdy zadziałają oba czujniki, zastosowany w detektorze specjalny algorytm cyfrowy ELSA w ułamku sekundy przeprowadza trzyetapową analizę sygnału, odfiltrowując zakłócenia naturalne i spowodowane przez zwierzęta oraz decyduje, czy alarm należy uruchomić.

EWOLUCJA CZUJKI KURTYNOWEJ

Po przeanalizowaniu słabych stron kurtynowych czujek zewnętrznych, konstruktorzy wyposażyli DualCurtain Outdoor w unikatowe rozwiązania techniczne rozszerzające pokrycie chronionego obszaru. Gdy włączona jest opcja Wykrywania w bliskim obszarze, górny sensor podczerwieni wykorzystuje dodatkowy wąski sektor obserwacji skierowany pod kątem 40 stopni w dół. Umożliwia to wykrycie ruchu w przypadku próby włamania w pobliżu obudowy DualCurtain Outdoor, rozwiązując problem martwego pola (typowy dla tego typu czujek). Ta opatentowana technologia Ajax Systems jest niezastąpiona przy ochronie fasad i złożonych struktur architektonicznych.

NIEZAWODNOŚĆ, KTÓRA STAŁA SIĘ NASZĄ MARKĄ

Ajax zadbał o to, aby detektor DualCurtain Outdoor mógł działać do 4 lat na dołączonych bateriach i zapewniał kompleksową ochronę przed sabotażem. Wszelkie problemy, takie jak próby wyłączenia czujki lub rozładowanie baterii są natychmiast zgłaszane przez system użytkownikom i agencji ochrony.

Czujka jest wyposażona w przycisk antysabotażowy, reagujący na zdjęcie urządzenia z mocowania i oderwanie od podłoża. Dzięki konfigurowalnemu interwałowi czasowemu komunikacji hub–czujka system jest w stanie zidentyfikować utratę połączenia z DualCurtain Outdoor w czasie nieprzekraczającym 1 min. Czujka spełnia wymagania klasy 2. zgodnie z normą EN 50131 i jest wyposażona w system antymaskingu, który wykrywa próby zasłonięcia pola widzenia lub zamalowania obiektywów.

DualCurtain Outdoor może pracować w trudnych warunkach środowiskowych. Jej obudowa jest zabezpieczona przed kurzem i zachlapaniem (klasa ochrony IP54) , a elektronika działa w temperaturze od -25°C do +60°C przy wilgotności do 95%.

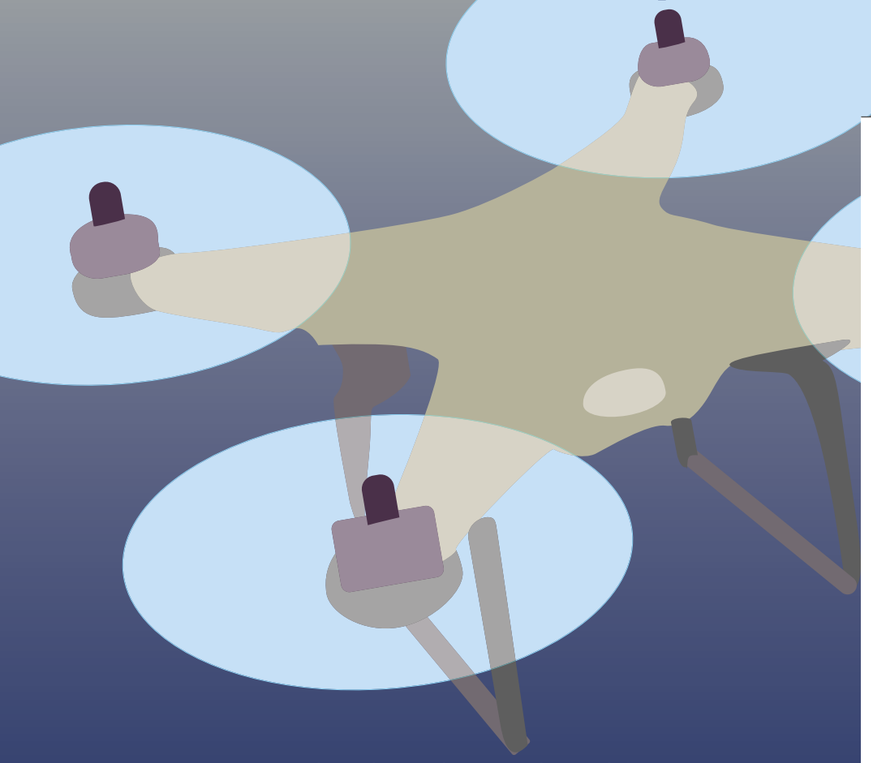
Połączenie wszystkich tych cech w jednym urządzeniu zapewnia użytkownikom spokojny sen, a agencjom ochrony – zaufanie do sprzętu, którego używają.

AJAX SYSTEMS POLAND

Fryderyka Chopina 41/2
20-023 Lublin
https://ajax.systems/pl/

Drony i systemy antydronowe

w branży security



Sektor bezzałogowych statków powietrznych (BSP), potocznie określanych mianem dronów, należy do jednych z najbardziej dynamicznie rozwijających się w przemyśle lotniczym na świecie. Polska nie stanowi wyjątku. Ten rynek w naszym kraju stale się rozwija i nabiera nowego wymiaru, kształtując wiedzę i świadomość potencjalnego użytkownika.

Katarzyna Niebrzydowska

Popyt na profesjonalne zastosowanie dronów wzrasta nie tylko na rynku komercyjnym, ale także w sektorze publicznym. Zwiększa się też świadomość wykorzystania dronów i urządzeń peryferyjnych im towarzyszących w takich sektorach, jak infrastruktura krytyczna, transport, telekomunikacja, energetyka, rolnictwo, budownictwo i ochrona. Przedsiębiorstwa zaczynają dostrzegać ich potencjał i korzyści w zakresie funkcjonalności, możliwości rozwoju, korzyści finansowych, poprawy bezpieczeństwa i rozbudowy systemów zarządzania.

Producenci dronów prześcigają się w tworzeniu i testowaniu nowych modeli o zaawansowanych funkcjach, mogących działać nawet w trudnych warunkach atmosferycznych. Szybko postępujący rozwój wyprzedza zdecydowanie wiedzę i wdrażanie procesów edukacyjno-rozwojowych. Warto skorelować edukację z postępem technologicznym jako szansę na poszerzenie potencjału dronów w aspekcie ich specjalistycznego zastosowania. Tę szansę wykorzystuje Polska, która znalazła się w czołówce krajów o największym potencjale rozwoju technologii dronów. Ważnym elementem są przepisy prawa regulujące loty dronami na poziomie krajowym. O statusie prawnym szerzej w artykule.

NOWELIZACJA PRZEPISÓW PRAWNYCH REGULUJĄCYCH LOTY DRONAMI

Świadomy uczestnik sektora dronów, mówiąc o bezzałogowych statkach powietrznych, ma na myśli nie tylko kwestie techniczne, ale również przepisy prawne, w których ramach użytkownik może poruszać się w codziennej pracy z dronem. Od 31 grudnia 2020 r. na terenie krajów Unii Europejskiej oraz w Liechtensteinie i Norwegii obowiązują wspólne przepisy dotyczące dronów, które zostały określone na podstawie Rozporządzenia Delegowanego Komisji (UE) 2019/945 z 12 marca 2019 r. w sprawie bezzałogowych systemów powietrznych oraz operatorów bezzałogowych systemów powietrznych z państw trzecich oraz Rozporządzenia Wykonawczego Komisji (UE) 2019/947 z 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych.
Regulacje muszą być w najbliższym czasie zunifikowane w krajach europejskich, czekamy więc na nowelizację ustawy – Prawo lotnicze. Niemniej mamy obowiązek już stosowania nowych przepisów, które wniosły zmiany, dając nam nowy porządek prawny. Główną zmianą jest brak podziału na loty o charakterze sportowym, rekreacyjnym lub zarobkowym. Korzystanie z dronów w celu komercyjnym w większości przypadków będzie ogólnodostępne. Sklasyfikowano wykonywane loty na następujące kategorie: otwarta, szczególna i certyfikowana, ze względu na stopień ryzyka wykonywanych operacji lotniczych. W kategorii otwartej można pilotować dron w celach zarówno zarobkowych, jak i rekreacyjnych. Ponadto dochodzi rozróżnienie operatora i pilota dronu. Obowiązkowa jest rejestracja dronów. Popatrzmy na poniższe bloki tematyczne:

REJESTRACJA DRONU

Chcąc latać dronem ważącym powyżej 250 g lub ważącym mniej niż 250 g, ale posiadającym rejestrator danych (np. kamerę) w kategorii otwartej, trzeba będzie zarejestrować się jako operator. Rejestracji dokonuje się poprzez stronę internetową Urzędu Lotnictwa Cywilnego (ULC). W tej kwestii będzie wymagane podanie imienia i nazwiska operatora, adresu zamieszkania lub siedziby firmy, numeru telefonu i adresu e-mail osoby fizycznej lub prawnej, w której imieniu odbywa się rejestracja. Każdy operator otrzyma indywidualny numer rejestracyjny, który będzie musiał umieścić na swoim dronie. Osoby powyżej 14. roku życia będą mogły zarejestrować się za zgodą opiekuna prawnego.

OBOWIĄZKOWE SZKOLENIE

Po obligatoryjnej rejestracji na stronie ULC każdy operator będzie musiał przejść proste szkolenie online zakończone testem, który obejmie 40 pytań wielokrotnego wyboru z zakresu bezpieczeństwa lotniczego, ograniczeń korzystania z przestrzeni powietrznej, procedur i regulacji lotniczych, ochrony prywatności i danych osobowych, ogólnej wiedzy nt. dronów, bezpieczeństwa i ubezpieczenia. Bez zdanego testu będziemy mogli latać tylko najmniejszymi BSP.

KATEGORIE LOTÓW

Według nowych przepisów klasyfikacja wykonywanych lotów jest oparta na stopniu ryzyka wykonywanych operacji lotniczych. Wyróżniamy trzy główne kategorie:

1. KATEGORIA OTWARTA – OPEN

Przeznaczona dla lotów o najniższym stopniu ryzyka. Loty w kategorii Open wykonuje się w podkategoriach A1, A2 i A3. Muszą zostać spełnione następujące warunki:

- dron należy do klasy C0, C1, C2, C3, C4 lub został skonstruowany do użytku prywatnego;
- waga dronu wynosi 25 kg lub jest mniejsza;
- lot jest wykonywany w zasięgu wzroku;
- operator zapewnia utrzymanie określonych odległości od osób;
- maks. wysokość lotów to 120 m nad ziemią;
- podczas lotu nie są przewożone materiały niebezpieczne ani zrzucane żadne inne materiały.

Podkategoria A1 (loty nad ludźmi) – drony klasy C0 (do 250 g), C1 (do 900 g), budowane samodzielnie (do 250 g); dopuszcza się przelot nad osobami postronnymi, zakaz lotów nad zgromadzeniami osób.
Podkategoria A2 (loty blisko ludzi) – drony w klasie C2 (do 4 kg); zakaz lotów nad osobami i zgromadzeniami osób, minimalna odległość od osób to 30 m lub 5 m, jeśli dron ma funkcję ograniczającą prędkość lotu do 5 m/s.
Podkategoria A3 (loty z dala od ludzi) – drony w klasie C3 i C4 lub budowane samodzielnie (do 25 kg); zakaz wlatywania nad osoby i zgromadzenia osób – odległość pozioma od osób i zabudowy minimum 150 m; obszary z założenia bez osób postronnych (pole, łąka).

2. KATEGORIA SZCZEGÓLNA – SPECIFIC

Do kategorii szczególnej zaklasyfikowano loty niemieszczące się w wytycznych kategorii otwartej, przede wszystkim ze względu na zwiększone ryzyko operacji dla osób trzecich. Grupa ta obejmuje operacje w warunkach VLOS i BVLOS.

3. KATEGORIA CERTYFIKOWANA – CERTIFIED

W kategorii certyfikowanej zobligowano do uzyskania zezwolenia na lot, jak w kategorii szczególnej. Dodatkowo trzeba mieć aktualny certyfikat operatora. Podsumowując, nowy system prawny jest złożony i wymaga od użytkownika wnikliwego zapoznania się z przepisami w celu zachowania bezpieczeństwa działań.

ZASTOSOWANIE DRONÓW DO CELÓW BEZPIECZEŃSTWA W BRANŻY SECURITY

Obecnie poszukujemy zaawansowanych form ochrony, które stanowią główne lub uzupełniające narzędzie do zapewnienia bezpieczeństwa, prewencji, ochrony i zarządzania. Dążymy do osiągnięcia stanu braku zagrożenia, dającego pewność i gwarancję utrzymania poczucia bezpieczeństwa. To poczucie, niezależnie od poziomu i zakresu, w znacznym stopniu rzutuje na złożoność problematyki w wielu sferach naszego życia i jest ciągle rozwijane, zwłaszcza w zakresie przedmiotowym.
Potrzeba braku zagrożenia dała impuls do wdrażania inteligentnych systemów zabezpieczeń do monitorowania, nadzorowania, sygnalizacji i patrolowania. Przejdźmy do przykładów, które w miarę potrzeb i wyobraźni ludzkiej mnożą się, a ich lista pozostaje otwarta.

1. MONITOROWANIE I KONTROLA MIEJSC TRUDNO DOSTĘPNYCH LUB NIEBEZPIECZNYCH

Dron z kamerami i innymi czujnikami pozwala na długotrwałe monitorowanie miejsc i obiektów trudno dostępnych, a nawet niebezpiecznych dla człowieka. Takimi obiektami są np. sieci energetyczne, sieci trakcyjne, rurociągi i inne. W trakcie monitorowania mamy możliwość przeprowadzenia szybkiej diagnozy w przypadku awarii. Dron może latać zarówno w ciągu dnia, jak i w nocy, niezależnie od warunków atmosferycznych.
Dzięki zaawansowanym możliwościom lot można zaplanować, a następnie wykonać w tzw. trybie autonomicznym. Operator dronu, wykonując lot, realizuje świadomie zaplanowaną funkcję monitorującą z uwzględnieniem strategicznych punktów objętych dozorem czy też patrolem. Porównując proces monitorowania wykonany przez człowieka z wykonanym przez dron, jednoznacznie stwierdzimy, że ten sam obiekt czy teren monitorowaliśmy kilka razy szybciej, z większą dokładnością i bez narażenia człowieka – pracownika ochrony na zagrożenia.

2. MONITOROWANIE STANU TECHNICZNEGO OBIEKTU W KONTEKŚCIE WCZESNEJ IDENTYFIKACJI ZAGROŻENIA

Przy użyciu dronu wyposażonego w kamery i inne urządzenia z łatwością można wykonać funkcję monitorowania stanu technicznego obiektów czy ogrodzeń na danym terenie, wychwytując naruszenia, zawaliska, uszkodzenia i inne. Dzięki obrazowi z kamery termowizyjnej zamontowanej na dronie można np. ocenić, jak dużo śniegu zalega na dachach, zwłaszcza dużych hal produkcyjno-magazynowych, i odpowiednio wcześnie zlecić ich odśnieżanie, by uchronić przed zawaleniem się dachu. Obraz z kamery dronu pozwala ocenić stan techniczny obiektu, następnie stanowi podstawę do przygotowania dokumentacji technicznej modernizacji i prac konserwacyjnych.
W trakcie patrolu z powietrza, używając urządzeń peryferyjnych, można wykryć każdą nieprawidłowość, podjąć czynności proceduralne i uchronić dany obiekt oraz ludzi przed niebezpieczeństwem i stratami. Przykładem może być wczesne wykrycie pożaru poprzez zlokalizowanie ukrytego źródła ciepła w takich obiektach, jak składowiska węgla, siarki i innych surowców na hałdach. Przydatne jest też np. wykrycie przekroczenia zadanego progu wielkości mierzonej przez czujnik gazu lub kamerę termowizyjną.

3. WERYFIKACJA ALARMU

Kamera na dronie pozwala szybko zweryfikować zdarzenie alarmowe wywołane w którymś z podsystemów, np. SSP lub ochrony perymetrycznej (przekroczenie ogrodzenia). W przypadku faktycznego wtargnięcia do chronionej strefy operator przy użyciu dronu może śledzić ewentualną drogę intruza.

4. PATROLE Z POWIETRZA

Dron ze specjalistyczną kamerą, wykonując przelot wzdłuż granicy strzeżonej strefy z dowolną liczbą punktów trasy i ścieżek, szybciej i dokładniej monitoruje znacznie większy obszar strefy patrolowanej. Kamera wykrywa intruza i utrwala jego wizerunek, co może stanowić materiał dowodowy dla przyszłego postępowania. Dzięki dodatkowym urządzeniom peryferyjnym, np. głośnika, można wezwać intruza do opuszczenia chronionego terenu. Z kolei kamery termowizyjne oraz te z obiektywem o dużym zoomie pozwalają wykryć nieuprawnione osoby w miejscach trudno dostępnych dla oka ludzkiego oraz wykryć podejrzane zachowania osób, nieprawidłowe ruchy aut w obrębie strefy monitorowanej i wcześniej zareagować.

5. KONTROLA STANU ILOŚCIOWEGO TOWARU W PRZYPADKU PODEJRZENIA KRADZIEŻY

Przy użyciu dronu z odpowiednią kamerą i oprogramowaniem można wykonać lot kontrolny nad obiektem składującym towar i dokonać pomiarów tego towaru, które dadzą nam obraz stanu ilościowego w porównaniu ze stanem np. sprzed doby. Towary nie zawsze są składowane na zamkniętym terenie, m.in. węgiel czy stal, stanowiąc łatwy łup dla zorganizowanych grup przestępczych.

JAK SIĘ BRONIĆ PRZED DRONAMI, CZYLI SYSTEMY ANTYDRONOWE (ASPEKTY PRAWNE STOSOWANIA, TAKTYKA, TECHNIKA I NIE TYLKO)

Pomimo różnorodnych i użytecznych możliwości zastosowania dronów w branży ochrony spotykamy się również z nieuprawnionymi próbami ich użycia w kontekście naruszenia prywatności, działań przemytniczych, szpiegowskich czy terrorystycznych na obiekty publiczne czy infrastruktury krytycznej. Każde takie nieuprawnione działanie ma za zadanie pozyskanie informacji o danym celu, rozpoznanie obiektu w celach rabunkowych, pozyskanie wiedzy o modelu prowadzonej działalności czy zbieranie danych o rozwoju firmy, co dotyczy zwłaszcza zakładów produkcyjnych.
Lista obiektów zagrożonych niepożądanymi działaniami dronów się wydłuża. Wynika to z coraz większej świadomości po stronie zarządzających danymi miejscami. Przedsiębiorcy dużych zakładów produkcyjnych, firm logistyczno-spedycyjnych, obiektów infrastruktury krytycznej, rządowych, rekreacyjno-sportowych i prywatnych dostrzegają problem szeroko pojętej inwigilacji przez dokonujących nieuprawnione loty nad ich obiektami. Powyższe działania stanowią podstawę dla producentów do tworzenia coraz nowocześniejszych urządzeń czy systemów do identyfikacji i neutralizacji dronów w sytuacji zagrożenia.
Warto wspomnieć o możliwościach formalnoprawnych zastosowania systemów antydronowych w praktyce, gdyż użycie takiego rozwiązania leży w gestii ograniczonej liczby instytucji i tylko w określonych przypadkach. Tę kwestię reguluje art. 126a ustawy – Prawo lotnicze:

ZNISZCZENIE LUB UNIERUCHOMIENIE BEZZAŁOGOWEGO STATKU POWIETRZNEGO ALBO PRZEJĘCIE KONTROLI NAD JEGO LOTEM

1. Bezzałogowy statek powietrzny, w tym model latający, może zostać zniszczony, unieruchomiony albo nad jego lotem może zostać przejęta kontrola, gdy:

1) przebieg lotu lub działanie bezzałogowego statku powietrznego:
   a) zagraża życiu lub zdrowiu osoby,
   b) stwarza zagrożenie dla chronionych obiektów, urządzeń lub obszarów,
   c) zakłóca przebieg imprezy masowej albo zagraża bezpieczeństwu jej uczestników,
   d) stwarza uzasadnione podejrzenie, że może zostać użyty jako środek ataku terrorystycznego;
2) bezzałogowy statek powietrzny wykonuje lot w przestrzeni powietrznej w części, w której wprowadzono ograniczenia lotów albo znajdującej się nad terytorium Rzeczypospolitej Polskiej, w której lot statku powietrznego jest zakazany od poziomu terenu do określonej wysokości.

2. Do zniszczenia lub unieruchomienia bezzałogowego statku powietrznego albo przejęcia kontroli nad jego lotem w przypadku, o którym mowa w:

1) ust. 1 pkt 1 lit. a, b i d – są uprawnieni funkcjonariusze Policji, Straży Granicznej, Służby Ochrony Państwa, ABW, Agencji Wywiadu, CBA, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Służby Celno-Skarbowej i Służby Więziennej, Straży Marszałkowskiej, żołnierze Żandarmerii Wojskowej i Sił Zbrojnych RP oraz pracownicy specjalistycznych uzbrojonych formacji ochronnych,
2) ust. 1 pkt 1 lit. c – są uprawnieni funkcjonariusze Policji, Straży Granicznej, Służby Ochrony Państwa, ABW, Służby Kontrwywiadu Wojskowego, żołnierze Żandarmerii Wojskowej oraz pracownicy specjalistycznych uzbrojonych formacji ochronnych,
3) ust. 1 pkt 2 – są uprawnieni żołnierze Sił Zbrojnych RP – na zasadach określonych w odrębnych przepisach.

Powyższy przepis wyraźnie określa listę podmiotów i listę przesłanek do zastosowania systemów antydronowych. Firmy ochrony należą do tych podmiotów, mieszczą się w pojęciu specjalistycznych uzbrojonych formacji ochronnych po spełnieniu ustawowych wymogów. Odnosząc się do rozwiązań technicznych, należy podkreślić, że rynek ten stale się rozwija, dając rozwiązania coraz lepszej jakości. Obecne systemy antydronowe opierają się na wielu sensorach/czujnikach (radar, kamera, detektory) czy detektorach akustycznych. Rozróżniamy systemy mające na celu neutralizację dronu, odesłanie dronu do operatora, wymuszenie lądowania lub w skrajnych przypadkach zniszczenie poprzez np. zestrzelenie. W tej technologii producenci stosują m.in. metody zagłuszania sygnału, systemy radarowe, metody kinetyczne oraz fizyczne systemy przechwytujące.

PODSUMOWANIE

Rynek dronów w Polsce stale się rozwija w aspektach zarówno technicznym, legislacyjnym, jak i systemów zarządzania. W kontekście branży zabezpieczeń wydłuża się lista zastosowań dronów w praktyce. Użytkownicy dzięki rozwojowi rynku stosują zróżnicowane modele wraz z urządzeniami specjalistycznymi i oprogramowaniem, budują odpowiednie procedury i systemy zarządzania. Podejmują również próby samoobrony przed nieuprawnionymi i niepożądanymi działaniami z użyciem dronów. Rynek dronów dostarcza coraz więcej rozwiązań stanowiących uzupełnienie systemu bezpieczeństwa.

KATARZYNA NIEBRZYDOWSKA

Ekspert ds. lotnictwa bezzałogowego. Od 2007 r. związana z branżą bezzałogowych statków powietrznych w lotnictwie cywilnym i wojskowym. Realizowała i nadzorowała projekty związane z dostarczaniem BSP na rzecz sił zbrojnych RP, sił specjalnych, administracji publicznej i prywatnych przedsiębiorstw. Autorka kilku publikacji z zakresu rynku BSP w kontekście bezpieczeństwa publicznego.

Postochrona w postcovidowych czasach

Czas na stewarding w biznesie

Tym artykułem inicjujemy cykl poświęcony przeobrażeniu zakresu działań na rzecz bezpieczeństwa i odporności organizacji. W kolejnych wydaniach będziemy się wpisywać w wątek przewodni numeru, przedstawiając różne oblicza zmieniającej się funkcji ochrony w biznesie. Do dyskusji otwierającej cykl zaprosiliśmy: Annę Kostkowską, wieloletnią menedżer z obszaru facility management, Łukasza Niewadę, wybitnego eksperta i praktyka z obszaru BHP, oraz Macieja Kazimierczuka, dyrektora ds. bezpieczeństwa.

Jacek Tyburek

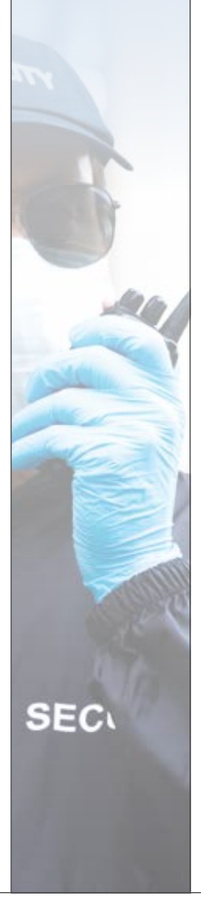
Minęło kilka tygodni od Warsaw Security Summit zorganizowanego przez redakcję „a&s Polska". Kilkaset osób śledziło spotkanie online, lecz tak naprawdę cieszyła możliwość osobistego spotkania twarzą w twarz koleżanek i kolegów z branży security. Świetne prezentacje przeplatane możliwością porozmawiania z tymi, których się dawno nie widziało.
Warsaw Security Summit to przede wszystkim seria merytorycznych prezentacji, wymiany doświadczeń i przedstawienia dokonań. Jako zespół Black Onion również mieliśmy możliwość podzielenia się doświadczeniem. Z naszego punktu widzenia szczególnie ważne było inauguracyjne wystąpienie Jacka Grzechowiaka i Piotra Kiliszka, którzy podsumowali czas pandemii i jej wpływ na branżę bezpieczeństwa.
Szczególnie mocno i – naszym zdaniem – słusznie wybrzmiała część wystąpienia poświęcona koniecznym zmianom sposobu realizacji usług przez firmy ochrony. Niewątpliwie wystąpienie to przyspieszyło uruchomienie dyskusji na temat zmiany funkcjonowania branży ochrony fizycznej.

Pandemia spowodowała, że służby ochrony obiektów realizowały zadania, które wcześniej nie należały do ich obowiązków. Tym samym zadania ochrony przesunęły się w kierunku funkcji wcześniej bardziej typowych dla służb BHP. Kontrola przestrzegania przepisów sanitarnych czy procedury zapewnienia dystansu społecznego to nie są klasyczne zadania pracownika wykonującego zadania zapobiegania stratom. Okres ten pokazał, że wzbogacenie zakresu zadań ochrony spotkał się z dużym uznaniem i poczuciem celowości (innej niż wymóg ubezpieczyciela) pracy ochrony w różnego rodzaju obiektach.
Dyskusje dotyczące kondycji ochrony bardzo szybko przechodzą w zgodne utyskiwania oraz wzajemne (firm ochrony, a także ich zleceniodawców) żale i uprzedzenia. Te dyskusje są zadziwiająco do siebie podobne. Media społecznościowe poświęcone tematyce profesjonalnej pełne są dyskusji na temat tego, jak być powinno. Każdy poważniejszy incydent, każda wpadka pracowników ochrony wywołuje wielodniowe dyskusje przedstawicieli branży. Mniej lub bardziej konkretne, ale zawsze pełne troski o przyszłość tej działalności biznesowej, która dla wielu jest nie tylko sposobem na zarabianie pieniędzy i realizowanie swoich ambicji, ale również autentycznej pasji i poczucia ważnego powołania. W społeczności profesjonalistów z różnych zakątków bezpieczeństwa podobne dyskusje są również na porządku dziennym. Powód jest prosty – wszyscy chcemy naprawić sytuację, świadczyć naszym klientom oraz potencjalnym klientom takie usługi, jakich oczekują.

Rozwijając temat, nie sposób nie zacytować Anny Kostkowskiej, eksperta branży FM z ponad 20-letnim stażem na wszystkich szczeblach kariery w międzynarodowych koncernach, wykładowcy zagadnień FM na Uniwersytecie Łódzkim na studiach podyplomowych, z doświadczeniem w zarządzaniu funkcją FM zarówno w dużych obiektach przemysłowych, jak i budynkach biurowych. Zapytana o swoje doświadczenia ze współpracą na linii FM i ochroną obiektu powiedziała:
Pandemia wymusza nowe rozwiązania biznesowe. Dziś przetrwa ten, kto najlepiej i najszybciej dostosowuje się do dynamicznie zmieniającego się środowiska. Bycie „agile" to jedna z podstawowych cech dzisiejszego biznesu. Czasy, gdy ochrona ma za zadanie weryfikację osób wchodzących do budynku, dobiegła końca. Potrzeba nam nowoczesnych rozwiązań, niezależnie czy funkcjonujemy w Londynie, Berlinie, Warszawie, czy Dubaju. Klient oczekuje zaskakujących i nowatorskich propozycji, które obniżą koszty, ale przede wszystkim zwiększą efektywność i będą niezawodne. Usługa FM, BHP czy security nabiorą nowego znaczenia. Synergia, komplementarność usług i sprawne zarządzanie pod jednym parasolem mogą zrewolucjonizować rynek. Branża security wymaga dofinansowania i zmiany myślenia, niezależnie od funkcji nieruchomości. Dobór wyselekcjonowanej kadry, szkolenia i rozsądne zarobki to niezbędny krok do sukcesu.
Ta efektywność i te nowatorskie rozwiązania to narzędzia, które na rynku są obecne. Trudno sobie wyobrazić lepszego ambasadora (rzecznika) dla większości tych produktów, jak właśnie firma ochrony. Wypowiedź potencjalnej klientki jest tylko pojedynczym głosem, ale tego rodzaju poglądy można usłyszeć częściej, niestety nierzadko z przykrymi uwagami pod adresem firm ochrony i ich pędu lub raczej braku pędu do ciągłej pracy nad zwiększeniem efektywności.

