a&S POLSKA
www.aspolska.pl

CZASOPISMO RYNKU SECURITY
nr 1/2018 (7)
styczeń/luty
15 zł (w tym 8% VAT)

raport
DRONY
DO OCHRONY

Przyszłość SECURITY

ISSN 2451-5175

KONDYCJA BRANŻY
Liderzy rynku podsumowują rok
O sukcesach i porażkach minionego roku oraz planach na kolejny rok opowiedzieli nam przedstawiciele najważniejszych firm branży security w Polsce.
str. 14

NOWE TECHNOLOGIE
Cyborgi, *deep learning*, sztuczna inteligencja
Czy będziemy musieli stać się cyborgami, aby stawić czoło przyszłości zdominowanej przez sztuczną inteligencję? Jak wykorzystać *deep learning*?
str. 26

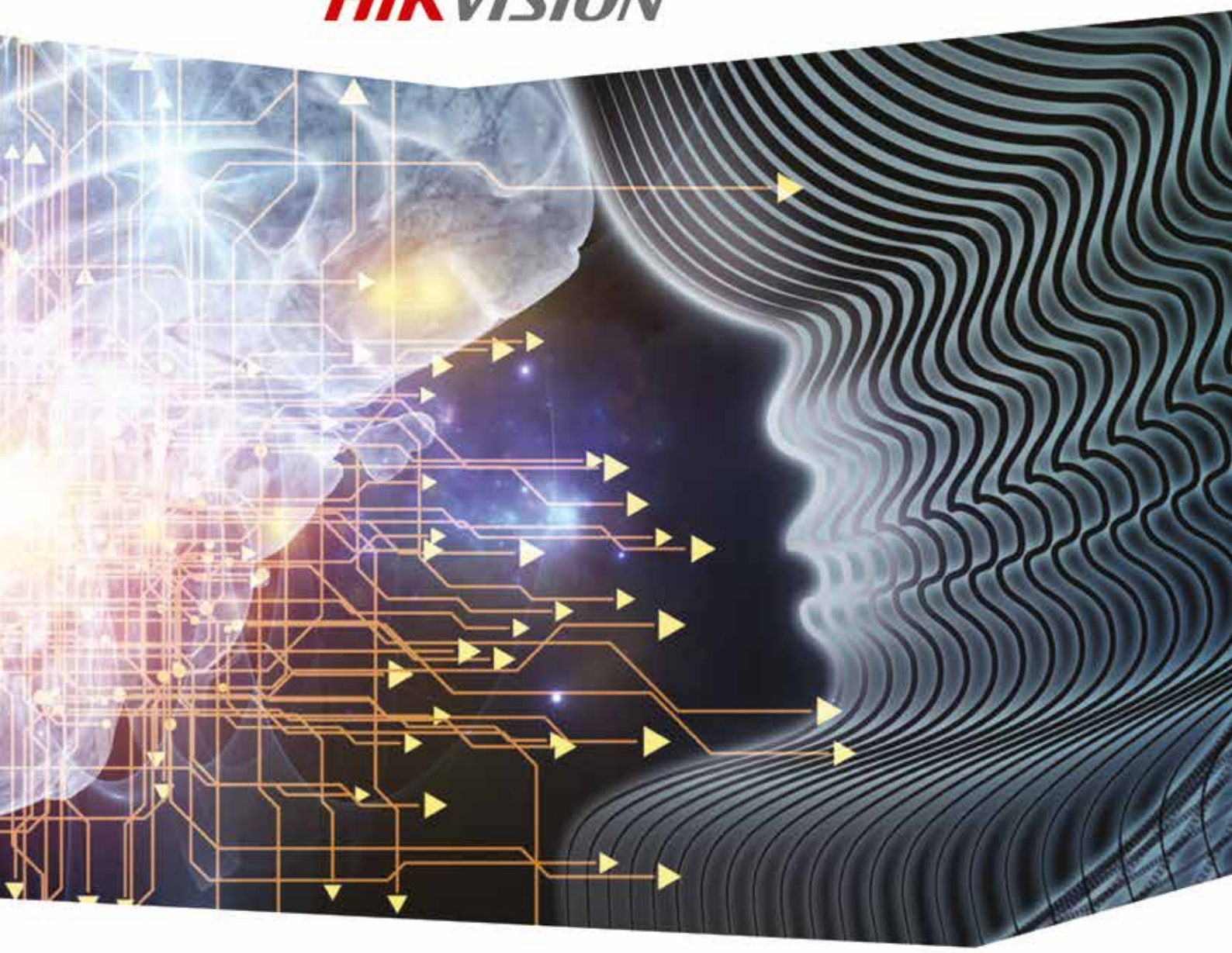
TEMAT NUMERU
Bezpieczeństwo transportu i logistyki
Telematyka, *machine learning*, termowizja – to tylko niektóre technologie sprawdzające się w tych skomplikowanych zastosowaniach.
str. 52

WIĘKSZA INTELIGENCJA.
WIĘKSZE BEZPIECZEŃSTWO.
TECHNOLOGIA DEEP LEARNING FIRMY HIKVISION

Hikvision Poland Sp. z o.o.
ul. Krakowiaków 50
02-255 Warszawa

T +48 22 4600150
info.pl@hikvision.com

HIKVISION



Hikvision patrzy w przyszłość i stale rozwija swoje technologie.
Jedna z nich - Deep Learning - zapewnia zupełnie nowe możliwości. Detekcja twarzy, zliczanie osób, identyfikacja pojazdów - wszystko to jest możliwe z nowymi produktami dostarczanymi przez firmę Hikvision.

Na tym nie koniec. Hikvision nieustannie pracuje, by dalej przekraczać granice!

- Detekcja twarzy
- Filtrowanie fałszywych alarmów
- Zliczanie osób
- Identyfikacja pojazdów
- Rozpoznawanie osób

@HikvisionPoland
www.hikvision.com/pl/

Drodzy Czytelnicy

Nowy rok rozpoczynamy tradycyjnie od wyznaczenia celów i zadań na najbliższe miesiące. Priorytetem dla nas jest utrzymanie bliskich relacji zarówno z branżą safety&security, jak i naszymi Czytelnikami. Ten często bezpośredni kontakt widać nie tylko na naszych łamach, ale także podczas organizowanych przez nas wydarzeń. **Śniadania ekspertów** wpisały się już w kalendarz branżowych wydarzeń. Dzięki nim udało nam się połączyć dwie strony rynku – oferentów i użytkowników systemów zabezpieczeń.

Cieszą nas opinie, że jesteśmy cenionym i – co najważniejsze – opiniotwórczym źródłem wiedzy branżowej. Rynek również pozytywnie zweryfikował pierwszy rok szerokiej działalności „a&s Polska". Cieszymy się, że wszyscy dotychczasowi partnerzy kontynuują współpracę z nami, wspierając nasze działania na rzecz branży. Witamy w tym gronie kolejne firmy, zarówno znane na polskim rynku, jak i debiutujące.

Nowy rok to także czas podsumowań. Co się udało zrealizować, a nad czym jeszcze trzeba popracować? Czym firmy zaskoczyły rynek, a co nie zostało przyjęte z entuzjazmem? Rozmawialiśmy o tym z **przedstawicielami najważniejszych firm na polskim rynku security** (s. 14).

W przyszłość patrzymy przez pryzmat nowych technologii, mających ogromny wpływ na rozwój również naszej branży: sztuczna inteligencja, *deep learning* i *machine learning*, rozszerzona rzeczywistość, Internet Rzeczy czy *Brain-Computer Interface*. Jak bardzo zmienią oblicze systemów security? Jak bardzo wpłyną na życie człowieka? Być może niedługo wszyscy będziemy cyborgami...

Nowoczesne rozwiązania cyfrowe są adresowane także **do sektora transportu i logistyki** (s. 52). Ten rynek wymaga od specjalistów security specyficznego podejścia, głównie ze względu na dynamicznie zmieniające się wyzwania i zagrożenia dla bezpieczeństwa.

Głębokie zmiany czekają także firmy ochrony. Problem opisujemy w dziale *Bezpieczeństwo biznesu* z punktu widzenia zarówno oferentów (s. 110), jak i ich klientów (s. 114).

W tym wydaniu prezentujemy też solidną dawkę wiedzy naukowo-technicznej. Zapraszamy Czytelników na **warsztaty z kamerami PTZ** (s. 36), które przeżywają obecnie rynkowy renesans. Przedstawiamy przy tym bogatą ofertę najnowszych i najbardziej popularnych modeli (s. 42). Z zakresu bezpieczeństwa pożarowego polecamy pogłębioną analizę przyczyn **pożaru w londyńskim metrze** (s. 84).

Rok 2018 rozpoczęliśmy imprezowo **w Dubaju** – bogatych w nowe technologie i innowacje **targów Intersec** nie sposób ominąć (s. 118). Przed nami kolejne inspirujące wydarzenia, które także będziemy relacjonować.

Marta Dynakowska
redaktor naczelna

Mariusz Kucharski
dyrektor zarządzający

Wydawca
a&s Polska Sp. z o.o.

Adres wydawcy i redakcji
a&s Polska
Rondo1 (10. piętro)
Rondo ONZ 1, 00-124 Warszawa
tel. +48 22 418 71 59
e-mail: info@aspolska.pl
www.aspolska.pl

Dyrektor zarządzający
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Dział reportażu
Andrzej Popielski

Dział marketingu i reklamy
Iwona Krawiec

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

Korekta
Jolanta Kucharska

Projekt graficzny
Sylwester Dmowski

Skład
Dorota Cybulska
Sylwester Dmowski

Prenumerata
www.aspolska.pl/prenumerata

BCS-P-5692RSAI

Wysoka rozdzielczość do 12 Mpx, najwyższej jakości moduł wizyjny z 22 krotnym zoomem, inteligentne funkcje to jedne z wielu atutów kamery BCS-P-5692RSAI. Wszystko to sprawia, że topowy model serii BCS Point prezentuje to co najważniejsze w systemach telewizji przemysłowej, idealnie ostry obraz w wysokiej rozdzielczości. Inteligentne funkcje, presety oraz nowatorskie rozwiązania pozycjonujące pozwolą kamerze spojrzeć tam gdzie chcemy, nawet bez konieczności obsługi urządzenia. Inteligentny promiennik podczerwieni o zasięgu do 250m dopasuje się do obserwowanego planu doświetlając scenę zarówno szerokiego planu jak i dużego przybliżenia.

- Przetwornik 1/1,7" 12 Mpx CMOS
- Kompresja wideo H.265/H.264/MJPEG
- Obsługa trzech strumieni wideo
- 20 kl./s przy 12.0 M (4000×3000)
- Obsługa ICR Dzień/Noc
- Funkcja DEFOG, Inteligentne funkcje
- Obiektyw 6.5~143 mm, 22×
- Promiennik IR LED SMART – do 250 m
- Funkcje automatyki: 255 presetów, 16 tras (po 32 presety), 16 ścieżek
- Obrót 360° (nieskończony), Tilt-15°~+90°
- Prędkość obrotu Pan 0,1°/s~240°/s (300°/s preset), Tilt 0,1°~160°/s (240°/s preset)
- 1 wejście/wyjście audio, 2 wejścia/1 wyjście alarmowe
- Obudowa IP66

BCS®

www.bcscctv.pl

W numerze...

raport DRONY DO OCHRONY

RAPORT: DRONY W SECURITY

BEZPIECZEŃSTWO BIZNESU

SERWIS INFORMACYJNY

Drony a bezpieczeństwo biznesu STR. 108

Bezpieczeństwo biznesu STR. 116

PRACOWNIK i jego kompetencje cyfrowe

Bezpieczeństwo pożarowe STR. 84

Serwis informacyjny STR. 118

Dyskretne 5-Mpix kamery sieciowe

AXIS
www.axis.com/pl

Zaawansowane technologicznie dyskretne kamery sieciowe AXIS Q3517-LV i AXIS Q3517-LVE dostarczają wysokiej jakości obraz o rozdzielczości 5 Mpix w skomplikowanym oświetleniu i trudnych warunkach eksploatacji, przy pełnej poklatkowości (maks. 30 kl./s).
Dzięki funkcji *Forensic WDR* obraz charakteryzuje się wysoką szczegółowością, a sceny z kontrastowo oświetlonymi obszarami są doskonale widoczne.
Dzięki technologii *Lightfinder* kamera generuje ostre, kolorowe obrazy przy słabym oświetleniu, a funkcja *OptimizedIR* zapewnia obraz bez szumu w całkowitej ciemności. Z kolei zastosowana technologia *Zipstream* zmniejsza zapotrzebowanie na przepustowość i pamięć nawet o 50%, zapewniając przechwytywanie ważnych szczegółów przy pełnej jakości obrazu.
Model AXIS Q3517-LV ma konstrukcję odporną na drgania i wstrząsy. Ochronę przed wnikaniem kurzu i wody zapewnia obudowa o klasie IP52 i IK10 (odporność na akty wandalizmu). Elektroniczna stabilizacja obrazu umożliwia uzyskanie niezakłóconego obrazu nawet w przypadku narażenia kamery na drgania.
Do portów wejścia kamery można dołączyć zewnętrzne czujki, a sygnał alarmu przesłać nawet po odcięciu połączenia, co przyspiesza reakcję na zdarzenie.
Dynamiczne nakładki pozwalają na elastyczne dodawanie informacji (tekst lub obraz) do strumienia wizji. Dostępny jest również opcjonalny mikrofon do rejestracji dźwięku.
Aplikacje do analizy *AXIS Motion Guard* i *AXIS Fence Guard* można pobrać i zainstalować bezpłatnie.

Seria kamer ARTR BCS

BCS
www.nsssystem.pl

Kamery BCS z funkcją ARTR to profesjonalne rozwiązanie pozwalające rozpoznawać tablice rejestracyjne przejeżdżających pojazdów. W ofercie są trzy urządzenia, z czego najnowszy jest model BCS-TIP8201ITC-II. Zaimplementowany w kamerze algorytm rozpoznaje numery rejestracyjne samochodów przejeżdżających z prędkością do 40 km/h. Promiennik podczerwieni umożliwia odczyt numerów tablic również w nocy, a funkcja HLC niweluje efekt oślepiania kamery światłami nadjeżdżających samochodów.
Rozpoznane numery tablicy rejestracyjnej pojazdu oraz jego zdjęcie mogą być zapisane na karcie micro SD o pojemności do 128 GB.
Dostęp do bazy zgromadzonych numerów tablic rejestracyjnych jest możliwy bezpośrednio z interfejsu Web urządzenia. Istnieje możliwość stworzenia „białej listy" pojazdów zarówno z poziomu Web interfejsu, jak i z menu rejestratora, do którego kamera jest podłączona. Rozpoznając numery rejestracyjne z bazy, kamera może wyzwolić przekaźnik i automatycznie otworzyć szlaban wjazdowy. Urządzenie wtedy działa jako autonomiczny punkt sterujący szlabanem lub w połączeniu z aplikacją BCS Manager tworzy rozległy i funkcjonalny system.
Aplikacja pozwala na podgląd online z kamer ARTR, pokazując jednocześnie obraz i odczytany numer tablicy rejestracyjnej.
Ważną funkcją systemu jest tworzenie raportów zarówno zbiorczych, jak i dla dowolnego numeru tablicy rejestracyjnej, czasu lub kamery w systemie. Całość sprawia, że seria kamer ARTR BCS staje się uniwersalnym rozwiązaniem dla małych i większych obiektów.

NKB5000 – sieciowa klawiatura HD

Dahua Technology Poland
www.dahuasecurity.com/pl

Dahua Technology wprowadza na rynek nowoczesną, wielofunkcyjną klawiaturę sieciową NKB5000. Urządzenie łączy funkcje klasycznego pulpitu sterowniczego do systemów CCTV (VSS) z dekoderem wizyjnym.
O ile funkcje umożliwiające sterowanie systemami dozoru wizyjnego za pomocą klawiatur są dosyć popularne i znane, o tyle zastosowanie wbudowanego dekodera – niekoniecznie. Urządzenie ma 4 wyjścia HDMI do podłączenia monitorów o rozdzielczości 4K bezpośrednio do klawiatury! Możliwości dekodowania strumieni są równie imponujące. Urządzenie jest w stanie wyświetlić bądź zapisać (na dysku USB) 4 kanały w rozdzielczościach 12 Mpix oraz 4K lub np. 16 kanałów full HD.
Klawiatura ma wbudowany ekran dotykowy o przekątnej 10,1" ułatwiający korzystanie z jej funkcji. Mnogość obsługiwanych urządzeń (m.in. rejestratory, kamery PTZ sieciowe i analogowe, dekodery, ściany wizyjne, wbudowane wejścia i wyjścia alarmowe czy dwukierunkowe audio) czynią ją produktem kompletnym i wielofunkcyjnym.
Oprócz przewodowego połączenia pulpitu z siecią IP można łączyć się bezprzewodowo za pośrednictwem Wi-Fi.
Do podstawowego pulpitu sterowniczego można dołączyć za pomocą technologii Bluetooth dodatkowy moduł z klawiszami.
Klawiatura NKB5000 została zauważona i doceniona. Przyznano jej prestiżową nagrodę *iF Design Award 2017*. Wyróżnienie to należy do najważniejszych w zakresie wzornictwa na świecie. Jest przyznawane przez międzynarodowe jury.

Satel®
MADE TO PROTECT

ACCO NET

SKALOWALNY SYSTEM KONTROLI DOSTĘPU

- centralne zarządzanie nieograniczoną ilością obiektów w różnych konfiguracjach struktury systemu
- zdalna kontrola umożliwiająca sterowanie i konfigurację systemu z dowolnego miejsca na świecie
- rozproszona struktura zapewniająca elastyczność instalacji

... a cały system umożliwia obsługę
aż **65 000** użytkowników!

SATEL sp. z o.o.
ul. Budowlanych 66, 80-298 Gdańsk, tel.: (58) 320-94-00
e-mail: satel@satel.pl, www.satel.pl

SAFESTAR System monitorigu zintegrowanego

DMSI
www.dmsi.pl www.safestar.pl

DMSI Software jest polską firmą nowych technologii, założoną w 2009 r. Od początku działalności koncentruje się na dostarczaniu nowoczesnych rozwiązań informatycznych w obszarze szeroko rozumianego monitoringu. Tworzy je zespół doświadczonych programistów.
Sztandarowym rozwiązaniem firmy jest SAFESTAR – nowoczesny i innowacyjny system monitoringu zintegrowanego i zarządzania bezpieczeństwem, działający w technologii chmury prywatnej. Ma bardzo duży zakres funkcjonalności – począwszy od klasycznego monitoringu sygnałów alarmowych, poprzez GPS, skończywszy na zaawansowanych funkcjach transmisji sygnałów wizji oraz fonii (*VoIP*). Wszystko jest dostępne przez Internet.
Istotnym elementem systemu SAFESTAR są dwie aplikacje mobilne: Patrol 2 – przeznaczona dla grup interwencyjnych i serwisu oraz PSC *(Personal Security Center)* – dla klientów końcowych.
Użytkownikami tego systemu są stacje monitorowania alarmów, stacje zdalnego dozoru wizyjnego, banki i firmy o charakterze globalnym oraz przedsiębiorstwa infrastruktury krytycznej. Klientami końcowymi korzystającymi z rozwiązania SAFESTAR są m.in. Pekao SA, Konsalnet, sieć sklepów Stokrotka. Firma świadczy również usługi dla średnich i małych agencji ochrony.
SAFESTAR zmienia wyobrażenie o współczesnym monitoringu, przenosząc klientów w inny wymiar technologiczny w ochronie. Po zalogowaniu się do systemu klienci otrzymują potężne narzędzie do zapewniania bezpieczeństwa.

Kolorowy obraz w nocy z kamer IP Tiandy
światło = widzenie

GENWAY
www.genway.pl

Gdy nadchodzi zmrok, spada zdolność widzenia. Sytuacja jest identyczna w przypadku kamer. Przy dużej ilości światła każde urządzenie przekaże obraz dobrej jakości, przy mniejszej natomiast na obrazie uwidoczni się szum, który zmniejszy szczegółowość. Z kolei przy większym spadku oświetlenia kamery przechodzą w tryb obserwacji czarno-białej. W takiej sytuacji można jedynie stwierdzić, czy auto lub ubiór osoby były jasne, czy ciemne. Szczegóły obrazu o małym kontraście zostaną utracone – skryją się w odcieniach szarości.
Najnowsze modele kamer Tiandy Starlight TC-NC23MS i TC-NC24MS przesyłają kolorowy obraz nawet przy oświetleniu 0,002 luksa. Dla porównania Księżyc w pełni oświetlający Ziemię ma natężenie 0,2 luksa, a oświetlenie uliczne w nocy wynosi 5 luksów.
W kamerze zastosowano przetwornik o wysokiej czułości i rozdzielczości 2 Mpix, który połączono ze szklanym obiektywem o jasności F1.2. Jest on typu motozoom, więc regulacja przybliżenia i ostrości odbywa się zdalnie. Ogniskowa obiektywu zawiera się od 2,8 do 12 mm. Oba modele mają klasę szczelności obudowy IP67.
W kamerach zaimplementowano funkcję inteligentnej analizy obrazu IVA, takie jak przekroczenie linii, naruszenie obszaru, detekcja tłumu, pozostawiony lub usunięty przedmiot, detekcja szybko poruszającego się obiektu, nietypowe zachowanie i nieprawidłowe parkowanie. Kamery są objęte 3-letnią gwarancją.

WiseNet Wave – superwydajność i intuicyjność dla Windows, Apple/Mac i Linux

Hanwha Techwin Europe
www.hanwha-security.eu/wisenet-wave

Na początku tego roku firma Hanwha Techwin wprowadziła do oferty zupełnie nowe oprogramowanie WiseNet Wave do zarządzania systemami dozoru wizyjnego i kontroli dostępu.
Łatwość i intuicyjność obsługi oraz niezwykła wydajność to najistotniejsze cechy nowego oprogramowania. Jako jeden z pierwszych na świecie producentów systemów zabezpieczeń Hanwha Techwin wprowadza wsparcie swoich produktów nie tylko dla systemu Windows, ale również Apple/Mac oraz Linux. Zdecydowanie zwiększa to elastyczność użytkowania oprogramowania i pozwala na pełne dopasowanie do potrzeb klienta bez konieczności inwestycji w nowy sprzęt komputerowy.
Swobodnie konfigurowalne widoki z kamer na ekranie o dowolnym podziale (z możliwością zmiany wielkości każdego pola), obracania pól o dowolny kąt, wirtualne wektorowe sterowanie PTZ oraz integracja z funkcjami analityki obrazu to kolejne użyteczne funkcje. Istotne jest także wsparcie dla nowych kamer wieloprzetwornikowych, a także urządzeń innych wiodących producentów kamer IP oraz systemów kontroli dostępu.
Funkcjonalność WiseNet Wave uzupełniają takie funkcje jak rejestracja strumieni, technologia serwerów awaryjnych *failover* i współpraca z urządzeniami mobilnymi. Istotnymi atutami nowego oprogramowania są także możliwość pracy w chmurze oraz wbudowany system autodiagnostyczny.

PCX46 APP

Pyronix
HIKVISION

Hybrydowy system alarmowy z aplikacją

Adaptowalny, funkcjonalny i pełen cech

PCX 46 APP jest profesjonalnym rozwiązaniem wysokiej klasy bezpieczeństwa z komunikacją IP. Przewodowe i bezprzewodowe, dwukierunkowe akcesoria powodują, że instalacja jest szybka i łatwa, a wszystko z obsługą przez aplikację HomeControl+, dającą użytkownikom pełną kontrolę nad ich systemem z dowolnego miejsca świata!

www.facebook.com/pyronix @pyronix Dołącz do nas na LinkedIn

Hikvision Poland, The Park, Office Building A Krakowiaków 50, 02-255 Warsaw
Tel: +48 22 460 01 50 E-Mail: info.pl@hikvision.com Website: www.pyronix.com

Kamera Turbo HD 4.0 z czujką PIR

Hikvision
www.hikvisionpoland.pl

Aby podnieść poziom bezpieczeństwa, firma Hikvision poszerza portfolio kamer analogowych o modele Turbo HD 4.0 z technologią PIR.
Poza podstawową funkcją, czyli dozorem wizyjnym, kamera udostępnia funkcję alarmowania – czujka PIR wspomaga detekcję ruchu.
Czujka PIR, czyli pasywna czujka podczerwieni, pozwala na niezawodne wykrycie ruchu intruza, nie reagując na ruch przedmiotów na wietrze czy zmieniające się oświetlenie, co zmniejsza możliwość powstawania fałszywych alarmów. Filtrowanie fałszywych alarmów pozwala nie tylko ograniczyć zapotrzebowanie na przestrzeń dyskową, ale też ułatwia przeszukiwanie według zdarzeń zarejestrowanego materiału wideo.
Kamery z wbudowaną czujką PIR o zasięgu 11 m będą dostępne w obudowie bullet, dome i cube (modele DS-2CExxD8T-PIR [L]). Ponadto dzięki technologii *Ultra Low-Light* dostarczają wysokiej jakości obraz nawet przy minimalnym oświetleniu 0,005 lx. Ponadto kamera w momencie alarmu włącza oświetlacz światła białego, dzięki czemu można uzyskać jeszcze bardziej szczegółowy obraz i łatwiej zidentyfikować potencjalnego przestępcę.
Kamery Turbo HD 4.0 z czujką PIR mają szeroki zakres zastosowań, dozorują m.in. prywatne posesje, punkty sprzedaży detalicznej czy inne obiekty – porty lotnicze i morskie, przejścia graniczne, przemysł, które wymagają stałego dozoru, a także w aplikacjach, w których koszt jest istotnym elementem.

Eagle Eye = bezpieczny monitoring w chmurze

Linc Polska
www.linc.pl

Eagle Eye to portal umożliwiający bezpieczne zarządzanie kamerami w chmurze. Dostęp do obrazu na żywo i nagrań jest możliwy w każdej chwili przez aplikację mobilną (Android i iOS) lub przeglądarkę internetową. Jednym kliknięciem można w dowolnym momencie dodać kamerę i ustawić czas przechowywania nagrań. Należność za korzystanie z portalu jest naliczana w formie opłaty miesięcznej, więc płaci się tylko za to, czego faktycznie się używa i potrzebuje.
Eagle Eye jest prosty w konfiguracji i współpracuje z większością popularnych modeli kamer. Nie wymaga instalacji dodatkowego oprogramowania, kluczy licencyjnych ani systemu operacyjnego.
Monitorowany obiekt można obserwować zdalnie z dowolnego miejsca na świecie o dowolnej porze (365/7/24). Wdrożenie w aplikacji mobilnej identyfikatora biometrycznego linii papilarnych *Apple Touch ID* minimalizuje ryzyko logowania osób trzecich. Po otrzymaniu wiadomości e-mail z powiadomieniem o ruchu otrzymuje się link do obrazu wraz z sygnaturą czasową danego wydarzenia. Za pomocą jednego kliknięcia można obejrzeć nagranie wideo. Łącząc rozproszone miejsca instalacji kamer, można łatwo odtworzyć widoki z kilku lokalizacji (pogrupować je) i uzyskać z nich podgląd. Kolory ikon (zielony i czerwony) pokazują stan działania kamery, co ułatwia zarządzanie systemem.
Eagle Eye z dowolną kamerą stanowią stabilny i bezpieczny system monitoringu wizyjnego w chmurze, z gwarancją cyberbezpieczeństwa i maksymalną elastycznością w wyborze kamer i ich lokalizacji.

TL-SG1005P i TL-SF1005P 5-portowe przełączniki PoE firmy TP-Link

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

TP-Link powiększyło portfolio przełączników PoE o dwa kolejne modele. TL-SG1005P oraz TL-SF1005P to wydajne i oszczędne urządzenia służące do budowy mniejszych sieci, dzięki którym można zasilić punkty dostępowe, kamery monitoringu wizyjnego, telefony IP lub inne urządzenia korzystające z technologii *Power over Ethernet* (PoE).
Model TL-SG1005P wyposażono w 5 portów RJ45 o prędkościach 10/100/1000 Mb/s, niewymagających konfiguracji. Cztery z nich obsługują funkcję PoE.
Przełącznik TL-SF1005P ma 5 portów RJ45 o prędkości 10/100Mb/s, które również nie wymagają konfiguracji, 4 z nich obsługują funkcję PoE.
Najważniejsze cechy i funkcje nowych przełączników:
- 5 portów, w tym 4 porty PoE zgodne ze standardami IEEE 802.3af,
- funkcja priorytetowania, dzięki której zabezpieczają system w momentach przeciążenia,
- łączna moc zasilania PoE:
  modelu TL-SG1005P – 56 W;
  modelu TL-SF1005P – 58 W,
- kompaktowe wymiary,
- metalowa obudowa,
- 5 lat gwarancji.

Przełączniki TL-SG1005P oraz TL-SF1005P to urządzenia proste w instalacji i obsłudze. Dzięki niezawodności i zapewnieniu wysokiej jakości transmisji 5-portowe przełączniki z czterema portami PoE stanowią idealne rozwiązanie stosowane do rozbudowy sieci domowej lub biurowej.

ViDiLine®

Wideodomofon IP

w najniższej cenie w Europie

Łączność bezprzewodowa | Zasilanie PoE | Integracja z kamerami IP | Łączność przewodowa

Genway
ul. Chopina 37, Płock
tel.: +48 24 264 77 33
e-mail: info@genway.pl

ViDiLine®

www.c5.genway.pl

* Szczegóły u naszych handlowców pod numerem telefonu: +48 24 264 77 33.

RYNEK SECURITY W POLSCE

Podsumowanie roku 2017

Wzrosty i spadki, przejęcia i fuzje, nowe produkty i innowacyjne technologie...
Jaki był miniony rok i czego spodziewamy się w 2018 r.? Zapytaliśmy o to przedstawicieli najważniejszych firm na polskim rynku security.

Joanna Skalbaniok

prezes
Assa Abloy Polska

Początek roku to w ASSA ABLOY czas podsumowań i okres, w którym wyznaczamy sobie nowe cele i zadania. Niewątpliwie poprzednie miesiące były dla naszej firmy bardzo dobre, sprawdziły się bowiem przewidywania zarządu zawarte w ubiegłorocznej prognozie biznesowej. Podobne rokowania dla rozwoju ASSA ABLOY obowiązują również w odniesieniu do 2018 r.

Miniony rok upłynął w naszej firmie pod znakiem intensywnej pracy, a wszystko za sprawą wprowadzania na rynek nowych, innowacyjnych rozwiązań. W 2017 r. na naszym rynku zadebiutował m.in. zamek ENTR, którego premiera odbiła się w mediach i branży szerokim echem. Wystartowaliśmy także z nowym projektem dla marki Yale, jakim jest platforma Smart Living. To seria domowych urządzeń bezpieczeństwa, które pomagają chronić, monitorować i kontrolować dom w dowolnym miejscu i czasie za pośrednictwem urządzeń mobilnych. W jej skład wchodzą m.in. systemy alarmowe, elektroniczne wizjery czy inteligentne zamki elektroniczne i biometryczne.

Na 2018 r. zaplanowaliśmy zakrojoną na dużą skalę kampanię promującą nowe rozwiązanie marki Yale. Ogromna popularyzacja urządzeń cyfrowych ze zdalną kontrolą dostępu to główny czynnik stojący za powstaniem platformy Yale Smart Living. Przeprowadzone na zlecenie ASSA ABLOY badania pokazują, że rynek rozwiązań *smart* jest rozwojowy. Z urządzeń mobilnych korzysta dziś 9% światowej populacji. Zgodnie z prognozami w 2019 r. odsetek ten wzrośnie do 12%, a trend będzie się umacniał. Tym, co skłania klientów do wyboru nowoczesnych technologii zabezpieczających, jest m.in. łatwa ich instalacja, niewątpliwy komfort i oczywiście zwiększone poczucie bezpieczeństwa.

Podsumowując poprzedni rok, warto także wspomnieć o stale rozwijającym się centrum badawczo-rozwojowym

Jakub Kozak

dyrektor sprzedaży w Polsce i krajach bałtyckich
Axis Communications

w Krakowie. Kilkudziesięciu inżynierów pracuje tam nad nowymi rozwiązaniami z zakresu elektromechanicznych systemów zabezpieczeń i kontroli dostępu.
Nie zamierzamy zwalniać tempa. Jednym z projektów zaplanowanych na nowy rok jest przebudowa naszej warszawskiej siedziby oraz uruchomienie pierwszego w Polsce *showroomu* ASSA ABLOY. W nadchodzących miesiącach będziemy się skupiać na spożytkowaniu tendencji rynkowych, wykorzystaniu swoich mocnych stron, stałym rozwijaniu oferty produktowej i umacnianiu stabilności firmy.
Ogromnym sukcesem, jakim możemy pochwalić się wraz z nowym rokiem, jest przejęcie firmy LOB S.A. Włączenie spółki do ASSA ABLOY jest podyktowane przede wszystkim koniecznością stałego umacniania wysokiej pozycji na rynku i dążeniem do jeszcze większej dywersyfikacji oferty produktowej. To także element długofalowej strategii polegającej na stałym zwiększaniu zaangażowania na rynkach wschodzących.