Bieżące wydanie „a&s Polska" jest poświęcone przemysłowi i roli, jaką w zakładach przemysłowych odgrywa bezpieczeństwo zarówno w postaci technologii, jak i usług ochrony. Zakłady przemysłowe to często wielkie, skomplikowane struktury operacyjne. Ochrona fizyczna nie ma tu łatwej roli. Trudno wykazać swoją przydatność i uzasadnienie ponoszonych kosztów ochrony takich obiektów. Zbyt skomplikowane struktury, zbyt wiele miejsc, w których może dojść do nadużyć, zbyt trudne do udowodnienia przypadki poważnego działania na niekorzyść firmy lub zapobiegania stratom z tytułu uszkodzeń lub niegospodarności. Te obiektywne trudności często spychają pracowników ochrony do realizacji bardzo prostych czynności, np. przy wjazdach na teren zakładu lub realizowania prostych patroli, które często nie przynoszą zbyt wielu korzyści oprócz iluzorycznego i niemożliwego do policzenia poczucia realizowania funkcji prewencyjnej. Tymczasem znane są przykłady wyposażania ochrony w zadania na rzecz innych służb wewnętrznych. Doskonale je opisuje kolejny nasz rozmówca, z którego doświadczenia jako menedżera BHP wyłania się bardziej optymistyczny obraz przyszłości. Jest nim Łukasz Niewada, menedżer BHP i audytor systemów zarządzania bezpieczeństwem. Zapytany o swoją percepcję współpracy z ochroną i działem bezpieczeństwa odpowiada:
Od 22 lat zajmuję się bezpieczeństwem pracy, starając się pomóc pracodawcom w zapewnieniu bezpiecznych

miejsc pracy, a pracownikom poczucia, że każdego dnia mogą cało i zdrowo wracać do domu. W ciągu mojej kariery behapowca doświadczyłem różnego podejścia do tematów bezpieczeństwa od strony zarówno pracodawcy, jak i pracownika. Kiedy odpowiadałem za wynik audytu ubezpieczyciela, zrozumiałem, że właściwie oszacowanie ryzyka pod wspólnym mianownikiem BEZPIECZEŃSTWA ZAKŁADU ma głęboki sens. Moja optyka – skoncentrowana na bezpiecznych warunkach pracy – znacznie się poszerzyła, kiedy wraz z zespołem interdyscyplinarnym złożonym z przedstawicieli działu zabezpieczenia, produkcji, finansów i BHP opracowywaliśmy scenariusze ryzyka do Planu Business Continuity.
Kolejny raz pełnej symbiozy i ciekawej współpracy pomiędzy obszarem BHP a działem zabezpieczenia doświadczyłem w momencie, kiedy mogłem wraz z kolegami współtworzyć powstające centrum monitoringu w zakładzie pracy zatrudniającym ponad 10 tys. pracowników. Mało kto wierzył, że ten pomysł wypali i będzie skuteczny. Życie pokazało, że wszystkie służby działające w zakładzie – BHP, Ochrona Zdrowia, Dział Zabezpieczenia i Straż Pożarna przy aktywnym uczestnictwie działu monitoringu są w stanie radykalnie skrócić czas reakcji na zagrożenie i błyskawicznie zareagować, niosąc niezbędną pomoc we właściwe miejsce.
Reasumując, behapowiec 20 kilka lat temu a obecnie to totalnie różna postać. Tak samo ochrona. Kilkadziesiąt lat temu wystarczyła polówka lub marynarka z napisem „Ochrona" (najlepiej, jakby pracownik miał odpowiednią grupę inwalidzką). Obecne czasy wymagają ogromnej zwinności, elastyczności, a nade wszystko odpowiedzialności wobec osób zajmujących się fizycznym zabezpieczeniem zakładu.
Opisywane przez Łukasza Niewadę doświadczenia są doskonałym przykładem tego, jak podejście do security w przemyśle może wywołać zmianę z korzyścią dla wszystkich służb funkcjonujących w zakładzie (lub grupie zakładów) w realizowaniu ich statutowej misji. W tym przypadku to funkcja security zainicjowała zmianę poprzez zaprojektowanie zintegrowanego centrum monitoringu dla kilku zakładów, obsługującego systemy dozoru CCTV, alarmowy i ppoż. Intensywna kampania informacyjna i promocyjna w zakładzie doprowadziła do opracowania koncepcji zintegrowanego działania służb. Uruchomiono prosty do zapamiętania numer telefonu alarmowego. Korzyści dla biznesu były oczywiste, nieoczywisty był sposób działania takiego zintegrowanego modelu. Konieczna była praca projektowa nad wypracowaniem algorytmu działania.



Inna zmiana w koncepcji zabezpieczenia i ochrony dotyczy wielkich imprez sportowych, z naciskiem na mecze piłkarskie. To imprezy gromadzące dziesiątki tysięcy osób, które są rozentuzjazmowane i których nastroje zmieniają się bardzo dynamicznie. Stewarding (pomysł na stewarda stadionowego) narodził się w Anglii w latach 80., gdy na stadionach w tym kraju królowały chuligaństwo i agresja. Pod koniec ub. wieku zjawisko to się nasiliło, stając się poważnym problemem związanym z bezpieczeństwem podczas imprez masowych. Steward jest członkiem służby informacyjnej. Do jego głównych zadań należy informowanie kibica o przyjętych rozwiązaniach organizacyjnych i dbanie o bezpieczeństwo podczas imprezy. Stewardem jest osoba pracująca podczas imprezy masowej, której nadrzędnym celem jest zapewnienie bezpieczeństwa jej uczestników oraz ogólnego zadowolenia z obsługi osobom uczestniczącym w wydarzeniu.

Koncepcja stewardingu, odpowiednio dostosowana do warunków obiektów, ma szczególne uzasadnienie w obiektach przemysłowych i handlowych oraz wielkich budynkach i kompleksach biurowych. Odpowiednie dostosowanie oznacza takie skonfigurowanie zadań, aby połączyć procedury wyposażonego w nowoczesne technologie centrum monitoringu/zarządzania obiektem z pracą pracowników realizujących „w terenie" zadania zlecone przez służby obiektu. Doświadczenie podpowiada, że dokonanie kompilacji możliwych do przekazania zadań kontrolnych i raportowych z różnych służb pracownikowi ochrony na patrolu (stewardowi obiektu) znacznie podnosi efektywność procesów. Przy wyposażeniu pracownika w technologie raportowe (panel raportowania z predefiniowanymi tzw. check listami, wraz z możliwościami wpisania raportów otwartych, wykonania zdjęć lub skanów) dostajemy bazę danych i statusów sytuacji w obiekcie, które budują *big data* o funkcjonowaniu obiektu. Stąd już tylko krok do zaawansowanej analityki, bardzo przydatnej do strategicznego zarządzania obiektem. I co najważniejsze, wielki krok do generowania oszczędności.

Czy takie funkcje służby ochrony są możliwe? Czy stewarding obiektowy jest możliwy? Zdecydowanie tak! Posłużę się cytatem z wypowiedzi Macieja Kazimierczuka, dyrektora działu administracji i bezpieczeństwa w Action SA:
Moja przygoda z branżą security rozpoczęła się 25 lat temu, w tym od 15 lat z branżą przeciwpożarową. W swojej pracy starałem się połączyć i zarządzać w sposób niekonfliktowy dwoma bardzo ważnymi aspektami w jednym przedsiębiorstwie. Bo przecież security musi dbać o to, aby drzwi były zawsze dobrze zamknięte, a ochrona ppoż., żeby te same drzwi były zawsze otwarte do ewakuacji. Od kiedy pamiętam, bardzo często dochodziło do konfliktów w tych dwóch sektorach, bo ludzie z obu stron delegowali obowiązki zbyt dosłownie. To powodowało niepotrzebne przeciąganie w czasie, a ponieważ w obu przypadkach trzeba działać szybko i zdecydowanie, narodził się pomysł na połączenie tych dwóch sprzeczności. Tak więc „ubrałem" security w ochronę przeciwpożarową, przeszkoliłem i przekonałem do raportowania.
Postanowiliśmy, że stanowisko dowódcy security i operatora obsługi SAP to jedno stanowisko 24-godzinne, i to właśnie on ma dostęp do wszystkich systemów bezpieczeństwa oraz ochrony przeciwpożarowej. Jako zwierzchnik pozostałych pracowników ma z nimi kontakt i może sprawnie zarządzać na wypadek powstania zagrożenia. Jest zobowiązany do ciągłego raportowania o stanie zabezpieczeń security i ppoż. Ważną kwestią jest to, że każdy pracownik security, oprócz znajomości planu ochrony, zna instrukcje bezpieczeństwa pożarowego oraz scenariusz pożarowy, co ułatwia pracę na poszczególnych posterunkach. Taki upgrade security nie jest aż tak skomplikowany, jak to się może wydawać. Kluczowe jest dobre wyszkolenie pracowników poprzez regularne audyty i ćwiczenia. Kwestie kontrolne można realizować za pomocą narzędzi elektronicznych, ale można to zrobić klasycznie przez odpowiednie wpisy w rejestrach kontrolnych.
Wśród wszystkich pracujących na stanowisku pracownika ochrony zdarzają się osoby, które należą do ochotniczych straży pożarnych. Ma to o tyle duże znaczenie, że ci ludzie mieli już możliwość ratowania zdrowia i życia ludzkiego oraz mienia. Takie rozwiązanie jest ważne, jeżeli chodzi o przygotowanie odpowiednich procedur w razie powstania zagrożenia. Pozwala na szybkie przekazanie niezbędnej wiedzy dowódcy akcji gaśniczej ze straży pożarnej, policji czy pogotowia ratunkowego, a jak wiemy, w takich sytuacjach liczą się rzetelna informacja i czas reakcji.

W świecie lawinowych zmian w technologiach bezpieczeństwa stajemy w obliczu trzech ograniczeń w pracy nad stałym podnoszeniem bezpieczeństwa i efektywności pracy oraz odporności biznesu. Pierwszym – moim zdaniem – jest czynnik ludzki, drugie to ograniczenia organizacyjne, które uniemożliwiają nadążanie za wdrażaniem coraz doskonalszych technologii pozwalających w pełni wykorzystać możliwości danych. Trzecim, chyba najmniej znaczącym obecnie ograniczeniem, jest budżet. Najpoważniejszymi ograniczeniami są czynniki ludzki i organizacyjny. Bardzo trudno nadążać za postępem technologii i zrozumieniem benefitów z nich wynikających.
Jednocześnie nawet najdoskonalsze technologie bez ludzi obsługujących system nie osiągną swoich możliwości. Koncepcja przeorganizowania działania służb obiektowych w kierunku stewardingu obiektowego nosi znamiona odpowiedzi adekwatnej do potrzeb biznesu.
Przytoczone wypowiedzi pokazują wprost, że biznes na takie rozwiązania czeka. Nie we wszystkich firmach są zatrudnieni menedżerowie ds. bezpieczeństwa czy odporności biznesu. Ci zatrudnieni przez organizację biznesową czy menedżerowie z firm ochrony mają potencjalnie wszystkie karty w rękach, aby odegrać rolę tych, którzy przeprowadzą zmianę. Należy podkreślić, że biznes w ramach zintegrowanych kosztów ponoszonych na utrzymanie obiektu, w tym ochrony, może uzyskać znacznie wyższą efektywność, a w efekcie duże oszczędności pośrednie i bezpośrednie.
Promowana przez nas koncepcja stewardingu obiektowego jest łatwiejsza do wdrożenia, niż się wydaje, a jej efekty przekraczają oczekiwania. Pojęcia takie, jak integracja, stewarding, analiza danych, wspólne serwisy czy efektywność, nabierają szczególnego znaczenia.

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. Obecnie związany z Black Onion Resilience Community.

REKLAMA

25 lat
z myślą o klientach

Rozmowa z Krzysztofem Bartuszkiem, prezesem Zarządu Securitas Polska

Securitas Polska świętuje 25 lat działalności. Gratulujemy! Jak patrzy Pan na całą branżę z perspektywy tych lat, co jest kluczem do sukcesu?
Dziękuję za gratulacje. Na sukces zawsze składa się wiele czynników, ale tym, co wyróżnia Securitas, jest długoterminowa strategia i jej konsekwentna realizacja. Nasz sukces to również synergia wiedzy, ludzi i technologii ze zdecydowanym naciskiem na ludzi. Nasz zespół to ludzie z wizją i pasją, którzy zdecydowali się działać w obszarze naszych wartości. Nasze logo to trzy kropki symbolizujące uczciwość, czujność i uczynność – wartości, które pielęgnujemy od 1934 roku, czyli od momentu powstania Securitas na świecie.

Mówiąc o ludziach, jakich cech poszukujecie Państwo u pracowników dzisiaj?
Nasi pracownicy muszą umieć obsługiwać urządzenia mobilne wyposażone w nowoczesne technologie. Nie dla wszystkich jest to łatwe, daje się tu zauważyć różnicę pokoleniową. Obsługujemy również zaawansowane systemy zabezpieczeń technicznych, tu potrzebujemy pracowników posiadających wiedzę specjalistyczną. Natomiast takie cechy jak uczciwość, zaangażowanie, lojalność, pracowitość i profesjonalizm, ceni każdy pracodawca. Osobiście doceniam bardzo poczucie humoru. Branża security nie jest najłatwiejsza, borykamy się na co dzień z bardzo trudnymi sytuacjami, dlatego pozytywne nastawienie i działanie ukierunkowane na cel bardzo pomagają.

Branża ochrony jest bardzo wymagająca, niewielu pracowników pracuje w jednej firmie przez wiele lat. Czy są tacy w Securitas?
Oczywiście, sam jestem przykładem pracownika z ponad 20-letnim stażem. Pracowników, którzy są z nami od 1996 roku, czyli od samego początku działalności Securitas w Polsce, jest ponad 30. Jestem z tego bardzo dumny. Ludzie zostają z nami na lata, a to jasno wskazuje, że jesteśmy organizacją, w której pracownicy dobrze się czują, są doceniani i mogą się rozwijać. Pielęgnujemy długoletnią współpracę i staramy się nieść ją na sztandarach. Jestem dumny z mojego zespołu, który liczy prawie 6 tysięcy pracowników w całej Polsce.

Jakie są obecnie wyzwania dla firm branży ochrony w porównaniu z tymi, które były w latach 90. ubiegłego wieku?
Paradoksalnie nie zmieniło się tak dużo. Nasz biznes budowaliśmy z myślą o klientach i o ryzykach, które u nich występowały. Oczywiście 25 lat temu były to głównie dosyć proste usługi ochrony fizycznej, ale Securitas zawsze inwestował w technologie. W tym 25-letnim okresie nastąpiła rewolucja przemysłowa, szereg rozwiązań technologicznych sprawił, że zaczęliśmy inaczej funkcjonować. Pracownik ochrony dzisiaj to inny pracownik niż 25 lat temu. Inne też stoją przed nami wyzwania. Nie dbamy jedynie o bezpieczeństwo, ale również wspieramy biznes naszych klientów, analizujemy procesy logistyczne, zarządzamy produkcją i zabezpieczamy szeroko rozumiane bezpieczeństwo pracy. Myślę, że ochrona stała się dużo bardziej wysublimowana i zaangażowana, jeśli chodzi o procesy występujące po stronie klientów.
Z drugiej strony, borykamy się z dużym rozdrobnieniem rynku, szczególnie w Polsce. Myślę, że to się jeszcze przez dłuższy czas nie zmieni, chociaż obserwujemy pewne procesy konsolidacyjne. Możliwość inwestowania w technologie sprawia, że część firm umacnia się na rynku, a te, które nie mają środków inwestycyjnych, przestają być konkurencyjne.

Czy ta tendencja będzie się nadal utrzymywać?
Myślę, że konsolidacje będą następowały. Pewnym ograniczeniem w rozwoju wielu firm są możliwości inwestowania. Największe firmy mają przewagę w tym zakresie, ale na rynku znajdzie się również miejsce dla firm niszowych. Konsolidacje z pewnością będą miały miejsce w przyszłości, choć teraz tak bardzo ich jeszcze nie widać. Szczególnie sytuacje kryzysowe, choćby takie jak pandemia, spowodują konieczność wprowadzania innowacyjnych rozwiązań w branży security, wymusi to rynek i zapotrzebowanie klientów. Wówczas w grę wchodzić będą kosztowne inwestycje i inne zasoby niezbędne do rozruchu biznesu, a to posiadają duże organizacje.

Jak Pan ocenia rozwój branży na przestrzeni ostatnich kilkunastu miesięcy, czy zmieniała się szybciej niż w ciągu ostatnich lat?
Myślę, że determinantem zmian są sytuacje kryzysowe. I rzeczywiście pandemia była takim kryzysem, który spowodował spore przyspieszenie w podejmowaniu decyzji. Można więc powiedzieć, że na pewno branża rozwija się szybciej. W przeszłości mieliśmy kilka takich kryzysów: finansowy i legislacyjny, kiedy w 1997 roku weszła w życie ustawa o ochronie osób i mienia. Na przestrzeni tych 25 lat pojawiały się kamienie milowe zmian związanych z ryzykiem. Pandemia jest jednym z takich kryzysów, kiedy zaczynamy myśleć szybciej, bardziej kreatywnie, szukamy nowych rozwiązań. I to również nastąpiło w Polsce.

Czy branża zmieniła się pod wpływem pandemii? Jak zmieniło się podejście do bezpieczeństwa w tym czasie?
Na początku wszyscy reagowaliśmy trochę spontanicznie, z takim ryzykiem do tej pory nie mieliśmy styczności, dlatego stosowaliśmy rozwiązania krótkoterminowe. Dziś sytuacja wygląda inaczej, wielu klientów chce inwestować w rozwiązania, które długofalowo zabezpieczają przed podobnymi zagrożeniami. Myślę, że pandemia i jej kolejne fale pokazały, że takie ryzyka będą wracały, a my powinniśmy szukać nowych technologii i inwestować w rozwiązania, które ograniczą kontakty bezpośrednie. I to się w tej chwili dzieje. Nasi klienci są gotowi, żeby inwestować w technologie, które pozwolą w sposób zdalny zarządzać bezpieczeństwem.

Zobacz online:
pełen wywiad w programie „Bezpieczny Biznes" wyemitowany w TV Biznes24 (https://youtu.be/oRQPtlq-BRQ)

Czy przygotowują się Państwo na czwartą falę? Jeśli tak, to w jaki sposób?
Przygotowaliśmy się na to już w zeszłym roku, ustalając trzy priorytetowe cele naszej działalności. Powiedzieliśmy sobie, że przede wszystkim musimy zabezpieczyć naszych pracowników, naszych klientów oraz nasze finanse. Cele pozostają niezmienne i konsekwentnie je realizujemy.

Mówił Pan o nowych technologiach, które są dzisiaj wdrażane. Czy sztuczna inteligencja zastąpi człowieka w branży ochrony i jaką perspektywę czasową dziś możemy przyjąć?
Myślę, że nie nastąpi to szybko. W najbliższych latach to nadal ludzie będą podejmować decyzje, a przede wszystkim reagować na zagrożenia i ryzyka. Na razie cała technologia, łącznie z AI, którą już zaczynamy wykorzystywać, to elementy uzupełniające, które pomagają nam w procesie decyzyjnym i pozwalają szybciej reagować na zagrożenia. Myślę, że mamy przed sobą nawet kilkadziesiąt lat, zanim technologia AI będzie mogła całkowicie zastąpić pracę człowieka w naszej branży. Na robotyzację, którą znamy z filmów science fiction, jeszcze poczekamy, ale prędzej czy później przyjdzie nam się z nią zmierzyć.

Czego więc Panu i firmie życzyć na kolejne 25 lat?
Myślę, że takiego zrównania rynku, czyli bezpiecznego środowiska biznesowego, które będzie całkowicie fair dla wszystkich jego uczestników. Z całą resztą, mając takich ludzi na pokładzie jak teraz, doskonale sobie poradzimy.

SECURITAS POLSKA
Postępu 6
02-676 Warszawa
securitas@securitas.pl

Rozwiązania Hikvision dla branży ochrony

Tomasz Migdał

Branża ochrony na przestrzeni kilku ostatnich lat bardzo się zmieniła. Wpłynął na to przede wszystkim bardzo duży wzrost kosztów pracy pracowników ochrony, spowodowany decyzjami o ozusowaniu umów na zlecenie, wzroście płacy minimalnej czy stawek godzinowych. Te zmiany przyczyniły się do tego, że zaczęto więcej inwestować w technikę i w bardziej wyszkolonych pracowników. Transformację tę przyspieszyła pandemia, podczas której zapotrzebowanie na ochronę fizyczną bardzo zmalało. Aktualnie wiele firm ochrony stosuje już nowoczesną technologię na masową skalę.

Dziś większość firm nadzoruje obiekty zdalnie za pomocą kamer wyposażonych w funkcje analityczne. To jest obszar, w którym Hikvision, jako największy światowy producent, ma dużo do zaoferowania. Wielu naszych klientów stosuje kamery wyposażone w technologię AcuSense, która wspierana przez algorytmy głębokiego uczenia, z bardzo dużą dokładnością rozpoznaje, czy alarm został wywołany przez osobę, pojazd lub inny obiekt. W zależności od tego, na czym operator stacji monitoringu chce skupić uwagę, alarm włącza się tylko w przypadku wykrycia tego konkretnego obiektu.

Dzięki AcuSense firmy ochrony mogą dużo szybciej reagować na zdarzenia na podstawie niezawodnych i zweryfikowanych alarmów o wtargnięciach na chroniony obszar. Mogą też wykorzystać wbudowane możliwości nadawania ostrzeżeń wizualnych (migające światło) i dźwiękowych (komunikat głosowy), które odstraszają potencjalnych włamywaczy przed wejściem na teren lub do budynku. W rezultacie użytkownicy przenoszą bezpieczeństwo na wyższy poziom, mogąc szybciej reagować na incydenty, jeszcze zanim dojdzie do strat lub szkód.

Najnowszymi produktami wprowadzonymi do sprzedaży są kamery ColorVu drugiej generacji, które rejestrują kolorowy obraz dobrej jakości nawet w bardzo słabych warunkach oświetleniowych. Dodatkowo są fabrycznie wyposażone w technologię AcuSense, co czyni je idealnym produktem dla firm ochrony.

Wzbogacone możliwości kamer Hikvision ColorVu o rejestrowanie szczegółów przy słabym oświetleniu są wynikiem zastosowania dwóch przełomowych rozwiązań w zakresie technologii sprzętowych: zaawansowanych obiektywów i wysokowydajnych przetworników obrazu. W wizyjnych systemach dozorowych informacje związane z kolorami mają kluczowe znaczenie dla identyfikacji szczegółów zdarzeń, zwłaszcza w nocy. Konwencjonalne kamery z oświetlaczami IR zapewniają w nocy jedynie obraz czarno-biały. W efekcie ludzie, pojazdy czy inne ważne obiekty mogą być rozmyte i wtapiać się w tło, co utrudnia rozróżnienie krytycznych elementów. Technologia Hikvision ColorVu rozwiązuje ten problem, umożliwiając kamerom generowanie kolorowych obrazów nawet w bardzo ciemnym otoczeniu.

Firmy ochrony – korzystające z takich produktów – mogą zredukować czas, który poprzednio musieli poświęcić na weryfikację zdarzeń alarmowych. Teraz analityka wskazuje, czy faktycznie pojawia się zagrożenie. Dzięki algorytmom głębokiego uczenia kamery ColorVu potrafią odróżnić ludzi i pojazdy od innych poruszających się obiektów, takich jak zwierzęta, liście czy deszcz. Alarmy zostaną wyzwolone tylko wtedy, gdy nastąpi właściwe wg wcześniej ustawionej klasyfikacji. Dzięki temu rozwiązaniu zarejestrowany materiał wizyjny można przeglądać wg kategorii (ludzie, pojazdy), a klasyfikacja obiektów znacznie poprawia wydajność wyszukiwania. Praca operatora staje się efektywniejsza, a firma ochrony może oferować swoje usługi większej liczbie klientów w bardziej konkurencyjnej cenie.

Nowo wprowadzone na rynek kamery ColorVu oferujące wzbogacone opcje obejmują modele zarówno analogowe Turbo HD (serie DF8T/DF3T/serie DF0T), jak i sieciowe. Dostępne są również kamery ColorVu 4K, które zapewniają kolorowe obrazy w ultrawysokiej rozdzielczości w dzień i w nocy. Dzięki lepszej jakości obrazu i bogatszym detalom kamery 4K ColorVu mogą być stosowane w jeszcze szerszym zakresie, wszędzie tam, gdzie niezbędne są wyraźne obrazy o wysokiej rozdzielczości.

Ponadto firma Hikvision dodała do nowych modeli ColorVu kamery zmiennoogniskowe, które pozwolą użytkownikom na powiększanie kolorowych obrazów nawet w nocy oraz idealne ustawienie kadru obserwacji.

Obiektywy kamer ColorVu zachowały superprzysłonę F1.0, co oznacza, że do przetwornika dostaje się czterokrotnie więcej światła niż w konwencjonalnych kamerach (z aperturą F2.0). Ma to kolosalny wpływ na jakość obrazu oraz działanie funkcji analitycznych.

GŁÓWNE KORZYŚCI Z ZASTOSOWANIA KAMER COLORVU:

1. Obraz o wysokiej rozdzielczości (4K) z dużą liczbą szczegółów.
2. Lepsze wrażenia wizualne:
   - zrównoważona jasność,
   - superprzysłona F1.0 i zaawansowany przetwornik obrazu gwarantują realistyczne odwzorowanie szczegółów,
   - doskonała skuteczność w warunkach słabego oświetlenia.
3. Całodobowe generowanie kolorowego obrazu o jakości ulepszonej przez technologię AcuSense.

Aby ochrona obiektu była kompleksowa, oprócz kamer systemu CCTV wyposażonych w funkcje analityczne firma Hikvision oferuje również systemy kontroli dostępu, sygnalizacji włamania, interkomy, głośniki IP oraz platformę do integracji i zarządzania systemami bezpieczeństwa HikCentral. Za jej pomocą z łatwością można zarządzać wszystkimi wymienionymi systemami, zapewniona jest także międzyoperacyjność. Codzienne operacje, chociażby najbardziej istotna wideoweryfikacja zdarzeń stają się bardziej efektywne.

Platforma HikCentral Professional umożliwia użytkownikom przeglądanie map i zdarzeń podczas podglądu obrazu na żywo oraz w materiale odtwarzanym, dostarcza raporty dotyczące stanu zasobów i liczby zdarzeń alarmowych, śledzi obiekt, dostarcza też okna podręcznych alarmów i wiele innych opcji. Jednocześnie moduł serwisowy tej platformy i raporty o błędach dla wszystkich powyższych systemów zapewniają poprawne działanie systemu.

Platforma HikCentral oferuje szereg modułów przydatnych w różnych zastosowaniach. Jednym z nich jest moduł ochrony perymetrycznej. W tradycyjnych systemach operatorzy muszą obserwować wiele monitorów, aby chronić strefę zewnętrzną firmy. HikCentral Professional VMS pozwala w inteligentny sposób łączyć informacje z różnych źródeł, aby zapewnić świadomość sytuacyjną i maksymalnie ograniczyć fałszywe alarmy.

Nowością – co należy podkreślić – jest możliwość łatwej integracji platformy HikCentral z istniejącymi programami, takimi jak AD Info, Kronos czy SafeStar, stosowanymi przez firmy ochrony w Polsce w swoich stacjach monitorowania. Wystarczy wykorzystać do tego specjalną wtyczkę software'ową HikCentral Gateway. Wówczas operator może skupić się tylko na oprogramowaniu stacji monitorowania, alarmy przychodzą automatycznie, co jest bardzo efektywne.

HIKVISION POLAND

ul. Żwirki i Wigury 16B, 02-092 Warszawa
info.pl@hikvision.com
https://www.hikvision.com/europe/

Perspektywy Przemysłu 4.0

Światowy rynek Przemysłu 4.0 ma wzrosnąć z 116,14 mld USD w 2021 r. do 337,10 mld USD w 2028 r., takie prognozy przedstawiono w raporcie Industry 4.0 Market Size, Share & COVID-19 Impact Analysis[1], opublikowanym przez firmę Fortune Business Insights™[2]. W raporcie przeanalizowano i pogrupowano dane dotyczące automatyki przemysłowej, inteligentnej fabryki i przemysłowego IoT w zakresie produkcji w branżach: energetycznej, motoryzacyjnej, petrochemicznej, lotniczej i obrony, FMCG w różnych regionach świata. Wynika z niego, że rynek w 2020 r. wart 101,69 mld USD, w latach 2021–2028 ma średnio rosnąć o 16,4%.

a&s Polska

ZWIĘKSZONE ZASTOSOWANIE ROBOTÓW PRZEMYSŁOWYCH

Przemysł na całym świecie zaczął akceptować stosowanie robotyki w każdym procesie produkcyjnym. Ciągły rozwój w tym zakresie jest jednym z najważniejszych czynników wzrostu produktywności. Międzynarodowa Federacja Robotyki (IFR) w swoim raporcie podała, że w 2017 r. na całym świecie powstało ok. 381 tys. jednostek zrobotyzowanych. Tylko w branżach motoryzacyjnej i automatyki przemysłowej zainstalowano ok. 2,1 mln samodzielnych robotów. Ich wykorzystanie wiąże się z wieloma korzyściami, m.in. wykonują powtarzalne czynności, eliminując potrzebę żmudnej pracy człowieka. Jednak systemy Przemysłu 4.0 są podatne na cyberataki. Uważa się, że ten czynnik w najbliższej przyszłości będzie hamował rozwój tego rynku.

TRANSFORMACJA TECHNIK AUTOMATYZACJI

W raporcie firmy Fortune Business Insights podano, że w 2020 r. rynek Przemysłu 4.0 w Europie wygenerował przychody w wysokości 34,60 mld USD. Przewiduje się, że będzie się rozwijał m.in. dzięki wdrożeniu przemysłowego Internetu rzeczy (IoT). Do jego wzrostu przyczyni się również transformacja technik automatyzacji. Coraz większe wydajności sieci i przetwarzania danych w czasie rzeczywistym będą kolejnym motorem rozwoju. W nadchodzących latach ze względu na upowszechnianie się automatyki przemysłowej i wdrażanie przełomowych technologii równie szybko będzie się też rozwijał region Azji i Pacyfiku.

W najbliższej przyszłości dominującą pozycję powinna utrzymać Ameryka Północna wdrażająca coraz szerzej technologie inteligentnych fabryk. Przewiduje się również znaczący wzrost rynku w regionie Azji i Pacyfiku ze względu na coraz większą rolę Korei Południowej, Chin i Japonii. Kraje te przeznaczają bardzo duże środki na wdrażanie przełomowych technologii i automatyki przemysłowej.

W światowej strukturze rynku Przemysłu 4.0 w 2020 r. segment automatyki przemysłowej stanowił 21,0% udziału. Pozostałe należą do inteligentnych fabryk i przemysłowego Internetu rzeczy (IoT). Wzrost zainteresowania Przemysłem 4.0 przypisuje się m.in. jego zdolnościom do automatycznej diagnostyki potencjalnych awarii i poprawy wydajności pracy maszyn produkcyjnych.

FUZJE I PRZEJĘCIA WZMACNIAJĄCE POZYCJE

Większość głównych dostawców rozwiązań dla Przemysłu 4.0, aby sprostać dużemu popytowi tego sektora, stosuje zaawansowane technologie poprawiające wydajność produkcji, np. druk 3D, cyfrowe bliźniaki[3]. Ponieważ rynek jest wysoko konkurencyjny, większość firm koncentruje się na strategii przejęć.

1 https://www.fortunebusinessinsights.com/industry-4-0-market-102375

2 Fortune Business Insights™ to firma zajmująca się badaniami rynku z siedzibą w Pune w Indiach. Posiada oddziały w USA i Wlk. Brytanii.

3 *Digital twin* odnosi się do cyfrowej repliki fizycznych obiektów, procesów i systemów.

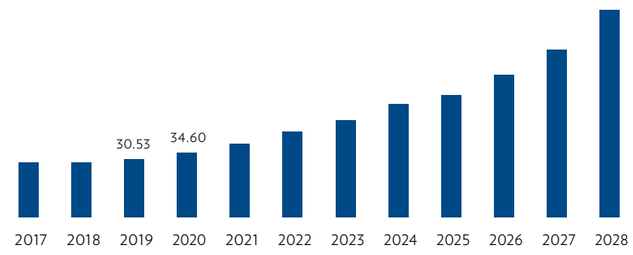
Zwiększone wskaźniki szczepień, złagodzone ograniczenia COVID-19 w wielu krajach pozwoliły podnieść prognozy gospodarcze, poprawiając perspektywy w sektorach produkcji przemysłowej i motoryzacyjnej (IM&A)[4]. W ślad za tym wiele firm dokonało już ponownej oceny własnych strategii, biorąc pod uwagę fuzje i przejęcia, co pozwoli dostosować ofertę i zwiększyć udziały w rynku. Jak podano w raporcie PwC[5] , wolumen transakcji IM&A w pierwszej połowie roku różnił się w zależności od regionu geograficznego. EMEA odzyskała pozycję lidera sprzed pandemii, jako region o największej aktywności transakcji, za nią uplasowały się Azja–Pacyfik i obie Ameryki.

Najwyższe wartości transakcji zanotowano w obu Amerykach, głównie za sprawą niektórych wielkich umów o wartości transakcji wynoszącej 5 mld USD lub więcej. Obejmowały one zapowiedzianą fuzję amerykańskiego producenta luksusowych pojazdów elektrycznych (EV) Lucid Motors z Churchill Capital Corp. IV (11,8 mld USD), fuzję firmy FLIR Systems z Teledyne Technologies (7,5 mld USD), zapowiedzianą fuzję brytyjskiego internetowego dealera samochodów używanych Cazoo z AJAX I (6,4 mld USD) oraz zapowiedzianą fuzję producenta samolotów elektrycznych Joby Aviation z Reinvent Technology Partners (5,0 mld USD). Trzy z tych firm są specjalnego przeznaczenia (SPAC), co podkreśla znaczenie tych struktur przejęć w sektorze IM&A w pierwszej połowie 2021 r.

Raport PWC przewiduje, że w drugiej połowie 2021 r. będą miały miejsce transakcje fuzji i przejęć, które przyspieszą transformację cyfrową, przynosząc zwiększone korzyści. Będą dotyczyć rozwiązań, które zwiększają wydajność operacyjną poprzez automatyzację produkcji lub wykorzystanie cyfrowych kanałów wejścia na rynek. Premii mogą spodziewać się osoby tworzące nowe strumienie przychodów z wartością dodaną. Zwiększy się również wdrażanie innowacyjnych technologii, które wspomogą firmy w nadążaniu za trendami branżowymi i przepisami oraz zobowiązaniami środowiskowymi, społecznymi i ładu korporacyjnego (ESG)[6].

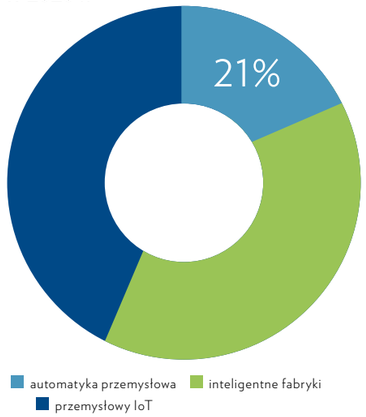
Technologie te różnią się w zależności od branży, obejmują akumulatory, pojazdy autonomiczne, materiały nowej generacji, produkcję z wykorzystaniem niekopalnych źródeł energii oraz narzędzia do monitorowania i raportowania wydajności ESG. Zwiększy się również drenaż talentów w celu pozyskania specjalistów, zwłaszcza z zakresu technologii lub inżynierii. Producenci oryginalnego sprzętu (OEM) będą nadal dokonywać przejęć i inwestycji w celu wzmocnienia lub budowy bardziej odpornych łańcuchów dostaw.

Rys. 1. Wielkość europejskiego rynku Przemysłu 4.0



www.fortunebusinessinsight.com

Rys. 2. Struktura rynku Przemysłu 4.0 w 2020 r.



GLOBALNE TRENDY W FUZJACH I PRZEJĘCIACH W SEKTORZE OBRONNYM

Można założyć, że budżety obronne będą wspierały zawieranie umów z powodu napięć geopolitycznych. Wydatki budżetowe na wojsko w jednych krajach wzrosły, deficyty fiskalne w innych oznaczają, że wydatki na obronę i inne wydatki rządowe znalazły się pod większą presją. Należy się spodziewać, że fuzje i przejęcia będą wzmożone, ponieważ firmy z branży obronnej przekształcają swoje portfele, by sprostać zmieniającym się oczekiwaniom. Niektóre z nich inwestują w partnerstwa, przede wszystkim z firmami technologicznymi i mniejszymi graczami, aby zdobyć umiejętności cyfrowe i móc konkurować.

Inwestycje w badania i rozwój są najwyższym priorytetem, zwłaszcza w lotnictwie komercyjnym, które kładzie nacisk na innowacje zwiększające wydajność paliwową i rozwój samolotów nowej generacji. Trwają zaawansowane badania skupione na napędzie elektrycznym i z wykorzystaniem wo-

4 Produkcja przemysłowa i sektor motoryzacyjny obejmują lotnictwo i obronność, motoryzację, usługi biznesowe, inżynierię i budownictwo oraz automatykę przemysłową.

5 https://www.pwc.com/gx/en/services/deals/trends/industrial-manufacturing-automotive.html

6 ESG – *Environmental* (środowisko), S – *Social Responsibility* (odpowiedzialność społeczna), G – *Corporate Governance* (ład korporacyjny).

doru, chociaż termin wprowadzenia nowych technologii na rynek jest ciągle jeszcze odległy. W nadchodzących miesiącach można spodziewać się fuzji i przejęć lub aliansów strategicznych pod wpływem ESG, ponieważ producenci OEM będą rozwijać różne technologie ku nowej przyszłości lotnictwa.

GLOBALNE TRENDY W FUZJACH I PRZEJĘCIACH W OBSZARZE PRODUKCJI PRZEMYSŁOWEJ

Wpływ COVID-19 na produkcję przemysłową nadal jest duży. Chociaż widać większy optymizm co do perspektyw wzrostu gospodarczego niż rok wcześniej, nadal obserwuje się znaczną zmienność wyników ekonomicznych i rosnące ceny surowców. Niedobór wykwalifikowanych pracowników w pewnych obszarach wiąże się z dodatkowymi wyzwaniami. Jednym producentom udaje się wrócić do poziomu działalności sprzed pandemii, inni nadal zmagają się z zakłóceniami łańcucha dostaw i potrzebą zmiany zdolności produkcyjnych w celu zaspokojenia niepewnego popytu.

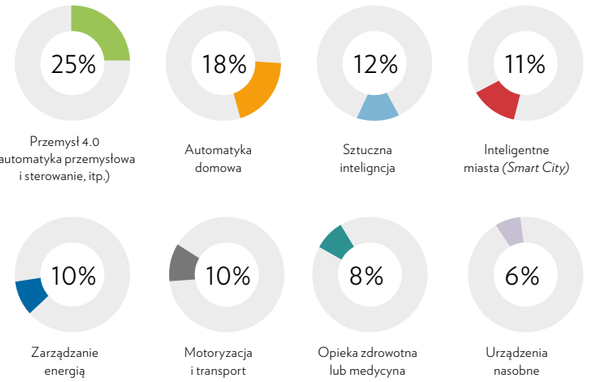
Analitycy PwC zauważają wyraźną tendencję do dokonywania fuzji i przejęć wynikającą z konieczności odzyskania rynku po zakłóceniach w 2020 r. Firmy tzw. repozycjonujące łączą się w celu wzmocnienia sił, aby wypełnić luki w kompetencjach (zwłaszcza talentów i technologii), regionalizacji łańcuchów dostaw, monetyzacji aktywów i napędzania ekonomii skali. Firmy borykające się z niedoborem siły roboczej zastanawiają się, w jaki sposób mogą wzmocnić ten obszar swojej działalności, a niektóre zawierają umowy, zapewniające dostęp do potrzebnych im umiejętności.

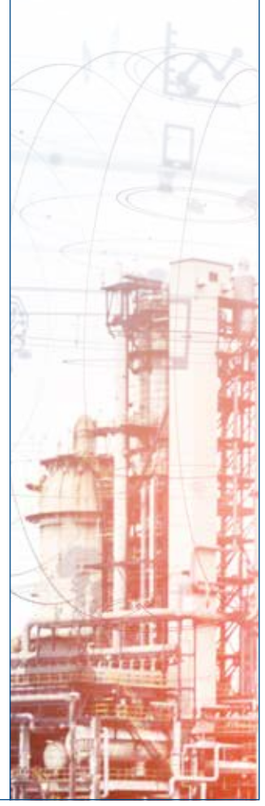
Inteligentniejsza produkcja, inteligentne technologie łańcucha dostaw – począwszy od Internetu rzeczy (IoT) i technologii czujników – to postępujący trend w celu usprawnienia operacji produkcyjnych, analizy danych umożliwiającej prewencyjne monitorowanie niezbędnych konserwacji urządzeń, ale nie tylko. Firmy oceniają transakcje pod kątem możliwości przyspieszenia transformacji technologicznej we wszystkich obszarach swojej działalności, w tym w procesach zaopatrzenia, produkcji oraz sprzedaży i dostaw do klienta.

Ponieważ firmy muszą kierować się również rentownością wzrostu, według analityków PwC wiele z nich rozważy zbycie niektórych aktywów jako sposób na skupienie się na swoich podstawowych możliwościach. Może to spowodować, że firmy ponownie rozważą decyzje typu *make-or-buy* i *outsourcing* w celu zmniejszenia kosztów i złożoności infrastruktury. Inne mogą zdecydować się na wprowadzenie we własnym zakresie pewnych działań wzmacniających odporność w swoim łańcuchu dostaw.

Producenci ponownie skupiają się na produktywności. Przewiduje się wzrost integracji i konsolidacji pionowej, ponieważ firmy będą dążyć do usprawnienia ogółu operacji i zwiększenia efektywności kosztowej poprzez skalowanie.

Rys. 3. Wielkość inwestycji w IoT





ROZWÓJ IOT

Prognozuje się, że liczba urządzeń IoT na świecie wzrośnie prawie trzykrotnie, z 8,74 mld w 2020 r. do ponad 25,4 mld USD w 2030 r. Takie dane podaje w swoim raporcie globalny dystrybutor elektroniki, firma Farnell[7]. Oznacza to, że rozwiązania oparte na komunikacji między urządzeniami połączonymi z Internetem na stałe zagoszczą praktycznie w każdym obszarze naszego życia – przemyśle, pracy, medycynie i ochronie zdrowia, edukacji, rozrywce czy miastach. Koncepcja *Internet of Things* będzie ewoluować do *Internet of Everything* (Internet Wszystkiego).

Światowymi liderami we wdrażaniu IoT są Stany Zjednoczone i Chiny. Największą liczbę urządzeń IoT (ponad 3 mld) ma Państwo Środka, będąc wciąż największym globalnym producentem tych rozwiązań. Swoją przewagę buduje, wykorzystując m.in. niskie koszty produkcji i szybką realizację zleceń, tym samym wzmacnia ekspansję na nowe rynki zbytu. Co prawda trwająca pandemia COVID-19, przerywając łańcuchy dostaw, zmieniła dynamikę rozwoju, ale Chiny powoli wychodzą z tego kryzysu. W Europie z kolei najwięcej w IoT inwestują Niemcy – ich wydatki na Internet rzeczy w 2019 r. wyniosły ponad 35 mld USD. Na drugim miejscu znalazły się Francja i Wielka Brytania, które wydały na Internet rzeczy ok. 25 mld USD.

Z badania przeprowadzonego przez Farnell wynika, że największy potencjał rozwoju dla IoT w najbliższych pięciu latach będą mieć Przemysł 4.0 – 25% wskazań i automatyka domowa – 18% wskazań *(rys. 3)*. Jednak, o ile wskaźnik potencjału dla Przemysłu 4.0 od 2018 r. stale wzrasta (2018 – 20%, 2019 – 22%, 2020 – 25%), o tyle dla *home automation* regularnie spada (2018 – 27%, 2019 – 22%, 2020 – 18%). Na liście kategorii o wysokim potencjale rozwoju IoT znalazły się także: sztuczna inteligencja, inteligentne miasta, zarządzanie energią, transport samochodowy, medycyna i ochrona zdrowia oraz urządzenia nasobne.

7 https://pl.farnell.com/internet-of-things(lad korporacyjny).

Genway oficjalny Dystrybutor Tiandy
Email : info@genway.pl Tel : +48-24-264-77-33
Strona : www.genway.pl Fax : +48-24-268-12-29

Centrum Testowania Technologii Przemysłu 4.0 na Śląsku

Przełom dla polskiego sektora przemysłowego

Centrum Testowania Technologii Przemysłu 4.0 zostało uruchomione przez firmę APA Group w Gliwicach. Projekt ma charakter edukacyjny. Jest skierowany do sektora przemysłowego. Pokazuje technologie Przemysłu 4.0 w rzeczywistym użyciu i uczy analizy kluczowych danych produkcyjnych.

PIERWSZE URUCHOMIENIE

Gliwicka firma APA Group w czerwcu br., podczas obchodów 20-lecia działalności, uroczyście uruchomiła Centrum Testowania Technologii Przemysłu 4.0. Goście, m.in. przedstawiciele producentów, eksperci automatyzacji, robotyzacji, reprezentanci instytucji gospodarczych, mieli okazję zobaczyć, jak człowiek wydaje polecenie poprzez smartwatch mobilnemu cobotowi (robotowi przeznaczonemu do bezpośredniej interakcji człowieka z robotem we wspólnej przestrzeni pracy), który następnie uruchamia manualnie proces produkcji na stacji ekspozycyjnej.

WYŻSZY POZIOM PRZEMYSŁU

Centrum Testowania Technologii Przemysłu 4.0 jest szansą dla firm na sprawdzenie nowoczesnych rozwiązań, na których opiera się koncepcja Przemysłu 4.0, takich jak IoT, *big data* czy *machine learning,* zanim w nie zainwestują. Stacja produkcyjna w Centrum Testowania Technologii Przemysłu 4.0 pozwoli gościom zarówno na miejscu w Gliwicach, jak i w pełni przez Internet wybrać przykładowy produkt, nadać mu cechy charakterystyczne, a następnie wytworzyć go, monitorując w czasie rzeczywistym każdy etap procesu produkcyjnego z zastosowaniem m.in. IoT, *big data* i *machine learning.* Po zakończonym cyklu użytkownik (menedżer, pracownik utrzymania ruchu, planista) otrzyma przyjazny raport z oznaczeniem wskaźników jakości, wydajności, kosztów czy zużycia energii i emisji CO_2. Pozwala to na precyzyjne oszacowanie, ile tak naprawdę kosztuje wyprodukowanie jednego komponentu. Tak szybka analiza danych i w tak szerokim zakresie nie była do tej pory dostępna dla sektora przemysłowego w Polsce.

PROJEKT WAŻNY SPOŁECZNIE

– W jednym z raportów Agencji Rozwoju Przemysłu możemy przeczytać, że gęstość robotyzacji w Polsce wynosi 46 robotów na 10 tys. osób. W Korei jest to 531 robotów, a w Niemczech 301. To teraz bije dzwon dla przedsiębiorców. Technologia, chociażby za sprawą takich platform, jak NAZCA 4.0, jest na wyciągnięcie ręki. Jesteśmy w przededniu ogłoszenia przez państwo polskie ulgi na robotyzację. Już dzisiaj można korzystać z licznych dofinansowań na innowacje. Nie ma na co czekać. Uciekający czas powoduje, że inni spijają śmietankę. Ci, którzy skorzystają z pierwszej fali Przemysłu 4.0, wykroją największy kawałek tortu – wyjaśnia Artur Pollak, prezes Zarządu w APA Group.

Projekt NAZCA 4.0 jest skierowany przede wszystkim do właścicieli zakładów produkcyjnych, ale także do menedżerów, automatyków, planistów czy kierowników produkcji. Żeby do niego dołączyć, trzeba skontaktować się z APA Group lub zapisać do grupy eksperckiej na LinkedIn („Industry 4.0 | IIoT | Automatyzacja – na poważnie").

– Kluczem do optymalizacji procesu jest zbieranie danych na jego temat i mierzenie go. Nie da się optymalizować czegoś, o czym nie mamy pojęcia. Więc najpierw musimy zebrać dane, zastanowić się, w czym tkwi problem i co moglibyśmy poprawić – mówi Maciej Walczak, kierownik projektów Industry 4.0 w APA Group. – *To jest projekt, który ma umożliwić firmom bycie jeszcze bardziej konkurencyjnymi, czyli wytwarzanie produktów spersonalizowanych, ułatwienie produkcji wydajnej, niskokosztowej, o wysokich parametrach produktu końcowego. Ma zwiększyć świadomość menedżerów i służb utrzymania ruchu na temat stanu naszych urządzeń produkcyjnych.*

APA GROUP

ul. Tarnogórska 251
44-105 Gliwice
https://www.apagroup.pl

2N® IP STYLE
wyznacza przyszłe standardy wideodomofonów.

Zwycięzca CE Pro BEST Product Award 2021 na wystawie CEDIA. Zaprojektowaliśmy nasz nowy wideodomofon z wyświetlaczem 10", aby przyciągał uwagę w każdym projekcie rezydencyjnym lub biurowym. Wyposażony w procesor AXIS ARTPEC-7, kamerę Full HD (5 MPix) oraz technologię WaveKey, 2N® IP Style wyznacza przyszłość domofonów na nadchodzące lata.

2N TELEKOMUNIKACE a.s., Modřanská 621, 143 01 Prague 4, CZ, +420 261 301 500, sales@2n.cz, www.2n.cz

Part of AXIS COMMUNICATIONS

Wyzwania ochrony obiektów rozproszonych

Obiekty rozproszone widzimy właściwie wszędzie. Zakłady produkcyjne w każdym zakątku naszego kraju wyglądają na miejsce wytwarzania towarów, ale proces produkcji zachodzi nie tylko w nich. Co więcej, z reguły odbywa się w wielu miejscach, nieznanych dla postronnego obserwatora, ale ochronie obiektów muszą one być znane, i to doskonale. Obiekty rozproszone są jednak najtrudniejsze i najciekawsze w przypadku ich ochrony.

Jacek Grzechowiak

Obiekty rozproszone, obecne w naszym życiu biznesowym już od wielu lat, stają się nieodłącznym elementem przede wszystkim segmentu produkcyjnego, w którym proces produkcji wyrobu gotowego zachodzi równolegle w wielu miejscach, przy czym pojęcie „miejsce" jest tu dość umowne, dotyczy bowiem zarówno budynków, jak i takich „miejsc" jak droga, linia kolejowa, a także morze i przestrzeń powietrzna, a nawet cyberprzestrzeń. Mamy więc „obiekt" zdecydowanie wielowymiarowy, w praktyce dość często też międzynarodowy, międzykontynentalny, globalny, mimo że wyrób gotowy wciąż wychodzi z jednego miejsca. Skoro więc mamy taki „obiekt", jego ochrona siłą rzeczy musi być tworzona i prowadzona z uwzględnieniem tych wszystkich „podobiektów" i „wymiarów", łącznie z prawnym i kulturowym, do tego postrzeganych przez pryzmat nie tylko lokalny, ale także międzynarodowy.

Nierzadko obiekty rozporoszone, w tej części stacjonarnej, jaką stanowią budynki i kompleksy budynków, składają się z obiektu głównego oraz obiektów wspomagających. Są one łączone procesami zachodzącymi zarówno pomiędzy nimi, jak i osobami funkcjonującymi w tych obiektach i procesach. Mamy więc całkiem ciekawą matrycę obiektowo-procesowo-personalną. Tworzenie i prowadzenie ochrony takich konglomeratów wymaga, oprócz znajomości procesów w nich zachodzących, także czuwania nad zmianami, które w poszczególnych obiektach i procesach będą przebiegały w różnym czasie, z różną intensywnością i wreszcie z różnym efektem, poczynając od powstawania obiektów i procesów, przez ich modyfikację, kończąc na likwidacji. Co więcej, niejednokrotnie likwidacja procesu nie musi oznaczać pustki czy prostego umiejscowienia w budynkach innego procesu, ale może prowadzić do pojawienia się wewnątrz naszej organizacji innego przedsiębiorstwa, które będzie z nami związane operacyjnie... albo nie. Będzie funkcjonowało w rytm naszych regulacji lub wprowadzi swoje, niekiedy całkiem odmienne, tworząc swego rodzaju enklawę. Czasem dochodzi wręcz do przedzielenia naszego obiektu i utworzenia dwóch odrębnych.

Dlatego obiekty takie są z jednej strony bardzo trudne do zarządzania ich ochroną, z drugiej – najciekawsze. Jak wiadomo, jedyną stałą rzeczą w biznesie jest zmiana. I to w ochronie obiektów rozporoszonych widać wyraźnie. Ta umowna matryca musi żyć. Musi być wciąż aktualizowana, aby „matryca obiektowo-procesowo-personalna ochrony" odpowiadała matrycy całego przedsiębiorstwa w każdym jej wymiarze.

OD CZEGO WIĘC ZACZĄĆ TWORZENIE OCHRONY TAKICH OBIEKTÓW?

Jak zwykle od początku. W tym jednak przypadku początkiem jest zrozumienie nie tylko rodzaju chronionego mienia i procesów, ale także wzajemnych relacji pomiędzy poszczególnymi obiektami i procesami. One bowiem będą bardzo mocno wpływały na potrzebę ochrony, która już nie jest stała, realizowana „tu i teraz" oraz „w ten sposób", ale bardzo często powstaje ad hoc, przynosząc potrzeby wcześniej nieistniejące, a także potrzeby istniejące bardzo krótko. Dotyczy to przede wszystkim obiektów produkujących krótkie serie wyrobów, chociaż produkt wielkoseryjny również może przynieść takie potrzeby. Wyobraźmy sobie bardzo popularny produkt. Taki, którego używamy codziennie, powszechnie dostępny, czyli niskowartościowy, np. pendrive. Produkt wytwarzany w gigantycznych ilościach. U wielu producentów. Zdecydowanie transgraniczny. Wydawałoby się, że ochrona będzie tu procesem powtarzalnym. Prostym do implementacji i trwającym na tyle długo, że jedna koncepcja będzie mogła być realizowana miesiącami, bez żadnych zmian.

Czy na pewno? Pomyślmy... Przychodzi okres świąteczny i producent wprowadza serię wzbogaconą o luksusową obudowę, np. z krzemienia pasiastego, a ponadto część tej partii dostaje jeszcze ozdobną ramkę ze srebra czy złota.... Zbliża się jubileusz tej firmy i wypuszcza ona serię ekskluzywną, bo oprócz obudowy z dużo droższego kamienia jubilerskiego mamy też autograf właściciela wykonany ze złotej nici, ale nade wszystko seria liczy precyzyjnie określoną liczbę produktów i kradzież choćby jednej sztuki ma wtedy zupełnie inny ciężar gatunkowy.

Te przykłady można przenieść na grunt wielu innych produktów, które zmieniając się pod wpływem jednego projektu, powodują de facto zmianę w strukturze obiektu i w konsekwencji konieczna jest znacząca zmiana systemu ochrony. Bo przecież pojawia się mienie, którego do tej pory nie chroniliśmy, a zasady jego ochrony są zupełnie inne. Limitowana seria ekskluzywna, do tego o zabarwieniu emocjonalnym, to nowe wyzwanie. A tu pojawiają się zagrożenia dotychczas u nas niewystępujące, od „prozaicznej" kradzieży, przez sabotaż, po terroryzm. I to wszystko z uwzględnieniem szerokiego spectrum dostawców i współpracowników, dotychczas u nas (a raczej dla nas) niepracujących.

Tak właśnie funkcjonują obiekty rozproszone, dziś już to zjawisko standardowe. Dlatego zrozumienie organizacji, jej poszczególnych komponentów oraz wzajemnych relacji jest kluczowe w tworzeniu efektywnego systemu bezpieczeństwa obiektu rozproszonego.

Jednak tego typu obiekty charakteryzują się także integrowaniem w swojej strukturze komponentów niezwiązanych bezpośrednio z ich kluczową działalnością, takich jak własne elektrownie (wszak już coraz częściej widzimy farmy fotowoltaiczne czy wiatrowe, zaopatrujące w energię zakłady przemy-

słowe), ujęcia wody i oczyszczalnie ścieków, zaawansowane elementy infrastruktury drogowej i kolejowej, a nawet żeglugi śródlądowej i morskiej. A przecież na tym nie koniec, bo są też własne kopalnie (i to wcale nie musi być węgiel) czy punkty przetwarzania odpadów produkcyjnych, które w niektórych gałęziach przemysłu stanowią pokaźne źródło dochodów, np. młóto (wysłodziny powstające w trakcie produkcji piwa, a będące cenną paszą) czy żużel stalowniczy będący cennym kruszywem drogowym. Rozproszenie organizacji więc jest coraz większe.

Jednak to wciąż nie koniec. Mamy przecież jeszcze naukowo-badawcze wsparcie procesu technologicznego, np. różnego rodzaju laboratoria badające jakość wyrobów – co istotne – na różnych etapach produkcji, a więc będące *de facto* częścią procesu produkcyjnego, mimo że wielokrotnie są odrębnymi podmiotami, zlokalizowanymi w pewnym oddaleniu od obiektu głównego. Podobnie rzecz się ma z utrzymaniem ruchu, w którego ramach elementy infrastruktury produkcyjnej podlegają naprawom czy regeneracji w miejscach oddalonych od obiektu głównego, często będących odrębnymi przedsiębiorstwami. Odrębnymi, ale przecież będącymi częścią naszego procesu. Mamy więc – parafrazując jedną z tez tegorocznego Warsaw Security Summit – „nie nasz obiekt, ale nasz problem".

Czy to już koniec rozproszenia? Oczywiście, że nie. To jedynie przykład. Każdy obiekt będzie miał inne, charakterystyczne dla niego części składowe, które mogą być stałe, ale mogą też pojawiać się incydentalnie.

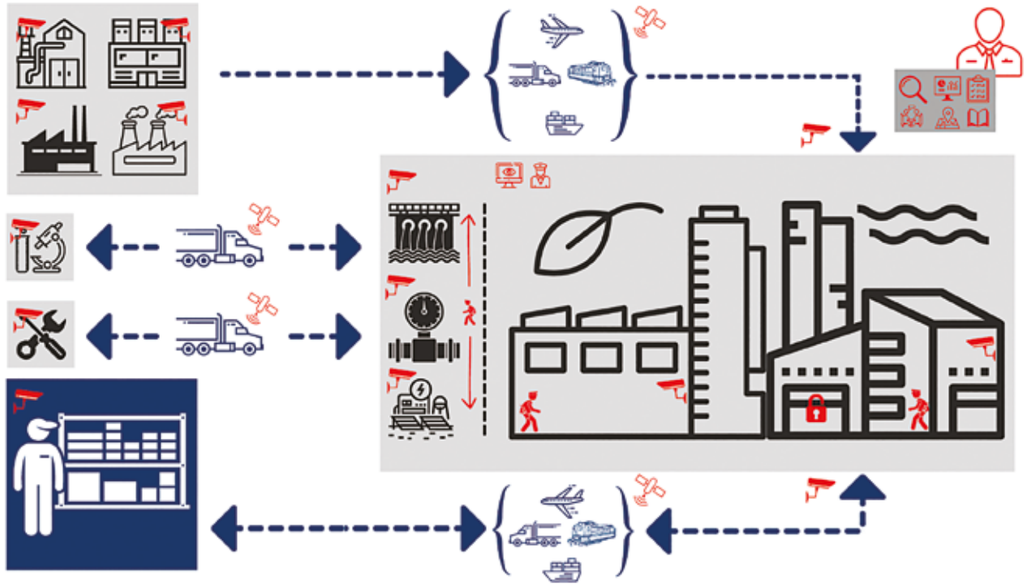
Mamy więc do zabezpieczenia całkiem spory kompleks, na który składają się następujące elementy:

- kompleksy budynków;
- rozległe obszary produkcyjne;
- elementy infrastruktury komunikacyjnej;
- elementy infrastruktury energetycznej;
- różnego rodzaju rurociągi;
- ujęcia wody, wodociągi, infrastruktura hydrotechniczna i oczyszczalnie ścieków;
- laboratoria i centra badawczo-rozwojowe;
- obiekty utrzymania ruchu;
- magazyny i centra logistyczne.

A wszystko to spięte procesami współistniejącymi i dziejącymi się w miejscach, na których bezpieczeństwo nie mamy wpływu (droga, linia kolejowa, morze, przestrzeń powietrzna), a więc musimy chronić sam proces. Na szczęście nie zawsze będą występowały wszystkie wymienione elementy, ale są miejsca, gdzie stan maksymalny istnieje. Obiekty tego typu w naturalny sposób będą wymagały jednoczesnego funkcjonowania wszystkich rozwiązań ochronnych oraz skupienia w strukturze ochrony osób z niekiedy unikalnymi kompetencjami, aby opracowany proces ochrony rzeczywiście obejmował wszystkie obiekty i procesy podlegające ochronie oraz posiadał zdolność objęcia ochroną procesów pojawiających się ad hoc i na krótki czas.

To trudne zadanie. Na szczęście z pomocą przychodzi technologia pozwalająca realizować procesy ochronne w różnej konfiguracji. W tego typu systemie będziemy z pewnością korzystali z zabezpieczeń mechanicznych i elektronicznych obsługiwanych przez pracowników ochrony oraz wewnętrzne działy bezpieczeństwa. Możemy więc spojrzeć w stronę synergii komponentu ludzkiego z technicznym oraz synergii w relacji dostawca usługi ochrony – klient.

W takim systemie ochrona fizyczna musi być już na innym poziomie niż znany nam z codziennej praktyki, niezbędne bowiem będzie posiadanie przez pracowników ochrony nie tylko kompetencji w zakresie obsługi systemów miejscowych, ale także reagowania na zdarzenia zaistniałe poza obiektem głównym, niekiedy także za granicą.



Schemat 1. Synergia komponentu ludzkiego z technicznym i relacji dostawca usługi ochrony – klient

Przykład: grudzień, późny wieczór, kierowca informuje ochronę, że ma symptomy skłonienia go do zatrzymania przez osobników niebudzących zaufania (cytuję słowa kierowcy). Pracownik ochrony przyjmujący to zgłoszenie szybko zorientował się, że prawdopodobnie kierowca ma do czynienia z tzw. metodą na koło, i przytomnie poinformował osobę, która zorganizowała ochronę doraźną tego kierowcy i jego pojazdu. Dzięki temu mógł bezpiecznie dojechać do miejsca, gdzie zgodnie z regulacjami dotyczącymi czasu pracy musiał zrobić przerwę. Takie przypadki zdarzają się i nie są wyłącznie problemem firm transportowych, uszkodzenie pojazdu czy tym bardziej kradzież prowadzi bowiem do zaburzenia ciągłości działania zakładu produkcyjnego. Drugi ważny aspekt – kierowca wiedział, gdzie zadzwonić, by uzyskać pomoc, a firma miała opracowany plan na taki wypadek oraz wyposażenie pozwalające szybko odnaleźć pojazd, co na drodze, w grudniową noc, wcale nie jest proste, a przecież bywają miejsca jeszcze trudniejsze do lokalizacji. Aspekt trzeci, nie mniej ważny: pracownik ochrony obsługujący ten incydent był zlokalizowany w odległości 610 km od miejsca zdarzenia, a ochrona podejmująca działania posługiwała się wyłącznie językiem niemieckim. Znajomość języka obcego przez koordynatora okazała się przydatna.