Po serii kilku lat dynamicznego wzrostu w 2017 r. poprzeczka została postawiona niezwykle wysoko. Oczekiwania Axisa wobec rynku polskiego były bardzo duże i w znacznej mierze zostały one spełnione. Szczególnie pozytywna okazała się druga połowa roku, kiedy zauważalny był wzrost w obszarze budownictwa i projektów finansowanych ze środków publicznych.
Największym sukcesem firmy w 2017 r. było umocnienie pozycji firmy Axis jako lidera w zakresie systemów dozoru wizyjnego dla obiektów infrastruktury krytycznej i obiektów przemysłowych. Kilku strategicznych klientów zdecydowało się na pełną standaryzację swoich rozwiązań zabezpieczeń technicznych opartych na rozwiązaniach naszej firmy.
Obecnie w branży zabezpieczeń możemy wyróżnić dwa trendy: komodyzację i erozję cen. Kamera w coraz większym stopniu staje się przedmiotem użytku codziennego, a jednocześnie w zastosowaniach profesjonalnych wymogi wobec systemów dozorowych pozostają bardzo wysokie. W związku z tym jednym z największych wyzwań 2017 r. stanowiło uświadomienie klientom, że za jakość warto płacić. Karty katalogowe z suchymi parametrami technicznymi nie odzwierciedlają prawdziwej jakości produktów.
Rok 2017 był kolejnym rokiem silnej polaryzacji rynku, na którym tworzy się coraz głębszy podział pomiędzy kamerami z najniższej półki sprzedawanymi w dużych ilościach a kamerami profesjonalnymi sprzedawanymi w ramach rozbudowanych projektów.
W roku 2018 przewidujemy dalszy dynamiczny wzrost i rozwój firmy na rynku polskim, czego odzwierciedleniem jest otwarcie nowego biura. Nowa siedziba ma być z założenia miejscem licznych spotkań. Wiemy, jak istotne jest edukowanie partnerów, dlatego nasze nowe miejsce zostało wyposażone w salę szkoleniową. Aby móc sprostać rosnącej liczbie pytań o wypożyczenia naszych produktów, przygotowaliśmy bogato wyposażony magazyn urządzeń demo.
Bardzo dobrze oceniamy perspektywy rozwoju rynku polskiego. Uważamy, że doskonała jakość produktów, doświadczenie i wiedza oraz klarowne zasady współpracy zawsze się obronią i będą podstawą do dalszego rozwoju. Chcemy dalej rozbudowywać portfolio produktów zarówno w zakresie kamer sieciowych, jak i produktów, które w ofercie Axisa pojawiły się stosunkowo niedawno, takich jak urządzenia kontrola dostępu, głośniki sieciowe, radary czy wideodomofony.
Jeśli chodzi o kierunki rozwoju przewidywane w roku 2018 na światowym rynku bezpieczeństwa, możemy wyróżnić dwa trendy ostatnich lat, które na stałe zagościły w powszechnej świadomości – chmury obliczeniowe (*cloud computing*) i Internet Rzeczy (*Internet of Things*, IoT). Oprócz niezaprzeczalnych korzyści przyniosły poważne implikacje: ogromny wzrost ilości danych przesyłanych z podłączonych urządzeń w celu ich przetwarzania i przechowywania, co z kolei wymaga coraz większej przepustowości łączy. Naszym zdaniem rozwiązaniem problemu jest *Edge computing* – przesunięcie przetwarzania danych na obrzeża sieci jak najbliżej źródła: danych. Znacząco zmniejsza to wymaganą przepustowość między urządzeniami a centrum danych. Trend ten wiąże się również z potencjalnymi obawami związanymi z ochroną i prywatnością danych: anonimizacja i szyfrowanie przesyłanych danych w urządzeniach peryferyjnych, zanim zostaną one przekazane dalej, to prawdopodobna odpowiedź na te obawy.
Pomimo przechodzenia do przetwarzania w urządzeniach brzegowych przetwarzanie w chmurze nadal będzie odgrywać znaczącą rolę w infrastrukturze IT. A jedną z zalet integracji pomiędzy chmurami jest znaczna redukcja wymaganych wewnętrznych usług IT. Co więcej, dzięki *cloud computing* można w efektywny sposób łączyć i wdrażać zaawansowane usługi

»

» od wielu dostawców za pomocą funkcji API, takich jak analityka danych, zarządzanie treściami i ich przechowywanie. Pozwala to skrócić czas wprowadzania produktów na rynek i szybko zwiększyć skalę prowadzonych działań. Wskazałbym również cyberbezpieczeństwo jako trend na najbliższych 12 miesięcy. Ciągłe doskonalenie sposobów ochrony urządzeń i usług sieciowych to niekończące się zadanie, a cyberprzestępcy dysponują odpowiednimi zasobami i wciąż próbują wynajdować i eksplorować luki w zabezpieczeniach.

Krzysztof Góra

dyrektor handlowy
Bosch Security Systems

Rok 2017 stanowił duże wyzwanie dla firm, które większość swoich działań sprzedażowych koncentrują na dużych projektach. Głównym powodem takiej sytuacji była nie najlepsza kondycja rynku budowlanego oraz mniejsza liczba inwestycji publicznych. Rynek budowlany zanotował dwucyfrowe spadki w roku 2016, a negatywna tendencja odwróciła się dopiero od drugiego kwartału 2017. Wzrosty rynku budowlanego ze względu na przesunięcie cyklu inwestycyjnego były dla branży safety & security odczuwalne dopiero w ostatnim kwartale 2017 r. Było to jednak ożywienie na tyle znaczące, że pozwoliło większości dużych graczy rynku projektowego odrobić straty z pierwszych trzech kwartałów roku.

W przypadku Bosch Security Systems dzięki projektom niezwiązanym bezpośrednio z kondycją rynku budowlanego wchodziliśmy w ostatni kwartał z satysfakcjonującym wynikiem a ostatnie trzy miesiące roku dodatkowo wsparte sprzyjającą koniunkturą pozwoliły na przekroczenie ambitnych planów sprzedaży.

Ubiegły rok to w Bosch Security Systems również kluczowe zmiany organizacyjne związane z rozszerzeniem regionu, jakim zarządzamy z Warszawy, o kolejny kraj: Ukrainę. Obsługa rynku znajdującego się poza Unią Europejską wymagała przeorganizowania procesów logistycznych i sprzedażowych.

Musieliśmy również zmienić zakres odpowiedzialności części członków polskiego zespołu tak, aby lepiej wspierać kolegów za wschodnią granicą. Wprawdzie zmiana ta weszła w życie od stycznia 2018 r., ale przygotowania do niej trwały od połowy 2017 r., czyli w okresie, w którym proces reorganizacji musieliśmy połączyć ze wzmożonymi działaniami sprzedażowymi.

Niemniej udało nam się pomyślnie sfinalizować proces reorganizacji bez uszczerbku dla codziennych zadań. W ramach podsumowań chciałbym tradycyjnie nawiązać również do tematyki wprowadzania na rynek nowych, innowacyjnych technologii wyznaczających trendy rozwoju branży. Sukcesy na tym polu dają wiele satysfakcji. W 2017 roku wyznaczyliśmy nowe standardy w zakresie systemów sygnalizacji pożarowej dzięki wykorzystaniu inteligentnej analizy obrazu, która do tej pory była zarezerwowana dla telewizji dozorowej. Takim właśnie rozwiązaniem jest AVIOTEC – pierwsza na rynku kamera, która bez fałszywych alarmów wykrywa pożar już w kilka sekund od jego powstania dzięki możliwości automatycznego rozpoznania dymu lub płomienia.

Mamy za sobą już pierwsze udane wdrożenia. Rośnie grono zadowolonych klientów, którzy wyrażają entuzjastyczne opinie na temat tego rozwiązania i rekomendują je innym użytkownikom. Tak było chociażby w przypadku Grupy EDF Polska.

Bieżący rok oraz najbliższe lata przyniosą sporo strategicznych zmian w Bosch Security Systems pod względem rozwoju portfolio produktów i obecności firmy w wybranych segmentach rynku. Mam tu na myśli procesy globalne i znając ich szczegóły mogę z całą pewnością stwierdzić, że firma zmieni się w większości kluczowych aspektów swojej działalności. O szczegółach nowych strategii będziemy sukcesywnie informować rynek. Z perspektywy naszego regionu będziemy mieli natomiast okazję sprawdzić skuteczność organizacji sprzedażowej w obsłudze 4 krajów: Polski, Czech, Słowacji i Ukrainy. Dla nas rok zapowiada się bardzo ciekawie, rynek budowlany rośnie, wkrótce dostawcy odczują lub już odczuwają ten pozytywny trend. Pewnym wyzwaniem dla generalnych wykonawców i firm instalacyjnych może być jednak znalezienie wykwalifikowanych pracowników oraz realizowanie zakontraktowanych już zamówień wg stawek, które w momencie ich negocjacji nie uwzględniały rosnących płac i cen materiałów.

Artur Hejdysz

prezes
C&C Partners

Rok 2017 był to dla nas rokiem pełnym wyzwań, jednak zakończył się bardzo dobrym wynikiem finansowym. Zaowocował pozytywnymi tematami w zakresie systemów zabezpieczeń.

Naszą domeną staje się głównie software. To element przewagi, jaką konsekwentnie budujemy, wykorzystując doświadczenia i zasoby firmy-córki C&C Technology zajmującej się pisaniem oprogramowania. Dzięki temu udaje się nam dopasowywać do potrzeb klienta. A przecież w obszarze infrastrukturalnym każdy projekt – w mniejszym lub większym stopniu – jest dostosowywany indywidualnie do klienta. Posiadamy też doświadczony zespół wdrożeniowy, który wspomaga naszych integratorów i instalatorów w procesie finalnego programowania systemów. Jeśli trzeba jeszcze głębiej ingerować w software, korzystając z zasobów C&C Technology, możemy modyfikować i integrować go z systemami firm trzecich.

Jednym z największych osiągnięć ubiegłego roku była realizacja inwestycji parkingowych. Dużym sukcesem firmy było wdrożenie i uruchomienie systemu Park Assist na pierwszych trzech parkingach. Łącznie nadzorujemy ponad 10 tys. miejsc parkingowych w Galerii Północnej w Warszawie, Galerii Jurajskiej w Częstochowie i Galerii Wroclavia we Wrocławiu. Powodzeniem zakończyły się wszystkie wdrożenia, dzisiaj klienci galerii w pełni mogą korzystać z inteligentnego systemu wskazywania miejsc parkingowych, aplikacji wyszukiwania swojego samochodu czy stałego monitorowania auta na miejscu parkingowym.

Wszystkie wymienione lokalizacje parkingowe są w pełni wyposażone w systemy zabezpieczeń, które również dostarczyliśmy.

Szybkie zmiany technologiczne i rynkowe wymuszają na nas ciągłe utrzymanie wysokiej pozycji. Szybko dostosowywaliśmy się do niezwykle dynamicznych zmian, jakie następowały na rynku zarówno w technologii, jak i w sposobie działania firm. Wykorzystaliśmy moment, potrafiliśmy wykreować pewne modele działania na nowo, opracowaliśmy wzory, w jaki sposób z danymi produktami powinno się działać na rynku. Sukcesem jest także fakt, że jesteśmy prekursorem pod względem technologicznym, ponieważ dostarczane przez nas rozwiązania częstokroć były nowe na rynku. Jednocześnie wybieraliśmy drogę działania, która pozwala nam w sposób partnerski budować relacje z klientami i wzajemnie się wspierać w tych inwestycjach, które realizujemy.

W minionym roku mogliśmy zaobserwować wynikający z rozwoju technologii trend dowodzący tego, że klienci przestają traktować systemy zabezpieczeń wyłącznie jako zbiór podłączonych urządzeń i oprogramowania, a zaczęli postrzegać bezpieczeństwo jako usługę zdalnego i profesjonalnego dozoru wizyjnego. Dominowała zasada oferowania indywidualnie dopasowanych kompleksowych systemów rozwiązujących konkretne problemy klientów zamiast sięgania po uniwersalne zestawy sprzętowe lub oprogramowanie.

Plany firmy na 2018 r.? Chcemy czerpać wiedzę od naszych zachodnich partnerów i wykorzystywać zaawansowane technologie, które często wyprzedzają możliwości technologii na rynku polskim. Wyzwaniem jest też rozwijanie zespołu inżynieryjnego, który daje przewagę we wszystkich realizowanych projektach.

W tym roku podjęliśmy już takie działania, weryfikując z naszymi partnerami i dostawcami możliwość rozszerzenia współpracy. Patrzymy na kraje na południe od Polski, ale wierzymy też w potencjał biznesowy Ukrainy. Liczę, że w ciągu 3–4 lat około ¼ biznesu firmy będzie stanowiła sprzedaż za granicą, ale mam też nadzieję, że wzrośnie wartość globalna sprzedawanych przez nas rozwiązań.

W tym roku aktualnym trendem będzie cyberbezpieczeństwo. Z całą pewnością będą miały miejsce kolejne ataki, dlatego tak ważne jest zwrócenie uwagi na pochodzenie produktów wykorzystywanych do instalacji systemów zabezpieczeń.

Andrzej Jarzyna

Sales and Operations Director
CCE & Nordic
Dahua Technology Poland

Styczeń zawsze był dla mnie czasem refleksji nad tym, co w minionym roku udało się osiągnąć, a co nadal pozostaje w sferze planów. Co należy kontynuować, a co wypadałoby udoskonalić. W każdym biznesie taki przegląd jest jak najbardziej wskazany, powiedziałbym nawet, że niezbędny. Wiadomo, ważne są cele, ale aby je osiągnąć, trzeba umieć znaleźć słabe punkty i dokonać usprawnień.

Zaczynając rok 2017, chcieliśmy przede wszystkim zbudować silny zespół, skutecznie wprowadzić markę Dahua Technology na rynek, by w drugiej połowie roku osiągnąć pozycję najważniejszego gracza na polskim rynku w obszarze telewizji dozorowej.

Cel pierwszy – budowa silnego zespołu – udało nam się zrealizować bardzo sprawnie i nadspodziewanie szybko. Dzięki temu, że przedsięwzięcie pod nazwą Dahua Technology Poland było uruchamiane przez grupę pasjonatów z olbrzymim doświadczeniem w branży, wiedzieliśmy, czego chcemy i kogo potrzebujemy do takiego zespołu. Dzięki naszym pierwszym działaniom jeszcze w 2016 r. pokazaliśmy, że jesteśmy otwarci na utalentowane jednostki, dla których ambitne wyzwania to cel sam w sobie. W drugim ruchu postawiliśmy na rekrutację młodszego pokolenia, osób niekoniecznie z doświadczeniem w branży, ale z otwartymi głowami i nowymi pomysłami, aby nasz projekt nie zamknął się w szklanej kuli własnego świata.

Skupiamy wokół siebie ludzi ambitnych i nastawionych na realizację zadań, potrafiących pracować pod presją czasu, nie zawsze w standardowych warunkach, a przede wszystkim pracować w grupie, dzieląc się wiedzą i doświadczeniem. Nasz zespół to sprawnie działająca mieszanka dwóch kultur. Połączenie doświadczenia rynkowego i produkcyjnego z młodością i nieszablonowymi pomysłami.

Mając taki zespół, łatwiej nam poszło z drugim zadaniem. Wiedzieliśmy, że są dostępne różne produkty i rozwiązania, a rynek potrzebuje wiedzy, jak to wszystko wdrożyć i osiągnąć sukces. Instalatorzy regularnie wskazywali, że są głodni szkoleń łączących wiedzę praktyczną z prezentacją możliwości sprzętu. Wszyscy nasi rozmówcy jasno dawali do zrozumienia, że szkolenia dla certyfikatów (tylko) wyczerpały swoją formułę i oni chcą czegoś więcej. Seria prezentacji *Starlightshow* opracowana przez Mateusza Zapotocznego razem z Arturem Prusinowskim i Karolem Narojczykiem była odpowiedzią na te potrzeby. Prezentacje odbywały się w każdym większym mieście w całym kraju. W drugim etapie ruszyliśmy z cyklem warsztatów w naszej siedzibie. W sumie przeszkoliliśmy ponad 3 tys. osób. Jako nasz olbrzymi sukces traktuję to, że większość uczestników zostawała do końca czy to prezentacji, czy też warsztatów. Bardzo często nawet godzinę po zakończeniu części prezentacyjnej wciąż odpowiadaliśmy na liczne pytania uczestników. Warsztaty często kończyły się w późnych godzinach wieczornych i to na życzenie uczestników, którzy chcieli maksymalnie wykorzystać ten czas.

Równolegle z częścią szkoleniową aktywnie braliśmy udział w seminariach i konferencjach przygotowanych przez instytucje branżowe. Byliśmy obecni na *Warsaw Security Summit,* dwukrotnie prezentowaliśmy naszą ofertę podczas SPIN, byliśmy na targach kolejowych, targach ochrony granic, konferencjach poświęconych więziennictwu, rozwojowi małych miast i gmin oraz wielu innych. Przekazaliśmy wiedzę na temat naszych rozwiązań olbrzymiej liczbie uczestników rynku. Nie bez znaczenia była też nasza aktywność w mediach społecznościowych i program lojalnościowy *The Best Program of Dahua.* Cieszę się, że duża liczba instalatorów utrzymuje z nami bezpośredni kontakt za jego pośrednictwem.

Niezależnie od działań kreujących zapotrzebowanie na produkt zajęliśmy się organizacją sieci dystrybucyjnej. Postawiliśmy na bardzo proste, a zarazem uniwersalne wartości, niezależnie od miejsca na świecie: na przewidywalność i zaufanie. Chcieliśmy, aby przekaz dla rynku był spójny i obejmował wszystkie aspekty działalności. Prostota przekazu, tradycyjne wartości, zaufanie, propagacja wiedzy – to wszystko sprawiło, że Dahua Technology stała się wiodącą marką na rynku.

Pozostaje ocena, czy staliśmy się najważniejszym graczem na rynku polskim, czy nie. Moim zdaniem to bardziej kwestia oceny samego rynku. Według naszych danych w najgorszym wypadku zajmujemy współdzielone pierwsze miejsce.

Co dalej? Rok 2017 był dla nas udany, ale nie możemy spocząć na laurach. Przed nami kolejne wyzwania, a i konkurencja nie śpi. Jesteśmy młodą organizacją i wiemy, co musimy usprawniać. Pokazaliśmy zalety produktów, teraz przyszedł czas na promowanie rozwiązań, a jest co promować. Nasza lista wdrożeń jest imponująca: system *smart city* w Hangzhou z zastosowaniem 20 tys. kamer czy rozwiązania na potrzeby igrzysk w Rio de Janeiro mówią same za siebie.

Nadal nasza oferta w Polsce nie obejmuje całości bogatej oferty Dahua

Technology. Na wdrożenie czeka cały obszar *smart home*, systemy alarmowe, kontrola dostępu, wiele rozwiązań z obszaru *display & control.* Centrala stale przekazuje nam informacje o różnych nowościach, które mogą sporo namieszać na rynku. Jest co robić, a mamy olbrzymi potencjał rozwojowy. Jedno jest pewne, nasz silny i ambitny zespół chce kontynuować wzrost na rynku polskim i jestem przekonany, że tego dokona, a rok 2018 w polskiej branży security będzie rokiem Dahua.

Rok 2017 był dla Hanwha Techwin Europe wyjątkowy pod wieloma względami. Wprowadziliśmy do oferty ponad 100 nowych produktów, przeprowadziliśmy wiele zmian w strukturze firmy, byliśmy obecni na wszystkich istotnych wydarzeniach branżowych w Polsce i Europie, a nasz serwis centralny w Holandii może być wzorem dla pozostałych firm w branży. Również wyjątkowa aktywność w zakresie szkoleń i prezentacji została bardzo wysoko oceniona przez klientów, którym serdecznie dziękujemy.

Ubiegły rok był niewątpliwie pasmem sukcesów Hanwha Techwin. Wśród ponad 100 nowych produktów wprowadziliśmy do oferty długo oczekiwaną serię kamer WiseNet X, następcę doskonale znanego WiseNet III. Udostępnienie 5-letniej gwarancji na wszystkie produkty IP dla partnerów naszego programu STEP oraz dynamiczny wzrost uczestników tego programu to kolejny duży sukces. Całość doskonale uzupełnia uzyskanie prestiżowego certyfikatu bezpieczeństwa cybernetycznego *Cyber Essentials.* Potwierdza to słuszność strategii najwyższej dbałości o bezpieczeństwo sprzętu i oprogramowania. Największym sukcesem są niewątpliwie doskonałe opinie klientów po międzynarodowej konferencji *WiseNet* w Barcelonie, lokalnej edycji *WiseNet STAR* i tournée *WiseNet Roadshow*. Napawają nas dumą i ogromnym optymizmem, dającym jeszcze więcej energii do kolejnych działań.

Nie ma jednak biznesu bez wyzwań. Największe z nich to migracja marki Samsung Security do marki WiseNet, a także rosnący dynamicznie udział chińskich producentów w polskim i europejskim rynku zabezpieczeń technicznych. Systematyczne i przemyślane działania planowania produktowego, utrzymanie najwyższej jakości, doskonały serwis i dobre działania marketingowe pozwoliły nam wyjść z tych trudnych zadań w doskonałej formie.

Jeśli chodzi o rynek w Polsce, można zauważyć kilka jasnych trendów, które są głównie konsekwencją dynamicznego rozwoju nowych technologii. Ogromny wzrost zainteresowania szeroko rozumianą sztuczną inteligencją, sieci neuronowe, systemy *deep learning* i zaawansowana analityka obrazu to najbardziej widoczny nurt tych zmian. Nowe życie technologii analogowej w postaci wyższych rozdzielczości systemów AHD, dalszy rozwój systemów kompresji H.265 i rozdzielczości 4K uzupełniają krótkie podsumowanie roku 2017. Wszystkie te nowości mogliśmy na żywo podziwiać m.in. na *Warsaw Security Summit*. Należą się słowa uznania i gratulacje dla „a&s Polska" za organizację chyba pierwszej tego typu i o takim rozmachu imprezy branżowej w Polsce.

Na bieżący rok patrzymy z dużym optymizmem. Blisko 100 kolejnych nowych produktów, systemy *deep learning,* nowe oprogramowanie WiseNet Wave, zupełnie nowa odsłona doskonale znanego oprogramowania WiseNet SSM, nieznane dotychczas na rynku polskim innowacyjne rozwiązania zaawansowanej analityki obrazu dla rynku transportowego czy dalszy rozwój programu partnerskiego STEP i systemu ochrony projektów to tylko drobny fragment naszych planów na 2018. Patrząc na polski rynek security, rysuje się tu kilka ważnych scenariuszy: wejście w życie regulacji RODO w maju z pewnością wymusi wiele zmian w podejściu do jakości systemów zabezpieczeń technicznych, a nie tylko ich ceny. Miejmy też nadzieję, że wróci do planów legislacyjnych długo oczekiwana tzw. ustawa o monitoringu wizyjnym. Zapewne nastąpi dalszy dynamiczny rozwój sztucznej inteligencji, *deep learning* itp. Jeśli chodzi o zagrożenia – przy doskonałych obecnie wskaźnikach ekonomicznych nie spodziewam się raczej kłopotów natury gospodarczej, jednak postępująca erozja cenowa rynku na skutek działań producentów z Chin może być wkrótce poważnym wyzwaniem dla całej branży w Polsce.

Piotr Rogalewski

Senior Pre-Sales & Technical Manager Poland & Baltics
Hanwha Techwin Europe

Tomasz Migdał

General Manager
Hikvision Poland

Rok 2017 był dla Hikvision Poland rokiem wytężonej pracy, która finalnie przyniosła oczekiwane rezultaty, czyli zrealizowanie większości założeń biznesowych. Przede wszystkim udało nam się solidnie zwiększyć udział w polskim rynku zabezpieczeń, w szczególności w obszarze telewizji dozorowej. To było również nasze największe wyzwanie z uwagi na bardzo aktywne działania konkurencji. Widać jednak wyraźnie, że pracując wspólnie ramię w ramię z dystrybutorami i integratorami, szczególnie tymi, którzy skoncentrowali się na współpracy z Hikvision, można realizować nawet bardzo ambitne plany. W roku 2018 chcemy nadal wraz z nimi się rozwijać i umacniać pozycję lidera, konsekwentnie realizując nasze strategiczne plany.

Wyraźnym trendem, który można było zauważyć w zeszłym roku na polskim rynku ochrony, był spory wzrost zainteresowania technicznymi systemami zabezpieczeń w ochronie obiektów z powodu zwiększenia kosztów ochrony fizycznej. Rozwój w tym segmencie będzie następował i przede wszystkim wykorzystanie tzw. zdalnego dozoru wizyjnego (stosowanie transmisji obrazów z chronionych obiektów do weryfikacji zdarzeń i podjęcia działań prewencyjnych) stanie się powszechne. Ułatwiają to spadek cen kamer i rejestratorów, nowe, bardziej efektywne metody kompresji obrazu (np. opracowany przez Hikvision kodek H265+), znacznie większa dostępność łączy cyfrowych do transmisji danych oraz dostępność dedykowanego oprogramowania do dozoru wizyjnego.

W obszarze projektowym coraz częściej wykorzystuje się kamery termowizyjne i zoptymalizowaną analizę obrazu w systemach ochrony obwodowej. Trend rozwojowy ma również integracja wszystkich systemów zabezpieczeń obiektowych.

Bardzo dużą szansę rozwoju branży widzimy w praktycznym zastosowaniu sztucznej inteligencji (AI) opartej m.in. na algorytmach *deep learning* (tzw. głębokiego uczenia). Hikvision inwestuje w rozwój technologii sztucznej inteligencji konsekwentnie od 2006 r. Dzięki temu w 2017 r. mogliśmy zaprezentować pełną ofertę produktów wykorzystujących tę technologię. Co warte podkreślenia, rozwiązanie to potrafi działać w strukturze rozproszonej, obejmującej przetwarzanie w obszarze zarówno chmury obliczeniowej, jak i tzw. *Edge computing* (czyli na poziomie urządzeń brzegowych). Dzięki temu rozbudowany zbiór instrukcji AI z poziomu chmury obliczeniowej jest wykorzystywany w sieciach lokalnych rejestratorów i serwerów, a także dalej – w urządzeniach brzegowych, takich jak kamery dozorowe i na odwrót. Ta trójwarstwowa architektura tworzy aplikację AI najnowszej generacji, jeszcze bardziej inteligentną, skuteczniejszą i znacznie szybszą.

Rok 2017 był kolejnym, w którym działania pracowników ochrony fizycznej coraz częściej wspierały rozwiązania techniczne. Zauważyliśmy, że coraz częściej klienci do zabezpieczenia swoich obiektów wybierają techniczne systemy zabezpieczeń. Ten trend był już wyraźnie dostrzegalny w roku 2016, a w ubiegłym przybrał na sile. Konsekwencją zmiany oczekiwań klientów jest dostosowanie do nich oferty firm działających w szeroko rozumianej branży zabezpieczeń. Warto zauważyć, jak szybko nastąpiła adaptacja do nowych warunków rynkowych. Naszym zadaniem jest wspieranie klientów, zarówno w realizacji ich potrzeb szkoleniowych, jak i dostarczaniu najnowocześniejszych rozwiązań technicznych, które umożliwią realizację nawet najbardziej złożonych projektów.

Od lat koncentrujemy się na wizyjnych systemach dozorowych oraz na systemach ochrony perymetrycznej. Ostatnio wzrosła popularność sprzedaży usług polegających na zdalnej wideoweryfikacji lub wirtualnych obchodach. Dla naszej firmy oznacza to olbrzymie możliwości rozwoju. Jesteśmy przekonani,

Ubiegły rok przyniósł nam wiele wyzwań i sukcesów. Ważnym aspektem dla polskiego oddziału Nedap było powiększenie zespołu. Wprowadziliśmy program współpracy z projektantami instalacji niskoprądowych. Uruchomiliśmy serię spotkań i szkoleń, dzięki którym przeszkoliliśmy wiele firm projektowych.

Rok 2017 obfitował w wyzwania w zakresie utrzymania bezpieczeństwa systemów informatycznych i security w wielu firmach. Pojawiły się spektakularne cyberataki (m.in. Petya, WannaCry), które sparaliżowały działanie wielkich organizacji. Cyberbezpieczeństwo stało się bardzo ważną kwestią, coraz więcej naszych klientów zaczęło zwracać uwagę na poziom zabezpieczenia systemu kontroli dostępu, począwszy od poziomu bezpieczeństwa technologii kartowej, skończywszy na zaawansowanych rozwiązaniach cy-

że w mijającym roku szanse te wykorzystaliśmy bardzo dobrze. Oznacza to również umocnienie na polskim rynku pozycji marek, które reprezentujemy.
Zrealizowaliśmy wraz z naszymi partnerami wiele projektów opartych na kamerach termowizyjnych FLIR. Coraz częściej nasi klienci doceniają niezawodność termowizji, w szczególności w połączeniu z analizą wizyjną. Kamery termowizyjne dają wyższą skuteczność detekcji nawet odległych obiektów, przy niskim poziomie fałszywych alarmów.
Dzięki kamerom MOBOTIX pomogliśmy wielu naszym klientom stworzyć bardzo nowoczesne systemy monitoringu wizyjnego. MOBOTIX to produkty, które można integrować z wieloma systemami, dzięki temu uzyskujemy bardzo kompleksowe i intuicyjne w obsłudze rozwiązania. Użytkownicy doceniają także jakość obrazu, wysoki poziom zabezpieczeń i długą ich żywotność.
Wiele firm z branży ochrony fizycznej wspierała swoich pracowników rozwiązaniami technicznymi. Dla tego segmentu rynku oferowaliśmy przede wszystkim rozwiązania marki ADPRO oraz HeiTel by Xtralis, pozwalające na świadczenie usług zdalnego dozoru wizyjnego w połączeniu z zaawansowaną analizą wideo. To pozwoliło nam także na dalsze zacieśnianie współpracy z firmami ochrony.
Patrząc na rok 2018 pierwszym istotnym wydarzeniem w kalendarzu będą zapewne targi SECUREX. Zaprezentujemy na nich wiele innowacyjnych rozwiązań. Nowościami wprowadzonymi do naszej oferty są między innymi radary różnego zasięgu oraz światłowodowy system ochrony perymetrycznej FFT. W kolejnych miesiącach na pewno skupimy się na zorganizowaniu szkoleń technicznych dla naszych klientów oraz wspieraniu ich w realizacji kolejnych projektów. Kolejnym wyzwaniem, które postawiliśmy sobie na ten rok jest rozwój oddziału warszawskiego, którego tworzenie już rozpoczęliśmy. Pozwoli to nam na bardziej elastyczne działanie na terenie całego kraju. Zapewne w roku 2018 na znaczeniu będzie zyskiwać cyberbezpieczeństwo oraz wykorzystanie analizy wideo w systemach zabezpieczenia technicznego. Podobnie jak w latach ubiegłych, współpracując z naszymi dostawcami, na te właśnie zagadnienia będziemy kłaść duży nacisk. Będzie to zatem dla nas zupełnie naturalny kierunek rozwoju. Sądzimy, że rynek wizyjnych systemów zabezpieczeń będzie nadal rozwijał się dynamicznie. Biorąc pod uwagę to, że od ponad 20 lat działamy w tej branży, pozytywnie patrzymy w przyszłość, robiąc to, w czym jesteśmy najlepsi i w czym się specjalizujemy.

Jakub Sobek

certyfikowany trener techniczny,
Linc Polska

bersecurity, umożliwiających zastosowanie pełnego rozwiązania *End to End Security.*
Następnym silnym trendem, który zaobserwowaliśmy w 2017 r., jest udział urządzeń mobilnych w systemach zabezpieczeń. Zastąpienie karty smartfonem, aplikacjami mobilnymi do zarządzania automatyką budynkową, wykorzystanie kodów QR do awizacji gości to tylko przykłady wykorzystania nowych technologii. Kolejnym trendem, który rozwija się dynamicznie, jest wykorzystanie biometrii w systemach kontroli dostępu i coraz bardziej zaawansowane metody autoryzacji. Mnogość różnych systemów (SKD, CCTV, SSWiN) sprawia, że klienci poszukują otwartych systemów, które zapewniają ich integrację. Zmieniają się zagrożenia i w związku z tym system musi mieć możliwość szybkiego dostosowania się do nowych wymagań. System kontroli dostępu, który jako inwestycja długoterminowa jest rozwiązaniem przyszłościowym, musi być odpowiedzią na zmieniające się zagrożenia. Ponieważ nasz system bazuje na otwartej platformie, klienci mają pewność, że dzięki AEOS nadal będą dysponować nowoczesnym systemem i mieć możliwość odpowiedzi na różne rodzaje ryzyka w przyszłości.
Na kolejny rok patrzymy z optymizmem. Zamierzamy otworzyć nowe, większe biuro w Warszawie. Zakładamy utrzymanie obecnych trendów w rozwoju. Zarówno w Polsce, jak i w całej Unii Europejskiej od maja zaczną obowiązywać przepisy europejskiego rozporządzenia o ochronie danych osobowych (RODO). Regulacja wprowadza duże zmiany w zakresie zarządzania danymi osobowymi przetwarzanymi przez firmy. Zmiany te będą miały duży wpływ na zarządzanie systemami *security.*

Anna Twardowska

Country Manager
Nedap Security Management

Optex, największy na świecie producent czujek zewnętrznych, pozytywnie ocenia wyniki w roku 2017. Firma cieszy się ze wzrostu sprzedaży swoich urządzeń. W 2018 roku otwiera się na nowy segment produktów. Ponadto przygotowuje swoje rozwiązania z wykorzystaniem technologii IoT.

Za największy sukces w roku 2017 uważamy pozytywną odpowiedź klientów na promowane przez nas od lat rozwiązania służące łatwej integracji czujek zewnętrznych do systemów bezprzewodowych innych producentów. Cieszymy się z zaufania do naszej marki wśród instalatorów i dystrybutorów.
Oddział Optex w Polsce odpowiada także za działania w innych krajach Europy Środkowo-Wschodniej. Dlatego też dużym wyzwaniem było wzmocnienie obecności OPTEX w Rumunii i Bułgarii. Wiemy, jak ogromne znaczenie ma lokalne wsparcie techniczne, więc z przyjemnością powitaliśmy w zespole nowego kolegę z Bukaresztu.
Zauważyliśmy wpływ zwiększenia płacy minimalnej na rynek zabezpieczeń elektronicznych, co wyraża się w inwestowaniu wielu klientów w rozwiązania lepszej jakości.
Trendem, który rozwijaliśmy w roku 2017, była integracja istniejących systemów w taki sposób, aby wspierać pracę operatora. Dużą w tym rolę odgrywa analityka wizyjna, ale informacje rynkowe mówią także o powrocie do sprawdzonych rozwiązań detekcji intruza z wykorzystaniem czujek ruchu. W obiektach o wyższym poziomie zabezpieczenia od fałszywych alarmów ważniejsza jest pewność, że zostaną wykryte wszystkie próby wejścia na chroniony teren. Połączenie dwóch technologii – wideo i czujek ruchu – zwiększa wiarygodność systemu.
W roku 2018 firma skupi się na promocji czujek zewnętrznych serii Shield. W produktach z tej linii niezawodna detekcja oraz rozwiązania ułatwiające instalację łączą się z nowoczesnym wzornictwem. Współpraca z uznanym biurem projektowym Ziba zaowocowała produktami, które trafiają w gust właścicieli domów i rezydencji.
Wyzwaniem będzie na pewno otwarcie nowego segmentu produktów – czujników przeznaczonych do systemów bram, garaży i parkingów. Jest to rozwiązanie spełniające podobną funkcję jak pętla indukcyjna, ale po-

Grzegorz Ćwiek

prezes
Schrack Seconet Polska

Lata 2015-2017 to najlepszy okres w historii naszej firmy nie tylko w Polsce, ale i na świecie.

Skupiając się jednak na rynku krajowym, ostatni rok można podsumować jako kolejny, najlepszy w historii, tak pod względem wyników sprzedażowych (znowu zwiększyliśmy udział w rynku), jak i rozwoju osobowego (do naszego grona dołączyło kilku nowych specjalistów), czy technologicznego (wprowadziliśmy szereg nowych rozwiązań technicznych).
Jak zwykle na początku roku dokonujemy rozmaitych podsumowań, tworzymy rozbudowane statystyki podjętych przedsięwzięć i omawiamy te kwestie razem z kolegami i koleżankami z innych krajów. Na początku stycznia 2018 roku, kiedy spotkaliśmy się w Wiedniu, na takim właśnie krótkim podsumowaniu dominowały niezwykle pozytywne emocje i coś, co nazwałbym potocznie: delikatnym „luzem". Wszyscy zajęci byli bardziej dyskusjami o planach wyjazdów na narty i ferie z dziećmi niż zwyczajowym, suchym dyskutowaniem o problemach rynkowych. Co ważne, rozmowy także u nas, w zespole polskim miały bardzo podobny charakter. Nawet narzekanie na konkurencję ;) ma dzisiaj nieco inny wymiar niż jeszcze kilka lat temu.
Sposób naszej pracy na rynku (jesteśmy tu już ponad 30 lat!) nabiera innego wymiaru. Zdajemy sobie coraz większą sprawę z wartości dodanej, jaką Schrack Seconet oferuje w Polsce, oraz dobrych i stabilnych rezultatów, jakie ta praca przynosi. Jeżeli polity-

zbawione kłopotów związanych z jej instalacją i konserwacją.
Firma Optex rozwija współpracę z największymi na świecie producentami systemów dozoru wizyjnego, jak Hikvision, Axis, Bosch, Milestone, ela-soft czy Genetec. W porównaniu do innych rynków udział projektów wykorzystujących czujki ruchu z komunikacją Ethernet jest w Polsce wciąż niewielki.
Jaka przyszłość stoi przed rynkiem security w Polsce? To, o czym niektórzy wspominali (także na łamach „a&s Polska") – CYBERBEZPIECZEŃSTWO. Wkrótce możemy oczekiwać większego zainteresowania ze strony użytkowników i projektantów sposobami unikania ataków hakerskich. Ponadto konkurencja globalnych firm na rynku lokalnym może przynieść sytuację podobną do rynku konsumenckiego – bardziej wydajne technologie będą w cenie rozwiązań poprzedniej generacji.
Polska „broni się" przed IoT. Uważam, że w niedalekiej przyszłości trzeba będzie pogodzić się z tym, że w systemach zabezpieczeń dla mniej wymagających obiektów rolę centrum zarządzającego będzie grała „chmura". Rozwiązanie, w którym czujka ruchu zasilana bateryjnie wyśle sygnał alarmowy poprzez publiczną sieć (np. sigfox), znacznie ułatwi instalację systemu alarmowego chroniącego np. uprawy… W krótszej perspektywie przyniesie ograniczanie udziału ochrony fizycznej na rzecz rozwiązań elektronicznych.
Miniony rok oceniam bardzo dobrze. Cele sprzedażowe zrealizowaliśmy z nawiązką, a jeszcze bardziej cieszy mnie fakt, że sukces jest widoczny we wszystkich grupach produktów – począwszy od czujek laserowych REDSCAN, skończywszy na najprostszych czujkach wewnętrznych serii RX Core. Przyczyniły się do tego zaangażowanie partnerów handlowych oraz stabilny kurs euro.

Jacek Wójcik

dyrektor zarządzający, Europa Środkowa i Wschodnia
Optex Security

cy nie popsują nam naszego podwórka (mówię głównie o klimacie dla inwestycji), możemy na nim pracować dalej przez wiele lat i cieszyć się dynamicznym rozwojem.
Za największy sukces firmy uznałbym możliwość niepowstrzymanego rozwoju mimo pojawiających się trudności na rynku budowlanym. Niekorzystne dla nieco słabszych firm zmiany w zasadach regulowania VAT oraz niedostatek wykwalifikowanej kadry przyczyniły się do spowolnienia realizacji projektów lub ich przesunięcia w czasie. Jak wiemy, rynek budowlany w Polsce jest najbardziej ryzykownym rynkiem dla działalności gospodarczej i niewielkie zmiany w skali makroekonomicznej wywierają poważny wpływ na branżę, pośrednio także naszą. Poradziliśmy sobie świetnie, nie tylko utrzymując dobrą pozycję rynkową, ale także zwiększyliśmy sprzedaż i zaangażowanie w najważniejszych projektach w kraju. Rok 2018 zapowiada się jeszcze bardziej obiecująco.
Największym wyzwaniem dla nas, jak i dla wszystkich producentów, wykonawców czy inwestorów w naszej branży będzie kontynuowanie pracy nad dobrym, wspólnym językiem komunikacji i zrównoważonym procesem współpracy. Branża budowlana boryka się z problemami kadrowymi, rosnącymi kosztami pracy i spadającymi marżami. Umowy podpisane 2 lata temu tracą rentowność w szybkim tempie, a ryzyko kontraktów rośnie; jedyną szansą dla wielu mniej odpowiedzialnych firm budowlanych wydaje się „wyciśnięcie" jak najniższych cen z dostawców lub producentów, zamiana rozwiązań technicznych z poprawnych na jak najprostsze i niekoniecznie właściwe technicznie dla danego typu projektu (ale tańsze). To z kolei odbijać się może w dłuższym okresie na jakości budowanych obiektów, bezpieczeństwie przebywających w nich ludzi i uderza w inwestorów – to dalej będziemy starali się tłumaczyć i czemu nadal będziemy się aktywnie przeciwstawiać.
Wszystkie strony procesu budowlanego muszą zdawać sobie sprawę z tego, że koszt inwestycji, jej przygotowania (architekci, projektanci), wykonania (generalni wykonawcy, wykonawcy branżowi, dostawcy, producenci) i późniejszego utrzymania (firmy serwisowe, obsługa techniczna itd.) nie może spadać; zamiast tego będzie rósł i udział poszczególnych stron procesu należy rozumieć i wyceniać rozsądnie, uczciwie, pozwalając tym samym na rozwój kadr i technologii.
Rok 2017 był pod tym względem nerwowy i był kolejnym, w którym ry-

»

» nek oczyszczał się z firm o słabszej kondycji finansowej i niższej jakości produktów i pracy. Czekamy na czas, kiedy praca na naszym rynku będzie bardziej przewidywalna, a walka konkurencyjna uczciwa, bardziej ekscytująca i mniej emocjonalna (oczywiście w tym negatywnym znaczeniu). Nadal obserwujemy szereg nieetycznych zachowań i nieuczciwych działań, które szkodzą całej branży i kreują złe nawyki wśród młodej kadry wchodzących na ten rynek specjalistów. Kreowanie nowych nawyków pracy na naszym rynku powinno być wyzwaniem dla nas wszystkich, a podstawą w tym zakresie jest dobry poziom edukacji. Tym będziemy się także nadal zajmowali.

W Schrack Seconet już wiele lat temu przeszliśmy do innego sposobu prezentacji rozwiązań i uświadamiania użytkowników w zakresie ich potrzeb sprzętowych, technologicznych, organizacyjnych. Będziemy mieli w tym roku możliwość zaprezentowania oferty na targach *Securex* w Poznaniu. Wielu producentów z naszej branży nie będzie obecnych, jednak my mamy zbyt wiele do pokazania, by nie skorzystać z tej okazji. Jesienią zorganizujemy także nasz sztandarowy projekt edukacyjny: *Ogólnopolskie Dni Zintegrowanych Systemów Bezpieczeństwa*, gdzie znowu wystąpimy z naszymi partnerami oraz gronem wybitnych specjalistów i ekspertów. Będziemy promowali nasze systemy bezpieczeństwa pożarowego, dźwiękowe systemy ostrzegawcze i rozwiązania integracyjne. Planujemy także szkolenia regionalne. Niemal każdego miesiąca będziemy w innym mieście, a do tego, przypomnę, prowadzimy szkolenia w naszych pięciu siedzibach regionalnych.

Nasza działalność w pełni odpowiada trendom rynkowym: największe zapotrzebowanie i uwaga rynku kierowane będą na systemy zintegrowane, o wysokiej elastyczności działania i odporności na nowe zagrożenia: płynące z cyberprzestrzeni, zachowań ludzkich (terroryzm i akty przemocy), katastrof naturalnych oraz zakłóceń w łańcuchu dostaw. Cieszę się, że działając w naszej branży, dla każdego z tych kluczowych zagrożeń możemy przedstawić dobre rozwiązanie technologiczne i organizacyjne.

Rok 2018 to przede wszystkim rok celebracji 20-lecia działalności naszej spółki prawa polskiego: Schrack Seconet Polska Spółka z o.o. Przypomnę, że Schrack Seconet działa w naszym kraju od połowy lat 90.

Robert Stanosz

Business Development Manager
Vivotek

Rok 2017 dla Vivotek w Polsce możemy uznać za udany. Choć silna deflacja średniej ceny systemu jest widoczna za sprawą wyniszczającego wyścigu do „dna ceny", to sprzedaż naszych produktów wzrosła.

Minionych dwanaście miesięcy spędziliśmy na intensywnej pracy i kontaktach ze współpracującymi z nami partnerami. Wdrożona przez nas strategia przyniosła wzmocnienie kanału sprzedaży dzięki silnemu wsparciu projektowemu i ochronie marży kanału sprzedażowego.

Równocześnie oferta Vivotek została uzupełniona o oczekiwane przez instalatorów małe, budżetowe produkty telewizji dozorowej. Segment kamer na rynek profesjonalny i projektowy wzbogaciliśmy o zaawansowane kamery H.265 *fisheye* i obrotowe ze zmiennoogniskowymi oświetlaczami IR. W tym roku nadal skupimy się na pracy z projektami i firmami poszukującymi marżowych i specjalizowanych produktów.

Międzynarodowe Targi Poznańskie

Nadchodzą cyborgi

Czy staniesz się jednym z nich?

Systemy kontroli dostępu zapewniają użytkownikom dostęp do budynków i pomieszczeń na podstawie autoryzacji i środków identyfikacji (kart, kodów PIN, numerów rejestracyjnych, smartfonów). Środki te stanowią zatem interfejs pomiędzy człowiekiem a systemem. Nie zapewniają jednak 100-procentowej pewności co do tego, kto stoi przed drzwiami, bo przecież karty lub kody PIN można przekazać innym.

Błażej Ożga

Należy szukać metod, które wypełnią lukę w interfejsie pomiędzy człowiekiem a systemem. Trzeba znaleźć metodę, która będzie bezbłędnie identyfikować ludzi w systemie, by uprawnionym osobom zapewniać dostęp do odpowiednich budynków, pomieszczeń i danych. Być może jedno z rozwiązań kryje się w świecie cyborgów.

Co to jest cyborg?

Po raz pierwszy określenie „cyborg" pojawiło się w latach 60. XX wieku i oznaczało osobę, która przebywała w przestrzeni pozaziemskiej, w szczególności w sztucznym dla niej środowisku. Dopiero w latach 90., przede wszystkim dzięki popkulturze, nabrało ono znaczenia znanego do dziś. Wyszukiwanie hasła „cyborg" przynosi różne definicje, wszystkie mają wspólny mianownik: cyborg to fizyczne połączenie człowieka i maszyny.

Naturalnie temat ten jest bogatym źródłem inspiracji dla scenarzystów filmów *science fiction*, a nam natychmiast przychodzą na myśl postacie przypominające RoboCopa.

Już teraz jednak funkcjonuje wśród nas wiele osób odpowiadających definicji cyborga. W ścisłym ujęciu osoby z rozrusznikiem serca również są cyborgami. Podobnie do tej kategorii można zaliczyć ludzi z protezami lub innymi pomocami technicznymi. Nagle słowo „cyborg" brzmi znacznie mniej przerażająco, a świat cyborgów wykracza poza filmy fantastycznonaukowe.

Tematyką cyborgów zajmują się badacze z różnych dziedzin. Prowadzą oni badania w obszarze medycyny, ale także nad możliwościami wykorzystywania cyborgów do innych celów. Kevin Warwick, profesor cybernetyki uniwersytetu w Reading, znany jako „kapitan cyborg", postawił sobie za cel ulepszanie ludzi, by w przyszłości byli oni w stanie (nadal) konkurować z robotami i maszynami. Już w 1998 r. wszczepił sobie w rękę implant RFID, którym sterował oświetleniem w swoim gabinecie. Warwick robi to nie dla zabawy. Jak mówi, *nie chcę być robotem, chcę być lepszym człowiekiem*. Zdanie to brzmi dość intrygująco, lecz trzeba postawić pytanie o granicę ingerencji w ciało ludzkie elementów obcych.

Przeglądając materiały dotyczące prac prowadzonych w tym obszarze, można dojść do wniosku, iż jeszcze jej nie wyznaczono. Amerykańska Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności DARPA prowadzi badania nad stworzeniem dwukierunkowego interfejsu mózg – komputer, który mógłby być wykorzystany w stworzeniu żołnierza przyszłości, dysponującego zdolnościami nadludzkimi. Takie rozwiązania, jak BCI *(Brain – Computer Interface*), nie są nowością, ponieważ już w 1924 r. udało się nagrać ludzką aktywność mózgu za pomocą elektroencefalografu (EEG). Jednak to dopiero teraz nauka będzie umożliwiała badaczom opracowanie wysoko zaawansowanych technologii działających w tym obszarze.

Naukowcy stworzyli już interfejs dwukierunkowy umożliwiający sterowanie ręką oraz odczuwanie dotyku. Co więcej, specjaliści z uniwersytetu w Arizonie opracowali interfejs wykorzystujący 128 elektrod umożliwiających człowiekowi w czasie rzeczywistym sterowanie wieloma dronami. *W tej chwili możemy dekodować proste czynności, takie jak zamknięcie i otwarcie dłoni czy też podniesienie łokcia, lecz nie jesteśmy w stanie dekodować bardziej złożonych zachowań* – powiedział prowadzący badania prof. Panagiotis Artemiadis.

Multimiliarder Elon Musk z kolei jest przekonany, że ludzie będą musieli stać się cyborgami, aby stawić czoło przyszłości zdominowanej przez sztuczną inteligencję. *Jeśli ludzie chcą dalej zwiększać wartość gospodarki, muszą zwiększyć swoje możliwości poprzez połączenie inteligencji biologicznej z inteligencją maszyny. Jeśli tego nie zrobimy, ryzykujemy, że staniemy się dla sztucznej inteligencji domowymi kotami* – stwierdził w jednym z wywiadów.

Prowadzone badania oraz wizje przypominają raczej wspomniane wcześniej filmy *science fiction,* ale czy na pewno? Sprawdźmy, jak to wygląda w przypadku identyfikacji w systemach kontroli dostępu i logowania do komputerów.

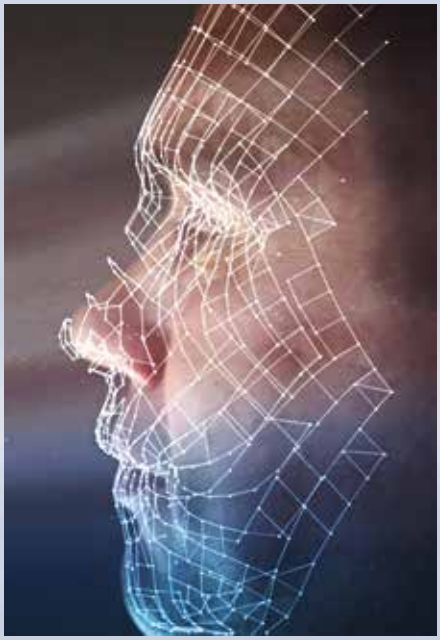
Czy cyborgi mogą być rozwiązaniem „problemu identyfikacji"?

W naszym życiu codziennym cyborgi stały się już faktem. Na całym świecie z rozrusznikiem serca żyje ponad 4 mln ludzi. Co roku liczba ta wzrasta o 700 tys. Dzięki miniaturyzacji w niedalekiej przyszłości będzie nawet możliwe wstrzykiwanie rozruszników osobom chorym. Taką technologię wdraża amerykański *start-up* Nanostim. Urządzenie opracowane przez tę organizację stanowi 10% wielkości klasycznego rozwiązania.

Chipy RFID

Czy badań nad cyborgami nie można wykorzystać do rozwiązania problemu identyfikacji? Skoro cyborg to fizyczne połączenie człowieka i maszyny, można wyposażyć ludzi w dodatkowe, unikalne cechy fizycznie związane z daną osobą, które mogą być stosowane przez komputery do jej identyfikacji. Innymi słowy, obecnie w systemach kontroli dostępu identyfikujemy się przy użyciu kart. A gdyby taka karta znajdowała się nie w portfelu, tylko w ciele? Realizacja tego w systemie kontroli dostępu jest bardzo prosta. Co więcej, za 99 dolarów można kupić zestaw „zrób to sam". Składa się on z chipa, igły i innych akcesoriów służących do samodzielnego wszczepienia znacznika NFC w dłoń.

Cyborg to fizyczne połączenie człowieka i maszyny. Ten temat jest bogatym źródłem inspiracji dla scenarzystów filmów *science fiction*, nam natychmiast przychodzą na myśl postacie przypominające RoboCopa.



Wszczepiliśmy sobie tag i co dalej?

Na rynku są dostępne co najmniej dwa modele tagów RFID, które można sobie samodzielnie wszczepić. Są to:

- tag 13,56 MHz ISO14443A wspierający NFC typ 2,
- tag 125 kHz ISO11784/785 ATA5577, kompatybilny z EM41xx oraz HID ProxCard II, umożliwiający klonowanie karty.

Chip NFC czy też obsługujący technologię 125 kHz można zaprogramować i używać go do różnych celów, np. otwierania drzwi lub logowania się do swojego komputera lub smartfonu bez konieczności wpisywania hasła. Wiele czytników obecnie dostępnych na rynku wspiera te technologie, więc nic nie stoi na przeszkodzie, aby budować systemy kontroli dostępu oparte na implantach.

Technologia BCI

A jeśli technologia BCI umożliwi w przyszłości zupełnie inną weryfikację lub identyfikację, np. zminiaturyzowane implanty stanowiące interfejs mózg – komputer (maszyna) potrafiące odczytywać aktywność mózgu w czasie rzeczywistym (podobnie jak EEG) albo urządzenia wysyłające odpowiednie sygnały wprost do kontrolera drzwi? Już dzisiaj jest to możliwe. W opracowaniu *Smart Brain Interaction Systems for Office Access and Control in Smart City* Ghada Al-Hudhud przedstawił kilka koncepcji sterowania za pomocą myśli urządzeniami znajdującymi się w naszym otoczeniu, w tym systemem kontroli dostępu [1]. W odróżnieniu od karty, czyli tego co mamy, czy też PIN-u, czyli tego co znamy, sterowanie mentalne jest czymś, czym jesteśmy. Podobnie jak biometryka, lecz z jedną zasadniczą różnicą – trudno wydobyć tę informację osobom trzecim mającym złe intencje.

Obecnie nie wydaje się to potrzebne, a konwencjonalne metody oferują na razie dostateczną funkcjonalność. Ale jedno jest pewne – interakcja pomiędzy ludźmi a maszynami będzie się zwiększać, jednocześnie kontrola sprawowana przez ludzi w trakcie takich interakcji będzie maleć. Kto dzisiaj ma jeszcze kontakt z pracownikiem banku, gdy wnioskuje o nową kartę płatniczą? Więcej interakcji z maszynami oznacza więcej haseł. Hasła trudno zapamiętać i raz za razem okazują się zawodne – albo na skutek ataków hakerów, albo przez ludzi, którzy wybierają słabe hasła.

Okazuje się bowiem, że ludzie wciąż używają tak prostych haseł jak: „123456”, „password”, „12345678”, „qwerty”, „12345”. Wymienione zwroty to pięć najbardziej popularnych haseł stosowanych przez miliony ludzi na całym świecie. Co musi się zmienić, abyśmy przywiązywali większą wagę do tego, jak silne hasło wybieramy do ochrony nie tylko naszej prywatności, ale również do zabezpieczenia naszego majątku?

A gdyby technologia cyborgów rozwiązała ten problem?

> Czy będziemy musieli stać się cyborgami, aby stawić czoło przyszłości zdominowanej przez sztuczną inteligencję? Jeśli tego nie zrobimy, ryzykujemy, że staniemy się dla sztucznej inteligencji domowymi kotami...

Zagrożenia

Wszczepianie chipów w celu pozbycia się kart dostępu jest krokiem drastycznym, wzbudzającym też zastrzeżenia praktyczne. Czy recepcjonistka wszczepi nowemu pracownikowi chip pierwszego dnia pracy? Co się stanie, gdy zmieni on pracę? Ponadto, podobnie jak w przypadku smartfonów, co roku pojawiają się nowe generacje chipów, więc czy co trzy lata trzeba będzie je aktualizować?

Kolejnym istotnym zagrożeniem jest cyberprzestępczość. Co może się stać, gdy okaże się, że noszone przez nas

w ciele urządzenia nie są bezpieczne? Badacze wykazali, że rozruszniki można zhakować. Amerykańska agencja FDA *(Food and Drug Administration)* oficjalnie przyznała, że niektóre modele tych urządzeń są podatne na działania hakerów. Osoby niepowołane mogą np. zdalnie rozładować baterię, wstrząsnąć pacjentem lub wyłączyć sygnał pobudzający pracę serca.

Co zatem w przypadku, gdy kolejny atak cybernetyczny nie będzie mieć na celu wyłączenia komputerów, lecz wyłączenie ludzi? Poza tym noszone przez nas chipy będzie można skanować w każdym miejscu i w każdym czasie. Z oczywistych względów nie będziemy w stanie ich zostawić w domu czy samochodzie, tak jak karty czy telefonu. Prowadzi to do pytań, jak ta technologia będzie mogła być wykorzystywana przez służby. Identyfikacją mogliby być zainteresowaniami również właściciele centrów handlowych, by otrzymywać szczegółowe informacje o klientach, np. kiedy przyszli, co kupili czy też jak długo stali przy półce z danym produktem. Wdrożenie tej wizji nie jest niemożliwe, wystarczy spojrzeć na rozwiązania przeznaczone do stosowania w magazynach, w których wykorzystuje się tagi RFID w celu monitorowania położenia danej paczki.

Istnieją też zastrzeżenia natury etycznej. Na razie mówi się o chipach, ale co się stanie, gdy badacz Kevin Warwick jednak będzie miał rację i będziemy mogli „robić aktualizację" ludzi? Czy właśnie tego chcemy? I czy ta możliwość będzie dostępna dla wszystkich, czy tylko dla osób z zasobnymi portfelami?

Inne możliwości

Oprócz badań nad cyborgami prowadzi się liczne badania nad wykorzystaniem cech biometrycznych do identyfikacji. Oczywiście otwieranie drzwi odciskiem palca jest mniej radykalne niż posiadanie technologii wszczepionej w ciało człowieka.

Elastyczność technologii będzie jednak rosnąć. Biometria może odegrać istotną rolę przy rozwiązaniu problemu identyfikacji. Jeśli jednak chcemy więcej, np. konkurować z robotami, być może będziemy musieli poszerzyć swoje horyzonty.

Czy wszyscy dostaną chipy?

Obecna metoda polegająca na wszczepieniu niewielkiego chipu pomiędzy kciuk a palec wskazujący stanowi pierwszy krok. Badacze, tacy jak Kevin Warwick, spoglądają daleko w przód i badają szersze pole w obszarze technologii cyborgów. Na razie możliwości są ograniczone, a karty, hasła i kody PIN wystarczają. Gdy jednak technologia wszczepiana znacząco zwiększy naszą wydajność, przyspieszy to jej akceptację. Wiele osób na pewno będzie reagować negatywnie, tak jak początkowo pokaźna grupa reagowała nieprzychylnie na e-maile i bankowość internetową w smartfonach. Na początku też byłem powściągliwy w kwestii instalowania aplikacji bankowych, ale zmieniłem zdanie. To samo obserwujemy w innych krajach. Z danych Eurostatu wynika, iż w 2008 r. z bankowości online korzystało 29% Europejczyków. W 2016 r. odsetek ten wyniósł już 49%, przy czym średnią podnoszą w szczególności kraje północy i zachodu Europy. Polska plasuje się obecnie na 24. pozycji.

Gdy korzyści zaczną przeważać nad wątpliwościami, cyborgi – tak jak smartfony – mogą stać się nowym standardem. Zatem kto wie, być może wkrótce będziemy potwierdzać swoją tożsamość zwykłym uściskiem dłoni, a może posuniemy się znacznie dalej.

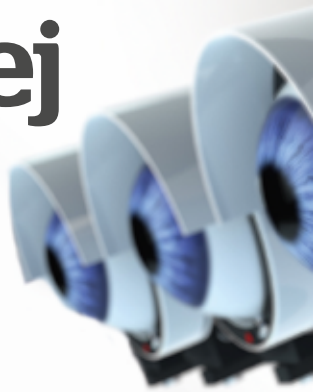
Literatura

[1] Ghada Al-Hudhud, *Smart Brain Interaction Systems for Office Access and Control in Smart City Context, Smart Cities Technologies*, 2016;
[2] Prof. Ivan Nunes Da Silva (Ed.), https://www.intechopen.com/books/smart-cities-technologies/smart-brain-interaction-systems-for-office-access-and-control-in-smart-city-context

BIO

Błażej Ożga
W branży security od ponad 12 lat, nie tylko jako specjalista, lecz również jako autor kilku innowacyjnych rozwiązań. W firmie Nedap Security Management odpowiedzialny za budowanie kanału wsparcia dla projektantów, architektów i konsultantów.

Sztuczna inteligencja w telewizji dozorowej



Systemy dozoru wizyjnego (VSS – *Video Surveillance System*) są dzisiaj najszybciej zmieniającym się segmentem w branży zabezpieczeń technicznych. Ze względu na coraz szersze zastosowanie kamer o wysokich rozdzielczościach budowanie coraz większych systemów VSS wiąże się ze znacznym zwiększeniem ilości danych związanych z prowadzonym dozorem wizyjnym.

Łukasz Lik

Gromadzenie, analiza i wykorzystanie danych z systemów dozorowych staje się coraz ważniejsze dla branży security. To właśnie ilość danych pozyskiwanych i przetwarzanych w systemach wizyjnych stała się motorem wprowadzania inteligentnych rozwiązań umożliwiających szybszą i skuteczniejszą ich analizę.

Użytkownicy systemów oczekują, że inwestycja w nowe produkty zapewni znacznie więcej niż tylko rejestracja obrazu, śledzenie obiektów czy zgrywanie materiału wizyjnego po zaistnieniu zdarzenia alarmowego. Od najnowszych technologii wymaga się m.in. ograniczenia siły roboczej i czasu potrzebnego na przeszukiwanie nagrań czy wykrywanie nieprawidłowych zachowań, a także stopniowego przechodzenia od alarmowania po wykryciu zdarzenia po alarmy w jego trakcie lub nawet przed incydentem. Zaspokojenie tych oczekiwań wymaga zaawansowanych technologii. Inteligentne funkcje analityki obrazu są dostępne od wielu lat, jednak wyniki ich zastosowania nie były idealne. Wprowadzenie technologii opartych na sztucznej inteligencji (AI), takich jak *deep learning* (głębokie uczenie) otwiera nowe, realne możliwości zastosowania analizy obrazu wideo.

Przewaga głębokiego uczenia

Funkcje zaprojektowane w tradycyjnych algorytmach analizy obrazu mogą być subiektywne. Bardziej abstrakcyjne cechy, które są trudne do opisania językiem programowania, często były pomijane. Dlatego algorytmy te dobrze działają w ściśle określonych środowiskach. Subtelne zmiany, takie jak jakość obrazu, gra świateł czy większa dynamika na scenie mogą powodować spadek dokładności rozpoznania. Czy jest zatem możliwe, by to maszyny wykrywały pewne „abstrakcyjne" cechy obiektu, pomocne w jego klasyfikacji i rozpoznaniu? Tak, jest możliwe! W rzeczywistości to właśnie cel sztucznej inteligencji.

> Głębokie uczenie symuluje strukturę mózgu człowieka, wykorzystując sztuczną sieć neuronową. Każdy sztuczny neuron to mały „program" połączony cyfrowo z innymi neuronami, tworząc kolejne warstwy.

Inspiracją dla technologii głębokiego uczenia jest budowa mózgu człowieka. Mózg można postrzegać jako bardzo złożony model głębokiego uczenia. Wielowarstwowa sieć neuronowa mózgu składa się z miliardów wzajemnie połączonych neuronów, a tych połączeń jest więcej niż neuronów. Głębokie uczenie symuluje tę strukturę, wykorzystując sztuczną sieć neuronową, w której każdy sztuczny neuron to mały „program" ściśle połączony cyfrowo z innymi neuronami, tworząc kolejne warstwy.

Podobnie jak w mózgu człowieka są obszary odpowiadające za pewne funkcje życiowe, tak w sztucznych sieciach neuronowych występują warstwy odpowiadające za określone zadania. Te wielowarstwowe sieci mogą zbierać informacje i wykonywać odpowiednie działania, przede wszystkim automatyczną ekstrakcję i reprezentację cech

(wzorców) występujących w danych uczących sieć, m.in. rozpoznawać twarze, marki pojazdów, gatunki zwierząt czy też zdarzenia, np. upadek.

Skąd ta „głębia"

Dzisiejsze algorytmy głębokiego uczenia mają bardzo złożoną strukturę. Czasami liczba warstw może przekraczać 100, co pozwala na przetwarzanie dużych ilości danych, np. w celu skomplikowanej klasyfikacji. Dane są analizowane warstwa po warstwie – im wyższy poziom warstwy, tym bardziej dostrzegane są szczegółowe cechy i analizowane od początkowego zrozumienia po dokładne rozpoznanie obiektu.

Głębokie uczenie jest oparte na algorytmie do samodzielnego wyodrębniania wzorców czy cech. W ten sposób jest w stanie wyodrębnić jak najwięcej elementów rozpoznawego celu, które są trudne lub niemożliwe do opisania. Posłużmy się krótkim przykładem. Powiedzmy, że kilkuletnie dziecko chcemy nauczyć, co to jest drzewo. Pokazujemy mu je w parku po kolei: dąb, buk, sosna. Gdy po pewnym czasie zapytamy, wskazując na świerk, co to takiego, otrzymamy odpowiedź – drzewo. Dziecko będzie później potrafiło rozpoznać ten obiekt na zdjęciu, kolorowance czy w filmie animowanym. W ten sam sposób działa technologia głębokiego uczenia.

Jedne z najbardziej bezpośrednich korzyści, jakie mogą zapewnić algorytmy głębokiego uczenia, to osiągnięcie porównywalnej lub nawet lepszej niż w przypadku człowieka dokładności rozpoznawania wzorców oraz możliwości klasyfikacji i rozpoznawania tysięcy cech.

Głębokie uczenie w systemach telewizji dozorowej

Technologie związane z głębokim uczeniem powoli wkraczają w codzienne życie – rozpoznawanie mowy w telefonach komórkowych czy pisma odręcznego itp. Pojawienie się tej technologii na rynku security było tylko kwestią czasu. Stosując algorytmy sztucznej inteligencji, można wzbogacić system telewizji dozorowej o takie funkcje analityki, jak rozpoznawanie twarzy, rozpoznawanie marek i typów pojazdów, wykrywanie cech ciała człowieka (np. płeć, wiek), analizowanie zachowania tłumu, śledzenie wielu celów jednocześnie itp.

Wszystkie inteligentne funkcje analizy obrazu wymagają odpowiednich urządzeń, począwszy od inteligentnych kamer, które w mniejszych aplikacjach mogą już same, bez użycia serwerów wykonywać zaawansowaną analizę. W dużych aplikacjach inteligentne kamery wstępną obróbką danych wspierają serwery, które dzięki temu mogą obsługiwać większą liczbę urządzeń.

Podsumowanie

Głębokie uczenie to kolejny poziom rozwoju sztucznej inteligencji. Nowe zaawansowane funkcje analityczne coraz częściej będą się pojawiać w systemach wizyjnego monitoringu miast czy budynków, usprawniając skuteczność i pracę całego systemu. Należy jednak pamiętać, iż integralnym i ciągle najważniejszym ich elementem jest człowiek. Dopiero perfekcyjna symbioza obu elementów: ludzkiego i technicznego zagwarantuje najwyższy poziom bezpieczeństwa.

BIO

Łukasz Lik
W branży zabezpieczeń od 7 lat, od 2014 r. w Hikvision Poland. Obecnie jest dyrektorem ds. technicznych. Specjalizuje się w projektowaniu i wdrożeniach systemów zabezpieczeń. Prowadzi liczne szkolenia techniczne.

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

10 trendów technologicznych roku 2018

Życie jest ciągłą zmianą – mawiał grecki filozof Heraklit. Potwierdzi to każdy, kto swoją pracę związał z technologią. Tempo wprowadzania innowacji technologicznych jest tak duże, że nawet najbardziej fantastyczna przyszłość może szybko przekształcić się w rzeczywistość.

Johan Paulsson
Axis Communications

Technologie osiągają swój kres, nieprzewidziane zdarzenia następują coraz szybciej, a innowacje przenoszą się z zastosowań konsumenckich do biznesowych (i odwrotnie), dlatego konieczne jest stałe poszukiwanie takich rozwiązań, które wnoszą nową wartość zarówno dla przedsiębiorców, jak i klientów. Oto najważniejsze naszym zdaniem trendy technologiczne, ktore będą miały wpływ na rozwój dozoru wizyjnego w 2018 r.