To, co dzieje się w transporcie, jest bez wątpienia częścią obiektu rozproszonego, wymagając zarządzania bezpieczeństwem w taki sam przezorny sposób, jak ochrona budynków, choć bez wątpienia z wykorzystaniem innych rozwiązań. Jednak „komponent ludzki" musi posiadać umiejętności działania w tego typu sytuacjach, z czym wiążą się także odpowiednie umiejętności komunikacji werbalnej, bo już intonacja głosu może wprowadzić spokój lub niepokój. A to w incydentach bardzo ważne. W takiej sytuacji kierowca jest już wystarczająco zdenerwowany. W tego typu obiektach, jak widać z powyższego przykładu, może zajść potrzeba znajomości języka obcego – przecież kierowcy transportują nasze produkty także za granicą, ale i cudzoziemcy transportują nasze mienie w kraju. Jest tu sporo potrzeb i wyzwań. Potrzebne jest jednak jeszcze coś. Tym czymś jest bliskość ochrony z menedżerami core business. Pozwala to na planowanie zadań ochronnych z wyprzedzeniem, dzięki czemu proste planowanie służby jest już ułatwione, a ochrona procesów, które wystąpią w przyszłości, może zostać opracowana z wystarczającym wyprzedzeniem, co daje szansę na dopracowanie szczegółów.

Obiekty rozproszone to także spore wyzwanie ekonomiczne, zwłaszcza w obecnych realiach rosnącej płacy minimalnej. Ta trudność wynika nie tylko z wpływu makroekonomii, ale także z konieczności zintegrowania całego wachlarza rozwiązań security, powodującego siłą rzeczy posiadanie rozwiązań o zróżnicowanym przeznaczeniu, różnej architekturze, ale i różnym poziomie generacyjnym. I to jest problem pierwszy, tak naprawdę będący początkiem drogi.

Technologie ochronne rozwijają się dziś wyjątkowo szybko, co jednak nie w każdym aspekcie jest pozytywne. Bezsprzecznym plusem są rosnące możliwości systemów. Niestety jest i minus w postaci absorpcji tych technologii przez agencje ochrony, bo przecież kupno nowoczesnych kamer, elementów sygnalizacji włamania i napadu czy geolokalizacji to dopiero początek drogi. Tu szefowie bezpieczeństwa muszą coraz częściej poświęcać czas na zapewnienie właściwego poziomu kompetencji pracowników ochrony, a to z kolei odrywa ich od ich *core businessu.*

Inną potrzebą generującą coraz większe nakłady finansowe jest zasilanie systemów zabezpieczeń technicznych (Z)T, które wraz z ich rozwojem staje się coraz bardziej wymagające i droższe. A trzeba pamiętać, że efektywny czas działania systemu zabezpieczeń jest równy najkrótszemu czasowi podtrzymania zasilania. Ponadto niezbędna staje się ochrona elementów infrastruktury elektro-energetycznej, gdyż są one częścią systemu bezpieczeństwa. Bilans energetyczny jest więc niezbędnym elementem zarządzania bezpieczeństwem. W obiektach rozproszonych jest to widoczne w sposób szczególny, gdyż duża część mniejszych obiektów wchodzących w ich skład jest już teraz chroniona wyłącznie przez systemy ZT. Utrata zasilania jest więc równoznaczna nie tylko utracie ochrony, ale wręcz jakiejkolwiek kontroli tych obiektów.

Ochrona obiektów rozproszonych wymaga gruntownego przygotowania, a jej stworzenie musi być realizowane w bezpośrednim związku z koncepcją funkcjonowania całej firmy. Tworzenie takiego systemu ochrony krok po kroku, poczynając od fundamentu, jakim jest pełna i gruntowna znajomość organizacji i procesów w niej zachodzących, poprzez analizę ryzyka mienia i procesów, dalej przez wybór rozwiązań bezpieczeństwa, prowadzący do świadomego wyboru urządzeń i wreszcie upewnienia się, że dostawca usług ochrony potrafi wykorzystać wszystkie możliwości tych urządzeń i ma wizję ich wykorzystania w przyszłości, pozwoli na stworzenie procesu o wysokim i długoterminowym efekcie operacyjnym i finansowym nawet w tak trudnym obiekcie, jakim jest obiekt rozproszony.

JACEK GRZECHOWIAK

Menedżer ryzyka i bezpieczeństwa. W ramach własnej działalności doradza organizacjom biznesowym w zarządzaniu ryzykiem. W przeszłości związany z grupami Securitas, Avon i Celsa, w których zarządzał bezpieczeństwem i ryzykiem. Absolwent WAT, studiów podyplomowych w SGH i Akademii L. Koźmińskiego. Gościnnie wykłada na uczelniach wyższych.

Nowoczesna ochrona obiektów infrastruktury krytycznej

Duża liczba kamer i obrazów przez nie generowanych wymaga skutecznego systemu VMS, umożliwiającego również integrację z innymi sieciowymi systemami zabezpieczeń elektronicznych. Pozwala to na zarządzanie różnymi systemami w ramach jednej, spójnej sieci i umożliwia lepsze wykorzystanie zaawansowanych funkcjonalności kamer, głośników czy urządzeń kontroli dostępu. W ramach takiego kompleksowego systemu bezpieczeństwa można zatem zarówno chronić obiekt infrastruktury krytycznej przed dostępem niepowołanych osób, jak i nadzorować procesy operacyjne, optymalizować wydajność produkcyjną, monitorować bezpieczeństwo pracowników i w czasie rzeczywistym oceniać ryzyko wystąpienia ewentualnych wypadków oraz im zapobiegać.

Sieciowe systemy AXIS zostały wdrożone w różnych obiektach infrastruktury krytycznej na całym świecie i przetestowane w najtrudniejszych warunkach produkcyjnych. W obiektach o strategicznym znaczeniu dla gospodarki zastosowane rozwiązania dostosowano do obowiązujących w danym kraju przepisów bezpieczeństwa. Zaprojektowano je tak, aby obejmowały cały teren zakładu: zarówno otoczenie, jak i wnętrza poszczególnych budynków.

KONKRETNE KORZYŚCI I REALNE OSZCZĘDNOŚCI

Przykładem może być elektrownia jądrowa Mochovce na Słowacji. Ze względu na jej strategiczne znaczenie dla gospodarki zasady ochrony obiektu reguluje ustawa. Kamery AXIS monitorują teren obiektu oraz przepływ ludzi i materiałów związany z budową kolejnych bloków elektrowni. W obszarach krytycznych, np. w strefach o zwiększonej radioaktywności, zastosowano specjalne kamery z ochroną przeciwwybuchową przeznaczone do pracy w skrajnie trudnych warunkach środowiskowych. Również one zostały połączone z systemami VMS i sygnalizacji włamania. Dzięki temu można zdalnie monitorować cały proces operacyjny i w czasie rzeczywistym reagować na zdarzenia w sytuacjach krytycznych, bez ryzyka potencjalnych przestojów produkcyjnych. Przekłada się to na ogromne, liczone w setkach tysięcy euro oszczędności i pozwala zoptymalizować zarządzanie obiektem.

Z kolei międzynarodowe przedsiębiorstwo EDP Energias de Portugal, które dostarcza energię elektryczną milionom klientów w różnych regionach świata, m.in. w Brazylii, borykało się z częstymi włamaniami na tereny obiektów i kradzieżami kabli. Dzięki zintegrowanym rozwiązaniom Axis – sieci obejmującej kamery, radary, głośniki audio, system VMS oraz urządzenia kontroli dostępu, udało się zmniejszyć liczbę włamań o 95%, a tym samym zapobiec wielu wypadkom śmiertelnym, do których dochodziło podczas tego typu incydentów. Niedawno firma EDP została uznana za najbardziej innowacyjne przedsiębiorstwo energetyczne w Brazylii.

NAJNOWSZE TECHNOLOGIE W OCHRONIE PERYMETRYCZNEJ

Skuteczność ochrony obiektów infrastruktury krytycznej zapewniają najnowsze technologie. Przykładowo, w zabezpieczeniu terenu przed intruzami świetnie sprawdza się system ochrony obwodowej Axis Perimeter Defender, który umożliwia dozór perymetryczny zarówno otoczenia obiektu, poszczególnych stref, dróg wewnętrznych, jak i budynków: hal produkcyjnych, magazynów czy pomieszczeń pracowniczych. Ta technologia pozwala w czasie rzeczywistym wykrywać potencjalnych intruzów w strefie obwodowej (wzdłuż ogrodzenia) i z dużą dokładnością weryfikować szczegóły zdarzeń. Jej istotną zaletą jest również możliwość zdalnej obsługi systemu bezpieczeństwa.

Do monitorowania dużych terenów stosuje się kamery termowizyjne i tradycyjne, wizyjne. Na obszarach słabo oświetlonych lub w całkowitej ciemności wykorzystuje się również kamery wielokierunkowe z funkcją podczerwieni i panoramicznym pokryciem obszaru obserwacji. Śledzenie intruzów umożliwiają kamery PTZ, które automatycznie przybliżają obraz i podążają za wykrytymi osobami i obiektami w ruchu. Zastosowane w kamerach inteligentne algorytmy analizy obrazu informują pracowników ochrony o każdym niepokojącym zdarzeniu, wysyłając odpowiedni komunikat ostrzegawczy. Kamery z systemem IP audio umożliwiają natomiast nadawanie komunikatów, które mają na celu odstraszyć intruzów. Wszystkie te rozwiązania poprawiają zatem szczelność systemu bezpieczeństwa: minimalizują fałszywe alarmy i pozwalają ograniczyć czasochłonne rutynowe patrole.

Nowoczesne cyfrowe systemy kontroli dostępu pozwalają natomiast na inteligentne kontrolowanie wejść personelu do poszczególnych stref, obiektów czy pomieszczeń, a także wyjść. Ponadto umożliwiają zarządzanie wizytami gości mających odpowiednie uprawnienia oraz kontrolowanie pojazdów, które mogą wjeżdżać na dany teren.

OPTYMALIZACJA ZARZĄDZANIA OBIEKTEM I PERSONELEM

Dzięki stosowaniu zintegrowanych rozwiązań bezpieczeństwa można również nadzorować pracę maszyn i optymalizować zarządzanie obiektem. Możliwość wykorzystania do tego tych samych urządzeń zainstalowanych w obiekcie, które służą do ochrony przed intruzami, pozwala znacznie zredukować koszty inwestycji w system monitoringu. Ta sama kamera może bowiem jednocześnie monitorować sprawność poszczególnych urządzeń i alarmować o ewentualnych nieprawidłowościach. Technologia umożliwia zatem zdalne rozwiązywanie problemów i może skutecznie wspierać procesy konserwacji i przeglądów technicznych.

Dzięki zaawansowanym funkcjom aplikacji analitycznych można m.in. kontrolować temperaturę i ciśnienie maszyn oraz weryfikować ewentualne nieprawidłowości i podejmować odpowiednie działania, zanim dojdzie do awarii urządzenia i konieczna będzie kosztowna naprawa. Taki monitoring pozwala na zdalną obserwację temperatury krytycznej, zarówno na krótkich, jak i długich dystansach. Nowoczesne systemy wizyjne umożliwiają tworzenie stref alarmowych, z których zostanie wysłane powiadomienie, gdy temperatura osiągnie poziom wyższy lub niższy od określonych wcześniej progów.

Nowoczesny sieciowy system dozorowy może również wspomagać zarządzanie bezpieczeństwem personelu obiektu infrastruktury krytycznej. Kamery sieciowe wyposażone w inteligentne oprogramowanie analityczne są w stanie w czasie rzeczywistym weryfikować, czy na terenie zakładu przestrzegane są przepisy BHP, np. czy pracownicy noszą odpowiednią odzież ochronną.

W rzeczywistości pandemicznej systemy wizyjne mogą wspierać właścicieli w dostosowywaniu się do nowych przepisów sanitarnych. Tutaj szczególnie przydatne mogą okazać się algorytmy analizy obrazu, np. wykrywające przekroczenie wirtualnej linii, w wyniku czego natychmiast zostanie nadany komunikat audio przypominający o konieczności zachowania wymaganego dystansu społecznego czy zdezynfekowania dłoni.

AXIS COMMUNICATIONS POLAND

ul. Domaniewska 44 bud. 4
02-672 Warszawa
www.axis.com/pl

System lokalizacyjny z kontrolą dostępu

rewolucjonizuje przemysł

Przemysł 4.0 stał się faktem. To już nie tylko określenie symbolizujące zmiany, ale także realny postęp przejawiający się w koncepcji łączenia urządzeń, gromadzenia wysokiej jakości danych i ich analizy. Koncepcja przyspieszyła na skutek pandemii COVID-19 sprawiając, że automatyzacja i podejmowanie decyzji tu i teraz to codzienność wielu firm produkcyjnych i centrów dystrybucyjnych. Tylko ten, kto stawia na szybkość reakcji, wygrywa w nowych realiach biznesowych, a bez rzeczywistych danych o procesach związanych z produkcją trudno tę walkę wygrać.

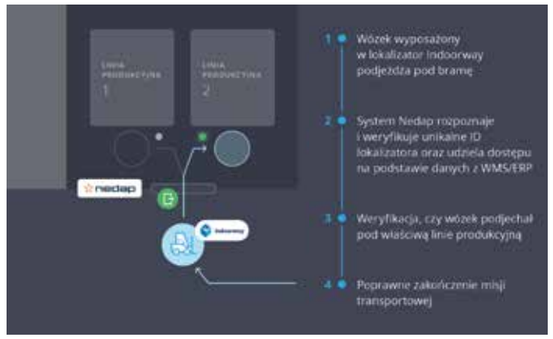
Czwarta rewolucja przemysłowa wprowadziła do przedsiębiorstw cyfryzację czerpiącą ze wszystkich współcześnie dostępnych narzędzi – Internetu, mocy obliczeniowych w chmurze, gromadzenia i analizy olbrzymiej ilości kompleksowych danych, czyli *big data,* autonomicznej robotyki, AI, VR, a także IoT – Internetu rzeczy. Ten ostatni nabiera coraz większego znaczenia, gdyż idące za IoT rozwiązania pozwalają na tworzenie zupełnie nowych modeli biznesowych. Ściśle przeplatając się z podejściem Przemysłu 4.0, tworzą nową wartość dodaną, co z kolei przekłada się na optymalizację całego łańcucha dostaw – od zarządzania produkcją i magazynem po transport towaru do klienta.

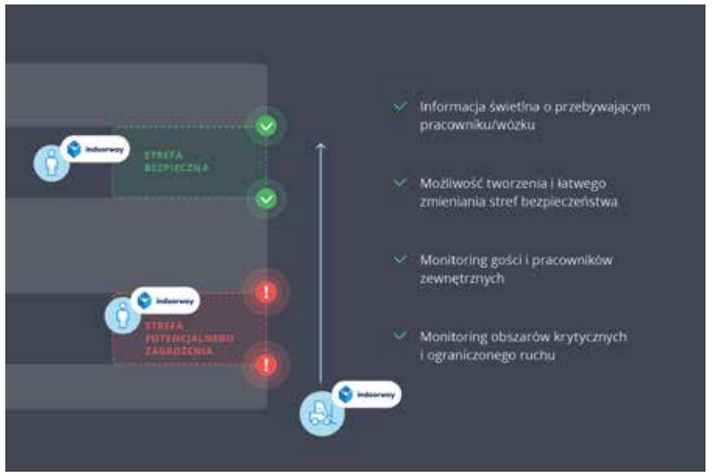
Dobrym na to przykładem są inteligentne czujniki lokalizacji, które zbierają i przetwarzają w chmurze obliczeniowej wysokiej jakości dane o procesach produkcyjnych oraz ruchu pracowników i wózków transportowych. W połączeniu z umiejętnościami, wiedzą i sprawdzonymi praktykami projektowymi specjalistów mogą stworzyć potężny i kompleksowy system do rozwiązywania najbardziej złożonych wyzwań. Jeśli do tego dodać rzeczywiste dane o przepływach, podejmowanie świadomych decyzji w celu poprawy wydajności procesów, lepszej alokacji zasobów i ograniczenia marnotrawstwa, zarządzanie oparte na danych stanie się złotym standardem w funkcjonowaniu przedsiębiorstw.

RZECZYWISTE DANE GWARANTUJĄ SUKCES

– Z naszych doświadczeń z wdrożeń systemu lokalizacji i analizy ruchu w ponad 25 zakładach produkcyjnych, m.in. LOTTE Wedel, Whirlpool, Solaris, Michelin, Dr Irena Eris, Famur, wynika, iż wiedza o aktualnej lokalizacji fizycznych zasobów jest bardzo często brakującym ogniwem do automatyzacji zbierania danych w czasie rzeczywistym lub poprawienia wydajności procesów – tłumaczy Adam Komarnicki, prezes zarządu Indoorway, firmy, która jako jedyna w Polsce spółka technologiczna działającą w obszarze Przemysłu 4.0, dostarcza autorski system RTLS *(Real-Time Location System).* Pozwala on na dokładne pomiary lokalizacji i analizę ruchu zasobów zaangażowanych w procesy produkcji i logistyki wewnętrznej, takich jak wózki widłowe, wózki autonomiczne AGV, pracownicy, półprodukty, wyroby gotowe czy też narzędzia.

– Od dawna bacznie obserwujemy branżę produkcyjną i w odpowiedzi na brak wysokiej jakości danych stworzyliśmy autorski i unikalny na polskim rynku system, który działa w oparciu o technologię Ultra Wide Band (UWB). Nie jest to więc jedynie system składający się z sensorów IoT, które tylko pozyskują dane, ale także zaawansowana analityka w chmurze, pozwalająca na dogłębne zrozumienie procesów występujących w firmach produkcyjnych i centrach dystrybucyjnych. Rozwiązanie dąży do poprawy doświadczeń klientów i zwiększenia ich poziomu zadowolenia, nie wymagając od nich zagłębiania się w samą technologię i szanując ich czas przy wdrożeniu na zasadzie end-to-end. To nowa jakość w zarządzaniu i duży krok w kierunku cyfrowej transformacji zakładów produkcyjnych. Usługa usprawni pracę firm opierających produkcję na analizach big data lub podążających w tym kierunku – dodaje Adam Komarnicki.





Bazujące na doświadczeniach z wizyt i rozmów z ponad stu przedsiębiorstwami rozwiązanie Indoorway zastępuje nieefektywne metody ręcznych pomiarów wydajności procesów, które – na podstawie obserwacji – dostarczają tylko szczątkowych danych słabej jakości. Automatyczne pomiary pozwalają natomiast na dokładne określenie skali problemu. W jednym przypadku okazało się, że np. po godzinie 18.00, kiedy większość kadry kierowniczej wychodzi z pracy, następuje spadek wydajności w transporcie wewnętrznym o 37 proc. Ponadto na podstawie analizy danych można z łatwością zredukować marnotrawstwo procesowe oraz nieplanowane przestoje produkcyjne, których źródła trudno zidentyfikować bez tak dokładnych danych. Według doświadczeń Indoorway już samo wprowadzenie i monitoring standardowych tras dla transportu wewnętrznego pozwala zwiększyć wydajność produkcji o 10 do 30 proc.

KONTROLA DOSTĘPU WSPIERA BEZPIECZEŃSTWO

Chcąc jeszcze efektywniej zarządzać pracą maszyn i ludzi, należy skupić się także na zachowaniu kontroli nad tym, co dzieje się na terenie zakładu. Za tego typu rozwiązaniem stoi system firmy Nedap.

– Nasz system reaguje na zagrożenia i pozwala na zarządzanie bezpieczeństwem strategicznie. W praktyce wygląda to tak, że kontroluje on dostęp lub w razie wypadku czy też awarii odcina strefy, do których poszczególni pracownicy lub podwykonawcy nie powinni wchodzić. Korzystanie z kontroli dostępu, szczególnie z modułami m.in. do zarządzania gośćmi i wykonawcami, daje pewność, że ludzie mogą wchodzić tylko do tych obszarów, do których są upoważnieni – mówi Anna Twardowska z firmy Nedap.

Takie rozwiązanie idealnie sprawdza się w przemyśle, gdzie kontrola dostępu (KD) ma bardzo istotne znaczenie dla ochrony ludzi i środowiska oraz w zarządzaniu ryzykiem mającym wpływ na zyski przedsiębiorstw. Integracja obu systemów – KD Nedap oraz RTLS firmy Indoorway – pozwala na zarządzanie uprawnieniami dostępu zasobów do wybranych stref w obiektach przemysłowych, bazując na ich lokalizacji w czasie rzeczywistym oraz w przypisanych zadaniach. Oba systemy da się ze sobą zintegrować za pomocą interfejsów webserwisowych. Zatem, gdy np. wózek widłowy wyposażony w lokalizator Indoorway podjedzie pod określoną bramę (tzn. wjeżdża w aktywną strefę otwierającą bramę), system KD Nedap dzięki integracji z systemem WMS/ ERP w czasie rzeczywistym zdecyduje o otwarciu, a sygnalizacja świetlna dodatkowo poinformuje operatora, czy podjechał pod właściwą lokalizację. Pozwoli to w pełni wyeliminować błędy ludzkie dzięki automatyzacji przepływu informacji i integracji lokalizacji Indoorway z systemami produkcyjnymi i kontroli dostępu.

– Wykorzystując technologię UWB, znamy dokładne położenie każdego monitorowanego zasobu w czasie rzeczywistym, ponieważ każdy z nich ma lokalizator z unikalnym numerem ID przypisywanym przez administratora obiektom takim jak wózki, pojazdy, osoby. Oprogramowanie Indoorway tworzy zaś wirtualne strefy, które połączone są odpowiednimi algorytmami z uprawnieniami zapisanymi w systemie kontroli dostępu – tłumaczy Adam Komarnicki.

– Dzięki temu, że system Indoorway wykrywa położenie każdego zasobu w czasie rzeczywistym, jest w stanie na bieżąco analizować, czy znajduje się on w odpowiednich strefach. Jeżeli przemieści się do strefy, do której ma uprawnienia, wówczas do systemu zostanie przesłane zdarzenie opisane jako wejście autoryzowane, co będzie widoczne dla operatora. Gdy dany zasób znajdzie się w strefie dla niego niedozwolonej, w systemie zostanie wyświetlone zdarzenie opisane jako wejście nieautoryzowane. Dzięki takiemu rozwiązaniu system Nedap może na bieżąco śledzić ruch zasobów, jak również reagować na incydenty – dodaje Anna Twardowska.

Integracja systemów rozwiązuje więc wyzwania kontroli przepływu – pozwala określić, czy właściwy surowiec lub półprodukt dojechał na właściwe stanowisko, a także czy nie został pomylony np. pas produkcyjny, co może skutkować wstrzymaniem produkcji do czasu oczyszczenia go z zanieczyszczeń. Tego typu rozwiązanie jeszcze lepiej dba też o bezpieczeństwo pracowników i stref roboczych.

Podsumowując, integracja systemu lokalizacyjnego Indoorway z kontrolą dostępu Nedap i systemem produkcyjnym niweluje błędy, zwiększa jakość i wydajność produkcji, zmniejsza ilość odpadów, optymalizuje czas pracy zespołu i kierowników lub liderów, a także tworzy bezpieczniejsze miejsce pracy.

INDOORWAY
ul. Wróbla 35
02-736 Warszawa
www.indoorway.com/pl

NEDAP SECURITY MANAGEMENT
al. Niepodległości 18
02-653 Warszawa
www.nedapsecurity.com/pl/

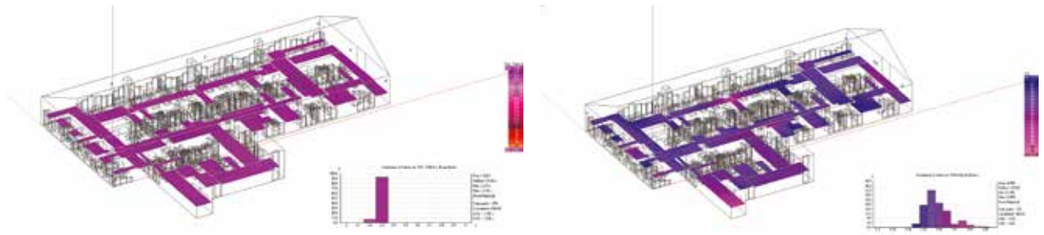
Instalacje DSO w obiektach przemysłowych

Często spotykamy się z sytuacją, kiedy pomimo braku wymogów o charakterze formalnoprawnym inwestor decyduje się na dobrowolne zastosowanie instalacji Dźwiękowego Systemu Ostrzegawczego (DSO). System ten spełnia funkcję elementu wspomagającego działania Systemu Sygnalizacji Pożarowej (SSP) podczas akcji ewakuacji osób z zagrożonej strefy/stref lub całego budynku.

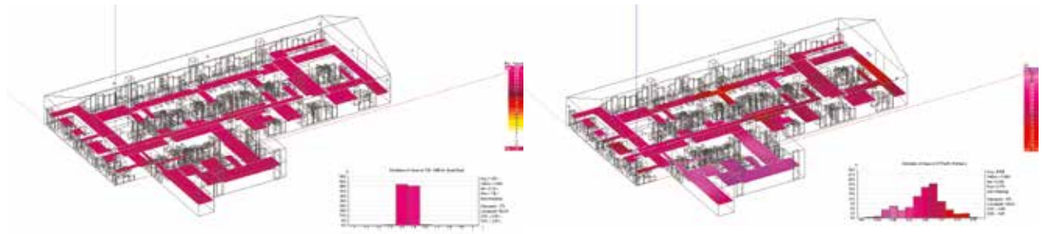
W obiektach przemysłowych podejście do projektowania już od samego początku nie może być realizowane trybem „szablonowym", co często jest spotykane i stosowane w przypadku projektowania instalacji DSO, np. w budynkach hotelowych, akademikach czy budynkach biurowych. Tam aspekt związany z nagłaśnianiem takich stref, jak pokoje hotelowe, biurowe, noclegowe czy korytarze komunikacyjne nie jest zagadnieniem skomplikowanym. Zazwyczaj w takich przestrzeniach mamy do czynienia z aranżacją wnętrz z zastosowaniem wykładzin dywanowych, mebli wypoczynkowych i elementów dekoracyjnych, takich jak kotary, zasłony, firanki zawieszone w oknach, a także łóżka, sofy, pościel. Wszystkie te elementy wyposażenia wnętrz pozytywnie wpływają nie tylko na efekt wizualny czy poczucie komfortu użytkownika, ale również na warunki akustyczne panujące w pomieszczeniu, np. czas pogłosu RT60 *(RT-Reverberation Time)*. W konsekwencji mają one duży wpływ na ostateczną wartość wskaźnika zrozumiałości mowy STI, który jest wyznacznikiem prawidłowo (lub nie) przygotowanej instalacji DSO.
W obiektach przemysłowych, np. halach produkcyjnych przemysłu ciężkiego czy spożywczego, najczęściej panują trudne warunki akustyczne. Hałas czy pogłos w takich przestrzeniach mogą uniemożliwić osiągnięcie odpowiedniej wartości wskaźnika zrozumiałości mowy. Ten sam problem dotyczy przemysłowych obiektów nieprodukcyjnych, np. serwerowni czy data center, gdzie dominującym czynnikiem wpływającym na pogorszenie zrozumiałości komunikatów głosowych jest hałas wywołany przez działające systemy wentylacji. Poziom hałasu w trudnych akustycznie przestrzeniach obiektów przemysłowych może wynosić nawet 100 dBA. Taka jego wartość przy dłuższej ekspozycji bez stosowania odpowiednich nauszników ochronnych lub stoperów może grozić nawet trwałym uszkodzeniem narządu słuchu.