1 Większa rola urządzeń brzegowych

Z dwóch niezaprzeczalnych dobrodziejstw technologicznych ostatnich lat – chmury obliczeniowej i Internetu Rzeczy (*Internet of Things*) – korzystają odbiorcy biznesowi i indywidualni. Efektem popularności obu rozwiązań jest jednak znaczące zwiększenie ilości danych przesyłanych z dołączonych urządzeń do centrów danych w celu przetwarzania i przechowywania, co wymagana określonej przepustowości sieci. Odpowiedzią na to wyzwanie jest przetwarzanie w urządzeniu brzegowym (*Edge computing*) zapewniające obróbkę danych w sieciowym urządzeniu końcowym, czyli blisko źródła danych. Pozwala to odciążyć sieć, umożliwia też anonimizację i szyfrowanie danych przed przesłaniem do centrum danych, zapewniając integralny i prywatny charakter takich informacji. Ponieważ stopień zaawansowania i jakość kamer sieciowych, głośników i innych urządzeń brzegowych stale rośnie, konieczne jest zrównoważenie przetwarzania w chmurze i urządzeniu brzegowym, by dostarczane dane były precyzyjne, wiarygodne i użyteczne.

2 Chmura-chmura

Powszechność przetwarzania danych w urządzeniu brzegowym nie oznacza wyparcia z infrastruktury informatycznej chmury obliczeniowej. Określenie chmura obliczeniowa sugeruje strukturę pojedynczą, faktycznie jednak odnosi się do wielu chmur wykorzystywanych na całym świecie. Liczba firm oferujących usługi oparte na chmurze zwiększa się, dlatego ekosystemy chmur są coraz częściej stosowanym punktem integracji, w odróżnieniu od tradycyjnych systemów lokalnych.

Jedną z korzyści wynikających z integracji różnych chmur jest redukcja usług informatycznych świadczonych na miejscu. Inną jest możliwość tworzenia i wdrażania poprzez rozbudowane interfejsy API zaawansowanych usług od wielu dostawców, takich jak analiza danych, zarządzanie treścią oraz pamięcią masową, co przekłada się na szybszą implementację i skalowanie.

3 Uczenie głębokie i uczenie maszynowe

Osiągnęliśmy już poziom pozwalający na realizację korzyści płynących z architektury głębokiego uczenia (*deep learning architecture*) oraz uczenia maszynowego (*machine learning*). Mamy ogromne zbiory danych do analizy, wystarczającą moc obliczeniową do wykonania zadania w rozsądnym czasie, zaawansowane algorytmy oraz wiele przykładów użycia. Wykorzystując najlepsze aplikacje głębokiego uczenia do interpretacji obrazu, rozpoznawania mowy i wsparcia w podejmowaniu decyzji, dysponujemy potencjałem analitycznym do zastosowań w branży security, który może imponować.

Nawet na poziomie podstawowym aplikacje głębokiego uczenia pozwalają usprawnić wizyjną detekcję ruchu, rozpoznawanie twarzy (obszar, w którym czołową pozycję zajmuje firma Herta, partner Axis) oraz śledzenie obiektów. Pomagają też eliminować fałszywe alarmy. Wspomagają projektowanie, konfigurację, optymalizację oraz zarządzanie urządzeniami w systemie.

Wraz z rozwojem aplikacji pojawia się możliwość dokonywania analiz predykcyjnych służących zapobieganiu zdarzeniom, np. atakom terrorystycznym.

4 Personalizacja a prywatność

Jednym z zastosowań głębokiego uczenia może być dostarczanie wysoko spersonalizowanych usług. Wyobraźmy sobie galerię handlową, w której twarz klienta jest rozpoznawana tuż po wejściu do sklepu, i na podstawie wcześniejszych zakupów, preferencji czy nawet ostatnio oglądanych towarów na jego smartfon są kierowane oferty handlowe. Taka sytuacja jest możliwa, co nie oznacza, że powinna mieć miejsce. Paradoksalnie, uzmysławia ona raczej potrzebę zachowania prywatności w zderzeniu z niemal niekontrolowanym wykorzystaniem danych osobowych przez sektor komercyjny i rozmaite organizacje.

Trwają prace nad wprowadzeniem przepisów prawnych regulujących te kwestie. W Unii Europejskiej ogólne rozporządzenie o ochronie danych (*General Data Protection Regulation*) ma wejść w życie w maju 2018 r., by zunifikować ochronę danych obywateli niezależnie od miejsca oraz sposobu ich przechowywania i wykorzystania.

5 Cyberbezpieczeństwo

Tak jak w minionym roku, cyberbezpieczeństwo musiało pojawić się na liście trendów na rok bieżący i kolejne lata. Wzmacnianie bezpieczeństwa cybernetycznego pozostanie zadaniem w realizacji, ponieważ dobrze przygotowani cyberprzestępcy nie zaniechają prób wykorzystania luk w każdej nowej technologii. W związku z tym, że liczba pracujących w sieci urządzeń rośnie w postępie wykładniczym, wzrasta ryzyko wystąpienia błędów w oprogramowaniu, które należy nieustannie identyfikować i naprawiać.

Brak reakcji może skutkować włamaniem do sieci, zarażeniem szkodliwym oprogramowaniem typu *ransomware* czy wystąpieniem kosztownej awarii.

6 Platformy realizujące zalety IoT

W ramach Internetu Rzeczy (w aspekcie bezpieczeństwa) osiągnięto punkt, w którym efektywne skalowanie, zbieranie i analiza danych oraz skuteczne zarządzanie siecią urządzeń jest możliwe dzięki zastosowaniu skalowalnej architektury. Platformy IoT umożliwiają urządzeniom różnych producentów współpracę i sprawną wymianę informacji w celu utworzenia inteligentnych systemów przy użyciu istniejącej infrastruktury sieciowej.

Tych 10 istotnych trendów technologicznych wpłynie na rozwój dozoru wizyjnego w 2018 r. To jednak nasze przewidywania. Być może także inne kierunki rozwoju „uskrzydlą" naszą branżę?

7 Łańcuch bloków – więcej niż bitmoneta

Dla wielu łańcuch bloków (*blockchain*) i bitmoneta (*bitcoin*) oznaczają to samo.

W rzeczywistości są to dwa odrębne pojęcia. Transakcja z wykorzystaniem bitmonet musi zostać potwierdzona w łańcuchu bloków, którego potencjał weryfikacyjny jest tak naprawdę nieograniczony. Jest to otwarta, rozproszona platforma księgowa umożliwiająca efektywne, kontrolowane i ciągłe księgowanie transakcji pomiędzy dwoma podmiotami. W tym roku łańcuch bloków będzie testowany w licznych zastosowaniach w wielu sektorach.

W branży security, przy założeniu, że zapewnia uwierzytelnienie dowolnej treści, łańcuch bloków mógłby być zastosowany do weryfikacji treści wizyjnych z wielu źródeł, np. z kamer noszonych na odzieży funkcjonariuszy służb porządkowych na użytek postępowań sądowych. Ponadto mógłby posłużyć do autoryzacji urządzeń dołączonych do sieci kamer.

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

8 Przełamywanie barier inteligentnego miasta

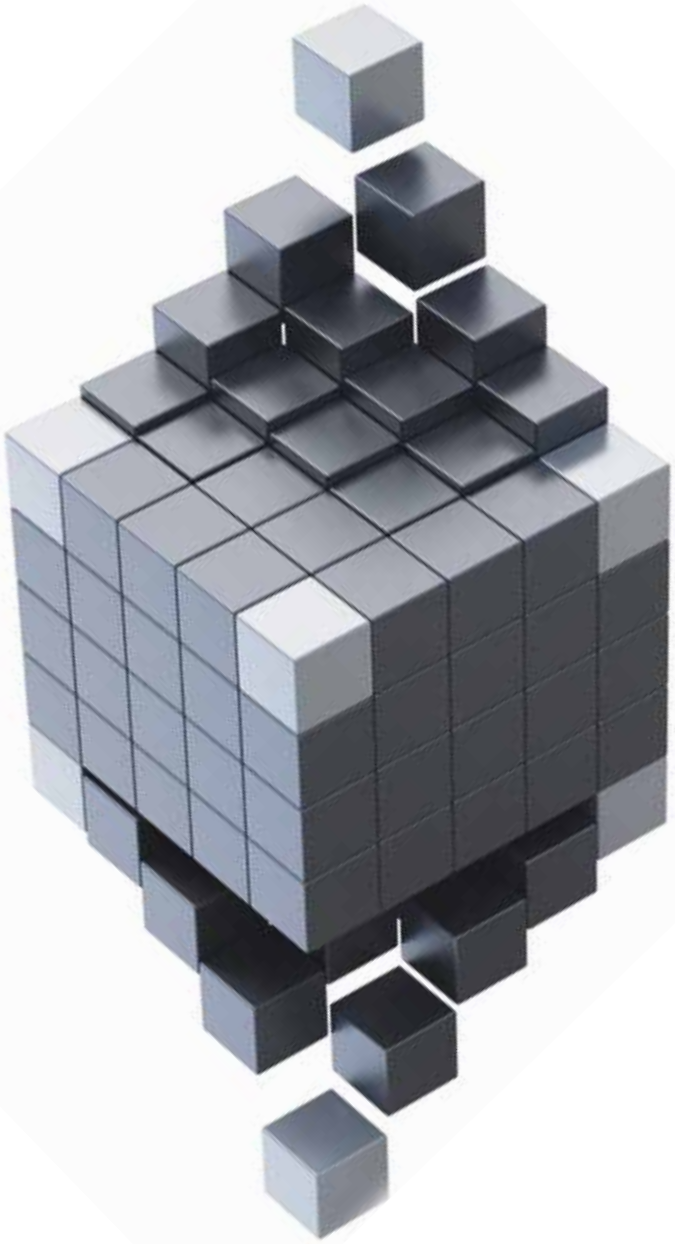
Koncepcja *smart city* nie jest nowa. Od kilku lat w przestrzeni miejskiej stosuje się coraz więcej różnego rodzaju czujników wspomagających rozwiązywanie problematycznych zdarzeń – od egzekwowania prawa po monitorowanie jakości powietrza. Ponieważ liczba mieszkańców miast na świecie stale rośnie (o 25% do 2050 r.), liczba czujników wspomagających tworzenie przyjaznego, zrównoważonego i bezpiecznego środowiska w mieście będzie się zwiększać.
Inteligentne miasto to wizja rozwoju skupiająca bezpieczne technologie informatyczne, technologie danych, komunikacyjne oraz IoT na potrzeby zarządzania majątkiem miasta. Większość części składowych majątku miasta działa indywidualnie, co stanowi barierę w wymianie informacji i utrudnia realizację koncepcji *smart city*.
Miasto jest inteligentne, gdy wszystkie dane są dostępne i możliwe do wykorzystania przez każdą z miejskich służb bądź jednostek. Skuteczne zarządzanie i radzenie sobie z takimi wyzwaniami, jak zapewnienie bezpieczeństwa mieszkańcom, przeciążenia w ruchu ulicznym, starzejąca się infrastruktura czy reakcje na zdarzenia w rodzaju katastrof naturalnych lub ataków terrorystycznych wymagają skoordynowanych analiz dostępnych danych, by dostarczyć odpowiednie i efektywne rozwiązania.

9 Nowy wymiar dzięki „czujnikom niewizyjnym”

Do tej pory podstawowe (o ile nie jedyne) dane dostępne operatorom systemów dozorowych stanowił obraz, który dostarcza, co oczywiste, jedynie perspektywę dwuwymiarową. Nowe „niewizyjne czujniki” pozwolą na uzyskanie widoku wielowymiarowego, dostarczając szereg danych umożliwiających szybszą i dokładniejszą ocenę sytuacji, a co za tym idzie szybszą reakcję, uruchomienie odpowiednich działań oraz minimalizację liczby fałszywych alarmów. Przykładowo technologia radarowa do wykrywania ruchu wykorzystuje fale elektromagnetyczne. Można też wymienić dobrze znane obrazowanie termowizyjne, a także detekcję dźwięku. Postęp w rozwoju tej drugiej technologii oznacza pozyskiwanie informacji, o które uboższe są źródła oparte jedynie na analizie obrazu.

10 Wirtualni asystenci i technologie rozszerzonej rzeczywistości z przeznaczeniem dla biznesu

Ostatni rok przyniósł znaczący wzrost zainteresowania wirtualnymi asystentami, np. Amazon Alexa, Google Home, Apple Siri i Microsoft Cortana. Ich pojawienie się w środowisku biznesowym jest kwestią czasu, jako że konsumenci oczekują tego samego poziomu pomocy technologicznej w pracy, jakim dysponują w domu. Podobnie jest w przypadku rzeczywistości rozszerzonej AR (*Augmented Reality*) – technologii stosowanej dotychczas w pewnych niszowych obszarach, takich jak wojskowość czy lotnictwo. Jej ogromny potencjał ujawnia się w zastosowaniach biznesowych.
Technologia rozszerzonej rzeczywistości jest obecnie dostępna w urządzeniach mobilnych oraz (coraz częściej) w urządzeniach osobistych. Jedną z oczywistych możliwości AR w zastosowaniach biznesowych jest wsparcie instalacji i utrzymania rozwiązań technologicznych, w których wizualne instrukcje mogą zostać nałożone na rzeczywisty widok oglądany przez instalatorów czy serwisantów, co ułatwia im pracę.



Stale poszukujemy takich rozwiązań, które wnoszą nową wartość zarówno dla przedsiębiorców, jak i klientów.

Experience The Next®

OTWARTA PLATFORMA INTEGRUJĄCA
SYSTEMY BEZPIECZEŃSTWA

Pobierz darmową wersję na axxonsoft.com/pl

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

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

Warsztaty z PTZ-kami update[1]

Schyłek rozwiązań typu PTZ zaczęto wieszczyć już w chwili intensywnego rozwoju kamer wysokiej rozdzielczości wyposażonych w obiektywy szerokokątne. Miały one zastąpić urządzenia, których praca jest oparta na mechanizmach pozycjonujących. Głównymi powodami były krótsza żywotność ruchomych elementów mechanicznych w porównaniu z układami elektroniki oraz coraz większa czytelność szczegółów w obrazach z kamer hemisferycznych.

Jan T. Grusznic

Prognoza ta się nie potwierdziła. Co więcej, nastąpiło zintensyfikowanie działań na rzecz lepszej integracji tych dwóch rozwiązań. Kamera PTZ umożliwia szybkie zbliżenia i podejrzenia szczegółów sceny nawet ze znacznych odległości, natomiast kamera wyposażona w obiektyw szerokokątny idealnie sprawdza się w oglądzie zdarzeń w pobliżu instalacji punktu kamerowego. W ślad za oczywistymi korzyściami, jakie dało połączenie tych dwóch technologii obrazowania, zaczęto eksperymentować z kolejnymi połączeniami kamer PTZ oraz termowizji lub radaru.

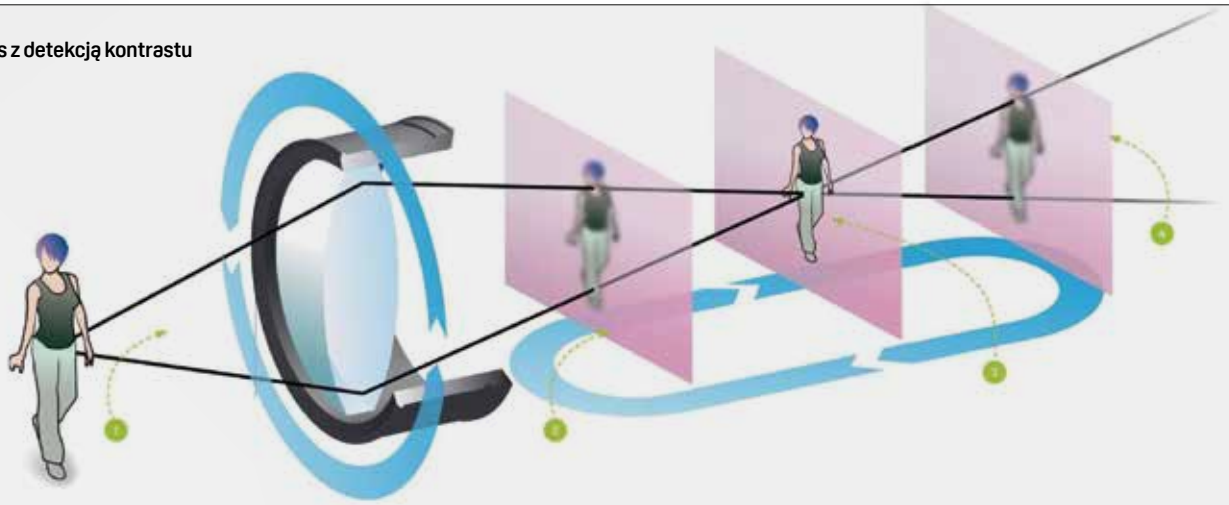
Kamery obrotowe mają coraz więcej funkcjonalności, więcej pamięci pozycji zaprogramowanych (presetów), szybciej się obracają, zapewniają automatyczne śledzenie oparte na coraz „mądrzejszych" algorytmach. Pomimo galopującego postępu technologicznego i wprowadzania kolejnych innowacyjnych rozwiązań ich podstawową funkcją nadal pozostaje tworzenie użytecznych obrazów z rozległego obszaru. W każdej chwili z kadru sceny ogólnej można dojrzeć szczegóły w miejscu odległym o kilkadziesiąt lub nawet kilkaset metrów. Kojarzymy je z miejskimi ulicami, gdzie pracują na rzecz poprawy bezpieczeństwa mieszkańców, z dozoru otwartych, rozległych przestrzeni stref produkcyjnych i lotnisk. Czasami stanowią dopełnienie systemu, a czasem jego podstawę. Niezależnie od miejsca instalacji ich misją jest pokrycie rozległego terenu wokół punktu obserwacji. Praca kamery PTZ jest oparta na mechanizmie obrotowym, który jest połączony z modułem optycznym wyposażonym w obiektyw typu motozoom z automatyką ustawiania ostrości (autofokus – AF). To właśnie ostatnia właściwość – autofokus – sprawia, że te rozwiązania wdarły się przebojem do większości instalacji systemów dozoru wizyjnego. We wcześniejszych (i cały czas dostępnych, lecz rzadziej już używanych) rozwiązaniach z niezależną kamerą, obiektywem ze zdalną regulacją ogniskowych oraz głowicą uchylno-obrotową brak automatycznego ustawiania ostrości często wymuszał interwencję człowieka w celu ustawienia pożądanej jakości obrazu. Stąd być może zakorzeniło się przekonanie, że za każdą kamerą stoi człowiek. Sterowanie kamerami na ogół przypisuje się przeszkolonym operatorom, którzy korzystają z nich na co dzień w miejskich lub gminnych systemach monitoringu. W przypadku zakładów przemysłowych sterowanie jest współdzielone między załogę zabezpieczającą obiekt, automatykę zakładu oraz analizę obrazu, a celem jest takie rozwiązanie, które zapewni ciągły nadzór procesów, nie angażując zanadto pracowników ochrony. Wykorzystuje się zaprogramowane pozycje, nagrane trasy, automatykę śledzenia w obszarach o niskim poziomie aktywności, wybrane algorytmy analizy obrazu [1] dla poszczególnych punktów dozoru oraz coraz bardziej złożoną integrację z urządzeniami zewnętrznymi.

AF – jak to naprawdę działa?

Zadaniem kamer PTZ jest szybkie dostarczenie czytelnego obrazu ze zbliżenia optycznego, dlatego niezwykle ważne jest jak najszybsze uzyskanie ostrości. Odpowiada za to mechanizm automatycznego ostrzenia, czyli autofokus (AF). Układy AF wykorzystywane w modułach optycznych kamer PTZ mierzą poziom kontrastu na przetworniku obrazu (tryb pasywny). Metoda ta polega na wykrywaniu różnic

[1] Autor wraca do tematu podjętego na łamach „Systemów Alarmowych" (SA nr 6/2014), poruszając kilka nowych wątków.

Rys. 1. **Autofokus z detekcją kontrastu**



1. **Zmiana sceny. Układ soczewek zaczyna się przemieszczać do tyłu (w tym przypadku).**
2. **Obraz nieostry o słabym kontraście. Soczewki są przemieszczane dalej w celu określenia punktu dla wyższego kontrastu.**
3. **Obraz ostry. Pomimo odnalezienia punktu ustawienia soczewek dających obraz o najwyższym kontraście soczewki są przesuwane dalej, aby sprawdzić, czy jest miejsce, w którym poziom kontrastu może być jeszcze wyższy.**
4. **Obraz nieostry o słabym kontraście – po przejechaniu punktu ostrości kontrast spada. Układ ustawia soczewki w miejscu, dla którego odnotowano najwyższy kontrast.**

Źródło: digitalcamerapolska.pl

w naświetleniu sąsiadujących grup pikseli obrazu poprzez analizę światła na matrycy światłoczułej. Gdy obraz nie jest ostry, przejścia między pikselami są łagodne i różnice w kontraście niewielkie. Im kontrast jest wyższy, tym większa ostrość obrazu. Pomiar następuje w określonym, wybranym polu autofokusa. W niektórych kamerach PTZ można wskazać obszar kadru, który ma być analizowany do pomiaru poziomu kontrastu. Co ważne, metoda detekcji kontrastu nie wymaga skomplikowanych mechanizmów pomiarowych. Jest bardzo dokładna (kluczowy jest tu odpowiedni algorytm), jeżeli w polu AF znajdują się zróżnicowane motywy, a nie gładka powierzchnia (to sprawia problem każdej pasywnej metodzie AF).

Sposób działania opisanego rozwiązania przedstawiono na *rys. 1.* W większości przypadków kamera „zgaduje", w którym kierunku ma przesunąć soczewki obiektywu, by kontrast się zwiększył. Jeśli wybiera zły kierunek, kontrast zaczyna się zmniejszać i operacja się wydłuża. Soczewki są przesuwane z powrotem, już w kierunku prawidłowym. Ale na tym nie koniec, skąd bowiem automat ma wiedzieć, że osiągnięto maksymalny kontrast? Przesuwa soczewki dalej, aż kontrast znów zacznie się zmniejszać i dopiero wówczas zawraca. Jak widać, proces ogniskowania chwilę trwa – soczewki w obiektywie przemieszczają się raz w jedną, raz w drugą stronę. Taka metoda prób i błędów prowadzi czasem do zjawiska zwanego *focus hunting* (efekt pulsowania), które objawia się „pompowaniem" obrazu podczas prób zogniskowania.

Focus hunting pojawia się w przypadku obserwacji scen słabo oświetlonych, a co za tym idzie o niskim współczynniku kontrastu. Problem przybiera na sile, gdy dodatkowo kamera obserwuje scenę o silnym oświetleniu skierowanym w jej stronę (np. światła z reflektorów samochodów lub oświetlenie wnętrza hali docierające przez otwartą bramę podczas nocnej obserwacji). Bardzo często w takich scenariuszach kamera niepoprawnie ustawia ostrość, koncentrując się na błędnym odczycie kontrastu, który jest spowodowany wewnętrznymi odbiciami promieni wewnątrz obiektywu. W efekcie obraz jest mocno rozogniskowany, a punkty świetlne tworzą tzw. efekt *bokeh*[2].

Producenci kamer PTZ opisane ograniczenia pasywnej metody ustawiania ostrości rozwiązują wielorako. Pierwszym i najczęstszym sposobem jest zapamiętanie pozycji soczewki skupiającej (ostrości) przy zapamiętywaniu prepozycji. W momencie zapisywania presetu do pamięci kamery zapisywane są, oprócz jego numeru i nazwy, różne zmienne, takie jak pozycja ogniskowej, pozycja wychylenia, pozycja obrotu, pozycja soczewki ogniskującej (fokus, czyli ostrość), a czasami nawet pozycja zamknięcia przysłony (w przypadku stosowania silnika krokowego). Gdy informacja o presecie została zapisana dla sceny kontrastowej, wtedy przywołanie presetu będzie gwarantowało uzyskanie ostrości bez efektu pulsowania (*focus hunting*) nawet w warunkach słabego oświetlenia, ponieważ pozycja soczewek skupiających będzie przywołana z bazy danych kamery. Trasa dozorowa zawierająca tak zaprogramowane pozycje będzie gwarantowała utrzymanie ostrości przez cały czas.

Drugim sposobem jest wykorzystanie stref ostrości. Jest to rozwiązanie podobne do zapamiętywania ostrości dla konkretnej prepozycji z tą różnicą, że wartość ustawienia soczewek skupiających jest podawana dla większego obszaru. Technicznie przypomina to tworzenie wirtualnej maski (trochę jak maski prywatności) dla kamery PTZ, która jest powiązana z koordynatami P/T (zakres pochylenia i obrotu), a czasami również z krotnością przybliżenia. W momencie, gdy kamera podczas wykonywania patrolu – trasy nagranej przez użytkownika – wchodzi w zakres koordynat P/T związanych ze strefą ostrości, automatyczny system ostrzenia przełącza się na wartości ustawienia soczewek skupiających dla tej strefy. Po wyjściu kamery ze strefy ostrości system AF jest załączany ponownie. Dzięki temu można utrzymać ostrość obrazu przy ciągłym patrolowaniu obszaru nawet dla tras zaprogramowanych przez operatora.

Trzecim rozwiązaniem jest wykorzystanie technik doświetlenia sceny zwiększających kontrast lub pomiaru odległości. Zasada pomiaru odległości opiera się na technice wykorzystywanej przez profesjonalne przyrządy pomiarowe stosowane w budownictwie. Czujnik laserowy zawiera diodę laserową, której zadanie sprowadza się do wyświetlania plamki promienia lasera na powierzch-

[2] W fotografii sposób oddawania nieostrości obiektów znajdujących się poza głębią ostrości. W Internecie są dostępne wizualizacje tego efektu.

ni mierzonego obiektu. Światło odbite od widzialnej plamki zostaje zobrazowane za pomocą obiektu światłoczułego. Obecnie można dokonywać pomiaru odległości z dokładnością do kilkunastu milimetrów metodą *time-of-flight* (ToF), wykorzystującą pulsującą wiązkę światła lasera, która jest emitowana przez czujnik i ulega odbiciu od obiektu. Odległość do obiektu określa się na podstawie pomiaru czasu upływającego od emisji wiązki do jej powrotu do czujnika po odbiciu. W ten sposób układ optyczny bazuje na bezwzględnych wartościach dostarczanych przez układ pomiarowy, utrzymując ostrość za każdym razem bez konieczności sprawdzania poziomu kontrastu na przetworniku.

W przypadku wykorzystania laserowych systemów pomiarowych należy pamiętać, że skoncentrowana wiązka laserowa może spowodować trwały uszczerbek na zdrowiu, jeśli energia emitera jest zbyt duża. Dlatego też w laserowych urządzeniach pomiarowych rzadko spotyka się klasę powyżej 1 (zgodnie z IEC 60825-1) lub 1M. Ogranicza to ich zasięg do ok. 100 m. Lasery tych klas są bezpieczne w racjonalnych warunkach pracy. Klasa 1M może być potencjalnie niebezpieczna, ale tylko w momencie obserwowania wiązki przez przyrządy optyczne.

Oświetlenie a bezpieczeństwo fotobiologiczne

Coraz powszechniejsze, trwalsze i wydajniejsze systemy oświetlenia podczerwienią integrowane w kamerach stałopozycyjnych doczekały się też pełnej integracji z kamerami PTZ. Pełnej, bowiem obecnie wbudowane oświetlacze w pełni współgrają z krotnością zoomu, zawężając kąt świecenia adekwatnie do kąta obserwacji. Dzięki temu są w stanie uzyskiwać akceptowalny poziom kontrastu w scenie odległej o 200 lub nawet 500 m od punktu kamerowego. Tak duże zasięgi wymagają sporej energii źródeł promieniowania, co przekłada się na zwiększenie zagrożenia fotobiologicznego. Oczywiście nie wszystkie źródła promieniowania są w takim samym stopniu potencjalnym zagrożeniem zdrowia, dlatego należało ustalić kryteria zagrożenia fotobiologicznego promieniowaniem optycznym emitowanym przez emitery stosowane w urządzeniach m.in. do dozoru wizyjnego.

Tabela 1. **Grupy ryzyka fotobiologicznego wg IEC 62471**

Grupa ryzyka	Ryzyko	Definicja
Zwolniony	brak	brak zagrożenia fotobiologicznego
RG-1	niskie	brak zagrożenia fotobiologicznego przy normalnych ograniczeniach behawioralnych
RG-2	umiarkowane	nie stanowi zagrożenia z powodu reakcji awersji na jasne światło lub dyskomfort termiczny
RG-3	wysokie	niebezpieczne nawet dla chwilowej ekspozycji

Tabela 2. **Wybrane zagrożenia dla oka i skóry oraz granice emisji dla grup ryzyka o działaniu ciągłym wg IEC 62471**

Niebezpieczeństwo	Wielkość mierzona	Zakres fali [nm]	Granice emisji		
			zwolniony	RG-1	RG-2
Zagrożenie oka podczerwienią	natężenie napromieniowania [$W*m^{-2}$]	780-3000	100	570	3200
Zagrożenie termiczne siatkówki	luminancja energetyczna [$W*m^{-2}*sr^{-1}$]	380-1400	28000/α	28000/α	71000/α
Zagrożenie termiczne siatkówki – słaby bodziec wzrokowy	luminancja energetyczna [$W*m^{-2}*sr^{-1}$]	780-1400	6000/α	6000/α	6000/α

α – rozmiar kątowy źródła w radianach. Kąt widzenia tworzony przez źródło obserwowane z wierzchołkiem przy oku obserwatora lub w punkcie pomiaru.
sr – pole widzenia: kąt przestrzenny widziany przez detektor (kąt odbioru), taki jak radiometr/spektroradiometr, z którego detektor odbiera promieniowanie.
$W*m^{-2}$ – natężenie promieniowania.

W tym celu została opracowana norma IEC 62471 (*Bezpieczeństwo fotobiologiczne lamp i systemów lampowych*), w której podano klasyfikację źródeł promieniowania (z wykluczeniem laserów) ze względu na bezpieczeństwo fotobiologiczne. Klasyfikacja ta opiera się na maksymalnych dopuszczalnych ekspozycjach (MDE) w całym zakresie promieniowania emitowanego przez dane źródło. Uwzględniono w niej poziom promieniowania emitowanego przez dane urządzenie (lampę lub system lampowy), zakres widmowy promieniowania i dostęp człowieka. W każdej grupie ryzyka ustalono kryteria czasowe dla każdego zagrożenia fotobiologicznego. Kryteria dobrano tak, aby stosowana wartość graniczna nie została przekroczona w danym czasie.

Zgodnie z IEC 62471 źródła promieniowania optycznego są klasyfikowane do grup ryzyka z zastrzeżeniem ich potencjalnego zagrożenia fotobiologicznego. Klasyfikacja jest oparta na ocenie ryzyka, którą przeprowadza się na poszczególnych składnikach lub produkcie końcowym na podstawie informacji uzyskanych od producenta. Źródła dzieli się na cztery grupy wg zagrożenia (*tab. 1*), wg limitu emisji oraz dopuszczalnego czasu ekspozycji przed przekroczeniem zagrożenia.

Istnieją różne zagrożenia biologiczne, które są rozpatrywane w różnych zakresach długości fal zgodnie z normą IEC 62471. Uwzględnia się biologiczny wpływ na oczy i skórę. W *tabeli 2* przedstawiono wybrane zagrożenia wynikające z zakresu długości fali pracy promienników stosowanych w dozorze wizyjnym.

Na potrzeby normy zdecydowano, że odległości, przy których podaje się wartości zagrożeń fotobiologicznych spowodowanych promieniowaniem lamp, powinny wynosić 200 mm dla wszystkich innych źródeł światła niż lampy stosowane w oświetleniu ogólnym. I tak:

- lampy IR nie stwarzają żadnego zagrożenia fotobiologicznego, jeżeli nie ma ryzyka zagrożenia termicznego siatkówki w ciągu 10 s ani zagrożenia oka napromieniowaniem podczerwonym w ciągu 1000 s. Również emitery, które generują promieniowanie IR bez silnego bodźca wizualnego (czyli mniej niż 10 cd/m^2) i nie stwarzają zagrożenia dla siatkówki bliską IR w czasie 1000 s ekspozycji, są zaliczane do grupy wolnej od ryzyka;
- promienniki IR sklasyfikowane do RG-1 nie stwarzają zagrożenia z powodu normalnych ograniczeń ekspozycji w warunkach użytkowania. Wymaganie to jest spełnione przez każdy emiter, któ-

ry przekracza granice grupy wolnej od ryzyka, ale nie stwarza zagrożenia termicznego dla siatkówki w czasie 10 s ani zagrożenia dla oka promieniowaniem IR w czasie 100 s;
- promienniki IR sklasyfikowane jako RG-2 nie stwarzają zagrożenia z powodu dyskomfortu termicznego. Wymaganie to spełnia każdy promiennik, który przekracza granice grupy RG-1, ale nie stwarza zagrożenia termicznego dla siatkówki w czasie 250 ms ani zagrożenia dla oka promieniowaniem IR w czasie 10 s;
- wszystkie promienniki sklasyfikowane jako RG-3 mogą stwarzać zagrożenie nawet przy chwilowej lub krótkiej ekspozycji i są zaliczane do grupy wysokiego ryzyka.

Jest mało prawdopodobne, aby emitery wykorzystywane w kamerach PTZ były klasyfikowane jako RG-3. Niemniej warto sprawdzić, do jakiej grupy producent je zaklasyfikował. Natomiast promienniki dużej mocy, które są w stanie oświetlić scenę z odległości 500 m, są na ogół klasyfikowane jako RG-2. Na *rys. 2* przedstawiono przykładową etykietę, jaka powinna się znajdować na urządzeniu klasyfikowanym wg IEC 62471 dla RG-2.

Ułomnością rozwiązania – kamery PTZ zintegrowanej z wysokoenergetycznym oświetlaczem IR – jest wygrzewanie całego układu kamery, w tym również przetwornika obrazu. Wpływa to na jakość obrazu w postaci widocznego szumu, który nie zależy od liczby fotonów padających na powierzchnię światłoczułą. Szum związany z temperaturą przetwornika CMOS ma charakter losowy i w każdej klatce inny rozkład przestrzenny. Nie ma prostej możliwości usunięcia szumu, jedynie można go uśrednić np. metodą filtracji dolnoprzepustowej, tracąc jednak część informacji. Drugą możliwością (ograniczoną do statycznych ujęć) jest wykonanie serii zdjęć i ich uśrednienie. Niedoskonałości obrazu stają się bardziej widoczne wraz ze wzrostem jego rozdzielczości. Oznacza to, że oprócz rozwiązania problemu z szybkim chwytaniem ostrości również szybkie odprowadzanie ciepła z układu, a przede wszystkim odseparowania go od obszaru instalacji układu CMOS staje się polem innowacyjnych rozwiązań inżynieryjnych pozwalających utrzymać wysoką jakość obrazu.