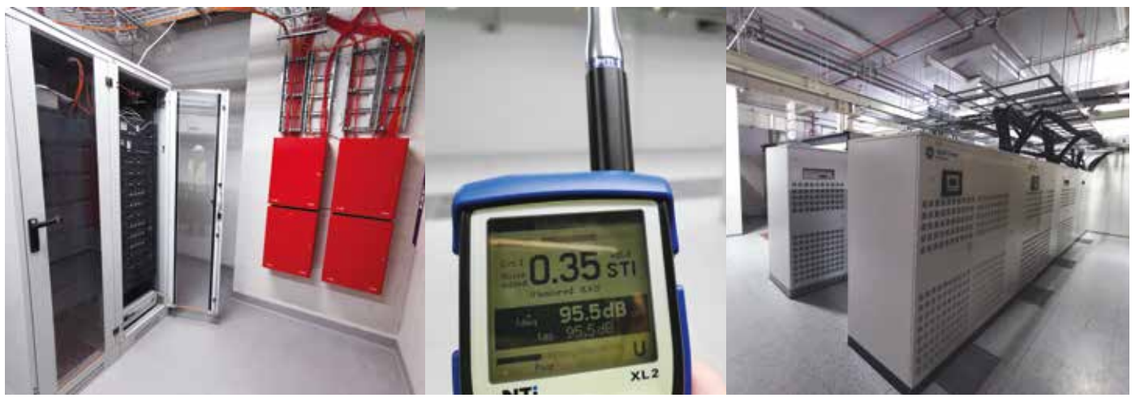
Nie wszystkie i nie całe obiekty przemysłowe są obarczone trudnymi warunkami akustycznymi – hałasem. Do tej grupy można zaliczyć różnego przeznaczenia magazyny, w których jedynymi urządzeniami generującymi hałas są wózki widłowe czy różnego rodzaju roboty transportujące regały czy palety z towarem, pracujące w tym samym czasie razem z załogą.
Gdy hałas i pogłos mogą odgrywać decydującą rolę w (nie)zrozumiałości komunikatów głosowych w obiekcie, bardzo istotne jest dokładne przeanalizowanie każdej z nagłaśnianych stref – z uwzględnieniem ich przeznaczenia, np. biura, serwerownie, korytarze – komunikacja, hala produkcyjna, montażownia – szczególnie pod kątem poziomu hałasu, jaki może w nich występować. W takiej sytuacji należy również przeprowadzić weryfikację pod kątem przyszłego wyposażenia tych przestrzeni, aranżacji – co będzie miało z kolei wpływ na czas pogłosu.
Już na etapie projektu, zanim zostaną dobrane komponenty systemu DSO – APS®-APROSYS, należy konsultować wszystkie te informacje z projektantami systemów bezpieczeństwa pożarowego oraz innych branż, architektami czy nawet inwestorem. Takie podejście umożliwia odpowiedni dobór rozwiązań zarówno w zakresie elementów składowych systemu DSO APS®-APROSYS, jak i samych głośników, z rozróżnieniem na typ: sufitowy, naścienny, projektor dźwięku, tubowy czy kolumna głośnikowa oraz odpowiedni dobór odczepów mocy transformatora – zapewniając tym samym właściwy poziom ciśnienia akustycznego wytwarzanego przez głośnik.
Ważnym elementem całej „układanki" jest doprecyzowanie informacji dotyczących rodzaju materiałów wykończeniowych, zastosowanych w rozpatrywanej przestrzeni, ze względu na nie tak rzadką konieczność przeprowadzenia dodatkowych obliczeń na podstawie symulacji akustycznych w dedykowanym programie komputerowym. Niekiedy bez wykonania takich symulacji – nawet wielokrotnie powtarzanych w celu optymalizacji doboru i rozmieszczenia materiałów dźwiękochłonnych (często nieprzewidzianych na etapie projektu architektonicznego) – nie będzie można przygotować prawidłowego projektu instalacji DSO. Takie zabiegi pozwalają na weryfikację koncepcji doboru i rozmieszczenia głośników oraz sprawdzenia, czy w konkretnych warunkach akustycznych ta instalacja ma szansę zadziałać skutecznie. Bardzo często dochodzi do sytuacji, kiedy główny wykonawca budowy jest postawiony przed faktem dokonanym i zmuszony do „uzupełnienia braków" w instalacji. Braki te często nie dotyczą części teletechnicznej, ale architektonicznej, np. konieczności dołożenia wełny mineralnej, tynku akustycznego czy innego materiału dźwiękochłonnego, bez którego po prostu system DSO „nie zagra" odpowiednio dobrze, tzn. w sposób wystarczający, aby spełnić minimalnie nawet wymagania projektowe.
Po wykonaniu symulacji akustycznych, z uwzględnieniem poziomu hałasu i całkowitej chłonności akustycznej pomieszczenia, można w znacznym stopniu zbliżyć się do warunków rzeczywistych, jakie będą w analizowanej przestrzeni w danym budynku przemysłowym.
Po dokonaniu rewizji instalacji i doprowadzeniu pomieszczeń do stanu docelowego, kolejnym i już ostatnim etapem jest przeprowadzenie pomiarów akustycznych w celu sprawdzenia i potwierdzenia prawidłowości zastosowanego rozwiązania. Pomiary są zazwyczaj wykonywane metodą obiektywną, czyli z wykorzystaniem dedykowanych mierników odpowiednio skalibrowanych przez producenta do szumu testowego STIPA (symulującego mowę ludzką). Po wykonaniu takich pomiarów sporządzany jest protokół z uzyskanymi wynikami wskaźnika zrozumiałości mowy STI. Jeśli są one na poziomie wartości minimalnej przewidzianej w projekcie dla danego obiektu (zazwyczaj zalecana to 0,5 STI), wówczas można przekazać instalację do odbioru technicznego przez inwestora i uzyskania pozytywnej opinii w zakresie ochrony przeciwpożarowej od PSP.
Zdarzają się oczywiście i takie sytuacje, że pomimo wykonania symulacji akustycznych i przeprowadzenia optymalizacji, w rzeczywistych warunkach wyniki pomiarów są niższe niż to wynikało z analizy na etapie projektu. Powodem tego może być wiele czynników, np. brak odpowiedniej dokładności na etapie tworzenia samego modelu, brak odzwierciedlenia parametrów akustycznych zastosowanych materiałów, brak aranżacji pomieszczenia, niespójny z rzeczywistością poziom hałasu lub brak dostrojenia samego systemu, z zachowaniem odpowiednich poziomów głośności w stosunku do panującego hałasu.
W takich przypadkach należy dogłębnie przeanalizować powód rozbieżności wyników uzyskanych metodą obliczeniową i uzyskanych bezpośrednio podczas pomiarów. Firma Schrack Seconet Polska we współpracy z siecią autoryzowanych partnerów zapewnia pełne wsparcie doświadczonego personelu na każdym etapie projektu systemu DSO – od opracowania koncepcji, poprzez projektowanie i instalację, po ocenę i weryfikację działania systemu.

Rys. 1. Przykłady wyników symulacji dla przestrzeni bez adaptacji (T30 = 2,38 s, STIPA ≈ 0,45)



Rys. 2. Przykłady wyników symulacji dla przestrzeni z adaptacją (T30 = 1,45 s, STIPA ≈ 0,66)



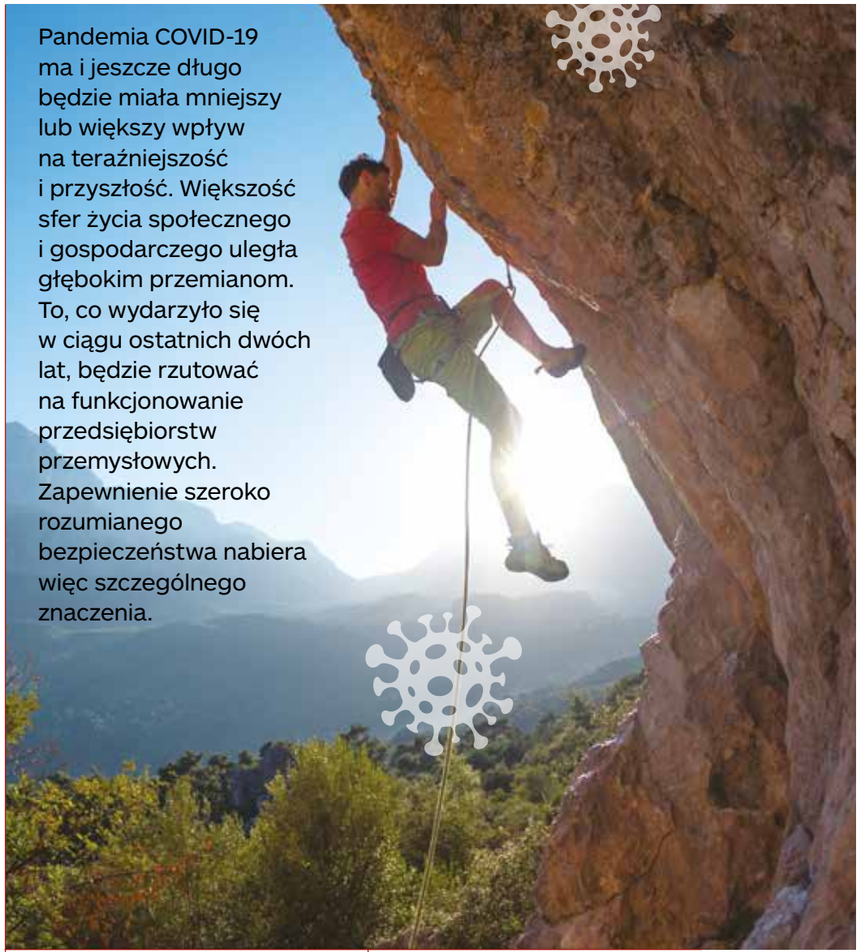


Fot. Realizacja Schrack Seconet - materiały firmowe

SCHRACK SECONET POLSKA
ul. A. Branickiego 15,
02-972 Warszawa
www.schrack-seconet.pl

Czym jest bezpieczeństwo

Wincenty Ignatowski



Pandemia COVID-19 ma i jeszcze długo będzie miała mniejszy lub większy wpływ na teraźniejszość i przyszłość. Większość sfer życia społecznego i gospodarczego uległa głębokim przemianom. To, co wydarzyło się w ciągu ostatnich dwóch lat, będzie rzutować na funkcjonowanie przedsiębiorstw przemysłowych. Zapewnienie szeroko rozumianego bezpieczeństwa nabiera więc szczególnego znaczenia.

Czym dla mnie – wieloletniego menedżera – jest bezpieczeństwo? Powinno być rozumiane jako stan pewności, spokoju, braku zagrożeń i być potrzebą do zaspokojenia, do czego muszą dążyć różne podmioty. Jak bowiem zauważył W. Fehler[1], (...) *współczesne zakłady przemysłowe, działając w warunkach gospodarki rynkowej z cechującą ją ostrą rywalizacją i ponadnarodowymi powiązaniami, chcąc poważnie i perspektywicznie myśleć o sukcesach, nie tylko nie mogą pominąć aspektu bezpieczeństwa, ale wręcz nadają mu znaczącą rangę w wewnętrznym katalogu celów.*

W dobrze zarządzanej organizacji takie podejście do bezpieczeństwa od wielu lat się nie zmieniło, nadal jest jedną z podstawowych potrzeb. Biorąc pod uwagę okoliczności, w jakich przyszło nam funkcjonować, zapewnienie bezpieczeństwa w obiektach przemysłowych jest rzeczywiście wyzwaniem. Szczególnie trudno o nie zadbać dzisiaj, gdy w celu zminimalizowania ryzyka zarażenia koronawirusem zarządy większości przedsiębiorstw wprowadziły regulacje nakazujące lub zachęcające pracowników do pracy zdalnej. W wyniku tych zabiegów, skądinąd słusznych ze względu na dbałość o zdrowie i życie pracowników, funkcjonowanie dużych zakładów produkcyjnych było i nadal jest niezwykle trudne, ponieważ nie można produkować towarów, pracując na odległość.

Praca zdalna stała się codziennością dla tych, których obowiązki mogą na taką formę sobie pozwolić (dotyczy to w dużej mierze menedżerów średniego i wyższego szczebla). Ograniczyło to jednak m.in. nadzór nad pracownikami, których praca na terenie zakładu przemysłowego jest niezbędna. Nawet gdy w przedsiębiorstwie wprowadzono z sukcesem nowoczesne i sprawdzone systemy zarządzania (m.in. LEAN), to człowiek nadal jest najważniejszym w procesie pracy, ale i najsłabszym ogniwem w łańcuchu produkcyjnym, wymagając permanentnego wsparcia.

Stąd funkcje kontrolne coraz częściej przejmuje AI[2] wykorzystywana w bezpieczeństwie w różnych dziedzinach produkcji. Wszyscy zdajemy sobie sprawę, jak ważne w zakładach przemysłowych są przepisy BHP ze względu na szeroki wachlarz zagrożeń zdrowia i życia pracowników.

Dlatego sztuczną inteligencję wykorzystuje się tu szeroko m.in. do rozpoznawania, czy pracownicy pracują w sposób bezpieczny dla siebie i innych. Jednym z ważnych elementów BHP jest konieczność noszenia kasków, okularów i środków ochrony indywidualnej (tzw. ubiory wysokiej widoczności). W tym przypadku sprawdza się system wykorzystujący gotową architekturę sieci neuronowej nauczonej rozpoznawania szerokiego zbioru danych. Taki system stosujący kamery wysokiej rozdzielczości i odpowiednie przetwarzanie obrazu pozwala na „wychwytywanie" osób, które świadomie lub nieświadomie ignorują konieczność stosowania odzieży ochronnej na terenie zakładu produkcyjnego.

Ważnym elementem wykorzystywanym tym razem do zapewnienia ochrony mienia o dużej wartości jest system rozpoznawania towaru po jego kształcie, frakcji lub innych parametrach. Zastosowany do nadzoru ruchu materiałowego na terenie obiektu przemysłowego system AI pozwala kontrolować przepływ towarów, samochodów, ruchu osobowego bez bezpośredniego udziału człowieka lub przy niewielkim jego udziale. Usługa rozpoznawania towaru, odróżniania pojazdów, wykorzystująca zaawansowane systemy teleinformatyczne może zostać udostępniona w chmurze w formie API[3] jako serwer z gRPC[4] pozwalający klientowi końcowemu w trybie *live* otrzymywać dowolną informację o transportowanym towarze. W przypadku jego niezgodności ze specyfikacją (WZ, list przewozowy itp.) osoba zdefiniowana w bazie danych jest natychmiast informowana o rozbieżności, co pozwala na podjęcie działań bez zbędnej zwłoki.

Innym przykładem wysoko zaawansowanej technologii, już szeroko stosowanej, jest Zintegrowany System Zarządzania Bezpieczeństwem. Dzisiaj trudno sobie wyobrazić zarządzanie bezpieczeństwem bez takich rozwiązań, gdy jeden system zarządzany np. przez aplikację tzw. *web service* sygnalizuje włamanie, napad, pożar oraz pełni funkcje systemu kontroli dostępu czy rejestruje obrazy z systemu telewizji dozorowej.

W kontekście CCTV menedżer bezpieczeństwa potrzebuje informacji – obrazu w trybie online w przypadku jakichkolwiek zdarzeń niepożądanych w obiekcie (np. naruszenie strefy detekcji ruchu w polu widzenia kamery). W szerszym kontekście zaś kieruje swoje zainteresowanie w stronę systemów, których odpowiedzią na wykrycie zagrożenia jest sygnał przekazywany do centrum odbiorczego, w którym wyspecjalizowany operator powiadamia o tym fakcie służby odpowiedzialne za bezpieczeństwo lub przekazuje informacje o charakterze serwisowym do instalatora konserwującego system i bezpośrednio do użytkownika.

W obliczu pandemii oraz nasilających się zagrożeń terrorystycznych jedynie policja lub przeszkoleni pracownicy grup interwencyjnych mogą zapewnić skuteczną i profesjonalną interwencję w razie wystąpienia zagrożenia bez narażania zdrowia i życia osób postronnych. Właśnie takie działanie dobrze wyszkolonych specjalistów będących członkami grup interwencyjnych wydaje się optymalne pod względem ekonomicznym i skuteczności.

W perspektywie kolejnych lat procesy kontrolne będą w pełni zautomatyzowane i będą odbywać się bez udziału człowieka lub przy niewielkim nakładzie jego pracy. Pracownik ochrony, słabo wykwalifikowany, bez umiejętności obsługi aplikacji w chmurze zostanie zepchnięty na margines rynku pracy. Zostanie zastąpiony wysoko wykwalifikowanym operatorem systemu dozoru wizyjnego, nie tylko potrafiącym obsługiwać wspomniane aplikacje, ale także posiadającym umiejętności analityczne, na których podstawie będzie natychmiast podejmować decyzje zapobiegające powstawaniu zdarzeń niepożądanych na terenie zakładu przemysłowego.

Mówiąc o wyzwaniach w zapewnieniu bezpieczeństwa, przed jakimi stoją podmioty za nie odpowiedzialne, należałoby wskazać trzech głównych interesariuszy:

1. Klient w rozumieniu osoby odpowiedzialnej za bezpieczeństwo na terenie obiektu przemysłowego, która musi dbać o ciągłe doskonalenie się i dostosowywanie polityki bezpieczeństwa do zmieniających się okoliczności. Każda organizacja, tym bardziej zakład produkcyjny ze względu na zagrożenia, na jakie jest narażony, musi się odpowiednio zorganizować, by zapobiegać kryzysom, stawić im czoło i zarządzać nimi na możliwie najlepszych zasadach, a także wyciągać właściwe wnioski.
2. Wyzwaniem dla każdego dostawcy rozwiązań security jest pomoc klientowi w zbudowaniu takiego systemu zabezpieczeń, który nie będzie ograniczał produkcji i rozwoju firmy.
3. Trudno sobie dzisiaj wyobrazić funkcjonowanie dobrze zorganizowanego zintegrowanego systemu zarządzania bezpieczeństwem bez udziału **integratora**[5]. Rola tego podmiotu jest ważna, ponieważ stanowi pomost pomiędzy klientem a dostawcą rozwiązań security. Mądry potrafiący słuchać potrzeb klienta integrator umiejący zaprojektować dostosowane do obiektu rozwiązania jest nie do przecenienia.

Zapewnienie bezpieczeństwa i profilaktyka w warunkach gospodarki rynkowej nie mogą być obce żadnemu z tych podmiotów. To wyzwania na teraz i na przyszłość. Taniej bowiem ukierunkować działalność na eliminowanie niepożądanych zjawisk, niż ponosić koszty ich skutków. Ważnym czynnikiem jest też zachowanie równowagi pomiędzy bezpieczeństwem a produktywnością. Zbyt wiele zabezpieczeń może przeszkadzać w prowadzeniu działalności, zbyt mało zaś naraża przedsiębiorstwo na szkody materialne i niematerialne, odpowiedzialność karną, cywilną, utratę wizerunku i reputacji przedsiębiorstwa. Wyzwaniem dla każdego dostawcy rozwiązań security oraz integratora jest pomóc klientowi zbudować taki system bezpieczeństwa, który nie będzie ograniczał produkcji i rozwoju firmy. Gdyby jakieś ograniczenia były niezbędne, korzyści materialne z zastosowanych środków bezpieczeństwa przewyższą straty spowodowane tymi ograniczeniami.

1 W. Fehler, *Bezpieczeństwo w biznesie*, Warszawa 2005, s.11.

2 Sztuczna inteligencja *(artificial intelligence)* – inteligencja wykazywana przez urządzenia (w przeciwieństwie do inteligencji naturalnej).

3 *Application Programming Interface* – interfejs programistyczny aplikacji.

4 gRPC – system zdalnego wywoływania procedur typu *open source*.

5 Integrator systemów *(systems integrator)* – podmiot (np. firma informatyczna lub niezależny konsultant) dysponujący aktualną wiedzą w zakresie sprzętu, oprogramowania, organizacji Informatycznych Systemów Wsparcia Biznesu wykorzystywanych m.in. w bezpieczeństwie przedsiębiorstwa.

WINCENTY IGNATOWSKI

Absolwent UW (Wydział Socjologii) oraz studiów podyplomowych z zakresu Bezpieczeństwa Biznesu w Wyższej Szkole Finansów i Zarządzania w Warszawie. Od 2001 r. menedżer ds. bezpieczeństwa w międzynarodowych korporacjach z branży logistycznej, handlowych, usługowych i produkcyjnych w Polsce i Europie. Specjalizuje się w polityce zapobiegania stratom *(Loss Prevention Policy)*, Corporate Security, bezpieczeństwie procesów operacyjnych oraz kwestiach związanych z polityką *compliance*.

Głos branży

JAK ZAPEWNIĆ BEZPIECZEŃSTWO I SPRAWNE FUNKCJONOWANIE OBIEKTÓW PRZEMYSŁOWYCH, ZWŁASZCZA W DOBIE PANDEMII? SWOIMI RADAMI DZIELĄ SIĘ PRZEDSTAWICIELE RÓŻNYCH SEKTORÓW GOSPODARKI.

Dariusz Wesołowski

Gunnebo Entrance Control

Odpowiedzialne zarządzanie obiektami przemysłowymi

Skuteczna ochrona każdego typu obiektu to połączenie środków ochrony fizycznej z zabezpieczeniami elektronicznymi. Jednak sukces nowoczesnych systemów ochrony w dużej mierze sprowadza się do odpowiedniego przygotowania infrastruktury oraz szybkiej gotowości działania.

Zarządcy obiektów przemysłowych stoją przed odpowiedzialnym zadaniem, ponieważ to na nich spoczywa wybór odpowiedniego systemu kontroli dostępu. Systemu, który będzie spełniał najważniejsze założenia dotyczące bezpieczeństwa osób i mienia, jak również odpowiadał za szereg dodatkowych zadań, takich jak zapewnienie odpowiedniej przepustowości przepływu osób i towarów. Wybierając system kontroli dostępu, menedżerowie ds. bezpieczeństwa powinni rozpocząć swoje działania od przeprowadzenia audytu bezpieczeństwa. Jego wynik wskaże potencjalne czynniki wpływające na powstanie zagrożeń wewnętrznych i zewnętrznych, na które obiekt będzie musiał być odpowiednio przygotowany. Audyt jest również punktem wyjściowym ułatwiającym wybór właściwych urządzeń fizycznych, którymi mogą być np. bramki sensoryczne, śluzy osobowe lub furty wysokie. Na podstawie wyciągniętych wniosków z przeprowadzonego audytu zarządcy będą mogli przygotować odpowiednią strategię operacyjną.

W sektorze przemysłowym systemy ochrony powinny być złożone ze wzajemnie uzupełniających się sekcji, które w pierwszej kolejności przeciwdziałają zagrożeniu, następnie pozwalają je skutecznie wykryć, a w krytycznej fazie zminimalizować jego konsekwencje.

Oprócz wyboru urządzeń zabezpieczających dostęp do określonych stref wewnątrz obiektów nie można zapomnieć o odpowiednim zabezpieczeniu terenu przyległego, za co odpowiadają systemy ochrony perymetrycznej. W ich skład wchodzą m.in. zapory drogowe, bollardy (pachołki) czy bramy szybkobieżne. Odpowiednie połączenie wszystkich elementów ochrony wewnętrznej i zewnętrznej umożliwi zarządcom przygotowanie systemu kontroli dostępu, który będzie zapewniać właściwy poziom ochrony.

Artur Pollak

APA Group

Cyberbezpieczeństwo niezbędnym elementem

Głównym zadaniem Przemysłu 4.0 jest kumulowanie danych i przetwarzanie dużych ich zbiorów. Istotną kwestią, o której każdy dostawca rozwiązań tego typu powinien pamiętać i wdrażać symultanicznie ze swoimi produktami, jest zapewnienie bezpieczeństwa cybernetycznego. Cyberbezpieczeństwo jest jednym z niezbędnych elementów, które otacza transfer danych, anonimizuje je po to, żeby gromadzone *big data* mogły funkcjonować w sposób bezpieczny. Wyciągane z analizy wnioski w żadnej formie nie mogą wpaść w niepowołane ręce. Od strony funkcjonalnej rozwiązania dla Przemysłu 4.0 powinny zapewniać totalną integrację: systemów kontroli dostępu, dozoru wizyjnego CCTV/VSS, sygnalizacji włamania i systemów przeciwpożarowych. Oznacza to, że w dobrze zabezpieczonych obiektach zaimplementowane rozwiązania Przemysłu 4.0 zbierają informacje ze wszystkich źródeł i pozwalają lepiej zarządzać bezpieczeństwem oraz ruchem osób znajdujących się w tych obiektach. Wzmocniona jest wtedy trafność podejmowanych przez człowieka decyzji, a całość może tworzyć podwaliny pod system ekspertowy. W momencie połączenia z rozwiązaniami typu *digital signage* – cyfrowymi podpowiadaczami mówiącymi, jak mamy się zachować podczas wystąpienia paniki lub zdarzenia niepożądanego – obiekt automatycznie wskaże najkrótszą drogę ewakuacji, podejmie decyzje o odcięciu poszczególnych stref, napięcia elektrycznego, dostępu tlenu w celu przygotowania bezpiecznej akcji ratunkowej.

Krzysztof Bartuszek

Securitas Polska

Rola pracownika ochrony

Celem ochrony jest zapewnienie szeroko rozumianego bezpieczeństwa obiektów przemysłowych, adekwatnie do zdiagnozowanych zagrożeń i potrzeb klientów. W zakładach przemysłowych największym ryzykiem jest zatrzymanie produkcji, któremu podporządkowane są wszystkie procesy związane z bezpieczeństwem. Dla ciągłości produkcji największym zagrożeniem jest pożar, który pojawia się najczęściej z powodu błędu człowieka lub jego celowego działania albo w wyniku awarii technicznej. Już dziś drony uzbrojone w kamery termowizyjne, dokonujące przelotów prewencyjnych, skutecznie diagnozują elementy infrastruktury, które w wyniku awarii mają podwyższoną temperaturę. Tym samym umożliwiają reakcję, zanim dojdzie do pożaru niszczącego infrastrukturę. W realny sposób zapobiegamy wstrzymaniu produkcji i ograniczamy koszty odbudowania zasobów firmy, nie mówiąc już o utracie rynków.

Przybywa zadań ochrony – nadzór i wsparcie bezpieczeństwa pracy, rejestrowanie nieprawidłowości w tym obszarze i pierwsza pomoc przedmedyczna, a także wsparcie procesów logistycznych, kierowanie ruchem czy awizacje. Najnowsze technologie pozwalają część zadań ochrony fizycznej realizować zdalnie i automatycznie. Czynności do niedawna wykonywane fizycznie przez pracownika ochrony, np. obchody, mogą być teraz przeprowadzone przez systemy telewizji dozorowej z funkcjami analityki obrazu. Również funkcje kontroli dostępu do wybranych obszarów można już w pełni zautomatyzować. Za przykład może posłużyć rozwiązanie Securitas smartGATE. Oprócz automatyzacji procesów przynosi także wymierne korzyści w postaci optymalizacji kosztów związanych z bezpieczeństwem obiektu oraz wnosi wiele istotnych informacji z punktu widzenia logistyki, np. dokładne dane o przybyciu kierowcy, czasie trwania załadunku czy też przyczynach anulowania zlecenia. System jest wyposażony w przejrzysty dashboard wraz z KPI, co pozwala zwiększać możliwości operacyjne klienta, a także skrócić czas obsługi zamówień.

Pracownicy ochrony cały czas pozostają jednak istotnym ogniwem w systemie bezpieczeństwa. Po pierwsze, muszą obsługiwać systemy, nawet jeśli są wysoko zautomatyzowane, a po drugie, może nawet ważniejsze, muszą na bieżąco reagować w sytuacji wystąpienia zagrożenia. Wsparcie mogą zapewnić rozwiązania z zakresu rozszerzonej rzeczywistości *(augmented reality)*, czyli powiązanie środowiska realnego z wygenerowanym komputerowo. Już dzisiaj można spotkać firmy, które w ten sposób szkolą swoich pracowników ochrony, np. podczas pozorowanych akcji ratowniczych czy ewakuacji w obiektach o podwyższonym ryzyku awarii przemysłowej. Podobne rozwiązanie stosuje branża motoryzacyjna na etapie montażu elementów wyposażenia pojazdów. Jesteśmy przekonani, że dobrze wykwalifikowani pracownicy ochrony wspierani nowymi technologiami to przyszłość, a w zasadzie już teraźniejszość branży security oraz wartość dodana dla naszych klientów, którzy są coraz bardziej wymagający w związku z szybko zmieniającym się otoczeniem biznesowym.

Krzysztof Pohorecki

BlackOnion – Resilience Community

Zmiany w podejściu do bezpieczeństwa

Sic transit gloria mundi (tak przemija chwała świata) – popularna sentencja łacińska nabiera w ostatnich czasach aktualności nie tylko ze względu na rodzaje procesów, które dzieją się globalnie, ale przede wszystkim na ich skalę, tempo zmian, bezpośredniość i siłę oddziaływania lokalnego. Nowa rzeczywistość, jakkolwiek ekscytująca, niesie coraz więcej zagrożeń i otwiera nowe obszary ryzyka często już kiedyś definiowanego, ale aktualnie materializującego się w zaskakującym tempie i z potężną siłą oddziaływania.

Największym wyzwaniem dla zapewnienia bezpieczeństwa, według mojej oceny, jest dostosowanie się do skali i szybkości rozwoju technologii, skutkującego niespotykaną dotąd komplikacją stosowanych rozwiązań, a przede wszystkim ich podatnościami na zagrożenia.

Zakres specjalistycznej wiedzy, szybkość jej przyswajania i kompilowania oraz umiejętność komunikowania i stosowania w praktyce wymaga nowej generacji „bezpieczników", a przede wszystkim gruntownej zmiany w percepcji „bezpieczeństwa".

Każdy obiekt, system, proces czy organizacja są tylko tak bezpieczne, jak świadoma, profesjonalna i zmotywowana jest grupa ludzi, którzy za jej zabezpieczenie odpowiadają. I nie mam tu na myśli struktur bezpieczeństwa w standardowym rozumieniu – te klasyczne formy przechodzą do historii w tempie zaskakującym głównie dla nich samych. Umiejętne – „mądre" (wolę zdecydowanie bardziej to określenie niż popularne „sprytne" czy „zwinne" smart) przekładanie owoców błyskawicznego postępu technologicznego na stosowane w praktyce systemy bezpieczeństwa, a przede wszystkim ich skalowanie, integracja i zabezpieczenie ich samych będzie największym wyzwaniem w nadchodzących czasach.

Janusz Syrówka

innogy Polska

Wdrażanie rozwiązań zintegrowanych

Systemy bezpieczeństwa mogą dziś zaoferować znacznie więcej niż stereotypowo przypisuje się tradycyjnemu pojęciu zabezpieczenia obiektu. Przemysł jest wyjątkowo wdzięcznym obszarem dla skorzystania z tej oferty. Dzisiejsze możliwości integracji rozwiązań, a także, w kolejnym kroku, opcje zarządzania przesyłaniem informacji płynących z systemów są ogromne. Bardzo często technologia nie stanowi już dla tych możliwości tak silnej bariery, jak wyobraźnia osób projektujących rozwiązanie. Uważam, że właściwsza nazwa to systemy bezpieczeństwa i wspierania procesów operacyjnych.

Naturalnym obszarem synergii jest obszar BHP – właściwe wykorzystanie telewizji dozorowej czy kontroli dostępu może być bezcenne z punktu widzenia zapobiegania wypadkom w pracy. Idąc dalej, systemy bezpieczeństwa mogą dzielić się informacjami także w innych obszarach, np. monitorowania temperatury, analizy obrazu nakierowanej na inne aspekty niż minimalizacja strat czy zasilanie informacjami systemów SIEM. To oczywiście tylko ułamek możliwości. Czy można osiągnąć podobny efekt, budując rozwiązania w ramach procesów technologicznych? Oczywiście można. Dlaczego więc warto „upychać" wszystko do systemu bezpieczeństwa? Korzyści jest wiele – oszczędzamy na inwestycji, upraszczamy utrzymanie (zapewne i koszty), ustanawiamy czytelną odpowiedzialność za sprawność systemu. I co ważne, takie rozwiązanie koncentruje koszty w jednym ośrodku, a to ułatwia ich monitoring i pozwala mierzyć efektywność zastosowanych rozwiązań.

Dużym wyzwaniem dla wdrażania rozwiązań zintegrowanych jest kwestia właściwego zaadresowania przez zarządcę jego potrzeb. Całościowe spojrzenie na prowadzoną działalność nie jest rzeczą łatwą. Pozostawienie wolnej ręki dostawcy rozwiązań jest niekoniecznie dobre. Przy nawet najlepszych intencjach spojrzenie dostawcy może być „skażone" perspektywą własnej oferty. To natomiast może być niekoniecznie najlepszą opcją dla klienta. Wyjściem z sytuacji jest poszukiwanie właściwych kompetencji poza organizacją i wsparcie procesu tworzenia założeń do budowanych systemów. Takie podejście ułatwi życie dostawcy, wykonawcy, a na koniec użytkownikowi. Poza tym taka konsultacja bardzo szybko przekształca się z kosztu w doskonałą inwestycję.

Jakub Sobek

Linc Polska

Koło zamachowe gospodarki

Nie ma produkcji przemysłowej bez wystarczających dostaw energii – to pewne. Elektryczność jest jednym z największych kół zamachowych współczesnej gospodarki. I właśnie problemy z dostarczeniem prądu elektrycznego należą do najczęstszych powodów zatrzymania produkcji. Choć nie na wszystkie awarie można mieć wpływ, to duży ich odsetek można przewidzieć i zareagować, nim dojdzie do sytuacji krytycznych. Bez względu na to, czy twoim obowiązkiem jest zagwarantowanie sprawności elektrowni, utrzymanie przepływu energii przez sieci dystrybucyjne, czy usuwanie awarii na poziomie budynków przemysłowych, zawsze potrzebujesz narzędzi, które pomogą ci szybko zdiagnozować problemy, zanim przekształcą się w kosztowne szkody.