Kopułka - okno na świat

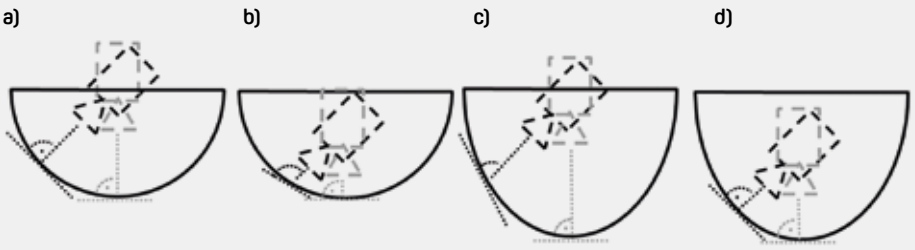
Niezmiennie od wielu lat stałym elementem znacznej liczby kamer PTZ obecnych na rynku jest kopułka, która może być wykonana z poliwęglanu (często spotykane rozwiązania wandaloodporne), akrylu (o mniejszej odporności na udary mechaniczne) lub nylonu (większa elastyczność). Każdy z wymienionych materiałów ma istotne właściwości optyczne, niepozostające bez wpływu na jakość uzyskanego obrazu. Kopuły poliwęglanowe mają stosunkowo grube ścianki, co w przypadku długich ogniskowych może stwarzać problem z uzyskaniem odpowiedniego poziomu ostrości, niewidoczny przy ujęciach o szerokim kącie. Choć kopuły poliwęglanowe cieszą się największym zainteresowaniem, są zastępowane przez akryl charakteryzujący się lepszymi właściwościami optycznymi.

Wbrew obiegowej opinii kopułki akrylowe nie są przeznaczone tylko do zastosowań wewnątrz budynków, spełniają swoje zadanie również w instalacjach zewnętrznych. Ich odporność na uderzenia nie przekracza 5 dżuli (IK08), co najczęściej jest wystarczające. Nylon, mało popularny materiał ze względu na skomplikowany proces wytwarzania, jest głównie stosowany w hermetycznych rozwiązaniach ciśnieniowych. Właściwości optyczne kopułek nylonowych można porównać z akrylem, choć z widoczną różnicą na korzyść tego drugiego.

Wielkość kopułek, ich osadzenie i montaż stanowi nieraz proces żmudnych obliczeń, aby znaleźć idealne dopasowanie. Dlaczego jest to tak istotne, pokazuje przykład obserwacji otoczenia za oknem. Gdy obserwujemy scenę na zewnątrz naszego domu lub biura (patrząc prostopadle przez szybę), jakość obrazu jest bardzo dobra. Gdy jednak zaczynamy obserwować scenę odległą, znajdującą się bardziej pod kątem, okazuje się, że płaska szyba obniża jakość widzenia i pogarsza skuteczność obserwacji. Wyobraź sobie, że wykonujesz tę samą obserwację, ale tym razem korzystasz z lornetki z 30-krotnym zbliżeniem. Problem przybiera na sile. Ten sam przypadek występuje w kamerach PTZ – nie we wszystkich, rzecz jasna, ale zdarza się, że obraz staje się znacznie lepszy po zdjęciu kopułki.

Kopuła sama w sobie nie musi stanowić problemu. Na *rys. 3a* i *rys. 3d* pokazano dwie różne krzywizny dające dobre rezultaty pomimo różnej konstrukcji kopuł. Z kolei na *rys. 3b* widać, jak przy idealnej krzywiźnie kopuły zbyt niskie osadzenie modułu optycznego wymusi w wybranych pozycjach modułu obserwację „pod kątem" do powierzchni kopuły – w konsekwencji spowoduje to problem braku ostrości przy znacznych zbliżeniach. Ale niższe osadzenie ma też plusy. Po pierwsze umożliwia obserwację nieco powyżej linii horyzontu (180°+), co jest korzystne w dozorze na dalekie odległości lub „pod górę". Po drugie zmniejsza dystans między wewnętrzną stroną kopułki a modułem, dzięki czemu mniejsza ilość promieniowania odbitego od wewnętrznej sfery kopuły trafia do oka kamery. Umieszczenie elementu optycznego wyżej (*rys. 3c*) spowoduje powstanie dużej liczby odbić i utrudni obserwację w nocy, gdy kamera jest zamocowana np. pod latarnią uliczną lub gdy zza kamery pada silne światło. Nie bez powodu zatem producenci wyposażają moduł optyczny

Rys. 2. **Informacja na produkcie o klasie RG-2.**



Rys. 3. **Schematyczne ujęcie czterech krzywizn kopuł wraz z modułami optycznymi kamer PTZ**

w wiele czarnych, otaczających elementów z tworzywa, ograniczając w ten sposób liczbę powstałych wewnątrz refleksów.
Kopułka powinna być regularnie czyszczona, a w przypadku widocznych zadrapań i uszkodzeń – wymieniona. W przeciwnym razie kurz, brud, promienie odbijające się w powstałych mikrouszkodzeniach będą pogarszały właściwości optyczne, a w efekcie obniżały jakość rejestrowanego materiału. A jeśli kamera nie ma kopułki? Coraz więcej kamer ma budowę „odkrytą" – tylko optyka znajduje się za płaską szybą o zwiększonej odporności na udary mechaniczne. Reszta jest „dostępna", co oznacza, że jest narażona na mechaniczną zmianę pozycji kamery lub wnikanie brudu zatykającego otwory wentylacyjne. W obu przypadkach warto sprawdzić, czy i w jaki sposób kamera powiadomi system lub operatora o wymuszonej zmianie pozycji oraz jak czyścić kamerę z nagromadzonego pyłu.

Czułość - dlaczego ślepnę?

Brak dokumentów normatywnych pomiarów czułości kamer doprowadził do pewnej dowolności badań i interpretacji wyników pomiarów. Tymczasem wartości pozbawione wspólnego mianownika, podawane przez producentów kamer PTZ, są trudne do porównania. Nie oznacza to, że są bezużyteczne.
Wartość czułości kamer zależy od wielu czynników, w tym m.in. od poziomu wzmocnienia wykorzystywanego przy pomiarze apertury obiektywu *f*, poziomu odbicia przedmiotu (sceny), na który było skierowane oświetlenie, czy temperatury barwowej (stopnie Kelvina) oświetlenia użytego podczas pomiaru. Odpowiednia modyfikacja parametrów zapewnia uzyskanie „lepszych" wyników umieszczanych w kartach katalogowych [2]. Tymczasem jakość obrazu oceniamy subiektywnie wg wierności odtworzenia kolorów, skali szarości, czy mówiąc ogólnie, po czytelności szczegółów w obrazie. Im skala odwzorowania jest szersza, tym wierniejsze odwzorowanie (*rys. 4a*). Przy mniejszym zakresie skali (*rys. 4b*) niektóre elementy są przedstawiane niepoprawnie (np. białe płaszczyzny), a detale są niewidoczne – jakość obrazu ubożeje.
Niestety wartości czułości kamer są „poprawiane" poprzez zwiększanie poziomu wzmocnienia sygnału, aż do wartości zmieniających obraz, utrudniający obserwację szczegółów. AGC (ARW – automatyczna regulacja wzmocnienia) jest rozwiązaniem wzmacniającym sygnał, który optycznie rozjaśnia obraz (rys. 2c). Takie rozjaśnienie tylko pozornie tworzy go subiektywnie lepszym. Detale są mniej wyraźne, o niższej rozdzielczości. Dlatego zasadne jest, aby poziom wzmocnienia podczas pomiarów był ustawiany na 0 dB, a wartość pomiaru była odnotowywana dla najgorszego przypadku, gdy poziom bieli jest jeszcze widoczny na tablicy testowej. Nie jest to jednak zapis normatywny, a wyłącznie zdrowy rozsądek.
Ponieważ porównywanie czułości kamer prowadzi na manowce (podaną wartość i tak trudno zweryfikować ze względu na wskazany brak norm pomiarowych), odwróćmy pytanie – jaki powinien być poziom oświetlenia sceny E_{scena}, aby obraz był użyteczny? Odpowiedź na to pytanie nie jest trudna, o ile znamy:

- wartość czułości kamery $E_{przetwornik}$
- poziom odbicia światła od sceny (odbiciowość sceny R_{scena})
- aperturę obiektywu *f*
- współczynnik przepuszczalności soczewek obiektywu (% zdolność przepuszczalności światła) *t*
- współczynnik odbicia światła od soczewek obiektywu (% poziom odbicia światła od soczewek) $R_{obiektyw}$

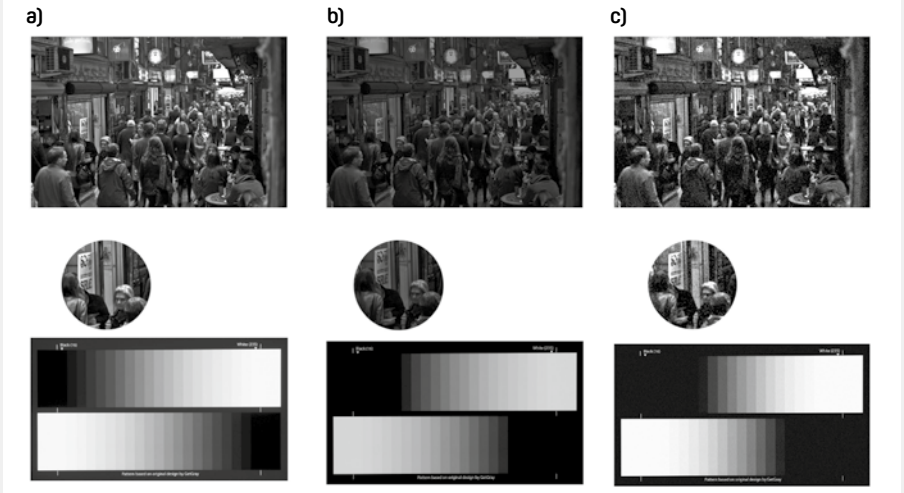
Zależność powyższych parametrów jest opisana wzorem:

$$E_{scena} = \frac{E_{przetwornik} \cdot f^2}{t \cdot R_{obiektyw} \cdot R_{scena}} \quad (1)$$

Uzyskanie informacji o wartości czułości kamery oraz wartości przysłony, przy jakiej wykonano pomiar, nie nastręcza problemu, ponieważ znajdziemy je w kartach katalogowych każdego szanującego się producenta. Pozostałe wartości często wiążą się z dostępem do badań z pomiarów, które nie są prezentowane publicznie. Dlatego trzeba przyjąć pewne założenia:

t = 0,7 (70%)
$R_{obiektyw}$ = 0,8 (80%)

Powyższe wartości odpowiadają przyjęciu najgorszego scenariusza, ponieważ dostęp do tych parametrów jest ograniczony (aby nie uznać za niemożliwy). Poziom odbicia sceny R_{scena} będzie się różnił w zależności od tego, co obserwujemy.
W *tabeli 3* zaprezentowano przykładowe, przybliżone poziomy odbicia promieniowania światła białego [3].
By uprosić sprawę profesjonalnym fotografom, na początku lat 50. XX wieku firma Kodak [4], chcąc wskazać poprawną procedurę pomiaru poziomu światła w scenie, sugerowała, aby wykonywać go z użyciem szarej karty Kodaka, co zapewni właściwe naświetlenie błony światłoczułej. Szara karta Kodaka powstała w trakcie długich badań pracowników laboratorium firmy, gdzie wykazano, że średni poziom odbicia otaczających nas przedmiotów wynosi ok. 20% (dokładnie 18%). Do dziś wszelkie urządzenia pomiarowe do ustalenia poziomu światła odbitego są kalibrowane zgodnie z zasadą przyjętą w latach 50. ub. wieku (światłomierze w cyfrowych apartach fo-



Rys. 4a. **Obraz reprezentujący scenę w idealnych warunkach oświetleniowych. AGC wyłączone (lub wzmocnienie na poziomie 0 dB)**
Rys. 4b. **Obraz reprezentujący scenę o niższym poziomie oświetlenia, gdzie reprodukcja szarości kończy się w połowie gamy szarości tablicy testowej, AGC wyłączone (lub wzmocnienie na poziomie 0 dB)**
Rys. 4c. **Obraz reprezentujący obraz ze sceny 4b przy uruchomionej automatyce wzmocnienia AGC do poziomu uzyskania poziomu bieli**

Tabela 3. **Szacunkowe poziomy odbicia światła białego w zależności od użytego materiału**

Materiał	Typowy poziom odbicia (światło białe)
Karta białego papieru	75%
Aluminium	75%
Szklane okna (szyby)	70%
Biała tkanina	65%
Świeżo lany beton	40–50%
Lakierowane drewno dębowe (jasne)	40–50%
Okładzina tynkowa	30–60%
Stal	25%
Żeliwo	25%
Otwarta przestrzeń (drzewa, trawa)	20%
Mur ceglany (świeżo postawiony)	10–30%
Mur ceglany (zwietrzały)	5–15%
Beton (zwietrzały)	5–15%
Matowa kartka czarnego papieru	5%

Tabela 4. **Szacunkowe zmiany oświetlenia w scenie dla zmieniającej się apertury względem wartości f/1.0**

Wartość przysłony *f*	Względna wartość zwiększenia poziomu oświetlenia w scenie w odniesieniu do f/1.0	Minimalny poziom oświetlenia w scenie
f/1.0	---	1,984 lx
f/1.2	44%	2,86 lx
f/1.4	96%	3,89 lx
f/1.6	256%	5,08 lx
f/1.8	324%	6,43 lx
f/2.0	400%	7,94 lx
f/2.4	576%	11,43 lx
f/2.8	784%	15,55 lx
f/4.0	1600%	31,74 lx
f/5.6	3136%	62,22 lx

tograficznych zgodnych z ANSI są kalibrowane z 12% poziomem odbicia) [5]. A jeśli tak, to i do naszego równania wstawimy wartość *Rscena* = 0,18 (18%). W ten sposób mamy już wszystkie zmienne potrzebne do równania.

Zatem przy założeniu, że kamera ma czułość 0,2 lx w trybie kolorowym dla przysłony f/1.6, to podstawiając te wartości do wzoru (1), otrzymamy wymagany poziom oświetlenia sceny:

$$E_{scena} = \frac{0{,}2 \cdot 1{,}6^2}{0{,}7 \cdot 0{,}8 \cdot 0{,}18} \cong 5{,}08\ \text{lx}$$

Dlaczego zatem przy poziomie około 5 lx w momencie zbliżenia obraz staje się bardziej zaszumiony, a szczegóły mniej czytelne? Powodem jest przyjęty standard podawania wartości czułości dla najniższej wartości przysłony *f*. Tymczasem ten parametr w modułach optycznych kamer PTZ zmienia się w całym zakresie ogniskowych, np. zakres 4–100 mm *f*/1.6–4.0 oznacza, że dla ogniskowej 4 mm najmniejsza wartość przysłony to *f*/1.6, a dla 100 mm najmniejsza wartość przysłony to *f*/4.0. Jest to istotne, ponieważ ilość światła przechodzącego przez przysłonę zmniejsza się wraz ze wzrostem wartości przysłony zgodnie z *tab. 4*.

Ilość światła w scenie, jaką wyliczyliśmy, dotyczyła najszerszego kąta obserwacji. W przypadku jego zawężenia okaże się, że dla przysłony *f*/4.0 wymagany poziom oświetlenia w scenie wynosi min 31,74 lx.

Należy w tym miejscu przypomnieć o przyjętych założeniach i braku wiedzy co do poziomu wzmocnienia w momencie pomiaru poziomu czułości kamery przez producenta. Wyniki pochodzące z powyższych wyliczeń mają zatem charakter jedynie orientacyjny. Są jednak pomocne w określeniu rzędu wielkości minimalnego poziomu oświetlenia sceny.

Integracja na zakończenie

Kamery PTZ to rozwiązanie bardzo popularne wśród sprzedawców i wygodne dla projektantów systemów chcących osiągnąć szybki efekt niewielkim kosztem:
• jedna kamera, która obserwuje bardzo duże przestrzenie, mająca mnóstwo zalet • jeden punkt kamerowy, jeden słup, jedno doprowadzenie zasilania i medium transmisyjnego. Co więcej, do dozoru rozległej przestrzeni jest wymagana tylko jedna licencja na oprogramowanie zapisu. Kamery PTZ zyskują przewagę dzięki wielokrotnemu zbliżeniu optycznemu, które umożliwia rozpoznanie osoby z odległości ponad 370 m (zbliżenie 30x) i w takim przypadku są trudne do zastąpienia. Cały czas jednak pozostaje trudność w jednoczesnej obserwacji ogółu i detali za pomocą kamer PTZ. Problem znany od dawna znalazł rozstrzygnięcie stosunkowo niedawno. Producenci kamer zdecydowali się wprowadzić do oferty rozwiązanie uzupełniające w postaci dodatkowych kamer stałopozycyjnych instalowanych dokoła jednostki PTZ lub kamery hemisferycznej. Jest ono dostępne w postaci dodatkowego modułu dokładanego do kamery PTZ lub już w wersji zintegrowanej, a rolą takiego zestawu jest niezależny dozór najbliższej przestrzeni wokół punktu kamerowego. Za pomocą dodatkowego modułu można sterować kamerą PTZ z poziomu obrazu z kamery (bądź jeśli jest ich więcej, obrazów z kamer) stałopozycyjnej oraz oznaczać na nim pozycję kamery szybkoobrotowej. Coraz powszechniejsza staje się również integracja z modułami termowizyjnymi i radarami zapewniająca lepszą automatyzację zadań.

Literatura

[1] *VCA*, Wyd. specjalne „SA" (2014 r.).
[2] Przykład „kreatywnego przeliczania" czułości przedstawiono w artykule nt. kamer dualnych vs. dzień/noc (cz. 1) dostępnym na sa-portal.pl.
[3] Na podstawie *The complete guide to cctv lighting* firmy RayTec.
[4] „Copying" (Kodak Publication No. M-1) (5th Ed.), Eastman Kodak Company, Published by Eastman Kodak Company, Rochester, NY, 1956.
[5] http://www.bythom.com/graycards.htm

BIO

Jan T. Grusznic Z branżą wizyjnych systemów zabezpieczeń związany od 2004 r. Ma bogate doświadczenie w zakresie projektowania i wdrażania rozwiązań dozoru wizyjnego w aplikacjach o rozproszonej strukturze i skomplikowanej dystrybucji sygnałów. Ceniony diagnosta zintegrowanych systemów wspomagających bezpieczeństwo.

Przegląd kamer PTZ

Kamery obrotowe należą do **najpopularniejszych urządzeń stosowanych w systemach dozoru wizyjnego.**

Wszechstronność i uniwersalność kamer PTZ sprawiają, że spotykamy je w miejskich systemach monitoringu wizyjnego, a także w instalacjach wojskowych czy przemysłowych. Postęp i spadające ceny pozwoliły zawitać takim urządzeniom również w prostszych, nawet konsumenckich aplikacjach.

Seria kamer sieciowych AXIS M50 PTZ

Dyskretne kamery sieciowe PTZ do monitorowania dużych obszarów.

- Funkcje PTZ w niezwykle dyskretnej obudowie
- HDTV 720p/SVGA i H.264
- Stopień ochrony obudowy IP51 i IP66
- Zasilanie PoE (IEEE 802.3af)
- Wbudowany mikrofon oraz funkcja detekcji audio (AXIS M5013/M5014)
- Odporność na akty wandalizmu (AXIS M5013-V/M5014-V)

Seria AXIS M50 PTZ obejmuje przystępne cenowo kamery PTZ. Nadają się one doskonale do zdalnego, dyskretnego monitorowania pomieszczeń, takich jak sklepy, hotele, recepcje biurowe, restauracje i magazyny. Modele odporne na akty wandalizmu sprawdzą się w zagrożonych obszarach.

Obudowa ochronna i łatwy montaż na suficie

Dzięki obudowie o klasie ochrony IP51 kamery sieciowe AXIS M5013/M5014 PTZ są zabezpieczone przed wnikaniem pyłu i kapiącej wody, dzięki czemu mogą rejestrować obraz wideo nawet przy włączonym systemie zraszaczy. Modele AXIS M5013-V/M5014-V PTZ są z kolei chronione przed wnikaniem pyłu i strumieniami wody pod wysokim ciśnieniem z dowolnego kierunku (klasa ochrony IP66).

Funkcja zasilania *Power over Ethernet* (PoE) umożliwia zasilanie kamer serii AXIS M50 przez sieć lub za pomocą zasilacza *midspan*, eliminując potrzebę stosowania kabli zasilających i obniżając koszty montażu.

Kamera sieciowa AXIS M5525-E PTZ

Kamera PTZ do montażu na zewnątrz i wewnątrz pomieszczeń

- Rozdzielczość HDTV 1080p i 10-krotny zoom optyczny
- 360-stopniowy obrót ciągły
- Technologia *Zipstream* firmy Axis
- Trzy profile scen
- Dwukierunkowa komunikacja audio oraz porty we/wy

Opłacalna inwestycja

Kamera AXIS M5525-E to doskonały wybór do dozoru sklepów, szkół, lobby i innych otwartych przestrzeni na zewnątrz i wewnątrz pomieszczeń. Ma przystępną cenę i jednocześnie wiele zaawansowanych funkcji, jakie mają kamery z najwyższej półki cenowej.

Nic się nie ukryje

Łatwo śledzić poruszające się obiekty dzięki rozdzielczości HDTV 1080p, 10-krotnemu zoomowi optycznemu i ciągłemu panoramowaniu w zakresie 360°. Kamera dostarcza zarówno szczegółowy obraz w zbliżeniu, jak i ogólny podgląd obszaru. Obsługuje również WDR – *Forensic Capture*, funkcję zapewniającą wysoką szczegółowość w przypadku jednoczesnego występowania w scenie jaśniejszych i ciemniejszych miejsc. Kamera ma wyjątkową czułość, zapewniającą rejestrację wysokiej jakości obrazów nawet podczas nagrywania w niemal całkowitej ciemności.

Wszechstronna

AXIS M5525-E to kamera do stosowania na zewnątrz i wewnątrz pomieszczeń, pasująca do wszystkich uchwytów PTZ firmy Axis. Zapewnia dwukierunkową komunikację audio, ma cztery porty we/wy.

Można wybrać jeden z trzech profili sceny: kryminalistyczny, wewnętrzny i zewnętrzny. Kamera automatycznie dostosowuje czas ekspozycji, balans bieli, aperturę, ostrość, kontrast i szum, dopasowując te parametry do konkretnego scenariusza. Dzięki temu można uzyskać doskonałą jakość obrazu i zapewnić niski koszt montażu.

Ostre obrazy. Małe zapotrzebowanie na przepustowość

Kamera AXIS M5525-E jest wyposażona w technologię *Zipstream* firmy Axis, która służy do analizy strumienia wizji w czasie rzeczywistym. Pozwala to na zachowanie pełni szczegółów przy niezmienionej jakości obrazu i jednoczesnym zmniejszeniu zapotrzebowania na przepustowość sieci i pamięć o nawet 50%.

Kamera sieciowa AXIS Q8685-E PTZ

Niczym nieograniczony widok i wyraziste szczegóły.

- Panoramowanie 360° i przechylenie 135° od podłoża po niebo
- Szczegółowość detali obrazu do zastosowań kryminalistycznych, przywracanie ostrości
- Połączenia sieciowe na duże odległości
- Ochrona przed działaniem warunków atmosferycznych, zdalna konserwacja
- Łatwy montaż

Kamera sieciowa AXIS Q8685-E PTZ umożliwia ustalenie prędkości dla nieograniczonego dozoru o dalekim zasięgu na rozległych obszarach na zewnątrz budynków.
Umożliwia wybór bardzo szybkiego lub bardzo powolnego panoramowania i pochylania – od 0,05 do 120 stopni na sekundę. Dzięki temu można uzyskać płynne panoramiczne obrazy i szybko reagować na zdarzenia.
Kamerę można montować na kolumnie, słupie lub ścianie, aby uzyskać widok panoramiczny 360° i widok od podłoża po niebo w zakresie od -90° do +45°.
Może pracować w ekstremalnych temperaturach; w ruchu jest w stanie wytrzymać huraganowe wiatry o prędkości do 47 m/s, a bez osłony przeciwsłonecznej – nawet 60 m/s.
Dzięki 30-krotnemu zoomowi optycznemu i wyjątkowym możliwościom panoramowania i pochylania kamera AXIS Q8685-E zapewnia identyfikację na duże odległości i szerokie pole widzenia w każdym kierunku.
Funkcja WDR *Forensic Capture* pozwala na uzyskanie wyraźnych szczegółów w scenach z ciemnymi i jasnymi obszarami. Funkcja przywracania ostrości umożliwia szybkie ustawienie ostrości w obrazie. Z kolei dzięki funkcji *Advanced Gatekeeper* (zaawansowany strażnik), ta sieciowa kamera PTZ automatycznie przybliża obiekty wykryte we wstępnie określonych obszarach.
Model AXIS Q8685-E ma niewielkie rozmiary. Montaż niemal w dowolnym miejscu umożliwiają różne akcesoria, takie jak gniazdo SFP (opcja podłączenia sieci światłowodowej, niedrogie rozwiązanie na duże odległości), czy wytrzymały przewód zasilający o długości 22 m. Konserwacja jest niezwykle prosta, ponieważ kamerę wyposażono w zdalnie sterowaną opcję mycia i trwałe wycieraczki.

BCS-P-5692RSAI: obrotowa kamera 12 MPX

W ofercie kamer BCS modelem z najwyższej półki jest BCS-P-5692RSAI.

Wysoka rozdzielczość do 12 Mpix pozwala oglądać plan obserwacyjny z większą liczbą szczegółów. Najwyższej jakości moduł optyczny z 22-krotnym zoomem sprawia, że obraz prezentowany przez kamerę jest ostry w pełnym zakresie ogniskowej. Inteligentne funkcje śledzenia obiektu zaimplementowane w kamerze pozwolą tak skonfigurować urządzenie, aby działało bezobsługowo. *Autotracking*, analiza obrazu, presety oraz nowatorskie rozwiązania pozycjonujące pozwolą kamerze spojrzeć tam, gdzie chcemy, nawet bez konieczności obsługi urządzenia.

Terminarz funkcji automatyki umożliwia dopasowanie kamery do specyfiki obiektu, optymalizując jej pracę. Inteligentny promiennik podczerwieni o zasięgu do 250 m dostosowuje się do obserwowanego planu, doświetlając scenę zarówno szerokiego planu, jak i dużego przybliżenia.
Wejścia i wyjścia alarmowe umożliwiają integrację z systemami alarmowymi lub kontroli dostępu. Duży wybór dodatkowych adapterów zapewnia sprawną instalację zarówno na ścianie, jak i słupie czy suficie. Wszystko to sprawia, że topowy model serii BCS Point oferuje to, co najważniejsze w systemach telewizji dozorowej: idealnie ostry obraz o wysokiej rozdzielczości.

Dahua: PTZ1A225U-IRA-N

Minisystem pozycjonujący o doskonałych parametrach.

Kamery PTZ cieszą się niesłabnącą popularnością, jednak jedna z ich cech immanentnych – wielkość – może budzić kontrowersje i nie wszędzie jest akceptowana.
Czy jesteśmy skazani na masywne, rzucające się w oczy głowice zawieszone nad naszymi głowami również w miejscach, gdzie wygląda to po prostu nieestetycznie i zwraca na siebie uwagę? Na szczęście nie.

Dahua wprowadza do oferty kamerę PTZ1A225U-IRA-N. To minisystem pozycjonujący, którego możliwości zdecydowanie nie są „mini". Urządzenie zamknięte w estetycznej i niewielkiej obudowie ma wymiary: ø291,5 x 161 x 153,4 mm i masę zaledwie 3,6 kg.

Aby zagwarantować obraz o doskonałej jakości, zastosowano znany z innych kamer Dahua przetwornik Sony STARVIS o przekątnej obrazu 1/2,8" i rozdzielczości 1920 x 1080. Gdyby jednak oświetlenie spadło poniżej poziomu minimalnego, przetwornik jest wspomagany promiennikiem IR o zasięgu do 150 m. Obiektyw o zakresie ogniskowych 4,8-120 mm umożliwia identyfikację osoby z odległości do 160 m.

Model PTZ1A225U-IRA-N wspiera zarówno standard kodowania H.264, jak i H.265, również w wersji Smart, umożliwia transmisję trzech strumieni wizji, pozwala także na zastosowanie różnych algorytmów inteligentnej analizy. Wiele funkcji wspomagających, takich jak WDR 120 dB, *defog*, elektroniczna stabilizacja obrazu czy redukcja szumu 2D i 3D umożliwia rejestrację klarownego obrazu w zróżnicowanych warunkach atmosferycznych i oświetleniowych.
Obudowa o klasie szczelności IP67 i odporności IK10 dopełnia obraz tego nietypowego urządzenia, które ze względu na specyficzną aparycję może budzić zainteresowanie na skostniałym rynku kamer PTZ.

MAZi: Kamera wielokanałowa IDH-23PTZ

Kamera panoramiczna
- 3 przetworniki, każdy 1/2,8" 2 Mpix, na obwodzie obudowy
- Pole widzenia każdego to 130° i podświetlenie IR

Kamera PTZ
- Przetwornik 1/2,8" 2 Mpix umieszczony w głowicy obrotowej
- Głowica obrotowa wyposażona w obiektyw z 4-krotnym zoomem optycznym

Nowy wymiar monitoringu

Rozwiązaniem łączącym szerokie pole widzenia z jednego punktu kamerowego z możliwością optycznego powiększenia jest kamera IDH-23PTZ. Kamera wyposażana jest w trzy kanały wizji zapewniające obserwację dookólną oraz jeden kanał do obserwacji PTZ. Operator, widząc zdarzenie na kanałach dookólnych, może je łatwo wskazać, oznaczając myszą, i skierować tam moduł PTZ. Kamera jest idealnym rozwiązaniem do monitorowania wnętrz budynków, sklepów i magazynów.

Przystosowana jest do montażu sufitowego (uchwyt IP-V300) oraz ściennego (uchwyt IW-V300).

Kamera zawiera najnowszy kodek H/265, wejście i wyjście audio, złącze na karty micro SD do 256 GB, możliwość zapisu na pamięciach NAS, analitykę obrazu (detekcję przekroczenia linii, wtargnięcia) oraz dostęp przez „chmurę".

Funkcja ANR *(Automatic Network Replenishment)* pozwala, w razie awarii łącza sieciowego, na zapis na karcie SD, a po odzyskaniu połączenia transfer zapisanych danych do urządzenia rejestrującego.

Wyłącznym przedstawicielem firmy MAZi Security Systems jest GDE Polska.

Hikvision: DS-2DF8836IX-AELW

Model należy do nowej generacji kamer PTZ z linii profesjonalnej Hikvision.

To pierwsza kamera obrotowa o rozdzielczości 4K w ofercie firmy, wyposażona w technologię *DarkFighter*. Bardzo czuły przetwornik obrazu CMOS o przekątnej 2/3" wspomagany przez najnowszej generacji procesor zapewnia płynny obraz w najwyższej rozdzielczości z szybkością 30 kl./s.

Dzięki technologii *DarkFighter* kamera generuje obraz bez utraty kolorów nawet przy bardzo słabym oświetleniu. Na uwagę zasługuje także jej układ optyczny. Obiektyw o 36-krotnym zoomie optycznym (7,5 – 270 mm) zapewnia wyjątkowy poziom szczegółów, a funkcja *Optical Defog* pozwala dostrzec obiekty nawet przez mgłę.

Układ optyczny został wyposażony w funkcję *Rapid Focus,* która ustawia ostrość podczas zmiany parametrów ogniskowej tak szybko, że użytkownik ma wrażenie ciągłego ostrego obrazu.

Uniwersalność kamery podkreślają silny WDR 120 dB oraz promiennik IR o zasięgu 200 lub 500 m (w zależności od wersji).

Model DS-2DF8836IX-AELW został wyposażony w procesor odpowiadający za pracę algorytmów *deep learning*. Wzbogaca to kamerę w funkcjonalności inteligentnego rozpoznania, identyfikacji i śledzenia obiektów.

Hikvision: DS-2DF8250I5X-AELW

Już w nazwie tego segmentu kamer *(Pan, Tilt, Zoom)* zawarto wyróżniającą go cechę – oprócz możliwości wychylenia poziomego i pionowego kamera musi oferować także zoom.
To właśnie na ten aspekt postawiono przy projektowaniu prezentowanego modelu DS-2DF8250I5X-AELW.

Urządzenie zostało wyposażone w unikatowy obiektyw o ogniskowej 6,6 – 330 mm, który oferuje 50-krotny zoom optyczny. Kamera ma także optyczną stabilizację obrazu, dzięki której nawet przy dużym przybliżeniu obraz jest stabilny w każdych warunkach.
Jako że model należy do serii profesjonalnej, znajdziemy tu wszystkie aspekty cechujące tę platformę.
Są to m.in. analiza obrazu oparta na algorytmach *deep learning*, WDR 120 dB i promiennik podczerwieni o zasięgu do 500 m.
Co równie istotne, kamera generuje obraz w rozdzielczości 1920 x 1080 pix z wykorzystaniem kodeka H.265.

Hikvision: DS-2DF6A236X-AEL

DS-2DF6A236X-AEL to model wyróżniający się w ofercie firmy Hikvision oryginalnym designem.

W przeciwieństwie do poprzedniej generacji kamer obudowa tego modelu nie ma klosza co pozwoliło uzyskać większy zakres wychylenia pionowego (od -20 do 90 stopni).