Problemy z elektrycznością mogą się pojawiać w miejscach, gdzie ta energia jest wytwarzana, np. w elektrowniach wiatrowych. Elementy turbin wiatrowych są podatne na zużycie, mogą się zepsuć. Kiedy tak się stanie, rezultatem może być kosztowny przestój lub poważny wypadek. Dlatego właśnie ciągłe kontrole są tak istotne. Wyjątkowo skuteczną technologią, pozwalającą na sprawdzenie wszystkich (elektrycznych i mechanicznych) komponentów turbiny wiatrowej i otaczającego ją systemu elektrycznego w celu wykrycia nieprawidłowości zanim dojdzie do awarii, jest termowizja. Zastosowanie kamery termowizyjnej zwiększa bezpieczeństwo pracy, pozwalając dostrzec problemy, nim rozwiną się one w sytuacje potencjalnie zagrażające życiu.

Problemy zdarzają się także w głównych punktach zasilających. Gdy jakieś połączenie elektryczne nie funkcjonuje prawidłowo, system przesyłowy może nie działać wydajnie i bezpiecznie. Należy regularnie sprawdzać wszystkie złącza, upewniając się, że są sprawne. Każdy system ma wiele małych styków i często są one umieszczone wysoko, poza zasięgiem pracujących osób. Złącza nagrzewają się, zanim ulegną awarii. Prowadzenie regularnego monitoringu termograficznego podstacji i linii przesyłowych za pomocą urządzeń termowizyjnych może dać pełny obraz potencjalnych problemów. Można mierzyć temperaturę z bezpiecznej odległości i diagnozować nieprawidłowości przed wystąpieniem przerw w dostawie prądu – minimalizując koszty napraw, maksymalizując żywotność sprzętu i utrzymując stałe zasilanie w obiektach.

Wykonując w przedsiębiorstwie analizę zagrożeń i szacując ryzyko, nie można zapominać o problemach z dostawą energii. To jedno z takich zdarzeń, które często ma wysokie prawdopodobieństwo wystąpienia i może przynieść negatywne skutki. Rozwiązania termowizyjne mogą na szczęście skutecznie zminimalizować takie zagrożenie.

Tomasz Migdał

Hikvision

Kluczowa jest elastyczność

Dziś w branży największa jest niepewność jutra. Pandemia pokazała, że nasze plany ulegają zmianie pod wpływem czynników, na które nie mamy wpływu. Poza konsekwencjami epidemicznymi związanymi z chorobą wywołaną wirusem SARS-CoV-2 i jego wariantami pojawiły się negatywne konsekwencje gospodarcze. Wiele firm musiało zmienić formę funkcjonowania, wiele zostało zamkniętych. Trzeba było nauczyć się błyskawicznego przystosowania się do nowych warunków i radzenia sobie z pojawiającymi się problemami. Jeśli nie będą potrafiły szybko się dostosować do wymogów, np. bezdotykowego mierzenia temperatury pracownikom czy kontroli utrzymania odpowiedniego dystansu między osobami, nie będą mogły działać.

Niezwykle przydatną umiejętnością jest tu elastyczność *(flexibility)*, która dla firmy jest kluczowa. Wielu zarządzającym przedsiębiorstwami pandemia uświadomiła, że umiejętność dopasowania się do zmian jest dziś warunkiem przetrwania firmy w bardzo konkurencyjnym środowisku. Problemem jest zwłaszcza załamanie się łańcucha dostaw i związane z tym konsekwencje wstrzymania produkcji nie tylko w branży security, ale i we wszystkich sektorach rynku.Trzeba liczyć się nawet z długoterminowymi brakami, ponieważ wyjście z kryzysu postpandemicznego nie nastąpi tak szybko. Zakłócenia w łańcuchu dostaw na całym świecie powoduje również wzrost cen zarówno komponentów, jak i gotowych wyrobów.

W tym aspekcie osobom zarządzającym przedsiębiorstwami przede wszystkim zaleca się dywersyfikację dostaw i długoterminowe ich planowanie. Jeśli tylko jest możliwość pozyskania lokalnych dostawców, warto ich poszukać. Ma się wtedy pewność, że gdyby któryś zawiódł, można liczyć na drugiego. Warto również w długoterminowym planowaniu uwzględnić dodatkowe zapasy, pozwalające zminimalizować skutki zakłóceń w łańcuchu dostaw.

Bogumił Szymanek

Axis Communications

AI w ochronie obiektów przemysłowych

Zastosowanie technologii sztucznej inteligencji w elektronicznych systemach zabezpieczeń znacznie ułatwia ochronę obwodową obiektów przemysłowych. Nowoczesne oprogramowanie pozwala skutecznie wykrywać i w czasie rzeczywistym weryfikować zdarzenia. Kamery z funkcją analizy opartej na technologii głębokiego uczenia są w stanie rozpoznać, np. czy na teren zakładu wbiegł intruz, czy może jednak tylko lis lub sarna z pobliskiego lasu. Pozwala to znacznie ograniczyć liczbę fałszywych alarmów i zoptymalizować pracę ochrony.

Zintegrowane rozwiązania umożliwiają kompleksową ochronę całego obiektu przed wtargnięciami intruzów w każdych warunkach oświetleniowych i pogodowych. Technologia wykorzystywana w nowoczesnych kamerach wizyjnych i termowizyjnych umożliwia m.in. śledzenie obiektów będących w ruchu i automatyczne przybliżanie obrazu. Dzięki oprogramowaniu analitycznemu opartemu na mechanizmach AI możliwe jest niemal bezbłędne rozpoznanie obserwowanego obiektu. Jeśli faktycznie jest to intruz, w systemie pojawia się alert ostrzegawczy, a pracownicy ochrony obiektu podejmują stosowną interwencję lub za pomocą urządzeń wyposażonych w systemy IP audio nadają komunikat głosowy mający na celu odstraszyć nieproszonego gościa.

Oprogramowanie analityczne umożliwia również skuteczną kontrolę dostępu na teren obiektu, np. poprzez weryfikację bazy numerów tablic rejestracyjnych pojazdów z uprawnieniami do wjazdu.

Istotnym trendem w projektowaniu systemów zabezpieczeń jest instalowanie zaawansowanego oprogramowania analitycznego bezpośrednio w urządzeniach brzegowych. Najnowocześniejsze kamery są w stanie nie tylko monitorować teren obiektu i przekazywać obraz, ale również w czasie rzeczywistym przetwarzać dane wizyjne i wyciągać wnioski. Oznacza to znaczną oszczędność przepustowości sieci oraz brak konieczności inwestowania w kosztowną infrastrukturę serwerową. Co więcej, znacznie przyspiesza to czas reakcji na ewentualne zdarzenia niepożądane, co może być

szczególnie istotne w przypadku ochrony obiektów o znaczeniu strategicznym, np. elektrowni.
Technologia sztucznej inteligencji pozwala znacznie rozbudować funkcjonalność poszczególnych urządzeń wchodzących w skład systemu zabezpieczeń elektronicznych oraz w istotny sposób zwiększyć jego skuteczność. Dzięki uczeniu maszynowemu algorytmy, na podstawie których kamery analizują obrazy lub sekwencje wideo, są nieustannie ulepszane. Informacje o zdarzeniach wysyłane do operatora mogą być zatem coraz bardziej precyzyjne.

Marcin Walczuk

BCS

Zabezpieczenie obiektów przemysłowych

Zabezpieczenie obiektów przemysłowych stanowi nie lada wyzwanie dla projektantów systemów zabezpieczeń. Muszą być one przede wszystkim skuteczne w swoim działaniu, zapewniać najwyższy poziom ochrony oraz spełniać wszystkie normy wymagane przepisami w tego typu obiektach. Niejednokrotnie utrudniem mogą być rozmiary takich zakładów, stwarzające problemy chociażby z przesyłaniem obrazu z kamer na większe odległości. Zdecydowanie się na zastosowanie w takiej sytuacji rozwiązań IP będzie jedynym słusznym pomysłem.
Wykorzystanie switchy z zasilaniem PoE uprości instalację, redukując ilość przewodów potrzebnych do jej wykonania. Jeśli dodatkowo switche będą obsługiwały łącze światłowodowe, zniknie problem przesyłu danych na odległość większą niż 100 m. Również zasilanie kamer z takiego switcha może się odbywać na większą odległość przy wykorzystaniu trybu long range PoE.
Spodziewamy się dalszego dynamicznego rozwoju systemów IP, który wynika z zastosowania najnowszych technologii pojawiających się na rynku. Inteligentna analiza wideo, sztuczna inteligencja wspierająca kamery termowizyjne, kamery do rozpoznawania numerów tablic rejestracyjnych czy identyfikacja twarzy to funkcje i rozwiązania, które zwiększą poziom zabezpieczenia obiektu. Ale aby było ono skuteczne, oprócz zastosowania urządzeń z najwyższej półki warto również zadbać o wyszkolenie pracowników ochrony. Tylko znając możliwości tych systemów, dotyczące np. analizy obrazu, mogą podnieść poziom skuteczności poprzez redukcję fałszywych alarmów. Ich liczba jest zdecydowanie mniejsza, niż ma to miejsce w klasycznych systemach CCTV. Ponadto obsługa tych zdarzeń jest szybsza ze względu na możliwość dokładnego określenia typu zdarzenia, czasu i miejsca jego wystąpienia oraz automatycznego uruchomienia z góry określonych procedur.
Przy zabezpieczeniu każdego typu zakładu przemysłowego (średniego, dużego, rozproszonego) wymagającego centralnej stacji monitoringu nieodzowne będzie niezawodne oprogramowanie CMS. Takie zadanie z powodzeniem może pełnić aplikacja BCS Manager, która zapewnia wsparcie dla wszystkich urządzeń BCS oraz urządzeń obsługujących protokół ONVIF. Do jej głównych funkcji należy podgląd na żywo oraz odtwarzanie zapisanych na rejestratorach nagrań, a także powiadamianie i zarządzenie zdarzeniami czy monitorowanie pracy operatora. To wszystko bez ograniczeń liczby kamer podłączonych do aplikacji, zależnie jedynie od specyfikacji jednostki, na której BCS Manager zostanie zainstalowany.

Krzysztof Kunecki

Schrack Seconet

Sterowanie urządzeniami ppoż. w obiektach przemysłowych

Zapewnienie optymalnej ochrony przeciwpożarowej w obiektach przemysłowych wymaga zastosowania urządzeń przeciwpożarowych charakteryzujących się ponadstandardowymi parametrami technicznymi i rozszerzonymi funkcjami systemowymi, aby spełnić specjalne indywidualne wymagania danego obiektu oraz obowiązujące przepisy formalne.
W zakresie sterowania automatyką pożarową wymagana jest możliwość wdrożenia indywidualnych procedur sterujących zgodnie ze scenariuszem pożarowym, z jednoczesnym uwzględnieniem współdziałania z urządzeniami technologicznymi/produkcyjnymi obiektu. W związku z tym kluczowe w tym aspekcie jest zastosowanie uniwersalnych urządzeń, które mogą łączyć wiele funkcji, w szczególności dotyczy to wykrywania pożaru i sterowania urządzeniami automatyki pożarowej. Zapewni to elastyczność przy budowie systemu i spójność całej instalacji, co przekłada się na łatwość zarządzania zintegrowanym systemem bezpieczeństwa pożarowego.
Zintegrowane centrale sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi powinny posiadać dodatkowe dokumenty certyfikacyjne potwierdzające spełnienie wszystkich wymagań dla funkcji związanych ze sterowaniem. Przykładowo, koncentrując się na najważniejszych sterowanych urządzeniach przeciwpożarowych obiektu przemysłowego, aby centrala mogła sterować np. urządzeniami przeciwpożarowymi w systemach kontroli rozprzestrzeniania dymu i ciepła (zgodnie z prEN 12101-9) czy stałymi urządzeniami gaśniczymi gazowymi, wodnymi, pianowymi i aerozolowymi, musi przejść specjalne badania atestacyjne i uzyskać certyfikat stałości właściwości użytkowych oraz świadectwo dopuszczenia CNBOP-PIB. Ponadto, aby spełnić wszystkie wymagania formalne, zasilacz centrali sterującej urządzeniami w systemie kontroli rozprzestrzeniania dymu i ciepła musi dodatkowo przejść badania laboratoryjne i uzyskać certyfikat stałości właściwości użytkowych na zgodność z normą EN 12101-10. Wchodząc na poziom wyższy, tzn. sterowania i zarządzania zintegrowanymi systemami bezpieczeństwa pożarowego, wymagane jest zastosowanie certyfikowanego Systemu Integrującego Urządzenia Przeciwpożarowe (SIUP).
Spełnienie opisanych wymagań jest niezbędne dla prawidłowej realizacji założeń projektowych, bezpiecznego wdrożenia systemu w obiekcie, co umożliwi formalny odbiór instalacji i późniejszą bezpieczną eksploatację.

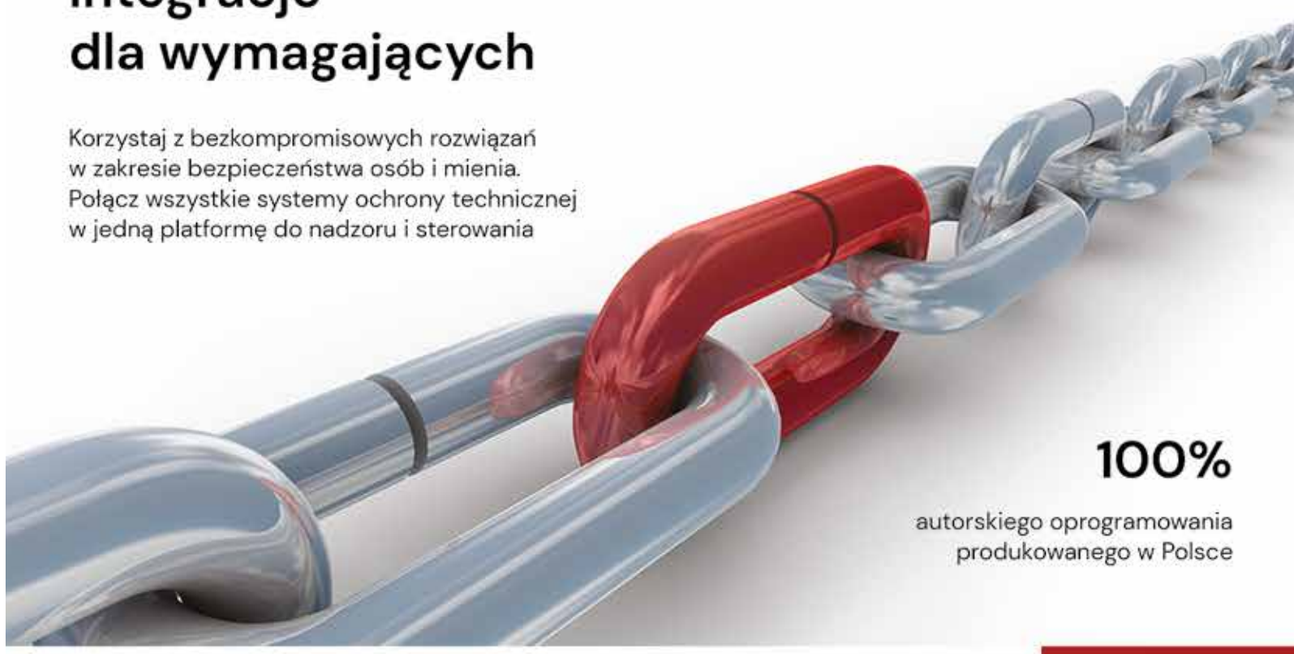
ARGUS

rodzina systemów integrujących klasy PSIM do zarządzania bezpieczeństwem obiektów

ARGUS WEB — bezpieczeństwo obiektów w przeglądarce internetowej
ARGUS RV — wysokowydajny system integrujący
ARGUS RV-C — sprzętowo-programowa platforma z certyfikacją CNBOP-PIB

Integracje dla wymagających

Korzystaj z bezkompromisowych rozwiązań w zakresie bezpieczeństwa osób i mienia. Połącz wszystkie systemy ochrony technicznej w jedną platformę do nadzoru i sterowania



100%
autorskiego oprogramowania produkowanego w Polsce

Telbud S.A.
ul. Krauthofera 23
60-203 Poznań

+48 61 866 88 48
www.telbud.pl
telbud@telbud.pl

1987
rok założenia

Jak zapewnić najwyższe

standardy bezpieczeństwa pożarowego

W obiektach, głównie tych funkcjonujących w ramach infrastruktury krytycznej, już na etapie projektowania należy określić możliwe zagrożenia i w odpowiedzi na nie dobrać odpowiednie systemy zabezpieczające, w tym urządzenia przeciwpożarowe. Większą efektywność działania, a więc i wyższy poziom bezpieczeństwa pożarowego obiektu zapewnia integracja wszystkich systemów ochrony przeciwpożarowej, niezależnie od producenta. Taką możliwość gwarantuje certyfikowany system integrujący urządzenia przeciwpożarowe (SIUP) CC Winguard. Należy mieć na uwadze, że system detekcyjny odpowiedzialny za ekspresowe wykrycie ognia stanowi autonomiczną część układu systemu bezpieczeństwa pożarowego obiektu.

CERTYFIKOWANY SIUP

W momencie zagrożenia pożarowego kierujący akcją ratowniczo-gaśniczą, dzięki integratorowi urządzeń przeciwpożarowych CC Winguard, może podjąć odpowiednie kroki według procedur bezpieczeństwa (scenariusza pożarowego) zdefiniowanych dla całego chronionego obiektu.
Wizualizacja i możliwość sterowania systemami przeciwpożarowymi z wykorzystaniem integratora CC Winguard poprawia bezpieczeństwo obiektu oraz pozwala na pracę nawet przy utracie zasilania podstawowego. Potwierdzanie bądź kasowanie alarmów pożarowych, sterowanie klapami pożarowymi, modyfikacje scenariusza pożarowego zgodnie z wytycznymi kierującego akcją ewakuacyjną to tylko niektóre z działań możliwych do przeprowadzenia w sposób szybki i sprawny z poziomu stacji operatorskiej.
Pełen zakres funkcjonalności integracji urządzeń przeciwpożarowych mogą zapewnić jedynie systemy certyfikowane, mające świadectwo dopuszczenia CNBOP-PIB.

PEŁNA GAMA MOŻLIWOŚCI

System integrujący urządzenia przeciwpożarowe (SIUP) jest kopalnią możliwości i korzyści na wszystkich etapach inwestycji i użytkowania obiektu – zarówno podczas projektowania, jak i w trakcie eksploatacji systemów przeciwpożarowych. Projektant ma w końcu możliwość zrealizowania koncepcji działania systemów ppoż., które do tej pory mogły być wyłącznie pomysłem. Wszystkie prace związane z wdrożeniem i późniejszą konserwacją systemu mogą zostać wykonane samodzielnie przez instalatora. W efekcie operator zyska komfort pracy dzięki intuicyjności rozwiązania. Inwestor z kolei będzie cieszył się najwyższym poziomem bezpieczeństwa, osiągając jednocześnie kompromis z wymarzoną architekturą wnętrza swojego obiektu.

PODSUMOWANIE

CC Winguard to nowa, aczkolwiek bazująca na sprawdzonym na rynkach światowych rozwiązaniu niemieckiej marki Advancis – WinGuard PSIM+, propozycja w zakresie integracji i wizualizacji systemów przeciwpożarowych, wspierająca podejście procesowe do zarządzania bezpieczeństwem. W ramach uruchomionego programu partnerskiego C&C Partners zapewnia program szkoleń produktowych, pełną lokalizację produktu oraz wsparcie sprzedażowe, uruchomieniowe i serwisowe.

C&C PARTNERS
ul. 17. Stycznia 119, 121
64-100 Leszno
www.ccpartners.pl
l.schmidt@ccpartners.pl

Tradycja
I NOWOCZESNOŚĆ

- NAJWIĘKSZY POLSKI PRODUCENT KOMPLEKSOWYCH SYSTEMÓW SYGNALIZACJI POŻAROWEJ I APARATURY RADIOMETRYCZNEJ
- PONAD 60 LAT DOŚWIADCZENIA
- SZEROKA GAMA INNOWACYJNYCH ROZWIĄZAŃ W ZAKRESIE OCHRONY PRZECIWPOŻAROWEJ
- NOWOCZESNE URZĄDZENIA OPRACOWYWANE PRZEZ ZESPÓŁ WYKWALIFIKOWANYCH I KOMPETENTNYCH INŻYNIERÓW
- SPECJALISTYCZNE SZKOLENIA I WSPARCIE TECHNICZNE DLA PROJEKTANTÓW ORAZ INSTALATORÓW W KRAJU I ZA GRANICĄ

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

Bezpieczeństwo nade wszystko

– liniowe detektory dymu HOCHIKI i ich zastosowanie

Technologia zabezpieczenia pożarowego może przyjmować różne formy. Decyzja dotycząca wyboru zarówno technologii, jak i produktów, które najlepiej nadają się do określonych zastosowań, może być zatem niełatwa. W artykule postaramy się pomóc w podjęciu tej decyzji. Przedstawimy czym są, jak działają oraz kiedy i gdzie należy zastosować liniowe detektory dymu FIREbeamXtra firmy HOCHIKI.

JAK DZIAŁA LINIOWY DETEKTOR DYMU FIREBEAMXTRA?

Liniowy detektor dymu FIREbeamXtra wykorzystuje wiązkę podczerwieni do wykrywania obecności dymu. Głowica detektora (nadajnik i odbiornik) jest zainstalowana na jednej ścianie, na końcu obszaru detekcji, a reflektor na przeciwległej. Nadajnik wysyła wiązkę podczerwieni, która odbita od reflektora wraca do odbiornika. Jeżeli w chronionej przestrzeni obecny jest dym przesłaniający emitowaną przez nadajnik wiązkę, w odbiorniku spada poziom odbieranego sygnału, co generuje zdarzenie alarmowe.

GDZIE I KIEDY ZWYKLE STOSUJE SIĘ LINIOWE DETEKTORY DYMU?

Liniowe detektory dymu FIREbeamXtra są przeznaczone wyłącznie do zastosowania wewnątrz. Są idealnym rozwiązaniem do ochrony ppoż. w dużych i wysokich budynkach o otwartej przestrzeni, tj. magazyny, centra handlowe, biblioteki, hale sportowe, baseny. Do zabezpieczenia tak dużej powierzchni wykorzystanie standardowych punktowych detektorów dymu wydaje się mało ekonomiczne. Dużo bardziej wydajnym rozwiązaniem jest zastosowanie omawianego, liniowego detektora dymu FIREbeamXtra, którego całkowity obszar detekcji wynosi aż 1050 m^2. Co więcej, po dodaniu zestawów powiększających reflektory obszar detekcji można zwiększyć do 2400 m^2, co odpowiada wielkości 9 kortów tenisowych!
Udogodnieniem jeśli chodzi o zastosowanie FIREbeamXtra w tego typu obiektach, szczególnie w kontekście ich wysokich sufitów, jest sposób montażu urządzenia. Czujka liniowa HOCHIKI wymaga mniejszej ilości okablowania niż tradycyjne czujki punktowe. Ponadto na potrzeby zabezpieczenia tak dużej powierzchni wystarczy jeden nadajnik/odbiornik i jeden reflektor. To z kolei upraszcza pracę instalatorowi, bo nie stwarza konieczności montowania wielu czujek na wysokości. Co więcej, detektor FIREbeamXtra jest wyposażony w dodatkowy kontroler instalowany na wysokości dostępnej dla stojącego człowieka. Ułatwia on zarządzanie urządzeniem – wyświetla wszystkie informacje dotyczące jego funkcjonowania. Dzięki temu zarządcy budynków i konserwatorzy mogą uruchamiać, monitorować i obsługiwać detektor bez konieczności wspinania się na wysokość miejsca jego instalacji. W przestrzeniach narażonych na niepożądaną ingerencję, np. hale sportowe, szkoły czy baseny, można alternatywnie zamontować kontroler wyżej, w miejscu niedostępnym dla osób niepowołanych.

KOMPATYBILNY, CZUŁY A JEDNOCZEŚNIE ODPORNY NA FAŁSZYWE ALARMY...

FIREbeamXtra firmy HOCHIKI jest w pełni kompatybilny ze znanym na całym świecie analogowym adresowalnym protokołem HOCHIKI ESP. Detektor jest adresowalny i zasilany bezpośrednio z pętli ESP. Ulepszona optyka i nowe oprogramowanie wewnętrzne sprawiają, że urządzenie jest wyjątkowo czułe, a przy tym odporne na fałszywe alarmy.
Podsumowując, w przypadku dużych otwartych przestrzeni wewnętrznych detektor FIREbeamXtra firmy HOCHIKI jest idealnym rozwiązaniem zapewniającym bezpieczeństwo życia i mienia. Ze względu na szybką, łatwą instalację i duży obszar detekcji jest bardziej ekonomicznym i bezpiecznym rozwiązaniem niż tradycyjne detektory punktowe, a dzięki dodatkowemu kontrolerowi łatwym w obsłudze i konserwacji.

MIWI-URMET
ul. Pojezierska 90A
91-341 Łódź
tel. 42 616 21 00
miwi@miwiurmet.pl
www.miwiurmet.pl

Zasil wiedzę o zasilaczach ppoż.

Projektanci, instalatorzy i konserwatorzy muszą mieć aktualną wiedzę o stanie prawnym i normalizacyjnej ocenie zgodności wyrobów budowlanych służących do ochrony przeciwpożarowej. Ma to istotne znaczenie zarówno dla nich, jak i organów nadzoru budowlanego, PSP oraz inwestorów czy deweloperów. Zdobyta wiedza umożliwi wybór wyrobu, który spełnia aktualne wymagania, jest bezpieczny i w pełni funkcjonalny.

a&s Polska

Dotyczy to również zasilaczy do urządzeń przeciwpożarowych. Głównym celem stosowania zasilaczy jest zapewnienie ciągłości dostawy energii do urządzeń wchodzących w skład instalacji sygnalizacji pożarowej SSP, instalacji dźwiękowych systemów ostrzegawczych DSO lub systemów kontroli rozprzestrzeniania dymu i ciepła SKRDiC.

Przez zasilacz należy rozumieć[1]:

Zasilacz stosowany w systemach sygnalizacji pożarowej – urządzenie stanowiące część składową systemu sygnalizacji pożarowej, które zasila energią centralę i inne części SSP. Może dostarczać energię z głównego źródła zasilania (sieci elektroenergetycznej) lub, po jej zaniku, z rezerwowego źródła zasilania (z baterii akumulatorów). Zasilacz może zawierać wielorakie źródła energii (np. sieć elektroenergetyczną i źródła rezerwowe).

Zasilacz stosowany w dźwiękowych systemach ostrzegawczych – urządzenie stanowiące część składową dźwiękowego systemu ostrzegawczego, które zasila energią centralę i inne części składowe DSO. Może dostarczać energię z głównego napięcia zasilania (sieci elektroenergetycznej) lub po jej zaniku z rezerwowego źródła zasilania (najczęściej z baterii akumulatorów). Zasilacz może zawierać wielorakie źródła energii (np. sieć elektroenergetyczną i źródła rezerwowe).

Wymagania i metody badań oraz kryteria oceny zasilaczy stosowanych w systemach sygnalizacji pożarowej określa norma PN-EN 54-4[2]. Zasilacz może dostarczać energię do central sygnalizacji pożarowej, central dźwiękowych systemów ostrzegawczych, sygnalizatorów akustycznych, sygnalizatorów optycznych itp.

Zasilacz stosowany w systemach kontroli rozprzestrzeniania dymu i ciepła – urządzenie stanowiące część składową systemu kontroli rozprzestrzeniania dymu i ciepła, które zasila energią centralę sterującą i inne części składowe systemu KRDiC. Może dostarczać energię z podstawowego źródła zasilania (sieci elektroenergetycznej) lub po jej zaniku z rezerwowego źródła zasilania (najczęściej z baterii akumulatorów). Zasilacz może zawierać wielorakie źródła energii (np. sieć elektroenergetyczną i źródła rezerwowe), może dostarczać energię potrzebną do codziennej wentylacji pomieszczeń i zasilania innych urządzeń przeciwpożarowych pracujących w warunkach pożaru.

Wymagania i metody badań oraz kryteria oceny zasilaczy stosowanych w systemach oddymiania określa norma PN-EN 12101-10[3].

Zasilacz stosowany w systemach sterowania oddzieleniami przeciwpożarowymi – urządzenie stanowiące część składową systemu sterowania oddzieleniami przeciwpożarowymi, która zasila energią centralę i inne części składowe systemu sterowania oddzieleniami przeciwpożarowymi. Zasilacz może dostarczać energię z podstawowego źródła zasilania (sieci elektroenergetycznej) lub po jej zaniku z rezerwowego źródła zasilania (najczęściej z baterii akumulatorów).

Ze względu na miejsce montażu wyróżniamy:

Zasilacze niezintegrowane umieszczane we wspólnej obudowie zasilanego urządzenia (np. z centralą dźwiękowego systemu ostrzegawczego) lub w oddzielnej obudowie (np. do zasilania czujek pożarowych, sygnalizatorów optycznych i akustycznych). Producent może określić zakres/y napięcia wyjściowego zasilacza.

Norma PN-EN 54-4 zaleca, aby obwody wyjściowe niezintegrowanych zasilaczy (w oddzielnej obudowie) miały dwa odrębne wyjścia zabezpieczone dwoma oddzielnymi bezpiecznikami. W sytuacji, gdy zasilacze nie mają tej funkcji, obowiązują liczne wyłączenia i ograniczenia w ich stosowaniu, m.in. nie mogą być stosowane do zasilania central sygnalizacji pożarowej, central dźwiękowych systemów ostrzegawczych, UTA, CSG.

Zasilacze zintegrowane umieszczane we wspólnej obudowie z innym urządzeniem (np. centralą sygnalizacji pożarowej, centralą dźwiękowego systemu ostrzegawczego). W przypadku zaniku napięcia głównego źródła zasilania, zasilacz powinien automatycznie przełączyć się na rezerwowe źródło zasilania. Po przywróceniu głównego źródła zasilania urządzenie powinno automatycznie przełączyć się na główne źródło zasilania. Uszkodzenie jednego ze źródeł zasilania nie powinno powodować uszkodzenia innego źródła zasilania lub uszkodzenia zasilania instalacji.

Zasilacz powinien rozpoznawać i sygnalizować następujące uszkodzenia[4]:

- zanik napięcia głównego źródła zasilania w ciągu 30 minut od wystąpienia zaniku,
- zanik napięcia rezerwowego źródła zasilania w ciągu 15 minut od wystąpienia zaniku,
- wysoką rezystancję wewnętrzną baterii i przyłączonych do niej elementów obwodów, np. połączeń, bezpieczników, w ciągu 4 h od zdarzenia,
- uszkodzenie urządzenia do ładowania baterii w ciągu 30 min od wystąpienia uszkodzenia.