Jednocześnie, zamontowana na odpowiedniej wysokości (około 3 m) nie zdradza kierunku obserwacji. Oczywiście, jak we wszystkich kamerach obrotowych z serii profesjonalnej, został zachowany standard IK10 i IP66.
W środku kamery znajduje się 2 Mpix przetwornik obrazu o przekątnej 1/1,9" z zaimplementowaną technologią *DarkFighter*, poprawiającą czułość. To wszystko sprawia, że kamera bez problemu może pracować w trybie kolorowym bez przerwy – 24/7.
Ponadto wyróżniają ją takie funkcje, jak *Rapid Focus*, WDR 120 dB, najnowsze kodeki obrazu oraz analiza obrazu oparta na *deep learning*.

Model DS-2DF6A236X-AEL jest zatem idealnym rozwiązaniem np. do miejskich systemów monitoringu wizyjnego.

Miwi Urmet: Interceptor HD PTZ IndigoVision

Interceptor HD PTZ to kamera idealna do zadań specjalnych.

Dzięki innowacyjnej konstrukcji kamera nie ma konkurencji na rynku. Niezawodna, wzmocniona konstrukcja (IP68, IK10) pozwala zastosować urządzenie w najbardziej wymagających systemach zabezpieczeń.
Interceptor HD PTZ ma rozszerzony zakres ruchów, co przy jej montażu dolnym redukuje do zera martwą strefę obserwacji. Oprócz podświetlacza podczerwieni wykorzystuje podświetlenie światłem białym. Dzięki temu możliwe jest śledzenie intruza nawet z odległości 250 m w rozdzielczości 1080p w kolorze. Dzięki zainstalowanej wycieraczce obraz z kamery jest czytelny nawet przy niekorzystnych warunkach atmosferycznych. Z kolei Interceptor HD PTZ w wersji z radarem jest idealnym narzędziem do śledzenia intruza w całkowitej ciemności lub w złych warunkach atmosferycznych.
Kamera wykorzystuje najnowszy przetwornik obrazu Sony CMOS Starvis, co gwarantuje doskonałą jakość obrazu w rozdzielczości HD w każdych warunkach oświetleniowych. Jest kompatybilna ze wszystkimi wersjami oprogramowania *Control Center* i stanowi część kompleksowego rozwiązania IndigoVision.
Dzięki tej kamerze żaden intruz nie może czuć się bezkarnie, naruszając obszar chroniony, a użytkownik ma zapewnione poczucie bezpieczeństwa.

Więcej na stronie internetowej dystrybutora: www.miwiurmet.pl lub producenta: www.indigovision.com

Hikvision: DS-2DE7430IW-AE

Nowości nie ominęły także serii ekonomicznej kamer Hikvision.
Model DS-2DE7430IW-AE to 4 Mpix kamera obrotowa dedykowana do systemów IP. Została wyposażona w przetwornik obrazu CMOS 1/1,9".
Kamera generuje obraz o rozdzielczości 2592 x 1944 z wykorzystaniem kodeka H.265. Ponadto wyróżnia się układem optycznym o 30-krotnym zbliżeniu optycznym.
Ma też wbudowany promiennik podczerwieni o zasięgu do 150 m.
Jest to korzystne cenowo rozwiązanie, gwarantujące bardzo dobrą jakość obrazu.

Cała seria, do której należy ten model, sprawdzi się w dozorze wizyjnym obszarów, takich jak drogi, place czy parkingi.

Panasonic: WV-X6531N

Odporna na warunki atmosferyczne kamera sieciowa full HD z technologią *Smart Coding*.

Technologia *Smart Coding* w standardzie kompresji H.265 inteligentnie redukuje wykorzystanie łącza nawet o 95 proc. w porównaniu ze standardem H.264, a to przekłada się na dłuższy czas nagrywania i mniejsze użycie pamięci.
Model WV-X6531N automatycznie rejestruje obrazy najwyższej jakości nawet w niezwykle trudnych i szybko zmieniających się warunkach otoczenia. Kamera ma 40-krotny zoom z inteligentną stabilizacją obrazu oraz inteligentny tryb automatyki (iA), który monitoruje dynamikę i ruch w obrębie sceny, automatycznie sterując najważniejszymi ustawieniami kamery w czasie rzeczywistym. Umożliwia to redukcję zniekształceń, takich jak rozmycie poruszających się obiektów.

Jednocześnie model WV-X6531N jest wyjątkowo odporny na warunki atmosferyczne. Kamera ma stopień ochrony obudowy IP66 i IK10. Może pracować w szerokim zakresie temperatury: od -50°C do 60°C. Ma też wytrzymały mechanizm obrotu/pochylenia.
Opcjonalnie kamerę można wyposażyć w funkcję *Vehicle Incident Detection* umożliwiającą wykrywanie jadących pod prąd lub stojących pojazdów i wysyłanie alertów do systemu dozoru wizyjnego lub zarządzania ruchem, by podjąć natychmiastowe działania. Dzięki temu, że funkcja jest wbudowana w kamerę, system nie wymaga stosowania dodatkowego serwera.
Kamera WV-X6531N ma ponadto wiele funkcji spotykanych zwykle w modelach najwyższej klasy. Rejestruje obrazy w rozdzielczości full HD 1920 × 1080 pix z prędkością 60 kl./s.

Technologia *Extreme Super Dynamic* zapewnia rozszerzony zakres dynamiki: 144 dB. Umożliwia kolorowy podgląd nocny (przy natężeniu światła od 0,001 do 0,015 lx). Doskonałą widoczność zapewnia też specjalna powłoka *ClearSight* nałożona na powierzchnię przezroczystej pokrywy obiektywu, która zapobiega formowaniu się na niej kropel wody.

Panasonic: WV-SUD638

Model WV-SUD638 Aero PTZ to smukła i wytrzymała na czynniki atmosferyczne kamera rejestrująca obrazy w jakości full HD.

Kamera doskonale sprawdza się m.in. w transporcie, systemie monitoringu miejskiego, w portach, na lotniskach i autostradach oraz w innych wymagających lokalizacjach, gdzie występują ekstremalne warunki atmosferyczne.
Aero PTZ rejestruje obrazy w rozdzielczości full HD 1080p z prędkością 60 kl./s. Ma 30-krotny zoom optyczny i specjalną aerodynamiczną konstrukcję, która umożliwia rejestrowanie obrazów nawet przy podmuchach wiatru sięgających 216 km/h.
Kamera jest wyposażona w hybrydowy system stabilizacji obrazu, składający się ze stabilizatora i czujników żyroskopowych, które kompensują ruchy silniczków odpowiedzialnych za pochylanie i obracanie urządzenia. Funkcja ta eliminuje problemy związane z przybliżaniem obrazu w trakcie silnego wiatru lub gdy kamera jest zamontowana na słupie albo odsłoniętym adapterze.
Aero PTZ jest wyposażona w mechanizm *Sphere Vision 3D* umożliwiający obrót w zakresie 360 stopni oraz pochylanie +/-90 stopni, a także w funkcję *Super Dynamic Light Range Compensation* zapewniającą szerszy zakres dynamiki w porównaniu z tradycyjnymi kamerami.
Model jest w pełni odporny na działanie wody i pyłu (IP67, NEMA-4X i IK10). Może pracować w temperaturze od -50°C do 55°C, a dzięki wbudowanej wycieraczce gwarantuje dobrą widoczność podczas deszczu lub śniegu i w błocie.
Kamera jest wyposażona w odszraniacz, który topi śnieg lub lód gromadzący się na przedniej szybie. Z kolei obudowa z włókna szklanego gwarantuje ochronę przed korozją. Zaletą Aero PTZ jest też niezwykle lekka osłona z tworzywa najwyższej jakości, pozwalająca zredukować koszty montażu, szczególnie w wysoko położonych miejscach.

Tiandy

INTELIGENTNA KAMERA PANORAMICZNA

LET'S STARLIGHT IT

- Opatentowana technologia obrazu panoramicznego "Beveled Joint"
- Modułowa budowa dopasowana do Twoich potrzeb: kamera 180°, kamera 360°, laser, termowizja itp.
- Automatyczne śledzenie z systemem wczesnego ostrzegania - Jedyny dostawca takiego rozwiązania na rynku
- Daleki zasięg widzenia do 1000m
- Wbudowany żyroskop zapewniający stabilny obraz w każdych warunkach
- SuperStarlight - Obraz w kolorze 24h

Tiandy Technologies Co.,Ltd.

Email: sales@tiandy.com
Phone: +86-22-58596065
Fax : +86-22-58596048
Website: en.tiandy.com

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

Zasilacz do zadań specjalnych

Pewność i efektywność zasilania to istotne zagadnienia, które muszą być poważnie potraktowane przy doborze urządzeń wchodzących w skład systemów zabezpieczeń. Rozumiane w szerokim zakresie bezpieczeństwo zasilania jest sprawą fundamentalną, gdyż w przypadku jego utraty lub poważnej awarii system może przestać funkcjonować – co może skutkować często bardzo poważnymi konsekwencjami.

Głównym elementem SSWiN są centrale alarmowe. Obecnie większość z nich ma wbudowany zasilacz i jest podłączana do sieci poprzez transformator, który nie tylko obniża napięcie, ale także stanowi separację galwaniczną. Co jednak w sytuacji, gdy wraz z podłączeniem do centrali kolejnego urządzenia zostanie przekroczona wydajność prądowa wbudowanego zasilacza? Jak należy postąpić w przypadku, gdy urządzenia takie jak ekspandery wejść/wyjść, moduły komunikacyjne, monitorujące czy chociażby czujki są znacznie oddalone od centrali lub gdy nie dysponujemy wystarczającą liczbą przewodów do ich podłączenia?

Zasilacze buforowe

W przypadku konieczności zwiększenia wydajności prądowej systemu, przy dużych odległościach między urządzeniami lub np. do zasilania modułów komunikacyjnych pracujących autonomicznie należy sięgnąć po zasilacze buforowe. Dzięki ich wykorzystaniu i montażowi w pobliżu zasilanej elektroniki unikniemy spadków napięć występujących na przewodach o znacznej długości, a także ograniczymy liczbę żył ciągnących się od centrali do urządzeń – niezbędne będzie wówczas jedynie ułożenie/wykorzystanie przewodów sygnałowych. Zasilacze buforowe, przy współpracy z akumulatorami, zapewniają zasilanym urządzeniom nieprzerwaną pracę nawet w przypadku awarii sieci energetycznej bądź też gdy zasilanie sieciowe jest przez wiele godzin niedostępne.

Jedno urządzenie wiele możliwości

Jednym z najbardziej zaawansowanych technologicznie zasilaczy buforowych jest model

ZASILACZ BUFOROWY APS-612

- zgodny z EN 50131-3 Grade 3, EN 60950-1 oraz EN 55011 Class B
- zasilacz impulsowy 12 VDC nie wymaga transformatora sieciowego
- łączna wydajność prądowa zasilacza 6 A: 3 A (wyjście) + 3 A (ładowanie)
- zabezpieczenia przeciwzwarciowe i przeciwprzeciążeniowe
- możliwość wyboru wartości prądu ładowania akumulatora (1,5 A/3 A)

Zaawansowany zasilacz buforowy APS-612 można wykorzystać m.in. do zasilania urządzeń medycznych lub w instalacjach automatyki przemysłowej czy w systemach infrastruktury krytycznej.

APS-612, którego parametry są „zakodowane" w nazwie – wydajność prądowa wynosi 6 A (3 A do zasilania urządzeń, 3 A do ładowania akumulatora), a napięcie zasilania 12 VDC. APS-612 w zakresie bezpieczeństwa odpowiada wymogom EN 60950-1, natomiast biorąc pod uwagę kryterium kompatybilności elektromagnetycznej, jest zgodny z EN 55011 Class B. Co należy podkreślić, model ten spełnia wysokie wymagania bezpieczeństwa Grade 3 określone normą EN 50131-3 – może być zatem stosowany tam, gdzie od systemów zabezpieczeń oczekuje się najwyższego stopnia ochrony.

Zasilacz ten może pracować jako źródło energii w systemach sygnalizacji włamania i napadu, kontroli dostępu czy CCTV. Ale to nie wszystko, z powodzeniem zasili elektronikę systemów automatyki przemysłowej, infrastruktury krytycznej czy urządzeń medycznych, np. w laboratoriach, gdzie urządzenia zasilające muszą sprostać restrykcyjnym wymaganiom norm.

Przy współpracy z urządzeniami SATEL dla wygody użytkowania można wykorzystać specjalne złącze 3-pinowe. Dzięki temu można szybko podłączyć np. ekspandery wejść/wyjść, centrale kontroli dostępu ACCO-NT czy nowe uniwersalne moduły: komunikacyjny GSM-X i monitorujący GPRS-A.

Budowa i szczegóły techniczne APS-612

Konstrukcja urządzenia bazuje na zasilaczu impulsowym o topologii LLC. Dzięki temu charakteryzuje się ono wysoką sprawnością, oferując bardzo dobre parametry pracy przy niskich stratach cieplnych. Opisywany zasilacz zawiera na wejściu filtr przeciwzakłóceniowy oraz aktywny układ korekcji współczynnika mocy PFC (do 0,98). Do sieci 230 VAC jest podłączany bezpośrednio, bez konieczności stosowania dodatkowego transformatora sieciowego.

APS-612 został wyposażony w układ mikroprocesorowej kontroli parametrów akumulatora oraz precyzyjnej regulacji napięcia ładowania prądem 1,5 A lub 3 A. Posiada także funkcję automatycznego odłączenia w przypadku nadmiernego rozładowania. Wszystko po to, aby ograniczyć możliwość uszkodzenia akumulatora oraz wydłużyć jego żywotność.

W zakresie bezpieczeństwa odpowiada wymogom normy EN 60950-1, natomiast biorąc pod uwagę kryterium kompatybilności elektromagnetycznej, jest zgodny z EN 55011 Class B.

Podsumowując, zasilacz buforowy APS-612 jest efektywnym urządzeniem zasilającym, które znajdzie zastosowanie m.in. w systemach alarmowych realizowanych w stopniu 3 (Grade 3) wg EN 50131. Wysoka sprawność, dobra wydajność prądowa oraz różnorodność zabezpieczeń to cechy, które z pewnością predestynują ten model do stosowania w wymagających elektronicznych systemach zabezpieczeń.

3 scenariusze rozwoju transportu

MOBILNOŚĆ W DOBIE CYFRYZACJI

**Czy przyszłość należy do samochodów elektrycznych?
Na czym polega Internet Aut?
Jak zmieni się system transportowy?**

Borys Cieślak
ekspert w zespole ds. sektora publicznego, innowacji i zachęt inwestycyjnych, Deloitte

Ambitna rządowa wizja rozwoju polskiej elektromobilności, zarówno prywatnej, jak i publicznej, może wydawać się trudna do zrealizowania. Powinna jednak skłaniać do refleksji nad przyszłością transportu miejskiego. Państwowym planom zarzuca się brak mechanizmów zwiększających popyt na auta elektryczne. Inne kraje wspierają ten obszar ulgami podatkowymi i dotacjami. Bardziej realna od masowej produkcji polskiego auta elektrycznego jest rządowa koncepcja polskiego e-autobusu. W czerwcu ub.r. z inicjatywy Ursus Bus zostało powołane konsorcjum, którego zadaniem będzie jego zaprojektowanie.
Niezależnie od działań rządu Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej ogłosił nabór na dofinansowanie zakupu przez samorządy autobusów elektrycznych. W puli środków jest 200 mln zł, w większości przeznaczonych na pożyczki. W niektórych polskich miastach autobusy z napędem elektrycznym można spotkać już dziś.

Nowe możliwości

Elektromobilność to tylko jeden z elementów coraz bardziej złożonego systemu transportowego. Rosnącą popularność współdzielenia podróży, wejście na polski rynek firmy Uber i protestujący

przeciwko niej taksówkarze, zmiany stylu życia mieszkańców miast (na zdrowszy), apele rowerzystów o nowe ścieżki rowerowe i rozbudowę systemów rowerów miejskich czy w końcu nieśmiało pojawiające się w polskich miastach auta na minuty – to nowości kilku ostatnich lat. Nowości, które trzeba uwzględniać w strategii i polityce transportowej miasta.

Podsumowaniem ostatnich zmian w sektorze transportu i refleksją nad możliwymi kierunkami jego rozwoju jest raport firmy Deloitte *Digital Age Transportation: The Future of Urban Mobility.* Autorzy zaznaczają, że naiwością byłoby formułować konkretne wizje, natomiast warto zastanowić się, dokąd doprowadziłaby ekstrapolacja obecnych trendów. W ten sposób nakreślili trzy scenariusze rozwoju transportu w dobie cyfryzacji:

1. INTERNET AUT

Samochody połączone z Internetem mogą zrewolucjonizować sektor motoryzacji, tak jak smartfony zmieniły telekomunikację – uważają Andreas Mai i Dirk Schlesinger z Cisco. Autorzy raportu zastanawiają się, jakie korzyści przyniesie nieuchronne połączenie aut za pomocą sieci Internet z innymi urządzeniami, z infrastrukturą drogową, źródłami danych i systemami transportu publicznego. Twierdzą, że wykroczą one poza rozrywkę i nawigację. Stała łączność ma umożliwić rozwój transportu intermodalnego i aut bezzałogowych.

Podmiotem w tym scenariuszu jest użytkownik, nie samochód. Auto stanie się tylko jednym z elementów ekosystemu. Mobilność ma być w przyszłości rozumiana jako usługa, a pytanie o dojazd będzie brzmieć nie „jak najszybciej dojadę tam moim autem/rowerem/autobusem", a „jak najlepiej tam dojadę". Aplikacja skonfiguruje dla nas optymalną kombinację środków transportu dla danej podróży.

2. DYNAMICZNE USTALENIE CEN

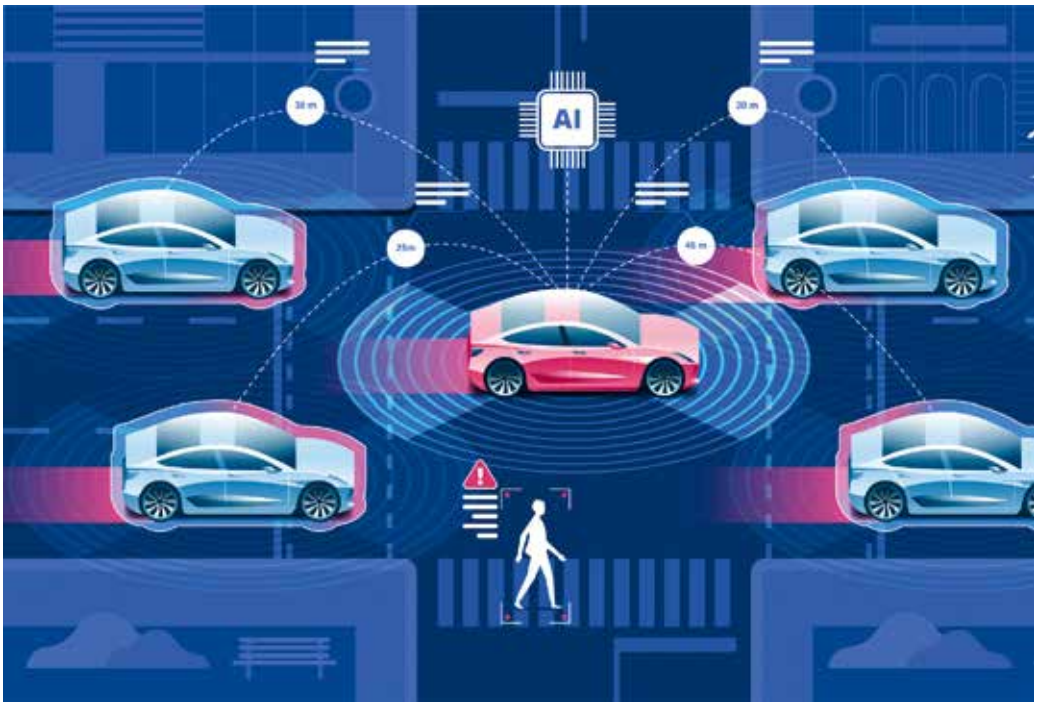
Linie lotnicze i hotele od lat dostosowują ceny do aktualnego popytu. Dzięki rozwojowi technologii mobilnych, systemów lokalizacji i płatności „bezdotykowych" dynamiczne ceny wkraczają również do sektora mobilności. Ich zastosowanie ma zwiększyć efektywność systemu transportowego. Kierowcy i pasażerowie będą znali faktyczne koszty swoich decyzji i będą wybierać czas, trasę i środek transportu, biorąc pod uwagę nie tylko własne potrzeby, ale także potrzeby innych uczestników ruchu. Osoby kierujące ruchem oraz dostawcy usług transportowych będą mogli dostosowywać ceny do bieżących warunków (np. korków, kosztów, popytu) i zachęcać użytkowników do wyboru preferowanych w danej chwili środków transportu. Przykładowo, gdy metro będzie przeciążone, jego potencjalni pasażerowie będą informowani o alternatywie, np. autobusie. Również w tym przypadku mobilność jest postrzegana jako usługa.

3. TRANSPORT SPOŁECZNY

Jednym z problemów współczesnego systemu transportowego jest brak komunikacji pomiędzy jego uczestnikami. Może się to zmienić wraz z rozwojem sieci społecznościowych oraz łączności między autami, infrastrukturą i użytkownikami. W tym scenariuszu mobilność w przyszłości będzie się opierać na współpracy sąsiadów, lokalnych społeczności, samorządu i osób zarządzających ruchem – będzie czymś więcej niż sumą indywidualnych podróży. Już dziś można zaobserwować przejawy takiego współdziałania. Współdzieląc auto z obcymi osobami (np. za pomocą platformy *ridesharingowej)*, wspólnie i indywidualnie zmniejszamy koszty podróży oraz zatłoczenie na drogach, ale także wybieramy kierowcę lub pasażera na podstawie opinii innych użytkowników. Innymi słowy, współpracujemy.

Który scenariusz się sprawdzi?

Przedstawione scenariusze nie wykluczają się, ale uzupełniają i mogą się równolegle rozwijać. To, jaki kształt przyjmie sektor transportu w dobie cyfryzacji, zależy od skomplikowanej gry pomiędzy sektorem publicznym i motoryzacyjnym, dostawcami technologii, przedsiębiorcami i wieloma innymi podmiotami. Istotna jest też strategia, jaka zostanie obrana wobec wyzwań, które niesie ze sobą każdy ze scenariuszy.



Telematyka

ZA KIEROWNICĄ BEZPIECZNIEJSZYCH I INTELIGENTNIEJSZYCH SAMOCHODÓW

Telematyka odgrywa kluczową rolę w bezpieczeństwie jazdy i zabezpieczeń samochodów. Jej podstawowymi elementami są nawigacja GPS, śledzenie pojazdów i bezpieczeństwo jazdy. **Ewolucja technologii IoT, aplikacje do zarządzania flotą, uwarunkowania prawne i rosnące wykorzystanie smartfonów przyczyniają się do rozwoju tego obszaru.**

Weili Lin
a&s International

Telematyka jest szeroko wykorzystywana w technologiach związanych z pojazdami. Łączenie telekomunikacji i informatyki zapewnia śledzenie lokalizacji, łączność bezprzewodową i systemową kontrolę elektroniki pojazdowej. Dzięki nowym generacjom technologii komunikacji – takim jak 4G czy oparta na radiowym standardzie 802.11p wydzielona łączność krótkiego zasięgu (DSRC – *Dedicated Short-Range Communications*) oraz Internet Rzeczy (IoT – *Internet of Things*) – usługi telematyczne nieprzerwanie się rozwijają, oferując więcej inteligencji i korzyści. Obecnie usługi telematyczne to nie tylko nawigacja GPS, śledzenie pojazdów i podstawowe funkcje związane z bezpieczeństwem jazdy. Przy użyciu zaawansowanej analityki danych i uczenia maszynowego kierowcy i zarządzający flotą mogą wykorzystywać informacje w celu zwiększania bezpieczeństwa jazdy i ograniczania zużycia paliwa. Mogą też korzystać z dodatkowych funkcji, takich jak przewidywanie przeglądu samochodu oraz wgląd w stan pojazdu i styl jazdy. Gdy pojazdy są połączone z chmurą, kierowcy mogą w czasie rzeczywistym otrzymywać powiadomienia o zajętości miejsc parkingowych, natężeniu ruchu i warunkach drogowych w okolicy, a także pobierać aktualizacje systemowe pojazdu.

Dla producentów samochodów bardziej inteligentne, skomunikowane rozwiązania telematyczne tworzą większą wartość. Powstają nowe modele biznesowe, takie jak UBI (*User-Based Insurance*), czyli indywidualne, oparte na danych telematycznych ubezpieczenia. Przykładem tego, jak klienci wykorzystują analitykę danych i uczenie maszynowe, jest telematyka w smartfonach zyskująca na znaczeniu w przypadku ubezpieczeń UBI i zarządzania flotą.

Rynek rozwojowy

Globalny rynek branży telematycznej odnotowuje w ostatnich latach pokaźne wzrosty, które mają się utrzymywać. Przewiduje się, że w ciągu kilku najbliższych lat komercyjna telematyka pojazdowa będzie rosnąć w tempie dwucyfrowym. Rynek telematyki pojazdowej obejmuje samochody osobowe oraz tabor pojazdów lekkich i ciężkich w segmencie komercyjnym. Według analiz to Ameryka Północna, Europa oraz region

Azji i Pacyfiku będą w nadchodzących latach największymi regionalnymi rynkami w światowej branży telematycznej.
W branży motoryzacyjnej region Azji i Pacyfiku przeżywa obecnie rozkwit – szybko rośnie tam liczba nowych aut projektowanych w celu zwiększenia sprzedaży systemów telematycznych i pozyskania abonentów usług.
Allen Cheng, Senior Industry Analyst w Market Intelligence & Consulting Institute (MIC), wskazuje, że w dużym tempie zwiększa się rynek w obszarze pojazdów pasażerskich w Indiach, notując dwucyfrowy wzrost w skali roku.
Systemy telematyczne są podstawą inteligentnych i skomunikowanych w sieci pojazdów, zapewniając szybki zwrot z inwestycji (ROI), zgodność z regulacjami rządowymi, poprawą bezpieczeństwa jazdy oraz lepsze zarządzanie zużyciem paliwa i wydajnością floty. Dla zarządzających flotą oraz firm logistycznych telematyka może pełnić ważną funkcję w biznesie, stając się generatorem przychodów (dzięki niej można sporo zaoszczędzić na paliwie). W swoim dorocznym raporcie firma TomTom Telematics – jeden z największych europejskich dostawców usług typu *connected car* i zarządzania flotą – twierdzi, że niektórzy klienci dzięki usługom dostarczanym przez TomTom uzyskali oszczędności na paliwie i wydajności pojazdów przekraczające 20 proc.
Z kolei z najnowszej publikacji firmy analitycznej Frost & Sullivan wynika, że „wykorzystując technologię *connected truck*, operatorzy floty będą mogli zoptymalizować takie czynniki, jak zużycie paliwa, konserwacje i wynagrodzenie kierowców, które w sumie tworzą ponad 60 proc. całkowitego kosztu posiadania. Koszt części, w tym smarów i opon, w przypadku ciężkiego pojazdu komercyjnego może przekroczyć w ciągu roku 3000 dol., a zastosowanie predykcyjnej konserwacji obniży go niemal o 20 proc.". Według Frost & Sullivan globalny rynek rozwiązań typu *connected truck* tworzy szansę wzrostu w branży komercyjnej telematyki pojazdowej mimo relatywnie wysokich cen tego rodzaju produktów.
Autorzy w raportach Markets and Markets przewidują, że wartość rynku komercyjnej telematyki pojazdowej zwiększy się z 7,3 mld dol. w 2017 r. do 18,4 mld dol. w 2022 r., przy średniej rocznej stopie wzrostu na poziomie 20,3 proc. Na rozwój rynku większe wykorzystanie rozwiązań i usług telematycznych wpływają coraz powszechniejsze regulacje rządowe wymuszające stosowanie systemów śledzenia, a także rosnące zapotrzebowanie na smartfony. Firma badawcza Technavio natomiast spodziewa się szybkiego rozwoju światowego rynku telematyki komercyjnej, szacując średnią roczną stopę wzrostu w okresie 2017-2021 na 18 proc. Jej zdaniem w 2021 r. połowa tego rynku będzie należeć do obu Ameryk.

Co jest ważne dla klientów

Większa dostępność nowych pojazdów i rosnące zainteresowanie klientów są motorem rozwoju rynku telematyki. Po stronie popytu najważniejsze jest zapotrzebowanie na nawigację, pomoc w nagłych sytuacjach oraz bezpieczeństwo i zabezpieczenie samochodów. Zdaniem autorów raportu *Strategy Analytics* producenci powinni skupić się na usługach zwiększających bezpieczeństwo. Analiza tego, czym najbardziej interesują się właściciele pojazdów klasy średniej w USA, wskazuje na usługi śledzenia, takie jak pomoc w razie kradzieży samochodu, natychmiastowe powiadamianie o wypadku, zdalna diagnostyka, zdalne uruchomienie i ostrzeżenia dla nastoletnich kierowców.
W przypadku telematyki komercyjnej dla klientów, takich jak zarządcy floty i firm logistycznych, największe znaczenie mają poprawa efektywności i wydajności floty, bezpieczeństwo jazdy, a także ograniczenie zużycia paliwa i kosztów operacyjnych. Zdaniem analityków z IHS Markit do roku 2022 r. ponad 85 proc. nowych pojazdów w Ameryce Północnej i Europie będzie wyposażonych w telematykę. W rozbiciu na poszczególne kraje ma to wyglądać następująco: USA – 87 proc., Kanada – 89 proc., Niemcy – 91 proc., Wielka Brytania – 92 proc., Chiny – 54 proc. Do tego czasu ponad połowa światowej floty pojazdów będzie skomunikowana w chmurze.
Aby poznać preferencje konsumentów w obszarze technologii motoryzacyjnych, IHS Markit przeprowadziło ankietę wśród ponad 5000 właścicieli pojazdów w USA, Kanadzie, Chinach, Niemczech i Wielkiej Brytanii, którzy planują w ciągu 3 lat nabycie nowego pojazdu. Wśród pożądanych funkcjonalności największym zainteresowaniem cieszyła się pomoc drogowa, powiadamianie o wypadkach i systemy nawigacyjne. Badanie ujawniło też znaczne zapotrzebowanie na zintegrowane aplikacje w nowych samochodach.

Ile konsumenci z różnych krajów są skłonni wydać na telematykę

Kraj	Kwota (USD)
USA	484
Kanada	168
Niemcy	402
Chiny	294
Wlk. Brytania	386

Źródło: IHS Markit

> Kierowcy mogą w czasie rzeczywistym otrzymywać powiadomienia o zajętości miejsc parkingowych, natężeniu ruchu i warunkach drogowych w okolicy, a także pobierać aktualizacje systemowe, gdy pojazdy są połączone z chmurą.

Telematyka wbudowana kontra smartfony

Bezpieczeństwo jazdy jest także priorytetem dla rządów na całym świecie. Rządowe regulacje nakładające obowiązek instalowania systemów telematyki pojazdowej powinny wpływać na rozwój rynku. Częściowo z ich powodu, a po części w wyniku zwiększonego zainteresowania klientów rozwiązaniami typu *connected car* producenci coraz chętniej wbudowują telematykę w nowe pojazdy.
Według najnowszego raportu Technavio segment wbudowanych systemów telematyki komercyjnej rośnie średnio o 17,5 proc. Według szacunków do końca br. pojazdy z wbudowaną telematyką będą stanowić ponad 75 proc. sprzedaży nowych samochodów sportowych w USA oraz 35 proc. globalnie. Z kolei z raportu firmy Markets and Markets wynika, że branża telematycz-

nych układów sterowania (TCU – *Telematics Control Unit*) ma być w latach 2017-2022 najszybciej rozwijającym się rynkiem w segmencie pojazdów drogowych. Według analityków z Markets and Markets do najważniejszych czynników decydujących o rozwoju tego rynku należą regulacje dotyczące bezpieczeństwa, takie jak europejski system szybkiego powiadamiania o wypadkach drogowych eCall oraz systemy odzyskiwania skradzionych pojazdów. Wszystkie samochody osobowe w Europie do końca 2018 r. mają mieć zainstalowane sterowniki TCU. Wielu spośród największych producentów samochodów, w tym General Motors, Mercedes-Benz, BMW i Audi, dostarczają usługi wbudowane, szczególnie w Ameryce Północnej i Europie.

Wraz z upowszechnieniem się smartfonów zmieniło się też zachowanie konsumentów. Coraz większa liczba użytkowników jest zainteresowana integrowaniem aplikacji mobilnych ze swoimi samochodami. Smartfony stały się także urządzeniami monitorującymi jazdę i tanią alternatywą dla wbudowanych systemów telematycznych. Coraz więcej firm wprowadza do swoich ofert technologię czujników IoT i analitykę danych, proponując właścicielom flot komercyjnych i ubezpieczycielom usługi analityki behawioralnej i rozwiązania telematyczne oparte na smartfonach.

Konwergencja branżowa

Dostawcy produktów i usług telematycznych – producenci sprzętu, dostawcy usług telematycznych (TSP – *Telematics Service Providers*), operatorzy telekomunikacyjni,

Telematyka staje się czymś więcej niż narzędziem do komunikowania samochodów i ludzi. Każdy *connected car* stanie się zestawem przemieszczających się po drodze sensorów w skomunikowanym mieście.

producenci samochodów i części samochodowych (np. GM z OnStar) oferują własne rozwiązania telematyczne. Na rynku pojawiło się wielu nowych graczy, stopniowo zwiększających swoje udziały. Niektórzy z nich starają się poszerzyć ofertę produktową poprzez fuzje i przejęcia innych podmiotów, a także w wyniku zawarcia partnerstwa. Tego typu działania nie znikną, tym bardziej że stale będą się pojawiać nowe technologie i modele biznesowe.

W miarę jak nowe technologie będą znajdować zastosowanie w samochodach, do rywalizacji dołączą kolejne firmy, oferując własne rozwiązania.