1 *Ochrona Przeciwpożarowa, Zasilacze do urządzeń przeciwpożarowych*, Standard CNBOP-PIB-0007:2016 wyd. 3. 2016

2 PN-EN 54-4:2001 + A1:2004 + A2:2007 *Systemy sygnalizacji pożarowej. Część 4: Zasilacze*

3 PN-EN 12101-10:2007 + AC:2007 *Systemy kontroli rozprzestrzeniania dymu i ciepła. Część 10: Zasilacze*

4 *Ochrona Przeciwpożarowa, Badania laboratoryjne zasilaczy do zasilania elementów systemów sygnalizacji pożarowej według PN-EN 54-4*, CNBOP-PIB 2015

REKLAMA

MERAWEX

Certyfikowane zasilacze i urządzenia ochrony przeciwpożarowej

Zasilacze 24Vdc systemów SSP i SKRDiC
ZSP135-DR, ZSP100

Zasilacze urządzeń przeciwpożarowych 230Vac i 24Vdc
ZUP-230V, ZUP-230V-BM

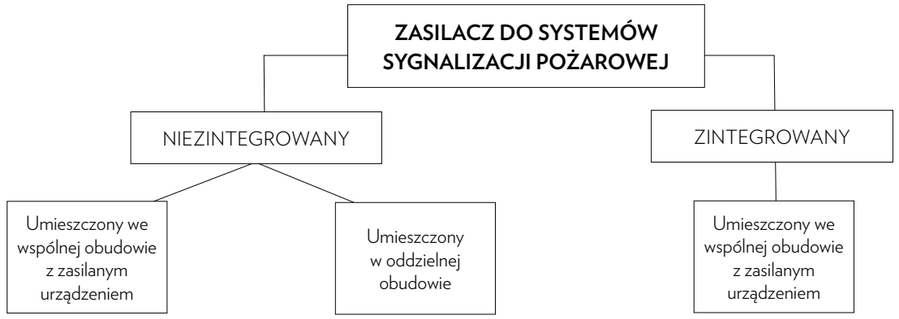
Centrale sterowania urządzeniami przeciwpożarowymi
CS-ZSP135

Akumulatory MXB z certyfikatem VdS od 7,2Ah do 65Ah **seria MXV**

Zasilacze dźwiękowych systemów ostrzegawczych 24Vdc i 48Vdc
ZDSO400

Poznaj naszą pełną ofertę na:
www.merawex.com.pl

MERAWEX Sp. z o.o. • 44-122 Gliwice • ul. Toruńska 8



Rys. 1. Podział zasilaczy do systemów sygnalizacji pożarowej (źródło: opracowanie CNBOP na podstawie PN-EN 54-4)

Szczególne wymagania techniczno-użytkowe dotyczą zasilania urządzeń przeciwpożarowych w dwóch stanach ich pracy – do momentu wykrycia pożaru (stan nienormalnej pracy urządzenia) i pracę w warunkach pożaru (stan normalnej pracy). W zależności od tego dobiera się rozwiązania techniczne zapewniające ciągłość funkcjonowania tych urządzeń: źródło (zasilacz) i sposób ich zasilania oraz odpowiednie kable.

WYBÓR ZASILACZA

Czym zatem kierować się przy projektowaniu odpowiedniego zasilacza urządzeń przeciwpożarowych? Przede wszystkim należy dążyć do spełnienia wymagań stawianych w normach. Trzeba też sprawdzić niezbędną dokumentację – m.in. certyfikaty potwierdzające zgodność z wymaganiami odpowiednich norm, które powinien posiadać producent, gdyż bez nich nie będzie możliwy odbiór systemu.
– *W Polsce wymagane są m.in. Krajowy Certyfikat Stałości Właściwości Użytkowych, Świadectwo Dopuszczenia i Deklaracja Stałości Właściwości Użytkowych (DoP). Pierwsze dwa dokumenty wydawane są m.in. przez CNBOP-PIB – instytut, który bada i dopuszcza do stosowania zasilacz. Z kolei trzeci dokument DoP wystawia producent. Jest on potwierdzeniem właściwości wyrobu budowlanego. Zawiera informacje dotyczące jego właściwości, parametrów, a także dokumentów, na podstawie których został przebadany. Podaje także nazwę jednostki badawczej, w której zostały przeprowadzone badania* – wyjaśnia Marek Dzioch z firmy Pulsar.
Wybierając konkretny model, należy zwracać uwagę na następujące parametry zasilacza:

1. Wartości prądu(ów) wyjściowego(ych).
2. Liczbę niezbędnych wyjść, z których każde musi być zabezpieczone odrębnym bezpiecznikiem znajdującym się w zasilaczu.
3. Maksymalną i minimalną pojemność baterii akumulatorów. Pojemność maksymalna odpowiednia do danego zastosowania musi być obliczana z uwzględnieniem współczynnika bezpieczeństwa 1,25 (musi być zwiększona o 25%).
4. Wyposażenie zasilacza w sondę temperaturową, dzięki której można wydłużyć czas eksploatacji akumulatorów.
5. Stopień ochrony obudowy i wynikającą stąd klasę środowiskową.

– *Trzeba mieć świadomość, że zasilacze do stosowania w ochronie przeciwpożarowej nie są urządzeniami uniwersalnymi, mogącymi współpracować z każdym systemem ppoż. na rynku* – zwraca uwagę Dariusz Cygankiewicz z firmy Merawex. – *Istnieje wiele urządzeń przeciwpożarowych, dla których zasilacze muszą też spełniać dodatkowe wymagania, np. odporność na bardzo duże prądy w momencie podłączenia urządzeń do zasilania. Dlatego zawsze przed wyborem zasilacza trzeba to sprawdzić.*

WSKAZÓWKI DLA PROJEKTANTA SYSTEMU, INWESTORA, UŻYTKOWNIKA

Projektant powinien mieć dostęp do wszelkich informacji na temat produktu. – *Projektując system pożarowy, często wykorzystuje się urządzenia różnych producentów, które muszą być kompatybilne, stanowić jednolitą całość. Do tego niezbędna będzie wiedza na temat parametrów elektrycznych, funkcji zasilacza oraz kompatybilnych urządzeń, które mogą z nim współpracować* – dodaje M. Dzioch.
Powinien mieć też wiedzę nt. możliwych zastosowań zasilaczy i kryteriów uwzględniania ich parametrów do konkretnych zastosowań i do sprecyzowanego scenariusza pożarowego. – *Przy doborze zasilacza i pojemności jego baterii akumulatorów projektant musi uwzględnić czas pracy w trybach dozoru i alarmu pożarowego oraz prądy potrzebne w tych trybach. W obliczeniach musi także uwzględnić pobór prądu na potrzeby własne. Powinien też upewnić się, czy przerwa w zasilaniu nie jest przeszkodą do jego poprawnej pracy przy zanikach sieci i nie doprowadzi do zresetowania się zasilanego urządzenia* – zaznacza D. Cygankiewicz.

Wszystkie te informacje projektant powinien znaleźć w materiałach udostępnionych przez producenta, pomocne będą biblioteki CAD, różnego rodzaju konfiguratory itp. narzędzia ułatwiające i skracające czas przygotowania projektu.
Inwestor przy wyborze rozwiązania powinien kierować się nie tylko ceną zakupu, ale także kosztami instalacji, eksploatacji i napraw pogwarancyjnych. Często naprawy pogwarancyjne stanowią znaczną wartość i podnoszą koszty całości systemu. Dlatego ważne jest, jaki okres gwarancji zapewnia producent.
Na inne funkcje zwraca uwagę użytkownik. – *Dla niego ważna będzie przede wszystkim łatwość instalacji, bezawaryjność zasilacza i ewentualna szybka pomoc producenta* – wylicza M. Dzioch. Jednak i on powinien mieć choć podstawową wiedzę na temat tych urządzeń. – *Na podstawie ogólnych przepisów z dziedziny ochrony ppoż. dotyczących zasilaczy i akumulatorów użytkownik powinien znać terminy i kryteria obowiązkowych corocznych przeglądów technicznych. Powinien monitorować wszystkie sygnały o uszkodzeniach tych urządzeń i podejmować decyzje o interwencjach, wyjaśniać przyczyny ich występowania oraz zlecać ewentualne naprawy upoważnionym serwisantom* – radzi D. Cygankiewicz.
Wojciech Rytlewski z firmy Mercor wylicza najczęstsze problemy użytkowników z doborem urządzeń SKRDiC. – *Z napływających do nas zapytań wynika, że to, z czym najczęściej mają problem, to prawidłowy, zgodny z prawem dobór sposobu zasilania urządzeń. Norma zharmonizowana PN-EN 12101-10 określa szczegółowo, w jaki sposób należy badać zasilacze. Tylko te o potwierdzonych właściwościach użytkowych, przeznaczone do zastosowania w systemach kontroli rozprzestrzeniania dymu i ciepła będą gwarantowały poprawną pracę przyłączonych do nich urządzeń w warunkach panujących w czasie pożaru, podczas którego może dochodzić m.in. do zapadów lub zaników zasilania lub do obniżenia jakości podawanego prądu.*
Z kolei na inne problemy zwraca uwagę Michał Zalewski, inżynier uruchomieniowy. – *Przy wyrafinowanych rozwiązaniach budynkowych coraz częściej spotykam się z uzupełnieniem zasilania urządzeń o Indywidualne Oceny (Dopuszczenia Jednostkowe). W takich przypadkach należy zachować ogromną ostrożność i zwrócić szczególną uwagę na testowanie tych układów po instalacji, gdyż procedura tej oceny nie zawiera (co oczywiste) testów laboratoryjnych. Zdarzało się, że błędy projektowe zakłócające pracę układu wykryliśmy dopiero po przeprowadzeniu kilkukrotnych real testów.*

R E K L A M A

KOMPLEKSOWE SYSTEMY ZĄBEZPIECZEŃ PRZECIWPOŻAROWYCH

» Systemy oddymiania » Systemy napędów » Systemy sygnalizacji pożarowej
» Systemy naturalnej wentylacji » Systemy zamknięć ogniowych

www.dhpolska.pl

D+H BUILDING ATMOSPHERE

Umowy konserwacyjne systemów zabezpieczeń a RODO

Piotr Świderski

Słowo „pandemia” odmieniane jest dzisiaj przez wszystkie przypadki. Widzimy, jak znaczący wpływ wywarła na naszą branżę, m.in. umożliwiła pracę hybrydową. Obecnie chyba już nikt nie wyobraża sobie świadczenia pracy tylko w biurze. Należy jednak pamiętać, że w naszych firmach pozostały m.in. elektroniczne systemy zabezpieczeń, które tym bardziej muszą działać niezawodnie, ponieważ osoby nadzorujące te obszary nie muszą być fizycznie obecne w danym pomieszczeniu. Jednym z kluczowych elementów utrzymania systemów zabezpieczeń w sprawności jest ich regularne sprawdzanie przez wykwalifikowanych pracowników technicznych. A jeśli mamy do czynienia z serwisem świadczonym cyklicznie, należy sporządzić umowę.

Większość z nas zdążyła się już przyzwyczaić, że RODO zakrada się prawie do każdego obszaru bezpieczeństwa. Nie inaczej jest z umowami na konserwacje systemów zabezpieczeń. W artykule przedstawię elementy związane z wymaganiami RODO w umowach serwisowych. Każda umowa powinna być sprawdzona przez dział, który w danej firmie zajmuje się obszarem danych osobowych.
Omówię przypadek, kiedy to my jesteśmy właścicielami odseparowanych elektronicznych systemów zabezpieczeń, co oznacza, że urządzenia należą do nas i są zainstalowane na naszej powierzchni. W takiej sytuacji najczęściej w bazie systemu kontroli dostępu (SKD) wprowadzamy użytkownika, definiując go odpowiednio imieniem i nazwiskiem oraz często dodatkowymi parametrami (stanowisko, dział, numer ID itd.). Tworzymy więc bazę z danymi osobowymi.
W systemach dozoru wizyjnego CCTV z kolei rejestrujemy obraz. Często głównym celem rejestracji jest wykorzystanie zapisanego materiału wizyjnego do identyfikacji osób, czyli niestety znowu dochodzą dane osobowe. Dlatego powierzając konserwację systemów bezpieczeństwa firmie zewnętrznej, musimy nadać jej dostęp do danych osobowych.
W związku z tym umowę o konserwację systemów bezpieczeństwa powinniśmy uzupełnić o umowę powierzenia lub inny instrument prawny, który zawierałby niezbędne elementy kształtujące stosunek powierzenia przetwarzania danych osobowych. Jest to wymóg wynikający z Ogólnego rozporządzenia o ochronie danych osobowych (art. 28 ust. 3 RODO). Aktualizuje się wówczas, gdy administrator danych (w tym przypadku my, jako właściciele zainstalowanych systemów) korzysta z usług podmiotu przetwarzającego, tj. podmiotu, który przetwarza dane osobowe w imieniu administratora (czyli firma świadcząca usługę konserwacji systemu).

W przypadku korzystania z usług serwisowania systemów monitoringu CCTV i kontroli dostępu dochodzi do przetwarzania danych osobowych przez firmę serwisową. Przetwarzanie bowiem, zgodnie z definicją Ogólnego rozporządzenia o ochronie danych (art. 4 pkt. 2 RODO), jest bardzo szeroko zdefiniowane i oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawie danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, tj. zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
W związku z tym, korzystając z usług firmy, której zlecamy wykonanie czynności serwisowych systemu monitoringu wizyjnego CCTV czy KD, dajemy pracownikowi podmiotu trzeciego dostęp (tymczasowy) do danych osobowych, umożliwiając w ten sposób ich przetwarzanie. To determinuje stosunek powierzenia przetwarzania danych osobowych, który nie jest stosunkiem kreowanym umownie, lecz wynika z okoliczności faktycznych stanowiących proces przetwarzania danych osobowych.
Powinniśmy sprawdzić, czy firma serwisująca, która będzie świadczyła wymienione usługi, zagwarantuje w umowie należyte wdrożenie technicznych i organizacyjnych środków mających zapewnić bezpieczeństwo powierzenia danych osobowych. W przeciwnym razie spowoduje to naruszenie Ogólnego rozporządzenia o ochronie danych (art. 28 ust. 1 RODO) poprzez powierzenie danych podmiotowi, który wdrożenia takich mechanizmów nie gwarantuje. Obowiązkiem administratora danych jest weryfikacja podmiotu, któremu dane powierza, i zapewnienie przez ten podmiot adekwatnych środków ich ochrony.
Należy też sprawdzić, czy dostawca posiada odpowiednie procedury opisujące, co należy wykonać podczas wystąpienia incydentu bezpieczeństwa (naruszenia ochrony danych osobowych), i czy administrator ma gwarancję, że zostanie o tym fakcie poinformowany w czasie wymaganym przepisami RODO. W przeciwnym razie może nastąpić naruszenie Ogólnego rozporządzenia o ochronie danych (art. 33 ust. 1 i 2 RODO) poprzez brak możliwości zgłoszenia naruszenia do organu nadzorczego w przewidzianym przepisami czasie (72 godziny od momentu stwierdzenia naruszenia) – brak notyfikacji w określonym czasie naraża naszą firmę bezpośrednio na karę.

W najbliższym czasie zapewne nie ucieknie my od tematyki RODO, dlatego warto się z nią zapoznać bliżej. Podczas projektowania systemu zabezpieczeń trzeba od razu planować, jakie dane będą w nim przechowywane i kto będzie miał do nich dostęp, a także tworzyć odpowiednie procedury, które określą m.in. postępowanie w przypadku wycieku danych osobowych lub ich utraty.
Tych samych standardów powinno się też wymagać od firm, które wykonują konserwacje systemów, w przeciwnym razie można narazić się na nieprzyjemności i duże kary. Mam nadzieję, że ta wiedza pozwoli przybliżyć tematykę RODO.

PIOTR ŚWIDERSKI

Absolwent PW Wydział Mechatroniki (mgr inż.). Ponad 10 lat doświadczenia w sektorze bezpieczeństwa. Obecnie Territory Security Leader w PwC.

Hardening systemów zabezpieczeń

na przykładzie systemu dozoru wizyjnego

W kolejnej części artykułów z cyklu cyberbezpieczeństwa w kontekście obszaru bezpieczeństwa fizycznego przyjrzymy się kwestii hardeningu. Podkreślę, jak bardzo to zagadnienie jest istotne w odniesieniu do projektowania, eksploatacji czy modernizacji elektronicznych systemów zabezpieczeń technicznych.

Tomasz Dacka

CZYM JEST HARDENING?

W tłumaczeniu na jęz. polski termin ten oznaczający „utwardzanie" pochodzi ze środowiska IT, gdzie jest stosowany od dawna. Obejmuje on dostosowanie środowiska do wymogów bezpieczeństwa, aby zapewnić ciągłość działania. Zazwyczaj jest to proces mający na celu zapewnienie zgodności z wdrożoną polityką bezpieczeństwa oraz ograniczenie zidentyfikowanych zagrożeń do poziomu akceptowalnego. Sprowadza się do odpowiedniej konfiguracji aplikacji, urządzeń i architektury IT w taki sposób, aby maksymalnie utrudnić dostęp do nich osobom niepowołanym, a jednocześnie zagwarantować odpowiedni dostęp do aktywów osobom do tego uprawnionym. Systemy zabezpieczeń technicznych spełniają tu takie same funkcje, jak inne aplikacje i z perspektywy bezpieczeństwa IT niczym się nie różnią. W naszym przypadku, rozważając „utwardzanie", powinniśmy brać pod uwagę przede wszystkim:

- system operacyjny wykorzystywany przez nasze urządzenia, aplikacje (kamery również go posiadają),
- stacje klienckie,
- serwery (fizyczne i wirtualne),
- systemy zapisu, np. macierze, karty SD,
- oprogramowanie zarządzające, np. VMS,
- aktywne elementy systemów, np. kamery, kontrolery, enkodery,
- sposób przekazywania informacji, w tym szyfrowanie danych w ruchu i w spoczynku,
- wykorzystywane urządzenia mobilne, gdy zachodzi taka potrzeba,
- urządzenia aktywne stosowane do wymiany informacji, np. punkty dostępu, przełączniki, routery czy zapory ogniowe,
- wdrożone standardy, np. zasada czystego biurka, least privilege, least functionality, aktualizowanie i „łatanie" systemów.

Skupimy się na obszarze wywodzącym się z bezpieczeństwa fizycznego. Przenalizujemy najważniejsze komponenty systemu CCTV/VSS. Przed przystąpieniem do procesu *hardeningu* danego systemu powinniśmy mieć rozeznanie na temat jego architektury, by włożony trud nie poszedł na marne.

PLUG AND PRAY

To parafraza założenia *plug and play*, terminu dobrze znanego i lubianego. Zapewne część czytelników pamięta czasy, kiedy po zainstalowaniu systemu operacyjnego Windows do pełni szczęścia brakowało dograna sterowników do odpowiednich elementów komputera (karty dźwiękowej czy graficznej) oraz urządzeń peryferyjnych, w odpowiedniej kolejności rzecz jasna. Pod koniec menedżer urządzeń informował, czy wgrane sterowniki są odpowiednie. Potem przyszła era *plug and play*, system operacyjny był domyślnie „gotowy" – wystarczyło dane urządzenie podłączyć i cieszyć się jego obsługą. Oddech i ulga, szczególnie dla mniej wtajemniczonych w komputerowe prawidła użytkowników: podłączam i od razu korzystam. Zakładam, że natura ludzka tak samo oddziałuje podczas uruchamiania systemów zabezpieczeń, np. systemów CCTV/VSS. Chcemy po zasileniu kamer szybko odnaleźć je w sieci, dobrać odpowiednie pola obserwacji, odpowiednio skonfigurować harmonogramy pracy, archiwum i sposoby wizualizacji dla operatora. System działa, jest gotowy, ale czy na pewno?

Obecnie dostarczane produkty maksymalnie ułatwiają ich adaptację i nie jest to oczywiście wada sama w sobie, mamy przecież do czynienia z coraz bardziej zaawansowanymi rozwiązaniami. Zatem jest to niejako system *plug and play.* Pytanie tylko, czy funkcjonalności, które tak bardzo ułatwiają pracę na etapie wdrożenia, nie będą znaczącą podatnością na etapie eksploatacji systemu. Czy podejście *plug and play* nie zamienia się nagle na *plug and pray?* Obszar ten został już dawno zdiagnozowany przez czołowych dostawców produktów na rynku security, dostrzeżono konieczność pójścia o krok dalej i „utwardzania" swoich systemów, aby już na etapie eksploatacji wyeliminować te podatności, które są znane i możliwe jest ich wykorzystanie przez intruzów (tworzenie exploitów). Powstały poradniki, tzw. *hardening guide.* To nic innego jak dobre praktyki, porady mówiące o tym, jak zminimalizować ryzyko powstałe w wyniku wdrożenia systemu bezpieczeństwa, wynikające z jego charakterystyki (np. kamery wykorzystujące do komunikacji protokół IP). Czy tego chcemy, czy nie, adresując jedno ryzyko (wdrażając system CCTV/VSS), możemy wygenerować inne (zostawiając otwarte cyfrowe furtki do tegoż systemu). Przyjrzymy się zatem, na przykładzie najważniejszych elementów systemu dozoru wizyjnego, na czym *hardening* polega w praktyce.

KAMERY

Rewolucja cyfrowa przyniosła również wymierne efekty w branży security. Oferty dostawców obfitują w kamery megapikselowe o dobrej czułości, a kamery stały się de facto małymi komputerami z licznymi dodatkowymi funkcjonalnościami (np. VCA). To zaleta, lecz nie ma róży bez kolców. Odpowiednia konfiguracja kamery stała się skomplikowana pod kątem zarówno odpowiedniego ustawienia sygnału wizyjnego, jak i zabezpieczenia kamery w obszarze IT. Złota zasada *hardeningu* mówi: **wyłącz wszystko, czego nie używasz i czego nie potrzebujesz.** Jeśli nie korzystasz z danego portu, danej usługi, a zostawisz tę furtkę otwartą, intruz chętnie z tego skorzysta, o ile będzie dysponował odpowiednimi środkami. Wszak nie ma w 100% bezpiecznych systemów, to jedynie kwestia czasu, aby ktoś odkrył podatność i ją wykorzystał. *Hardening* jest właśnie po to, by ten czas wydłużyć do tego stopnia, by stało się to nieopłacalne lub pozwoliło wykryć próbę włamania.

NA CO ZWRÓCIĆ UWAGĘ W PRZYPADKU KAMER:

Ekspozycja na zewnątrz – nie zaleca się, aby dostęp do kamer był realizowany spoza sieci korporacyjnej. Takie działanie wystawia defensywę na wiele dodatkowych wektorów ataku. Problem jest złożony i zawsze powinien być szczegółowo omawiany z działami bezpieczeństwa IT. Często mierzymy się z tą kwestią w momencie zapewnienia dostępu do wizji z urządzeń przenośnych (telefonów, laptopów, tabletów).

Architektura – zaleca się, aby systemy bezpieczeństwa działały na wydzielonej fizycznie lub logicznie sieci. Dobrze, by dostęp serwisu (gdy jest świadczony przez firmy trzecie) był realizowany przez stacje przesiadkowe, z możliwością nagrywania sesji.

Hasła – należy bezwzględnie zmienić domyślne hasła administratora i użytkowników, a także zapewnić unikatowość wszystkich haseł, unikając sytuacji, w której jedno hasło pasuje do wszystkich kamer.

Usługi – należy wyłączyć usługi, z których w codziennej eksploatacji systemu nie korzystamy, np. FTP, Multicast, Audio, QoS, ONVIF, SSH czy Telnet.

Aktualizacje firmware'u – należy korzystać z narzędzi (cyfrowy podpis) umożliwiających sprawdzenie, czy aktualizacja, którą chcemy wgrać do kamery, rzeczywiście pochodzi ze źródła producenta, upewniając się, że atrybut integralności został zachowany (nikt nie modyfikował oprogramowania, które ufnie instalujemy w kamerze). Jest to szczególnie ważny aspekt w momencie implementacji nowego systemu. Wszystkie kamery powinny przed instalacją zostać zaktualizowane do najnowszego firmware'u.

Certyfikat – kamera, jak każdy inny host w sieci, powinna przedstawiać się swoim certyfikatem (wydanym przez producenta bądź nadanym wewnątrz organizacji przez zaufane CA), a komunikacja powinna odbywać się za pomocą bezpiecznego protokołu HTTPS.

Konto administratora (root) – powinno służyć jedynie czynnościom bezpośrednio związanym z uprawnieniami administracyjnymi. Na potrzeby codziennego użytkowania powinno się zgodnie z zasadą least privilege utworzyć konto operatora z ograniczonymi uprawnieniami.

Czas i data – w celu zachowania spójności weryfikacji informacji (materiałów wideo) zaleca się, aby czas i data wszystkich kamer w systemie był zsynchronizowany. Można to uzyskać za pomocą serwera NTP (*Network Time Protocol).*

Porty – adekwatnie do usług, powinniśmy zostawić otwarte tylko te porty, z których korzystamy. Należy wziąć pod uwagę np. to, czy porty obsługujące usługi typu discovery, przydatne na etapie konfiguracji, są nadal pomocne na etapie eksploatacji.

Filtrowanie adresów IP – gdy znamy już tabelę ruchu i adresy wszystkich uprawnionych klientów, warto stworzyć tzw. białą listę adresów IP. Tylko adresy, które znajdują się na liście, będą mogły uzyskać dostęp do kamery.

Pozostaje kwestia szyfrowania strumieni wizyjnych. Z jednej stro-

ny daje to komfort i poczucie bezpieczeństwa, z drugiej – wymaga dodatkowego czasu i zasobów. Zastosowanie szyfrowania wiąże się z przeprowadzeniem oddzielnej analizy. Być może nie wszystkie punkty kamerowe tego wymagają lub architektura IT jest wystarczająca do zapewnienia atrybutów poufności, integralności i dostępności (*Confidentiality, Integrity, Availability* – CIA). Zalecam stosowanie protokołu HTTPS do celów administracyjnych, np. przeglądania ustawień kamer, do szyfrowania strumieni można wykorzystać protokół SRTP. Oba przypadki wykorzystują szyfrowanie symetryczne AES o długości klucza 128 bitów, co w zupełności wystarcza.

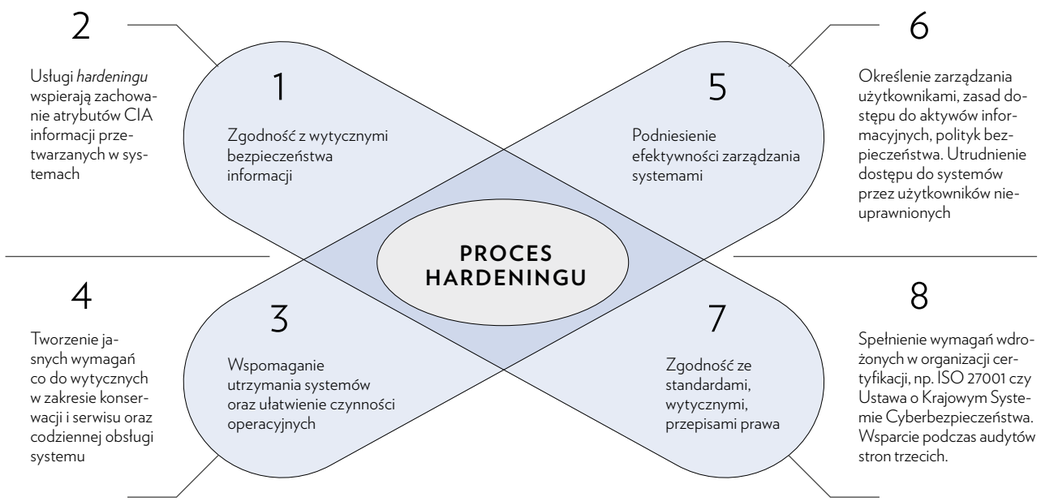
VMS (VIDEO MANAGEMENT SYSTEM)

VMS stanowi niejako serce każdego systemu dozoru wizyjnego. Jest odpowiedzialny za kompleksowe zarządzanie materiałem wideo. Nie dziwi zatem fakt, że skoro kamery podlegają procesowi utwardzania, VMS również będzie tego wymagał. Na szczęście generalne zasady są bardzo podobne. Włączamy to, co potrzebne, resztę wygaszamy. *Hardening* VMS bezpośrednio wiąże się z tematyką *hardeningu* serwerów, stacji klienckich i systemów operacyjnych. Gros dobrych praktyk opisanych przy kamerach ma również zastosowanie w tej części (praca w wydzielonej sieci czy otwarcie tylko używanych i znanych portów, uwierzytelnianie certyfikatami). Każdy dostawca może mieć nieco inne podejście i zalecenia, szczegółów należy szukać w dedykowanych poradnikach *(hardening guide).* Przy wyborze dostawcy warto sprawdzić, czy taki dokument istnieje i co zawiera. Jego jakość trzeba omówić z pracownikami obszaru odpowiedzialnego za cyberbezpieczeństwo.

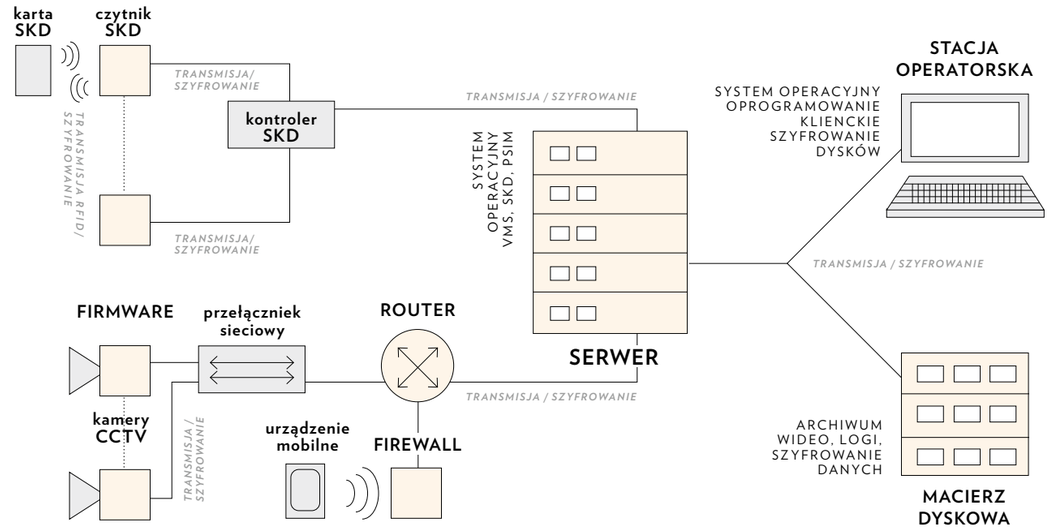
System operacyjny – zaleca się pracę na zaktualizowanym systemie operacyjnym, dzięki czemu będziemy adresować te podatności, które zostały już wykryte. Niestety z tym wątkiem wiąże się pewne ryzyko. Aktualizowanie „na ślepo" systemów operacyjnych po wydaniu aktualizacji może skutkować niepoprawnym działaniem VMS (Microsoft nie uzgadnia kompatybilności z dostawcami VMS), dlatego za każdym razem wymagany jest kontakt z dostawcą VMS i upewnienie się, że aktualizacja jest bezpieczna z punktu widzenia zachowania stabilnego działania oprogramowania. Ważnym aspektem jest też zachowanie ciągłości działania wszystkich dodatkowych integracji (aplikacji).