Zarządzanie flotą jest ważnym obszarem zastosowania telematyki i w tym segmencie rynku doszło do kilku istotnych przejęć i fuzji. Przykładowo w rocznym raporcie firmy Verizon wykazano, że IoT jest najszybciej rozwijającym się obszarem działania tego operatora. Trzeba wiedzieć, że to dzięki przejęciu spółek Fleetmatics i Telogis w 2016 r. Verizon stał się główną firmą telematyczną w USA, umacniając swoją pozycję na rynku IoT, szczególnie w zakresie telematyki i skomunikowanych rozwiązań dla transportu. Z kolei koncern Michelin przejął NexTraq, amerykańskiego dostawcę telematyki dla flot komercyjnych, dzięki czemu ma przyśpieszyć swój strategiczny rozwój w obszarze telematyki, zwiększając zasięg geograficzny i konkurencyjność na rynku technologii i usług zarządzania flotą w USA. Continental, inny znany producent, zintegrował konwergentną platformę sieciową Carnegie Technologies z inteligentnym rozwiązaniem telematycznym dla producentów pojazdów, rozbudowując sterownik TCU nowej generacji o element analityki i diagnostyki oparty na chmurze obliczeniowej.

Wobec rosnącego zapotrzebowania na elektronizację i cyfryzację nowi gracze z branży IT stają się konkurencją dla firm dominujących dotychczas na rynku, a rozwój technologiczny może przeobrazić łańcuch dostaw w przemyśle motoryzacyjnym. *Wraz z pojawieniem się nowych graczy w branży telematycznej obserwujemy dużą presję ze strony producentów wyspecjalizowanych w obszarach IT, pamięci, kamer oraz paneli LCD* – twierdzi Allen Cheng. Po stronie popytu specjalista z MIC wskazuje na rozwój technologii HMI (*Human-Machine Interface*) oraz nowe usługi o wartości dodanej jako czynniki, które będą stymulować na rynku potrzebę wymiany pojazdów.

Przyszłość kształtuje IoT

To Internet Rzeczy – wykorzystujący zaawansowaną technologię czujników, gromadzenie danych w czasie rzeczywistym oraz analitykę w chmurze – stoi za technologicznymi innowacjami i transformacją sektora telematyki pojazdowej. Dzięki IoT usługi telematyczne nowej generacji będzie cechować większa inteligencja i zdolności komunikacyjne, dostępne będą aktualizacje systemowe w pojazdach, a do dyspozycji klientów zostaną oddane platformy zarządzane.

Jeśli chodzi o usługi w chmurze na świecie, to Allen Cheng zwraca uwagę, że liderzy tego rynku, tacy jak Amazon, Microsoft czy Google, mogą nawiązywać – jako dostawcy infrastruktury cyfrowej – partnerstwa z branżą telematyczną. Tego rodzaju współpraca ułatwi dostawcom rozwiązań telematycznych dalsze optymalizowanie wydajności, skróci czas projektowania i za-

pewni efektywność kosztową. Przykładowo MiX Telematics hostuje swoją aplikację SaaS (*Software-as-a-Service*) w infrastrukturze Amazon Web Services, uzyskując w ten sposób bardziej ekonomiczne rozwiązania *disaster recovery* i *backupu*.
Ponieważ dane są cennym zasobem w erze IoT, to ich monetyzacja stanie się podstawowym celem firm telematycznych. Gdy pojawią się nowe modele biznesowe wynikające z transformacji cyfrowej, można się spodziewać, że branża *connected car* będzie zarówno generować, jak i przetwarzać nie mniej mobilnych danych niż smartfony. *Konsumenci w Azji bardziej od abonamentowych wolą usługi freemium. Dlatego aby generować przychód, dostawcy usług telematycznych muszą w gospodarce danymi przyjąć odpowiednie modele biznesowe, takie jak cyfrowa reklama, albo pójść na współpracę z innymi podmiotami, np. firmami ubezpieczeniowymi* – tłumaczy przedstawiciel MIC.
Ponieważ coraz więcej samochodów jest połączonych z nowymi usługami różnych dostawców, kwestią newralgiczną staje się cyberbezpieczeństwo. Allen Cheng zwraca uwagę, że przełamanie zabezpieczeń pojazdu może wpłynąć na bezpieczeństwo jazdy i naruszyć prywatność kierowcy. *Uwzględnianie aspektów ochrony prywatności i zabezpieczeń w fazie projektowania staje się obecnie zasadą podczas konstruowania pojazdów* – wyjaśnia.
Telematyka staje się czymś więcej niż narzędziem do skomunikowanych samochodów i ludzi. Może ona tworzyć powiązania między pojazdami, infrastrukturą drogową i platformami w chmurze. W tym sensie każdy *connected car* stanie się zestawem przemieszczających się po drodze sensorów w skomunikowanym mieście albo rejonie.
Elektronizacja i cyfryzacja pojazdów jest trendem wyróżniającym się. W dającej się przewidzieć przyszłości samochody spełnią wizję autonomicznej jazdy, komunikując się ze sobą za pośrednictwem platformy w chmurze albo wykorzystując inne, znane z powieści *science fiction* technologie. Inteligentna centralna jednostka sterowania w samochodach nowej generacji stanie się ich podstawą, szczególnie w pojazdach elektrycznych.
Kierowcy również zaczęli żyć cyfrowym stylem życia i ich nawyki wpływają na projektowanie samochodów. Oczekuje się, że kolejna generacja systemów samochodowych będzie stale połączona z siecią i aktualizowana w bezprzewodowym trybie OTA (*Over-The-Air*) lub przy użyciu innych nowych technologii, w których zostanie uwzględnione znaczenie stabilności łącza sieciowego i bezpieczeństwa danych. Telematyka stacje się popularnym narzędziem w zarządzaniu flotą i aplikacjach ubezpieczeniowych i te zastosowania będą miały duży udział w rozwoju rynku w ciągu najbliższych lat.
Można oczekiwać, że nowa generacja usług telematycznych będzie wykorzystywać większą inteligencję i łączność oraz oferować użytkownikom aktualizacje systemowe i zarządzane platformy oparte na analityce w chmurze i IoT.

Efektywne zarządzanie ruchem dzięki *machine learning*

Uczenie maszynowe (*machine learning*) zwiększa możliwości monitorowania ruchu drogowego i analizy danych. Poprawia dokładność detekcji oraz przetwarza dane zbierane przez kamery i sensory w informacje, które mogą zostać wykorzystane w zapobieganiu wypadkom, eliminowaniu korków, zwiększaniu efektywności operacyjnej i planowaniu infrastruktury drogowej.

Weili Lin
a&s International

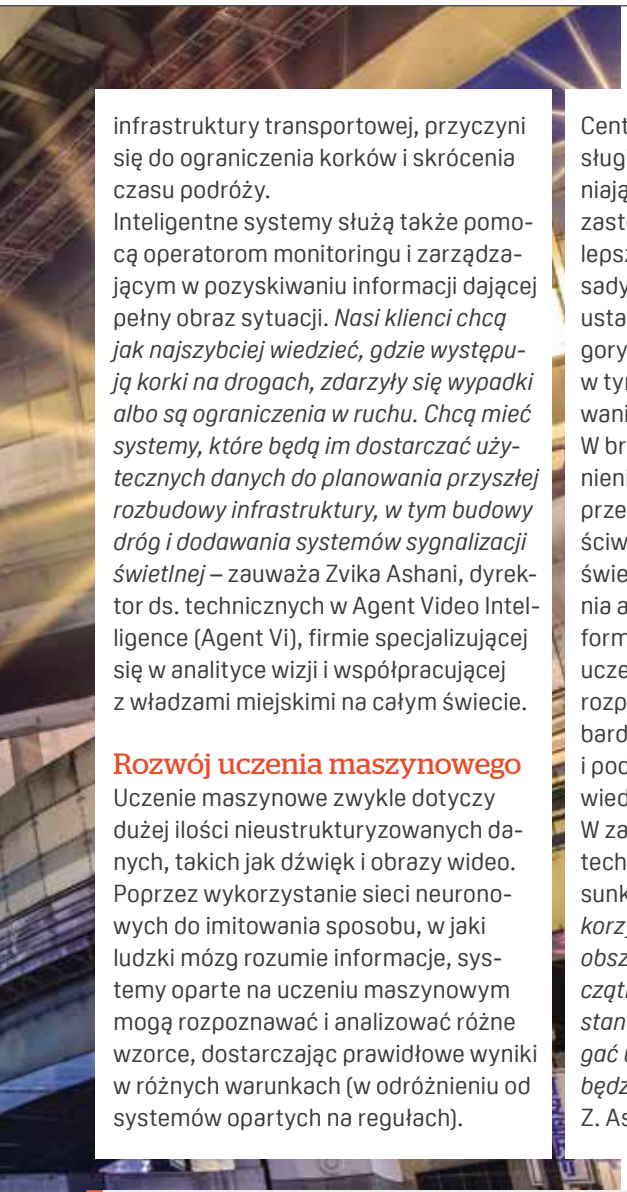
Na podstawie danych ONZ przewiduje się, że do 2030 r. niemal 60 proc. ludności będzie mieszkać na terenach zurbanizowanych. To pokazuje, z jak wielkim obciążeniem będą miały do czynienia systemy transportu drogowego. Zwiększenie liczby mieszkańców i pojazdów na drogach stawia rządy państw przed wieloma wyzwaniami dotyczącymi takiego zarządzania ruchem, by drogi były nie tylko przejezdne, ale także bezpieczne. Dzięki postępowi technologicznemu coraz więcej miast wykorzystuje sztuczną inteligencję (AI) do analizowania wzorców ruchu, zwiększania efektywności monitoringu, wprowadzania automatycznego wykrywania wypadków i szybkiego reagowania.

Firma Zion Market Research szacuje, że światowy rynek analityki wizji osiągnie wartość 11,1 mld dol. do 2022 r., przy średniej rocznej stopie wzrostu wynoszącej 34,3 proc. w latach 2017–2022. Największy udział w nim w ub.r. miała branża transportowa, a zwiększenie złożoności tego segmentu będzie w najbliższych latach wpływać na wzrost zapotrzebowania na analizę danych wizyjnych. Monitorowanie ruchu drogowego to główne zastosowanie wymagające od systemów analizy obrazów dostarczania dokładnych informacji.

Poradzenie sobie z olbrzymią ilością danych jest wyzwaniem dla operatorów monitorujących warunki drogowe na obszarze całego miasta. W efektywnym zarządzaniu ruchem może pomóc uczenie maszynowe. System może wykorzystywać dane nie tylko do analizy ruchu, ale także do przewidywania potencjalnych wypadków i zapobiegania im. W przyszłości te inteligentne systemy mogą zastąpić ludzi w podejmowaniu decyzji w razie wypadków.

Uczenie maszynowe w najbliższych latach będzie się bardzo szybko rozwijać w związku z przyspieszonym wprowadzaniem inteligentnych technologii przez władze miast. *Machine learning* nie musi się ograniczać do ruchu drogowego, można je wykorzystywać we wszystkich rodzajach transportu, także na kolei i lotniskach.

Nowe technologie staną się ważną częścią inteligentnych systemów transportu, w dużym stopniu ograniczając liczbę wypadków będących skutkiem percepcyjnego bądź poznawczego przeciążenia kierowców, błędu człowieka bądź niesprzyjających warunków środowiskowych. Użycie nowych rozwiązań usprawni planowanie, poprawi wykorzystanie



infrastruktury transportowej, przyczyni się do ograniczenia korków i skrócenia czasu podróży.
Inteligentne systemy służą także pomocą operatorom monitoringu i zarządzającym w pozyskiwaniu informacji dającej pełny obraz sytuacji. *Nasi klienci chcą jak najszybciej wiedzieć, gdzie występują korki na drogach, zdarzyły się wypadki albo są ograniczenia w ruchu. Chcą mieć systemy, które będą im dostarczać użytecznych danych do planowania przyszłej rozbudowy infrastruktury, w tym budowy dróg i dodawania systemów sygnalizacji świetlnej* – zauważa Zvika Ashani, dyrektor ds. technicznych w Agent Video Intelligence (Agent Vi), firmie specjalizującej się w analityce wizji i współpracującej z władzami miejskimi na całym świecie.

Rozwój uczenia maszynowego

Uczenie maszynowe zwykle dotyczy dużej ilości nieustrukturyzowanych danych, takich jak dźwięk i obrazy wideo. Poprzez wykorzystanie sieci neuronowych do imitowania sposobu, w jaki ludzki mózg rozumie informacje, systemy oparte na uczeniu maszynowym mogą rozpoznawać i analizować różne wzorce, dostarczając prawidłowe wyniki w różnych warunkach (w odróżnieniu od systemów opartych na regułach).

Centra monitorowania ruchu muszą obsługiwać wiele danych w stale zmieniającym się środowisku, dlatego takie zastosowanie wydaje się jednym z najlepszych dla uczenia maszynowego. Zasady ruchu drogowego są zasadniczo ustalone i jasne, toteż nadzorowane algorytmy uczenia maszynowego znajdują w tym sektorze powszechne zastosowanie.
W branży transportowej mamy do czynienia z obszernym zestawem reguł oraz przewidywalnych właściwych i niewłaściwych zachowań, dlatego jest ona świetnym kandydatem do wprowadzania automatyzacji wyszukiwania informacji w obrazie. W tym środowisku uczenie maszynowe ma zdolność do rozpoznawania nie tylko reguł, ale też bardziej skomplikowanych scenariuszy i podejmowania na ich podstawie odpowiednich działań.
W zastosowaniach transportowych technologia *machine learning* jest stosunkowo nowa i cały czas ewoluuje. *Wykorzystanie uczenia maszynowego w tym obszarze znajduje się wciąż w fazie początkowej, ale pewnego dnia stanie się standardem. Gdy ludzie zaczną dostrzegać udane wdrożenia, użycie technologii będzie rosnąć wykładniczo* – przewiduje Z. Ashani.

Guy Baron, dyrektor ds. technicznych w firmie Qognify, spodziewa się, że coraz więcej inteligentnych czujników wyposażonych w pakiet inteligentnych algorytmów będzie wdrażanych w ramach infrastruktury transportowej. Mogą one przetwarzać duże ilości danych w czasie rzeczywistym, a jednocześnie ułatwiać optymalizowanie operacji poprzez automatyczne identyfikowanie „przyczyny i skutku", a także dostarczać rekomendacje operatorom w celu zmiany decyzji operacyjnych i optymalizacji wyniku. *To już się dzieje. Można zauważyć znaczący wzrost tego trendu, gdy jest wykorzystywany potencjał IoT. Dla dostawców, integratorów systemowych i klientów machine learning, big data i sztucznej inteligencji stają się elementem kluczowym* – zauważa.

Wykrywanie obiektów i przewidywanie zdarzeń

W porównaniu do innych technik uczenie maszynowe zapewnia większą dokładność detekcji i klasyfikacji, np. wielkości pojazdu. Poprawia trafność i szczegółowość w klasyfikowaniu pojazdów, m.in. określaniu liczby osi przy naliczaniu opłat za przejazd lub odróżnianiu małych i dużych samochodów ciężarowych.
Jeszcze kilka lat temu technologie anali-

MACHINE LEARNING W URZĄDZENIACH BRZEGOWYCH I W CHMURZE

By zwiększyć wydajność systemu, firmy wbudowują algorytmy uczenia maszynowego w kamery, serwery lub w chmurę.
Zamiast przesyłać cały strumień wizji, można najpierw przetwarzać dane w urządzeniach brzegowych, a następnie metadane wygenerowane przez kamery wykorzystujące algorytmy uczenia maszynowego przekazywać do serwera. Pozwala to oszczędzić czas i pasmo oraz ogranicza obciążenie serwerów lokalnych i w chmurze. Takie rozwiązanie stosuje Bosch Security Systems w kamerach przeznaczonych do monitorowania i zarządzania ruchem drogowym. *Kamery mają zaimplementowaną tę technologię, moc obliczeniowa rośnie wraz z dodaniem kolejnej kamery do systemu monitoringu. Nie ma więc potrzeby stosowania dodatkowego serwera albo zwiększania zasobów w chmurze* – mówi Constant Rutten z Bosch Security Systems.

Gdy ilość danych wytwarzanych, rejestrowanych i analizowanych wzrasta, potrzebujemy większej mocy obliczeniowej na brzegu sieci, potrzebnej dla obciążających zasoby algorytmów. W odpowiedzi na to zapotrzebowanie będzie instalowanych coraz więcej urządzeń wyposażonych w procesory graficzne GPU lub układy logiczne FPGA – podkreśla Guy Baron z firmy Qognify.
Problemem jest wysyłanie danych wizyjnych z wielu kamer do serwera. Największą przeszkodą w przetwarzaniu danych wizyjnych w chmurze jest wąskie pasmo. Firma opatentowała architekturę rozproszonej analityki wizji, w której zadanie przetwarzania obrazu jest dzielone pomiędzy komponent brzegowy w sieci zdalnej lokalizacji a serwer oparty na chmurze. Zapewnia to wysoką wydajność analityki, jednocześnie eliminując potrzebę przesyłania strumieni wizji do chmury. Kamera dokonuje wstępnego przetwarzania i przekazuje tylko niewielką ilość danych do dalszego przetwarzania w chmurze, dzięki czemu dane są przesyłane w czasie rzeczywistym. W rezultacie system może obsługiwać dużą liczbę kamer bez przeciążania pasma.
Nowa architektura systemowa, znana jako *fog computing* (mgła obliczeniowa), może ułatwić przetwarzanie dużych ilości danych zbieranych przez czujniki.
Założenia architektury systemowej muszą być weryfikowane i z czasem się zmieniać. *Cloud computing* stał się standardem, ale do analizowania dużych ilości danych prawdopodobnie będzie potrzebny model bardziej hybrydowy. *W takiej architekturze dane będą zbierane i obrabiane przez algorytmy uczenia maszynowego w urządzeniach brzegowych albo w ich pobliżu, a następnie przekazywane do chmury do dalszego przetwarzania i długoterminowego przechowywania.*

Zastosowanie inteligencji opartej na *deep learning* i CV (*computer vision*)

	Deep learning			Computer vision		
	Kamera (brzeg)	Serwer (lokalnie)	Serwer (chmura)	Kamera (brzeg)	Serwer (lokalnie)	Serwer (chmura)
Detekcja obiektu	+			+		
Klasyfikacja obiektu	+	+	+		+	+
Rozpoznanie prostego obiektu	+	+	+		+	+
Rozpoznanie złożonego obiektu		+	+			+
Baza danych		+	+		+	+
Analiza i predykcja			+			niezalecane

zy obrazu zastosowane do śledzenia ciężarówek i mierzenia przepływu pojazdów w zatłoczonym środowisku (takim jak autostrada albo miejska ulica wypełniona wieloma różnymi obiektami – ludźmi, autobusami, motocyklami i rowerami) nie były wystarczająco dokładne. Algorytmy uczenia maszynowego, analizując dane pochodzące z kamer i czujników, wykrywają pojawienie się nietypowych wzorców, takich jak blokada drogi czy tłum na środku jezdni. System uczy się wzorców występujących w mieście w różnych porach dnia oraz dniach tygodnia i stale je aktualizuje.

Technologia *deep learning* jest odmianą *machine learning*, powszechnie stosowaną w przetwarzaniu obrazów statycznych i sekwencji wideo. Firma PureTech Systems wykorzystuje ją do uzupełniania innych metod analizy danych wizyjnych. Jest bardzo efektywną techniką klasyfikowania obiektów i eliminowania szumu w obrazie. Gdy mamy do czynienia ze skomplikowaną sceną bądź schematem detekcji opartym na obrazie o dużej rozdzielczości, *deep learning* okazuje się wyjątkowo przydatne w dokładnym identyfikowaniu celów. Jeśli system został poddany ćwiczeniom z wystarczającą liczbą wzorców, to potrafi rozróżniać, czy ma do czynienia z wypadkiem samochodowym, czy nagromadzeniem pojazdów. Algorytmy mogą analizować odległości pomiędzy autami pod różnymi kątami i na tej podstawie podawać precyzyjne informacje. Wypadki drogowe to zdarzenia nieuniknione i trudne do przewidzenia. Inteligentna predykcja ułatwia zapobieganie im na skrzyżowaniach, może też dostarczać wartościowych informacji.

> Dane z kamer można wykorzystywać nie tylko do analizy ruchu, ale także do przewidywania potencjalnych wypadków i zapobiegania im.

Rynek dysponuje już opartym na uczeniu maszynowym programem predykcyjnym, który przewiduje kolizje, wykorzystując metadane generowane z kamer do określania danych trajektorii pojazdu, a następnie koreluje je z informacjami z innych czujników (radaru lub systemów lokalizacyjnych GPS w pojazdach komunikujących się poprzez DSRC). Program predykcyjny jest uruchomiony na komputerze umieszczonym przy drodze, w pobliżu skrzyżowania.

Możliwości predykcyjne są ważne w określaniu, gdzie mogą wystąpić wypadki. Jeśli coś się zdarzy w określonym rejonie, inteligentny system powinien przewidzieć, że w ciągu kilku minut coś się wydarzy na innym obszarze.

W najbliższej przyszłości inteligentne systemy powinny już automatycznie podejmować decyzje i działania w przypadku nagłych zdarzeń. System może nauczyć się wzorców zdarzeń drogowych i tego, jak postępować w razie incydentu. Jeśli zdarzy się wypadek samochodowy, może określić, ile potrzeba karetek, i połączyć się z najbliższą placówką pogotowia lub policją w celu wezwania pomocy.

Bardziej wydajny monitoring

Wcześniej operatorzy przez wiele godzin oglądali na ekranach monitorów mnóstwo obrazów z kamer monitoringu ruchu ulicznego. Zmęczeni i rozpraszani często reagowali na incydenty z opóźnieniem. Rozwiązanie oparte na uczeniu maszynowym może wspomóc zespoły monitorowania. Taki system może wyświetlać powiadomienia, gdy wykryje wypadek. Platformy uczenia maszynowego mogą zapewniać działanie w trybie: 24 godziny, 7 dni w tygodniu przez cały rok, licząc, klasyfikując, śledząc, oceniając prędkość i identyfikując anomalie, bez najmniejszych śladów zmęczenia. Dzięki nim operatorzy będą bardziej efektywni przy podejmowaniu działania w razie wypadku.

Uczenie maszynowe dopasowuje wzorce i wykonuje zadania kognitywne na dużej ilości danych, które tradycyjnie musiałyby być przeskanowane i przetworzone ręcznie. Dzięki algorytmom uczenia maszynowego, które przetwarzają zapis wideo i rozpoznają obiekty, można udostępnić użytkownikom prosty i szybki mechanizm analizowania treści obrazu. W rezultacie przy wykonywaniu tego zadania mogą znacząco zredukować czas i nakład pracy.

System oparty na uczeniu maszynowym sam się uczy. Nie wymaga od użytkowników dostrajania i ustawiania parametrów, by osiągnąć dużą dokładność. To ogromny postęp. Użytkownik nie musi posiadać głębokiej wiedzy na temat dostrajania systemu, by osiągnąć pożądaną wydajność, gdyż system zrobi to za niego. Jest więc łatwiejszy we wdrożeniu i eksploatacji – wyjaśnia Z. Ashani.

W najbliższej przyszłości systemy będą umiały automatycznie identyfikować rodzaje ryzyka drogowego i problemy z bezpieczeństwem, przewidywać powstawanie korków, jednocześnie sugerując działania korygujące.

Większa dokładność, identyfikacja

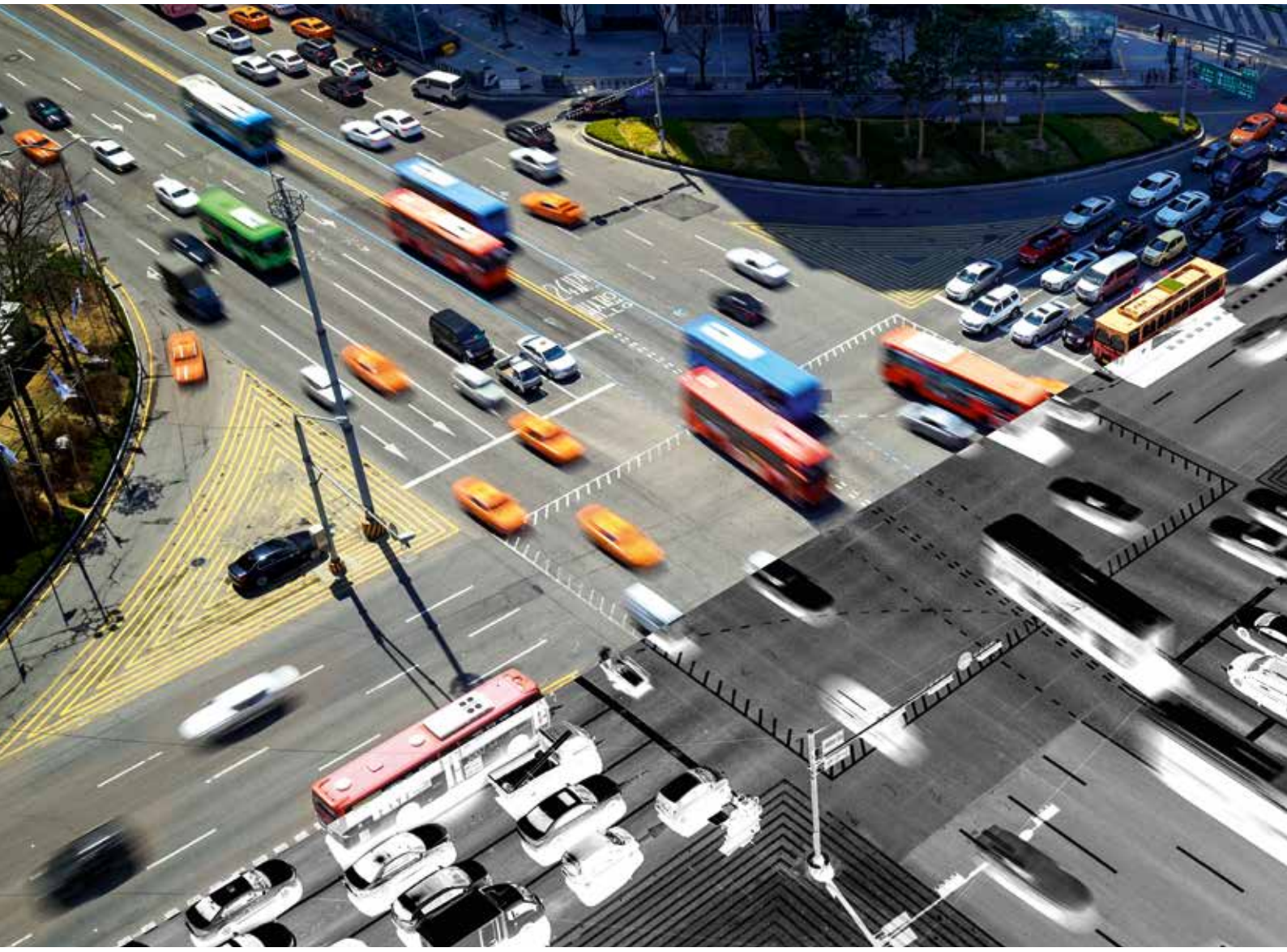
Jedną z największych korzyści płynących z uczenia maszynowego jest duża dokład-

ność algorytmów i większa niezawodność kamer dozorowych. Automatyczne technologie wizyjne już od ponad dekady są wykorzystywane w aplikacjach monitorowania ruchu ulicznego. Uczenie maszynowe wyraźnie wpływa na jakość wyników dostarczanych przez zautomatyzowane aplikacje monitoringu dzięki bardziej precyzyjnej detekcji zdarzeń oraz większej wiarygodności w niesprzyjających warunkach atmosferycznych i przy nieodpowiednim oświetleniu. W porównaniu do starszych technologii analizy obrazu nowe rozwiązanie zapewnia także udoskonalone śledzenie pieszych, rowerów i pojazdów w złożonej scenerii drogowej, z wieloma pojazdami i osobami poruszającymi się w polu widzenia kamery. Oferuje też nowe rodzaje analizy, które wcześniej nie były dostępne, np. wykrywanie nieprawidłowo zaparkowanych pojazdów dostawczych, powodujących w mieście poważne utrudnienia w ruchu.

Technologia skupia się na specyficznych szczegółach pojazdów, zapewniając większe możliwości detekcji. *Wcześniej technologie inteligentnej analizy wizji i fonii miały wąskie gardła, były mało precyzyjne i nie nadawały się do zastosowań biznesowych. Dopiero po dodaniu do systemów modeli uczenia maszynowego nastąpił znaczący wzrost dokładności w rozpoznawaniu ludzi, samochodów, dróg i innych ważnych elementów związanych z transportem* – opowiada Daniel Chau, dyrektor marketingu zagranicznego w Dahua Technology. Dahua rozpoczęła prace badawcze nad inteligentnymi algorytmami w 2009 r. i jest bliska zastosowania technologii uczenia maszynowego w swoich kamerach do identyfikacji pojazdów i ludzi oraz analiz statystycznych. Algorytmy uczenia maszynowego natomiast mogą w bardziej usystematyzowany sposób rozpoznawać cechy samochodów, takie jak typ, marka, model i kolor. *Łącząc różne elementy w jednej analizie można zidentyfikować namierzany pojazd, nawet gdy nie zostały zarejestrowane jego numery rejestracyjne* – wyjaśnia D. Chau.

Podsumowanie

Technologia uczenia maszynowego znalazła już zastosowanie w zarządzaniu ruchem, przed nią jednak długa droga do upowszechnienia. Systemy obsługujące *machine learning* wymagają dużych mocy obliczeniowych, dlatego produkty mające wspierać takie algorytmy muszą dysponować większymi mocami obliczeniowymi. Ponadto dobry system oparty na uczeniu maszynowym wymaga, by wszystkie jego elementy, w tym czujniki i analityka danych, generowały poprawne wyniki. Aby osiągnąć większą wydajność w monitorowaniu ruchu i zarządzaniu nim, trzeba dobrze poznać nową technologię, zanim się ją wdroży.



Termowizja wspomaga zarządzanie ruchem

Wraz z postępującą urbanizacją i wzrostem populacji rośnie zapotrzebowanie na coraz bardziej wydajne i efektywne systemy zarządzania ruchem ulicznym. **Wykorzystanie obrazowania termowizyjnego w ramach kompleksowego systemu zarządzania ruchem zapewnia operatorom bardziej dokładną i efektywną kontrolę.**

ZARZĄDZANIE RUCHEM: ŚWIATŁO WIDZIALNE vs. TERMOWIZJA

W zarządzaniu ruchem najpowszechniej wykorzystuje się kamery operujące w świetle widzialnym, to jednak użycie kamer termowizyjnych przynosi korzyści, których nie zapewnią inne rozwiązania.

Klasyczne kamery dozorowe zyskały dużą popularność w zastosowaniach związanych z zarządzaniem ruchem. Wynika to z ich zdolności do dostarczania operatorowi systemu natychmiastowej informacji zwrotnej w przypadku zdarzenia drogowego i na tej podstawie podjęcie dalszej akcji.
Takie kamery do tworzenia obrazu potrzebują światła odbitego od obiektów, dlatego ich efektywność i możliwości detekcji w największym stopniu zależą od warunków oświetleniowych w otoczeniu.

Większość kamer stosowanych w dozorze wizyjnym i zarządzaniu ruchem działa w świetle widzialnym, zwykle w zakresie długości fali od 0,4 do 0,8 m (do 1 m w przypadku urządzeń czułych także na bliską podczerwień). Klasyczne kamery dozorowe mogą więc wykrywać jedynie te obiekty, które są oświetlone przez słońce lub sztuczne źródła światła, np. oświetlenie uliczne.

Przypomnijmy, że każdy obiekt, czy jest to człowiek, zwierzę, czy pojazd albo drzewo, emituje energię cieplną zależną od dwóch czynników: właściwej sobie temperatury i rodzaju materii. Wszystkie obiekty o temperaturze powyżej zera Kelwina emitują ciepło z zakresu dalszej podczerwieni (od 8 do 12 μm). Kamery termowizyjne wykorzystują technologię, która jest czuła właśnie na dalszą podczerwień, co oznacza, że wykrywają wyłącznie promieniowanie emitowane przez obiekty.

Kamery obrazowania termowizyjnego mogą zapewniać stałą widoczność i niezawodność w wykrywaniu obiektów – w trybie 24/7, bez względu na warunki oświetleniowe, atmosferyczne czy środowiskowe, takie jak mgła czy dym. To sprawia, że sprawdzają się w zarządzaniu ruchem, w którym otoczenie monitorowanych obiektów ciągle się zmienia.

Eifeh Strom
a&s International

W kategoriach dokładności i efektywności kamery termowizyjne jako sensory termowizyjne w połączeniu z innymi sensorami (czujnikami) kompleksowego systemu zarządzania ruchem mają wiele do zaoferowania.
Obrazowanie termowizyjne ma już długą historię w zastosowaniach militarnych i ochronie perymetrycznej. Choć w przypadku wykorzystania tej techniki w zarządzaniu ruchem nie jest jeszcze powszechne, to użycie czujników termowizyjnych w różnych branżach wyraźnie rośnie.
Firma analityczna Markets and Markets szacuje, że światowy rynek obrazowania termowizyjnego powiększy się z 7,7 mld dol. w 2016 r. do 10,3 mld dol. w 2021 r. przy rocznej stopie wzrostu 5,9 proc. Wynika to z rosnącego zapotrzebowania na kamery termowizyjne w związku ze spadkiem ich cen. Poza tym rozwój rynku stymuluje też większy popyt na kamery termowizyjne we wszystkich zastosowaniach komercyjnych, w tym transporcie. Jak wynika z badania Markets and Markets, zapotrzebowanie na obrazowanie termowizyjne w segmencie motoryzacyjnym ma stymulować rynek przez kolejnych pięć lat.

Większe wykorzystanie kamer termowizyjnych w przemyśle samochodowym w celu zmniejszenia związanego z jazdą ryzyka (szczególnie w nocy) to jedna z podstawowych przyczyn ożywienia rynku obrazowania termowizyjnego w tego typu zastosowaniach – napisano w raporcie.
Chociaż zastosowanie obrazowania termowizyjnego w motoryzacji nie jest tym samym, co wykorzystanie tej technologii w zarządzaniu ruchem, to potrzeby w sektorze transportowym mogą z siebie wynikać. Co więcej, wobec rosnącego zapotrzebowania na zarządzanie ruchem łączenie różnych technologii, w tym właśnie obrazowania termowizyjnego, przyczyni się do

tworzenia jeszcze bardziej efektywnych rozwiązań.