Serwerownia – serwery powinny pracować w odpowiednich warunkach. Serwerowniom należy zapewnić restrykcyjną kontrolę dostępu oraz odpowiednie warunki środowiskowe i ciągłość działania.
Architektura – jeśli zarządzamy systemem rozproszonym, zaleca się stosowanie tunelowania VPN. Architektura sieci jest domeną działów IT, warto wspólnie przeanalizować wymagania producenta VMS i zweryfikować je z wdrożonymi politykami w naszej organizacji.
Użytkownicy – podobnie jak przy kamerach, zaleca się tworzenie kont z uprawnieniami adekwatnymi do przydzielonych im zadań, niewskazana jest eskalacja uprawnień, ról. Niektórzy producenci zalecają wykorzystywanie użytkowników domenowych (Windows Active Directory) do logowania się do stacji klienckich. Niedopuszczalna jest praca na domyślnych hasłach, powinno się korzystać z funkcji wymuszania używania silnych haseł.
Aplikacje – nie zaleca się instalowania na serwerze innych aplikacji niezwiązanych bezpośrednio z VMS.
Urządzenia przenośne – podłączanie pamięci zewnętrznych USB, kart SD czy telefonów powinno zostać zablokowane. Pozwoli to uniknąć przedostania się złośliwego oprogramowania z urządzeń, którymi w pełni nie zarządzamy.
Bazy danych – dostawca VMS powinien dostarczyć instrukcję bezpiecznej komunikacji z bazą danych (np. z serwerem SQL). Zaleca się przetrzymywanie w bazie wszystkich zdarzeń (logów) określonych jako istotne z punktu widzenia bezpieczeństwa oraz wdrożenie szyfrowania plików.

Rys. 1. Korzyści płynące z przeprowadzonego procesu utwardzania



Rys. 2. Główne obszary *hardeningu* na schemacie uproszczonej infrastruktury sieciowej



Porty, protokoły – tak jak w przypadku kamer, otwieramy tylko te porty, które producent VMS określa jako konieczne do działania poszczególnych usług odpowiedzialnych za poprawne działanie naszego systemu.
Archiwum wideo – powinno się określić następujące ustawienia: nazewnictwo, ścieżki dostępu, uprawnienia, czas przechowywania, maks. rozmiar bazy danych i reguły nadpisywania. Zaleca się też włączenie podpisu cyfrowego materiałów wideo (dzięki czemu zachowujemy atrybut integralności w momencie eksportu) oraz określenie metody szyfrowania nagrań wraz z dodatkowym hasłem dostępu.
Logowanie – zaleca się stosowanie dwuskładnikowego uwierzytelniania (2FA) użytkowników. Jeśli zachodzi konieczność zdalnego logowania, wskazane jest wykorzystanie tunelowania VPN.
Klienci mobilni – urządzenia mobilne, które mają mieć zdalny dostęp do systemu, muszą spełniać następujące wymogi: pobranie aplikacji z autoryzowanego źródła dostawcy lub wewnętrznego repozytorium organizacji, urządzenia powinny zostać zabezpieczone zgodnie z polityką departamentów bezpieczeństwa IT i używane zgodnie z wytycznymi.

POLITYKA BEZPIECZEŃSTWA

Proces *hardeningu* powinien być jednym z niskopoziomowych elementów szeroko rozumianej polityki bezpieczeństwa. Jest to proces zmienny w czasie, co oznacza, że raz utwardzony system w perspektywie czasu może być rozpatrywany jako podatny na nowe zagrożenia. Swoisty „rachunek sumienia" powinien być przeprowadzany co najmniej raz do roku. Zdaję sobie sprawę, że nie we wszystkich typach obiektów „utwardzanie" znajdzie zastosowanie. Zapewne są miejsca, gdzie systemy tzw. *out of the box* się sprawdzą. Decyzja, czy warto proces utwardzania przeprowadzać, powinna być skutkiem dokonanej analizy ryzyka oraz świadomości tego, że taki proces w ogóle istnieje i jakie zapewnia korzyści. W ostatnim czasie świat obiegła informacja o włamaniu się do systemu CCTV jednego z irańskich więzień. Intruzi dokonali tam głębokiej penetracji systemu, dostali się również do archiwów wideo.
W obiektach o charakterze krytycznym elektroniczne systemy zabezpieczeń technicznych są tak samo ważne jak inne systemy teleinformatyczne, które wspólnie odpowiadają za bezpieczeństwo chronionych aktywów (ludzie, informacje, urządzenia, reputacja itp.). Nie ma zatem powodu, by były inaczej traktowane, wszak *hardening* infrastruktury IT jest działaniem normalnym. W przeciwnym razie w pieczołowicie budowanym cyfrowym murze zawsze znajdzie się obluzowana cegła.

„NOWA" USŁUGA

Element utwardzania infrastruktury zabezpieczenia technicznego powinien być integralną częścią prac wdrożeniowych i podlegać weryfikacji przy ich odbiorach. To żądanie musi jednak wyjść od użytkowników końcowych tworzących odpowiednie wymagania na etapie rozpisywania przetargów. Liczę również na aktywizację branży security, podnoszenie kwalifikacji specjalistów oraz poszerzenie oferty wykonawców o usługę „utwardzania".
Istotną kwestią jest również konieczność współpracy z obszarem IT security, gdyż ich rady oraz doświadczenie mogą okazać się tutaj kluczowe. Jeśli dołożymy do tego proaktywne działania naszego obszaru, będziemy w stanie uszczelnić (w rozumieniu wielopoziomowej ochrony) domyślnie skonfigurowany system. Przed zamkami przecież nie na darmo budowano fosy, a szkło wzmacnia się m.in. procesem hartowania.

TOMASZ DACKA

Ekspert bezpieczeństwa fizycznego. Z branżą związany ponad 12-letnim doświadczeniem, zwolennik holistycznego podejścia do zarządzania bezpieczeństwem. Prywatnie entuzjasta architektury przedwojennej Warszawy.

AXIS Q6078-E PTZ z cyberzabezpieczeniami

Axis Communications wprowadza na rynek kamerę AXIS Q6078-E PTZ oferującą obraz o wyjątkowo wysokiej jakości dzięki rozdzielczości UHD 4K i 20-krotnemu zoomowi optycznemu. Urządzenie zapewnia znakomity widok ogólny oraz poziom odwzorowania szczegółów z wyraźnymi ostrymi kolorami.

Ta najwyższej klasy kamera PTZ obsługuje aplikację Autotracking 2 z funkcją „kliknij i śledź", a także dynamiczny kompas ułatwiający szybką orientację w czasie aktywnego śledzenia obiektów.
Producent zadbał o cyberbezpieczeństwo – urządzenie ma wbudowane zabezpieczenia, takie jak podpisane oprogramowanie sprzętowe i bezpieczny start, które dają pewność, że zainstalowane będzie tylko autoryzowane, niezmodyfikowane oprogramowanie sprzętowe. Ponadto moduł TPM *(Trusted Platform Module)* z certyfikatem FIPS 140-2 na poziomie 2. zapewnia bezpieczne przechowywanie wszystkich kluczy kryptograficznych i certyfikatów, dzięki czemu nawet w razie naruszenia zabezpieczeń nic im nie grozi.
Najważniejsze cechy kamery:

- Rozdzielczość UHD 4K i 20-krotny zoom optyczny
- Wyjątkowej jakości obraz o znakomitym odwzorowaniu szczegółów
- AXIS Object Analytics – preinstalowane rozwiązanie działające na krawędzi sieci (w kamerze) pozwala na detekcję oraz klasyfikację obiektów
- Technologia Zipstream z obsługą formatów H.264 i H.265
- Wbudowane cyberzabezpieczenia.

Kamera jest przeznaczona do montażu na zewnątrz budynków. Jej obudowa ma klasę IP66/67, IK10, NEMA 4X, co oznacza, że kamera jest odporna na pył, deszcz, śnieg i wstrząsy.
Zastosowana funkcja *Arctic Temperature Control* umożliwia uruchamianie i użytkowanie urządzenia w temperaturach od -40°C do 50°C.

Więcej: www.axis.com/pl-pl

Nowe rejestratory NVR Wisenet wykorzystują AI do obsługi kamer bez tej funkcji

Pięć nowych rejestratorów NVR z serii Wisenet P wprowadzonych na rynek przez Hanwha Techwin pozwala na dodawanie metadanych do obrazów utworzonych przez kamery Wisenet bez funkcji AI. To umożliwia szybkie i bezbłędne wyszukiwanie osób i pojazdów w materiale wizyjnym.

W rejestratorach NVR zgodnych z NDAA jest zainstalowana aplikacja do analizy treści obrazu oparta na sztucznej inteligencji i głębokim uczeniu. Aplikacja nie wymaga licencji i oferuje szeroki zakres kryteriów wyszukiwania, np. rozpoznaje osoby w określonej grupie wiekowej lub o określonej płci, mające cechy szczególne, np. okulary czy torbę.
Podobnie można zawęzić kryteria wyszukiwania pojazdów (rower, motocykl, samochód osobowy, autobus, ciężarówka). Rejestratory można tak skonfigurować, aby w przypadku wykrycia obiektu zgodnego z zaprogramowanymi kryteriami wysyłały powiadomienia alarmowe w czasie rzeczywistym.
Nowe rejestratory NVR obsługują wybrane kamery stałopozycyjne, PTZ, dookólne, wielokierunkowe i termowizyjne z serii Wisenet X, P, Q i T. Podobnie jak w przypadku 32- i 64-kanałowych rejestratorów NVR Wisenet X, realizują wszystkie funkcje wbudowane w kamery Wisenet serii P z AI, w tym wykrywanie twarzy i tablic rejestracyjnych.
Operatorzy systemów mogą w pełni wykorzystać funkcjonalność rejestratorów NVR za pomocą UX 2.0 – nowego interfejsu użytkownika, który oferuje konfigurację okienek wizyjnych metodą przeciągania i upuszczania oraz funkcję podglądu obrazów na osi czasu, a także umożliwia edycję wszystkich ustawień w jednym oknie.
Inne dostępne funkcje:

- rejestracja obrazów z kamer sieciowych do 32 Mpix, z sumaryczną prędkością 400 Mb/s,
- maks. 16 kieszeni na dyski SATA HDD o maks. pojemności 10 TB każdy. Możliwość pracy w trybach RAID-5 i RAID-6,
- podwójne wyjścia HDMI o rozdzielczościach obrazu 4K i 1080p HDMI,
- jednoczesne odtwarzanie obrazów ze wszystkich kanałów wizyjnych,
- dynamiczna obsługa zdarzeń (m.in. alerty e-mail, sterowanie ustawieniami kamer PTZ, sygnalizacja dźwiękowa połączona z komunikatami na monitorach operatora),
- obsługa kamer Wisenet z AI o rozdzielczości 8K,
- zgodność z ONVIF Profile S.

Więcej: www.hanwha-security.eu/pl

Fiera Milano zaprasza na targi SICUREZZA 2021

Już ponad 200 firm potwierdziło udział w targach SICUREZZA 2021, które odbędą się w Mediolanie w dniach 22–24 listopada. Wydarzenie będzie okazją do poznania nowinek technologicznych, najbardziej zaawansowanych rozwiązań dostępnych na rynku oraz najnowszych trendów.

Targi SICUREZZA powracają razem ze SMART BUILDING EXPO, imprezą automatyki domowej i budynkowej oraz integracji technologicznej. W tym samym czasie odbędą się również Targi MADE, wiodące wydarzenie dla branży budowlanej we Włoszech. Te trzy imprezy rozpoczną się jednocześnie w Fiera Milano (Rho) 22 listopada 2021 r.

Oferta produktowa
Na SICUREZZA 2021 będzie można spotkać się osobiście i porozmawiać z producentami, a przede wszystkim poznać dostępne na rynku najnowsze urządzenia do ochrony ludzi, towarów i środowiska. Urządzenia ze wszystkich segmentów rynku pozwolą na przegląd najbardziej zaawansowanych rozwiązań dostępnych w każdym obszarze zastosowań.

Producenci i dystrybutorzy systemów dozoru wizyjnego zapewnią przegląd technologii mających zastosowanie w sektorach zarówno publicznym, jak i prywatnym: od kamer dozorowych o ultrawysokiej rozdzielczości po kamery termowizyjne, od oprogramowania do zarządzania danymi po systemy analizy wizji, które umożliwiają inteligentny odczyt danych.

W tej edycji będzie też zaprezentowana bogata oferta produktów antywłamaniowych, z udziałem wiodących marek włoskich i międzynarodowych. Przedstawione zostaną m.in. zintegrowane systemy zabezpieczeń dla przemysłu, handlu i instytucji rządowych, innowacyjne systemy mgły wodnej, a także wiele produktów dla sektora mieszkaniowego, coraz bardziej zintegrowanych z zaawansowanymi rozwiązaniami automatyki domowej.

Organizatorzy duży akcent położą na temacie cyberbezpieczeństwa: szerokopasmowe zintegrowane rozwiązania, zarządzanie chmurą, sztuczna inteligencja i IoT, które coraz częściej stosuje się w systemach zabezpieczeń technicznych – na pierwszy plan wysuwają się więc kwestie bezpieczeństwa danych. Zgodność z przepisami RODO staje się wymogiem zarówno producentów, jak i instalatorów, ponieważ biorą oni odpowiedzialność za ochronę danych osób „śledzonych" przez systemy zabezpieczeń.

Po raz kolejny na targach zostanie zorganizowana Cyber Arena, czyli przestrzeń wystawiennicza i szkoleniowa, gdzie eksperci ds. bezpieczeństwa, naukowcy i przedstawiciele firm będą analizować trendy, dzielić się najlepszymi praktykami i prezentować najnowsze innowacje z zakresu cyberbezpieczeństwa. Cykl Cyber Security Talks to spotkania z ekspertami, którzy przedstawią swoje opinie na temat głównych trendów. Z kolei Cyber Security Tips to krótkie sesje szkoleniowe z poradami i sugestiami gotowymi do natychmiastowego wykorzystania.

Nie zabraknie również prezentacji oferty systemów kontroli dostępu oraz systemów przeciwpożarowych i zabezpieczeń mechanicznych.

Bezpieczeństwo związane z COVID-19
Organizatorzy zadbali o bezpieczeństwo sanitarne gości. Dzięki współpracy z zespołem ekspertów i głównymi firmami z branży przygotowano specjalną instrukcję w zakresie powstrzymania rozprzestrzeniania się koronawirusa. Zawarto w nim rekomendacje dotyczące bezpiecznej organizacji imprez targowych, w pełnej zgodności z przepisami i zaleceniami zdrowotnymi.

Wprowadzone zostaną zielone przepustki, dostępne będą maseczki. Szczególną uwagę organizatorzy zwrócili na dostęp do targów: punkty dla pieszych i pojazdów zostały przedefiniowane w celu prawidłowego zarządzania ruchem.

Ponadto procedury dostępu zostaną zautomatyzowane poprzez wykorzystanie technologii cyfrowych. Specjalna aplikacja zapewni dostęp do szeregu usług, w tym szybkiej ścieżki, rezerwacji miejsc parkingowych i restauracji. Dodatkowo strefy gastronomiczne zostały rozplanowane w taki sposób, aby zapewnić odpowiedni dystans społeczny.

Dzięki tym prostym i jasnym zasadom będzie można bezpiecznie poruszać się po stoiskach, spotykać się i wymieniać poglądami, chroniąc w ten sposób siebie i dbając o zdrowie wszystkich innych uczestników.

Więcej informacji o konferencji znajduje się na: www.sicurezza.it

Wystartował sklep internetowy D+H Polska

4 października br. wystartowała witryna zakupowa D+H Polska. Sklep oferuje kompleksowe rozwiązania obejmujące: systemy oddymiania i naturalnej wentylacji, systemy sygnalizacji pożarowej oraz napędy do okien i klap dymowych.

Po zapoznaniu się z bazą produktów w internetowym sklepie można łatwo i szybko złożyć zamówienie – po dodaniu artykułów do koszyka wystarczy wypełnić formularz, pozostawiając swoje dane kontaktowe. Doradca skontaktuje się, by przedstawić indywidualnie skalkulowaną ofertę. Każdy oferowany w sklepie produkt jest prezentowany wraz z informacją o podstawowych cechach i parametrach technicznych oraz ceną (w kwotach netto i brutto).
Klienci mogą liczyć na konsultacje z ekspertami i doradztwo w zakresie doboru produktów i rozwiązań. Indywidualne podejście do realizowania zamówień i bezpośredni kontakt to również okazja do zadawania pytań, otrzymania specjalnego rabatu oraz ustalenia indywidualnych warunków dostawy, a także montażu czy późniejszego serwisu. Zachęcamy do poznania rozwiązań D+H Polska, do zakupu produktów i kontaktu z doradcami.

Sklep D+H Polska jest dostępny pod adresem www.sklep.dhpolska.pl

Integracja BMS Nazca APA Group z RACS 5 firmy Roger

System kontroli dostępu klasy Enterprise o nazwie RACS 5 firmy Roger zyskał w ostatnich 5 latach sprzedaży renomę atrakcyjnego, sprawdzonego rozwiązania na rynku projektowym, co przekłada się zarówno na kolejne ciekawe realizacje, jak i zainteresowanie innych dostawców rozwiązań na tym rynku.

System RACS 5 może być integrowany z innymi systemami informatycznymi za pośrednictwem tzw. usługi Serwera Integracji. Integracja RACS 5 z systemem Nazca BMS została zrealizowana przez APA Group właśnie w oparciu o ww. usługę. W wyniku opracowanej integracji system Nazca BMS umożliwia:

- gromadzenie i przegląd danych z bieżącej pracy systemu RACS 5,
- weryfikację osób wchodzących/wychodzących, (dziennik zdarzeń),
- zdalne otwieranie/zamykanie przejść,
- czasowe odblokowanie/zablokowanie przejść.

Opracowane rozwiązanie znajduje najczęściej zastosowanie w budownictwie komercyjnym i sektorze przemysłowym, jednak może być z powodzeniem wykorzystywane tam, gdzie jest potrzebna wizualizacja systemu kontroli dostępu oraz kontrolowanie jego stanu z poziomu systemu klasy BMS.

Więcej: www.roger.pl

Fot.: System antenowy ILS LOC (Instrument Landing System localizer)

Telbud SA modernizuje lotniska Sił Zbrojnych RP

W 2018 r. Ministerstwo Obrony Narodowej wybrało połączoną ofertę Telbud SA i firmy Thales w ramach programu modernizacji lotnisk i zwiększenia ich potencjału wojskowego. Inwestorem wojskowym jest 17. Terenowy Oddział Lotniskowy w Gdańsku.

Do tej pory Siłom Zbrojnym RP przekazano w użytkowanie kompletne systemy radionawigacji ILS/DME na lotniskach w Powidzu i Mińsku Mazowieckim.
Obecnie Telbud SA prowadzi jeszcze prace na lotniskach w Krzesinach, Dęblinie, Mirosławcu i Świdwinie, które mają się zakończyć jeszcze w 2021 r. Na przyszły rok zaplanowane są prace na lotniskach wojskowych w Łasku, Gdyni Babie Doły, Cewicach i Malborku.

System radionawigacji ILS/DME *(Instrument Landing System/ Distance Measuring Equipment)* wspomaga lądowanie samolotów w warunkach ograniczonej widoczności. Nowe systemy podniosą więc potencjał wojskowy lotnisk, zwiększając bezpieczeństwo operacji lotniczych. Lotniska dołączą też do portów, z których będą mogły korzystać samoloty NATO w warunkach wysokiego poziomu bezpieczeństwa.

Więcej: www.telbud.pl

Spotkanie z technologiami bezpieczeństwa

Carrier Fire & Security Polska

W ramach zaznajomienia z działalnością Carrier Fire & Security w Polsce firma na początku września br. zorganizowała Road Show po swoim kompleksie laboratoriów badawczo-rozwojowych w Gdańsku. W spotkaniu uczestniczyło blisko 80 partnerów firmy z całej Polski.

Goście zwiedzili wybrane laboratoria badawcze rozlokowane na pięciu kondygnacjach nowoczesnego biurowca. Zwiedzającym zaprezentowano laboratoria:

- kompatybilności elektromagnetycznej,
- czujek ruchu, tzw. *Walk Test Lab,*
- czujek stłuczenia szyb,
- systemów wykrywania pożaru AUTRONICA,
- systemów gaszenia mgłą wodną Marioff,
- komorę bezechową i klatki Faradaya.

W drugiej części spotkania Maciej Sobczyk, dyrektor centrum badawczo-rozwojowego w Gdańsku, omówił strukturę i zakres działalności grupy Carrier na świecie, natomiast Maciej Brzyski, kierownik sprzedaży produktów security marki Aritech, przedstawił polski dział Carrier Fire & Security. Tomasz Żuk zapoznawał gości ze zmianami w oddziale wsparcia technicznego i nowościami w ofercie produktowej. Piotr Ejma-Multański zaprezentował certyfikowany, autonomiczny, bezprzewodowy system sygnalizacji pożarowej Smart-Cell. O zarządzaniu systemami w chmurze w technologii Ultrasync opowiadał Jarosław Gibas, pokazując, jak można wpierać budynkowe systemy bezpieczeństwa za pomocą platformy ATS8600.
Z kolei Sebastian Nowak przybliżył gościom Modulaser – wielostrefową, modułową czujkę zasysającą dymu obsługiwaną za pośrednictwem protokołu TCP/IP.
Przykłady rozwiązań ochrony perymetrycznej wspieranej przez zintegrowany system zabezpieczeń elektronicznych: SSWiN, KD oraz CCTV zaprezentował Przemysław Szczuka, natomiast najnowsze rozwiązania z zakresu CCTV, w tym systemy do zliczania osób, kamery ANPR oraz system TruVision Navigator, przybliżył Maciej Kułakowski.

Więcej: https://pl.firesecurityproducts.com/pl/

REKLAMA

ARITECH

Advisor Advanced

Przenieś cyberbezpieczeństwo na wyższy poziom

Innowacyjny

Skuteczny

Idealny dla klienta

Aritech jest globalną marką firmy Carrier reprezentującą rozwiązania zabezpieczeń dla klientów prywatnych, komercyjnych i korporacyjnych. Oferujemy zintegrowaną platformę bezpieczeństwa w obszarze systemów alarmowych, kontroli dostępu, wideo i wykrywania pożaru. Aritech cieszy się zaufaniem klientów od ponad 40 lat.

Odwiedź: **pl.firesecurityproducts.com**

Carrier

Wydajny i bezpieczny VMS

na systemie LINUX

Wavestore wprowadził kolejną wersję swojego otwartego i wyjątkowo bezpiecznego oprogramowania do zarządzania wideo (VMS) opartego na systemie Linux. Taka architektura oferuje wiele korzyści w aspekcie bezpieczeństwa w porównaniu z jej odpowiednikami opartymi na systemie Windows™.

Przykładowo na VMS Wavestore nie mają wpływu luki w systemie Windows i nie ma czasochłonnych aktualizacji systemu, wymagających zazwyczaj wstrzymania pracy oprogramowania zarządzającego. Ma ono natomiast pełną kontrolę nad tym, które konkretne komponenty systemu operacyjnego Linux są używane, i wyłącza wszystkie nieistotne obszary, aby znacznie zmniejszyć zagrożenie potencjalną podatnością na ataki oraz zwiększyć wydajność instalacji.
Nowa wersja VMS v6.28 stanowi kolejny duży krok naprzód, ponieważ umożliwia bardzo wygodną obsługę zdarzeń alarmowych w czasie rzeczywistym oraz wydajne wyszukiwanie na podstawie metadanych pochodzących z analityki wideo wbudowanej w wybrane modele kamer zgodnych z ONVIF. Dzięki temu określone scenariusze alarmowe są wyzwalane tylko wtedy, gdy wystąpią określone okoliczności, np. gdy samochód osobowy przejeżdża przez obszar, w którym dozwolony jest wyłącznie ruch ciężarówek, albo w obszarze, na którym obowiązuje limit osób, a przebywa ich więcej.
Do wyboru jest wiele reguł alarmowych, np. wjazd i wyjazd z obszaru, usunięcie lub pozostawienie/bezczynność obiektu czy stłoczenie osób lub obiektów. Reguły są programowane i uruchamiane nie w kamerach lub na dodatkowym, powiązanym serwerze analitycznym, ale na serwerze Wavestore.
Oprogramowanie sprawdzi się zarówno w już istniejących systemach obejmujących nowe rozwiązania różnych producentów, jak i w nowych instalacjach, umożliwiając łatwe i bezpieczne zarządzanie nimi.

Więcej:
https://www.linc.pl/wavestore/

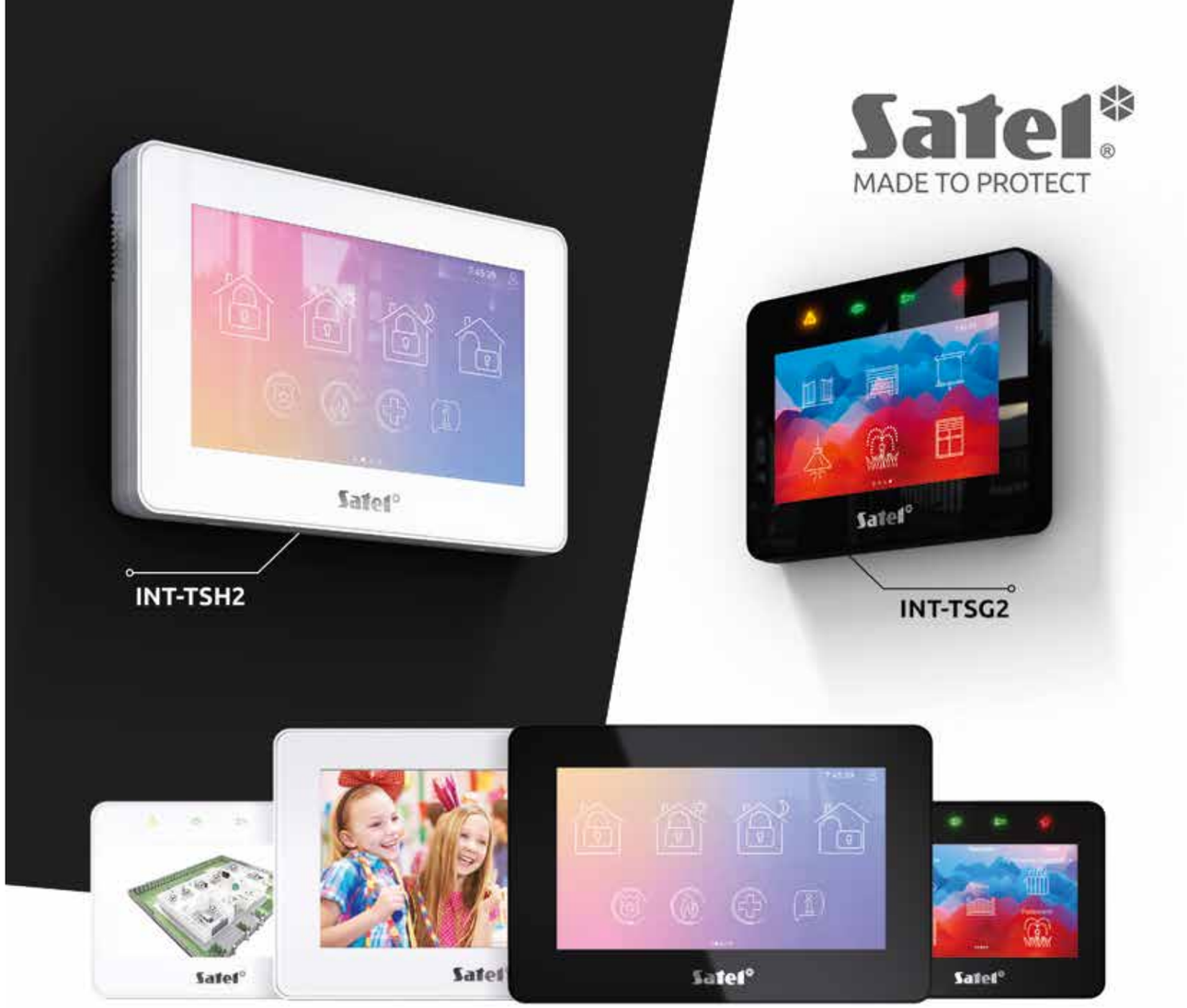
Zwiększ zasięg dzięki odpowiedniej antenie

Wraz z rosnącą liczbą osób pracujących w domu wzrosło zapotrzebowanie na stabilne, niezawodne i szybkie usługi internetowe. Często usługi te opierają się na mobilnym dostępie do Internetu.

Routery wdrażane przez operatorów mają przeważnie wbudowany odbiornik z już zintegrowanymi antenami. Takie routery zostały zaprojektowane głównie dla obszarów, gdzie rozmieszczenie stacji bazowych jest gęste. Wielu użytkowników jest jednak rozczarowanych prędkością połączenia. Słaba jakość sygnału wynikająca z wykorzystania wyłącznie wewnętrznych anten skutkuje niską wydajnością, a tym samym niezadowoleniem użytkowników.

Zastosowanie anten zewnętrznych może znacznie poprawić elastyczność całego systemu. Znajdują one zastosowanie zarówno w instalacjach domowych, jak i profesjonalnych systemach ochrony. Szeroka oferta anten pozwala na wybór odpowiedniego rozwiązania zarówno do stacjonarnych, jak i mobilnych systemów zabezpieczenia technicznego, które ciągle zyskują na popularności.
Skupienie się na technologiach bezprzewodowych uczyniło z firmy Poynting światowego innowatora produktów antenowych. Poynting jest właścicielem ponad 50 patentów i projektów szeroko stosowanych w autorskich, unikatowych rozwiązaniach antenowych do ulepszonej komunikacji bezprzewodowej LTE, 3G, Wi-Fi, RF i innych zastosowań. Anteny są stale testowane i poddawane niezależnym certyfikacjom, gdyż wysoka jakość oferowanych produktów jest dla nas najważniejsza.
Skontaktuj się z nami, a pomożemy w wyborze właściwych anten do Twojego projektu.

Więcej:
https://smart-i.pl/poynting/



INT-TSH2 i INT-TSG2

NOWA JAKOŚĆ W STEROWANIU

systemami alarmowymi i automatyki budynkowej

Zeskanuj kod QR telefonem
i przejdź do serwisu YouTube

www.satel.pl

DualCurtain Outdoor

Bezprzewodowy zewnętrzny dwukierunkowy kurtynowy czujnik ruchu

Niezależna konfiguracja dla obu kierunków

Dwukierunkowy czujnik ruchu o wąskim kącie widzenia

30m

Monitoruje aktywność w linii 30 m

IP54

Odporny na pył i rozpryski

Darmowe aplikacje dla instalatorów i użytkowników końcowych

ajax.systems

macOS Windows iOS Android

Miłego oglądania