Dlaczego termowizja

Jednym z największych atutów kamer termowizyjnych w różnych zastosowaniach branżowych jest ich zdolność do „widzenia" w ciemności i podczas niesprzyjających warunków atmosferycznych. Mogą one także mierzyć temperaturę dowolnego obiektu w swoim polu widzenia, wykrywając pożar w jego początkowej fazie w całym obszarze detekcji.

Termowizja, w odróżnieniu od innych technologii wykrywania pożaru, nie wymaga kontaktu z płomieniem lub rozgrzanymi gazami. Nie musi też dojść do rozprzestrzeniania się dymu, by kamera wykryła zwiększone wydzielanie się ciepła w efekcie pojawienia się pożaru lub nieprawidłowości w działaniu pojazdu – mówi Michael Deruytter, dyrektor ds. innowacji w firmie FLIR Intelligent Transportation Systems.

Dodatkowa korzyść polega na tym, że dzięki technologii obrazowania termowizyjnego operatorzy mogą widzieć poprzez dym. Ta cecha może ratować życie w wypełnionych dymem tunelach, dostarczając zespołom strażaków informacje o miejscu pobytu ludzi.

Należy pamiętać, że kamery termowizyjne nie wykorzystują światła widzialnego, ale promieniowanie cieplne emitowane przez wszystkie obiekty w polu widzenia. Dlatego ich działania nie zakłóca ani blask słońca, ani ciemność. Nie przeszkadzają im też światła reflektorów, cienie, mokra ulica, śnieg czy mgła. Tym samym są idealnym elementem rozwiązania do monitorowania ruchu drogowego w trybie 24/7.

Termowizja i analityka ruchu drogowego

Obrazowanie termowizyjne nie tworzy kompleksowego rozwiązania do zarządzania ruchem. Przy zastosowaniu analityki wideo kamery termowizyjne okazują się jednak bardzo przydatne.

Obraz z kamer termowizyjnych przypomina ten przetwarzany przez kamery operujące w świetle widzialnym, zwłaszcza jeśli chodzi o kształt rejestrowanego obiektu. *Dlatego analityka wideo dla klasycznych kamer – rozwiązania pod kątem wykrywania kształtów, detekcji ruchu, wykrywania intruzów czy liczenia ludzi – może być użyta także w przypadku kamer termowizyjnych* – twierdzi Emmanuel Bercier, Strategic Marketing Manager we francuskiej firmie ULIS produkującej przetworniki termowizyjne.

> Inteligentne kamery termowizyjne wykryją np. stojący na drodze pojazd lub jazdę pod prąd. Przyspieszy to interwencję służb nadzoru ruchu i ratunkowych.

Ponieważ kamery termowizyjne wykrywają ciepło emitowane przez obiekty, te obiekty są bardzo wyraźnie widoczne na tle otoczenia. W rezultacie upraszcza to analitykę wideo, ponieważ nie ma potrzeby uwzględniania zmiany oświetlenia lub efektu cienia.

Kamery termowizyjne doskonale nadają się do wykorzystania analityki wideo, ponieważ piksele na obrazie reprezentują informacje o cieple – im cieplejszy jest obiekt, tym więcej emituje energii termicznej. I nawet ekstremalnie zimne obiekty, do -243°C (blisko 0 Kelwina), emitują energię termiczną. Kamery termowizyjne wykrywają ciepło wydzielane przez samochody, rowerzystów i pieszych.

Związana z detekcją informacja może być wykorzystana do klasyfikacji obiektu albo uczestnika ruchu, co pozwala na szybkie podejmowanie decyzji w sterowaniu ruchem na skrzyżowaniach – tłumaczy Michael Deruytter.

Inteligentne kamery termowizyjne są także wykorzystywane do wykrywania incydentów, takich jak zatrzymanie pojazdu na drodze czy jazda pod prąd, co przyspiesza interwencję nadzoru ruchu oraz służb ratunkowych.

Wyzwania dla termowizji w kontroli ruchu

Chociaż kamery termowizyjne zapewniają lepszą detekcję, to powinny być wykorzystywane głównie w połączeniu z kamerami operującymi w świetle widzialnym. *Ostatecznie to kombinacja obu rodzajów urządzeń zapewni najlepszą dokładność detekcji i identyfikacji, np. numerów rejestracyjnych pojazdów* – twierdzi Emmanuel Bercier.

Technologia zarówno termowizyjna, jak i oparta na świetle widzialnym mają unikalne zalety, stosowanie obu tworzy perfekcyjne połączenie.

Podejście wielosensorowe jest wykorzystywane w zaawansowanych systemach dozoru wizyjnego i ochrony granic. Użyta w nich kombinacja kamer klasycznych i termowizyjnych służy do wykrywania wielu różnych zagrożeń – wyjaśnia Michael Deruytter. W przypadku zarządzania ruchem dzięki połączeniu obu technologii w jednym systemie nadzór może wykorzystywać doskonałą detekcję zapewnioną przez kamery termowizyjne, jednocześnie otrzymując wiele szczegółowych informacji dostarczanych przez klasyczne kamery o rozdzielczości HD.

Czynnikiem ograniczającym wykorzystanie przez użytkowników końcowych i integratorów systemowych kamer termowizyjnych w zarządzaniu ruchem jest cena rozwiązania. Jak twierdzi Emmanuel Bercier, w ciągu ostatniej dekady koszty zostały znacznie zredukowane. Można obecnie znaleźć kamery termowizyjne do zarządzania ruchem w przystępnych cenach, rzędu kilkuset dolarów. Przypominają one powszechnie dostępne urządzenia, ponieważ opierają się na standardowym protokole i interfejsach. Przekłada się to na łatwiejszą integrację z nową lub istniejącą infrastrukturą.

Zauważamy, że coraz więcej integratorów systemów zarządzania wideo (VMS) rozważa użycie kamer termowizyjnych. Także infrastruktury są niemal gotowe do przyjęcia technologii obrazowania termowizyjnego – uważa Emmanuel Bercier.

Podsumowanie

Wobec ciągłego spadku cen rozwiązań termowizyjnych i rosnącej potrzeby zarządzania ruchem coraz więcej systemów będzie wykorzystywać technologię obrazowania termowizyjnego. Sama termowizja nie jest idealnym rozwiązaniem do zarządzania ruchem, ale jako część większego systemu, z klasycznymi kamerami i analityką wideo, ma znaczący wpływ na zwiększenie jego dokładności i efektywności.

Bezpieczeństwo i wydajność

- Rozwiązania mobilne dla pojazdów transportu publicznego

Automatyczne i bezprzewodowe tworzenie kopii zapasowych nagrań wideo podczas postoju w zajezdni.

- Zapewnienie bezpieczeństwa pasażerów podczas wsiadania i wysiadania z autobusu, za pomocą kamer monitorujących obszary wewnątrz i na zewnątrz pojazdu.
- Łatwe wykrycie aktu wandalizmu dzięki zapisanemu materiałowi wideo.
- Monitorowanie trasy pojazdu oraz rejestracja nietypowych sytuacji (np. gwałtowne hamowanie).

CE FC ISO 9001:2000

www.dahuasecurity.com/pl

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

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

Komunikacja pod specjalnym dozorem

W ostatnich latach rozwój transportu publicznego w Polsce nabrał dynamiki. **Przeprowadza się remonty dworców, rozbudowuje lotniska i buduje nową linię metra, a także zwraca uwagę na poprawę komunikacji zarówno miejskiej, jak i dalekobieżnej.**

IP Hikvision XM6122


Hikvision iDS-2XM6810F


IP Hikvision XM6522

Piotr Świder
Hikvision Poland

Polska wyróżnia się na tle Europy pod względem liczby fabryk autobusów, tramwajów czy pociągów. Polskie firmy wygrywają kontrakty na dostawy środków komunikacji na całym świecie. Również operatorzy – zarówno ogólnopolscy, jak i lokalni – modernizują swój tabor. Na ulicach wielu miast pojawiły się nowe autobusy (również elektryczne) i tramwaje, operatorzy kolejowi oferują przejazdy coraz nowocześniejszymi składami pociągów (EZT).

Modernizacja dotyczy jednak nie tylko komfortu. Wprowadzono także systemy informacji pasażerskiej, nowoczesne automaty biletowe, czytniki kart, inteligentne systemy zarządzania ruchem czy monitoring wizyjny. Według badań nawet 86% ankietowanych chce, by w każdym pojeździe komunikacji publicznej były kamery. Niemal 90% twierdzi, iż pod nadzorem kamer czuje się bezpieczniej. Statystyki wskazują, że ich zastosowanie ma duży wpływ na realny poziom bezpieczeństwa, m.in. spada liczba kradzieży i rozbojów. Mniejsza liczba przestępstw i poczucie bezpieczeństwa mają bezpośredni wpływ na atrakcyjność i postrzeganie miasta czy przewoźnika przez mieszkańców i turystów.

Hikvision, jako światowy lider i największy producent urządzeń dozoru wizyjnego, oferuje specjalną linię produktów przeznaczoną do tego typu zastosowań. Powstają one w ścisłej współpracy z producentami środków transportu. Dzięki temu wiadomo, jakie wymagania stawiają użytkownicy końcowi oraz co jest dla nich najważniejsze.

Nowa seria kamer IP Hikvision XM6122 jest coraz częściej instalowana w pojazdach transportu publicznego również w Polsce. Zapewniają one szerokie pole widzenia bez „martwych stref", są też odporne na akty wandalizmu i sabotaż. Ważne, aby rejestrować wyraźne i szczegółowe obrazy przez całą dobę. Kamery zostały więc wyposażone w oświetlacze IR. Ponieważ natężenie światła może się zmienić, np. w przypadku wjazdu samochodu do tunelu czy na stację, rozwiązaniem są technologie WDR oraz BLC chroniące przed prześwietleniami. Kamery spełniają wymagania odpowiednich norm, mają specjalistyczne certyfikaty (EN50155, EN45545, EMARK, IP66 czy ECE-R118).

W ofercie firmy są również specjalne kamery lusterkowe IP Hikvision XM6522 (IK10, IP68), dzięki którym kierowca może ocenić, co aktualnie dzieje się w obrębie pojazdu oraz kiedy może otworzyć lub zamknąć drzwi.

Ciekawym rozwiązaniem, które pomaga optymalizować sieć połączeń, są kamery do zliczania pasażerów Hikvision iDS-2XM6810F. Zamontowane nad wejściem do pojazdu dostarczają dane o liczbie osób wsiadających i wysiadających z pojazdu. Dzięki temu narzędziu operator zyskuje niezbędne informacje do oceny, czy dane połączenie jest rentowne lub czy niezbędne jest uruchomienie dodatkowych połączeń na danej linii lub o określonej porze.

Aktualnym i przyszłościowym kierunkiem rozwoju systemów dozoru wizyjnego w pojazdach jest analityka wizji. Już teraz Hikvision dysponuje technologią, dzięki której kamera ocenia zachowanie kierującego pojazdem. Automatycznie wychwytuje, w którą stronę patrzy kierowca, czy podczas jazdy pali papierosa lub rozmawia przez telefon komórkowy. Kamera wykryje, czy kierowca jest zmęczony lub rozkojarzony. Po detekcji nieakceptowalnych zachowań samoczynnie wysyła do dyspozytora ruchu alert wraz ze zdjęciem.

To potrafimy już dziś. Również dziś potrafimy z bardzo wysoką skutecznością rozpoznawać i porównywać twarze. Zatem być może już w niedalekiej przyszłości zamiast biletu wystarczy zdjęcie... Jeszcze kilka lat temu można by myśleć, iż jest to pomysł *science fiction* z powieści Stanisława Lema, ale Hikvision, jako prekursor rozwoju technologicznego, jest już na to niemal gotowy.

TKH GROUP
TKH SECURITY SOLUTIONS

PROJEKTUJ, BUDUJ, ZARZĄDZAJ...

www.ccpartners.pl

Pociągi na bezpiecznych torach

W gospodarce wielu krajów koleje spełniają istotną funkcję. **Dlatego ich bezpieczeństwo ma ogromne znaczenie, a wszelkie incydenty mogą mieć poważne konsekwencje ekonomiczne.**

Na świecie położono ponad 1 mln km torów, co wystarczyłoby do okrążenia Ziemi ponad 30 razy. Nic dziwnego, że znaczenie kolei jest tak duże. Nie tylko zapewnia transport ludzi, ale także odgrywa kluczową rolę w handlu i gospodarce. Bezpieczeństwo kolei jest podstawowym elementem związanej z nimi działalności operacyjnej.

W ubiegłym roku doszło do wielu poważnych wypadków kolejowych, w niektórych zginęli ludzie. Większość tych tragedii była następstwem wykolejenia się pociągów, a przyczyną wypadków był najczęściej błąd człowieka, nieprawidłowe działanie lub defekt torów. Są jednak także przykłady zaplanowanych ataków, takich jak ten z marca 2017 r., którego celem był pociąg Bhopal–Ujjain Passenger w Indiach. Na początku ubiegłego roku instytut Middle East Media Research z siedzibą w Waszyngtonie ujawnił i przetłumaczył poradnik Al-Kaidy wyjaśniający, jak własnoręcznie skonstruować urządzenie służące do wykolejania pociągów. Publikacja zawierała także przewodnik dla terrorystów po sieciach kolejowych w USA i Europie.

W zapobieganiu incydentom – zarówno przypadkowym, jak i zaplanowanym – szczególnie istotne staje się zabezpieczenie kolei i dostarczenie wiedzy przewoźnikom o sytuacji na torach.

Wyzwania

Monitorowanie torów kolejowych i związanej z nimi infrastruktury nie jest łatwe. Zdaniem Emina Simseka, dyrektora ds. rozwoju biznesu w regionie EMEA (Europa, Bliski Wschód i Afryka) w firmie Bosch Security Systems, wyzwania dotyczące bezpieczeństwa kolei można podzielić wg ich ograniczeń konstrukcyjnych i operacyjnych.

Na koleje składają się różnego typu struktury, takie jak stacje kolejowe, bocznice, tunele oraz obiekty techniczne, w tym zajezdnie, magazyny i budynki nieobsługiwane przez ludzi. Bocznica, tunel albo otwarta linia to konkretne przestrzenie. Trzeba też brać pod uwagę różne warunki środowiskowe czy takie struktury, jak przejścia nad i pod torami, a także tunele. Decydują one o wyborze środków, jakie powinny być zastosowane. Duża złożoność systemu na większych obszarach to konieczność spełnienia różnorodnych wymagań i potrzeba integracji wielu środków – wyjaśnia Emin Simsek.

Zadanie skomunikowania obszarów zaludnionych powinno zakładać również łatwy dostęp do kolei. Prowadzi to do zwiększenia liczby pasażerów, przewoźnicy muszą więc znaleźć równowagę pomiędzy efektywnością i dodatkowym wykorzystaniem istniejących systemów a funkcjami prewencji wdrożonych systemów. W tych warunkach łatwość działania dotyczy zagadnień instalacji, utrzymania, dodatkowego sprzętu lub koniecznego oprogramowania, w aspekcie czasu serwisowania i prostoty obsługi.

Wobec ograniczeń fizycznych kolejnym wyzwaniem jest znalezienie sposobu na obsługę większej liczby pasażerów – nie można po prostu powiększyć stacji. Tym samym liczba urządzeń brzegowych, takich jak kamery i czujniki, pozostaje ograniczona. Aby rozwiązać ten problem, rozważa się użycie inteligentniejszych kamer, integracji podsystemów i korelacji gromadzonych danych.

Inteligencja sama w sobie jest wyzwaniem. Trzeba odpowiedzieć na pytania, czy system generuje mniej fałszywych alarmów, czy łatwo skonfigurować lub skalibrować kamery, czy będzie można podczas dochodzenia przeszukać nagrania wg różnych kryteriów. Należy rozważyć problemy pod kątem percepcji człowieka. Jeśli zainstalowane rozwiązania nie spełniają kryteriów na określonym poziomie, operator może zaniechać użycia wielu funkcji albo przeoczyć alarmy generowane przez systemy.

> Można mieć nadzieję, że nowe technologie dadzą przewoźnikom i pracownikom kontroli ruchu lepszy obraz sytuacji na torach, a w przyszłości większe możliwości zapobiegania wypadkom.

Bezpieczniejsza kolej

Warunki na kolei nieustannie się zmieniają. Problemem systemów monitoringu wizyjnego są zmienne warunki oświetleniowe i atmosferyczne. Z tym wyzwaniem można sobie poradzić, stosując promienniki podczerwieni, kamery typu *bullet* lub termowizyjne oraz korzystając z „inteligencji" w kamerach monitorujących strefę przytorową. W ten sposób urządzenia te stają się proaktywną częścią zastosowanego systemu security.

EKONOMIA SIECI KOLEJOWYCH

Kolej ułatwia transport towarów, ludzi i surowców. Z tego względu pełni kluczową funkcję w gospodarce.

USA, posiadając ponad 250 tys. km linii kolejowych, są liderem pod względem długości sieci kolejowej. Tylko w 2014 r. przekładało się to na 1,5 mln zatrudnionych na kolei i wynik finansowy przewozów towarowych rzędu 274 mld USD (dane z badania Towson University Regional Association of American Railroads, czerwiec 2016).

Chociaż Koleje Indyjskie stały się areną wielu tragicznych wypadków, to wciąż jest to jedna z najbardziej wykorzystywanych i nadmiernie eksploatowanych sieci kolejowych na świecie. Koleje są tam także jednym z największych pracodawców, zatrudniając ponad 1,3 mln osób. Co więcej, analiza domu maklerskiego JM Financial dowodzi, że w nadchodzących latach znaczące inwestycje w sektor kolejowy dałyby w obszarze PKB Indii efekt mnożnikowy rzędu 5,7 proc. Koleje odgrywają także bardzo ważną rolę w gospodarkach Rosji i Chin, do których należą dwie z największych sieci na świecie (po USA). Obie zatrudniają też rzesze pracowników – Koleje Rosyjskie blisko 1 mln, a Kolej Chińska ok. 2 mln. Sieci kolejowe w Rosji, USA i Chinach mają tak wielkie znaczenie także dlatego, że to trzy spośród czterech największych krajów na świecie.

Technologia pozwala zmniejszyć ograniczenia monitoringu wizyjnego. Połączenie najnowszych przetworników obrazu z funkcją redukcji szumów zapewnia doskonałą czułość kamer. Poza tym kamera może identyfikować kilka incydentów, generując jednocześnie alarmy w trakcie ciągłej analizy obrazu w czasie rzeczywistym. Kamery wysyłające do operatora sygnały alarmu o krytycznych zdarzeniach stają się wirtualnym członkiem zespołu ochrony.
W odpowiedzi na zmienne warunki środowiskowe i strukturalne pojawił się duży wybór kamer, które mogą być zastosowane w każdych warunkach. Stosowane technologie umożliwiają rozróżnianie szczegółów obrazu nawet przy oświetleniu 0,0008 lx. Ponadto inteligentna analityka obrazu, wykorzystująca różne algorytmy, zapewnia wysoki poziom dokładności w obsłudze krytycznych aplikacji. Potrafi odróżnić faktyczne incydenty od typowych fałszywych alarmów generowanych w trudnych warunkach środowiskowych, jak śnieg, wiatr, deszcz, odblaski na wodzie i odległość, które mogą utrudniać interpretację obrazu.

Ochrona przed cyberatakami

Cyberataki często goszczą na czołówkach serwisów informacyjnych. Celem globalnych działań cyberprzestępców staje się wszystko – od osobistych informacji kredytowych po systemy ochrony zdrowia (a to zagraża życiu pacjentów). Wobec strat powodowanych przez ataki rośnie potrzeba stosowania skutecznych zabezpieczeń sieciowych.
Na początku ub.r. cyberataki uderzyły w niemieckiego przewoźnika kolejowego Deutsche Bahn oraz narodowy system kolei we Francji. Na szczęście incydenty te nie spowodowały poważnych strat materialnych, ale doprowadziły do chaosu i napędziły strachu. Ponieważ koleje stają się coraz bardziej inteligentne i zautomatyzowane, coraz częściej będą znajdować się na celowniku hakerów. Szacuje się, że wartość globalnego rynku inteligentnych kolei wzrośnie z 10,5 mld USD w 2016 r. do blisko 20,6 mld USD w 2021 r.
Koleje muszą więc uwzględniać zagrożenie atakami na systemy bezpieczeństwa. Urządzenia brzegowe muszą być zabezpieczone przed działaniami cyberprzestępców. Wprawdzie niezależne sieci są zaprojektowane pod kątem bezpieczeństwa, to i tak systemy SCADA czy NVR są narażone na różnego typu cyberataki. Dlatego należy rozważyć zabezpieczanie danych z kamer, jednostek nagrywających i innych urządzeń security.

> Aby zwiększyć bezpieczeństwo, właściciele kolei i taboru mogą wykorzystywać informacje dostarczane przez technologię *big data* w celu utworzenia inteligentnej bazy danych uzyskiwanych z monitorowanych pociągów.

Przyszłość w ochronie kolei

Bezpieczeństwo kolei musi uwzględniać każde zagrożenie, począwszy od ataków terrorystycznych i wykolejeń pociągów, skończywszy na wypadkach na przejazdach kolejowych. Dlatego należy stosować odpowiednie środki zapobiegające wszelkiego typu incydentom. Obecnie wdrażane są różne technologie mające zwiększyć ochronę sieci. Wykorzystuje się m.in. drony, które mogą kontrolować mniej dostępne i odległe rejony.
Można mieć nadzieję, że nowe technologie dadzą przewoźnikom i pracownikom kontroli ruchu lepszy obraz sytuacji na torach, a w przyszłości większe możliwości zapobiegania wypadkom.

Technologia zapobiega wypadkom kolejowym

Przyczyną wielu wypadków kolejowych są błędy człowieka. Czy technologia może im zapobiec?
Wykolejenia pociągów – zarówno osobowych, jak i towarowych – są, niestety, częstszym zjawiskiem, niż mogłoby się wydawać. W dziesiątkach poważnych wykolejeń na świecie ginią rocznie tysiące osób. Tylko w ubiegłym roku do takich groźnych wypadków z ofiarami śmiertelnymi doszło m.in. w USA, Wielkiej Brytanii, Indiach, Grecji i Belgii. W celu ograniczenia liczby takich zdarzeń rządy na całym świecie wprowadzają nowe standardy i regulacje. Obejmują one implementację zaawansowanych technologii, które mają usprawnić zarządzanie kolejami i zwiększyć ich bezpieczeństwo.

PTC

W roku 2008 USA w celu zwiększenia bezpieczeństwa kolei przyjęły ustawę *Rail Safety Improvement Act*. Uchwalenie tego prawa nastąpiło po kolizji pociągu towarowego z kolejką podmiejską, do której doszło w Chatsworth, na przedmieściach Los Angeles. W wypadku zginęło 25 osób, a 100 zostało rannych. Część uchwalonego aktu dotyczyła technologii PTC (*Positive Train Control*), która miała być zainstalowana w sieciach kolei pasażerskich oraz towarowych pierwszej klasy do końca 2015 r. (termin zakończenia wdrożenia przesunięto następnie na rok 2018). Zgodnie z wytycznymi amerykańskiego Departamentu Transportu oraz Federalnej Administracji Kolei (FRA): *PTC ma zostać zainstalowana i zaimplementowana na głównych liniach kolejowych oznaczonych jako Class I (roczny przewóz ponad 5 mln ton brutto), którymi przewozi się materiały trujące i niebezpieczne, a także na dowolnych głównych liniach służących do transportu pasażerów między miastami i w komunikacji podmiejskiej.*
FRA szacuje, że wdrożenie obejmie niemal 97 tys. km torów i ok. 20 tys. lokomotyw. Jak wynika z *Rail Safety Improvement Act*, wszystkie systemy PTC muszą niezawodnie i funkcjonalnie zapobiegać kolizjom pomiędzy pociągami, wykolejeniom z powodu nadmiernej prędkości, wjazdom na odcinki w remoncie czy kontynuowania jazdy pomimo zakazu. FRA zwraca uwagę, że *systemy PTC powinny zapewniać także interoperacyjność, by wyposażone w PTC lokomotywy przejeżdżające przez tereny objęte działaniem innego PTC mogły się z tym systemem komunikować i odpowiednio reagować, co zapewni niezakłócony przejazd.*
Wdrażaniu technologii PTC towarzyszą jednak problemy i głosy oponentów. Przykładowo, organizacja *Association of American Railroads* (AAR) wskazuje, że tego typu system wymaga bardzo złożonych technologii, potrafiących analizować i uwzględniać dużą liczbę zmiennych związanych

z działaniem kolei. Ponadto technologia musi umożliwiać automatyczne i wiarygodne interpretowanie informacji i bezpieczne zatrzymanie pociągu. Przeciwnicy PTC wątpią, by technologia ta była na tyle zaawansowana i wyrafinowana, by móc efektywnie i wydajnie spełniać swoje zadania. Kolejnym problemem jest koszt implementacji. Według obliczeń całkowity szacunkowy koszt rozwoju i wdrożenia PTC dla kolei towarowych wynosi 10,6 mld USD; dodatkowe 3,5 mld USD dołożą koleje pasażerskie. Te liczby nie uwzględniają kolejnych milionów dolarów, które każdego roku trzeba będzie wydać na utrzymanie systemu.
Bez względu na wątpliwości koleje amerykańskie muszą wdrożyć technologię PTC do końca tego roku (przy czym niektóre z nich, po spełnieniu określonych kryteriów, mogą liczyć na wydłużenie terminu do roku 2020).

INTELIGENTNE BAZY DANYCH

Aby zwiększyć bezpieczeństwo, właściciele kolei i taboru mogą wykorzystywać informacje dostarczane przez technologie *big data*. Projekt *Asset Health Strategic Initiative* (AHSI) dotyczący amerykańskiej branży kolejowej zakłada budowę inteligentnej bazy danych uzyskiwanych poprzez monitorowanie kolei i stanu pociągów.
Dotychczas koleje w dużej mierze polegały na danych zbieranych przez detektory ulokowane na poboczach – rozwiązania znajdujące się przy torach monitorowały przejeżdżające składy, by określić, czy wybrany element (wyłącznie z ich obszaru serwisowania) wykazuje już oznaki zużycia. Niestety jednak, o ile pociągi (należące do różnych organizacji) regularnie przemieszczały się po wielu sieciach kolejowych, o tyle zbierane dane już nie były wymieniane. Tylko dana sieć dysponowała informacją, jak pociąg zachowywał się na jej torach. Dawało to niekompletny obraz, który spowalniał diagnozę potencjalnych problemów systemowych i opóźniał konieczną naprawę.
Dzięki agregacji punktów zbierania danych z amerykańskich sieci kolejowych oraz informacji od spółek i linii kolejowych utworzona inteligentna baza danych daje szansę na zapobieganie wypadkom. Stworzy pełny obraz sytuacji na torach.

BIG DATA POMOCNE W ZAPOBIEGANIU WYPADKOM KOLEJOWYM

Koleje mogą czerpać korzyści z *big data*. Analityka wielkich zbiorów danych ma ogromny potencjał. Stosując złożone reguły do gromadzonych danych, przewoźnicy mogą rozwiązywać mniejsze problemy, zanim staną się one wielkimi.
Zgodnie z definicją *American Association of Railroads* (AAR), te złożone reguły to protokoły bezpieczeństwa tworzone na podstawie kombinacji czynników związanych z ryzykiem awarii elementu wyposażenia. Dotyczą one wielu możliwych problemów – od wadliwych hamulców po wyeksploatowane koła.
Tworzenie reguł jest możliwe dzięki istnieniu kolejowych „hurtowni danych", które gromadzą już setki terabajtów informacji o wyposażeniu kolei. To więcej danych od setek milionów cyfrowych zdjęć. Aby przewozy towarowe stały się bezpieczniejsze, koleje muszą przewidzieć te rzadkie sytuacje, w których urządzenia lub tory ulegają awarii. *Big data* umożliwia zidentyfikowanie kombinacji tych czynników, które powodują problemy.
Organizacja AAR i poszczególne sieci kolejowe w USA rozpoczęły już definiowanie kombinacji defektów, które przełożą się na czynniki tworzące złożoną regułę. Przykładowo, awarii mogą ulec koła wagonu – dopuszcza się pewien poziom zużycia, ale ważne, by mały problem nie stał się wielkim. Może temu zapobiec analiza *big data*. Wyszukując kombinacje defektów, inżynierowie kontroli są w stanie wychwycić te czynniki, które powodują problemy eksploatacyjne.
AAR spodziewa się, że im więcej danych będą gromadzić koleje, tym więcej złożonych reguł będzie można opracować.

DETEKCJA WYKOLEJEŃ I PĘKNIĘĆ TORÓW

Do najbardziej przeciążonych na świecie należą tory kolejowe w Indiach. To państwo przoduje też w tragicznych statystykach wypadków kolejowych. Tylko w ubiegłym roku doszło tam do kilku groźnych incydentów, m.in. zamachu bombowego. Poważnym problemem są też wykolejenia z dużą liczbą ofiar. W październiku 2016 r. wykoleił się pociąg pasażerski – zginęło 150 osób, rannych było dużo więcej. Był to najbardziej tragiczny wypadek kolejowy w tym kraju od 1999 r. Po tym zdarzeniu rząd indyjski zdecydował się zwiększyć nakłady na rozwój technologii, które mają zapobiec katastrofom.
Placówka naukowa *Indian Institute of Technology Kanpur* (IIT Kanpur) pracuje obecnie nad projektem urządzenia do detekcji wykolejeń w formie sprzętu pokładowego. Urządzenie będzie zintegrowane z mechanizmami hamulcowymi i ma pomóc ograniczyć straty, gdy pociąg traci kontakt z szynami.

Natomiast w *Indian Institute of Technology Madras* (IIT Madras) trwają prace nad rozwojem systemu do wykrywania pęknięć szyn. Do tej pory nie było rozwiązania do automatycznej detekcji tego rodzaju uszkodzeń – przewoźnicy mogą jedynie polegać na ultradźwiękowych testach szyn, przeprowadzanych co dwa miesiące przez ekipy specjalistów, oraz na raportach dostarczanych przez maszynistów. IIT Madras zamierza stworzyć system, dzięki któremu proces testowania ultradźwiękami będzie miał postać cyfrową.

Nadzieja w technologii

Powstało już wiele systemów i technologii, które mogą pomóc w zapobieganiu wypadkom kolejowym. Wraz z rozwojem technologicznym są one stale udoskonalane. Chociaż nie są w stanie zapobiec wszystkim katastrofom ani uchronić przed spontanicznymi bądź zaplanowanymi działaniami przestępczymi, to ich implementacja pomaga ograniczyć liczbę ofiar i podnieść poziom bezpieczeństwa na kolei.

BEZPIECZEŃSTWO w transporcie ciężkim

Kluczową sprawą w transporcie jest bezpieczne i skuteczne realizowanie zleceń. Służą do tego różne narzędzia, których odpowiednia kompilacja może okazać się kluczem do sukcesu i przewagi nad konkurencją. **Wśród optymalnego zestawu narzędzi obowiązkowy jest system GPS, który może udostępniać różne funkcje.**

Andrzej Nowak

Lokalizacja GPS jest już powszechnie stosowana we flotach ciężkich. Stanowi tani i efektywny sposób na lokalizację pojazdów, identyfikację kierowców i śledzenie towarów. Ważne, by system pozwalał na udostępnianie informacji za pomocą API giełdom transportowym i ewentualnym zleceniodawcom przewoźnika. Dzięki dobremu interfejsowi API inne systemy za zgodą właściciela mogą pobierać lokalizację pojazdu i ją przetwarzać. Przykładem takiej integracji jest udostępnianie lokalizacji pojazdu firmy podwykonawczej firmie zlecającej przewóz, np. DHL czy UPS.

Zaawansowane systemy monitorowania GPS pozwalają na **korytarzowanie**, czyli przygotowywanie tras dla pojazdów i alarmowanie za każdym razem, kiedy pojazd opuści zaplanowaną trasę, zjeżdżając na nieplanowany postój lub myląc drogę. Możliwa jest natychmiastowa reakcja operatora lub właściciela. Takie rozwiązanie okazuje się nieocenione przy transportach, które są obarczone dużym ryzykiem, np. papierosów. System musi wspierać przesyłanie alarmów w czasie rzeczywistym za pomocą co najmniej poczty elektronicznej i wiadomości SMS do więcej niż jednego odbiorcy.

Eco-driving jest funkcjonalnością, która budzi skrajne emocje, jednak po głębszej analizie i wielu testach należy stwierdzić, że wprowadzenie zasad *eco-drivingu* i ich egzekwowanie prowadzi do dużych oszczędności. Wiąże się to z tym, że taki mechanizm pozwala eliminować agresywną lub bezmyślną jazdę kierowcy, co przekłada się na większą dostępność floty, mniejszą liczbę awarii i większe bezpieczeństwo ładunku. *Eco-driving* w przypadku pojazdów ciężarowych, wraz z analizą użycia **retardera** oraz **sprzęgła**, istotnie wpływa na obniżenie kosztów serwisowych floty dzięki wymuszeniu prawidłowej obsługi pojazdu. Stosunek liczby hamowań z użyciem jedynie retardera do liczby hamowań hamulcem powinien wynosić 9:1, dopiero wtedy można uznać, że jadąc, kierowca przewiduje warunki na drodze i stosuje się do zaleceń producenta pojazdu. System wykrywa też przyspieszanie mimo włączonego zwalniacza lub jazdę na niedomkniętym sprzęgle. Statystyki pokazują także czas spędzony na postoju z włączonym silnikiem. Analiza *eco-drivingu* powinna umożliwiać sprawdzenie przeciążeń, jakie działały na pojazd i ładunek. To oznacza, że gwałtowne hamowanie lub zbyt szybko pokonany zakręt zostanie wykryty i zaraportowany. Stosując systemy z rozbudowanym *eco-drivingiem* skierowanym do flot ciężkich, można skutecznie walczyć z nieprawidłową eksploatacją pojazdów ciężarowych.

Tachograf to jedno z najważniejszych urządzeń w pojeździe ciężarowym i dlatego system monitorowania musi bezwzględnie umożliwiać integrację z nim. Takie rozwiązanie pozwoli na pobieranie plików DDD tak, by spełnić wymóg ustawodawcy. Ponadto system zidentyfikuje kierowcę, który aktualnie prowadzi pojazd, i umożliwi indywidualną ocenę eko nawet w przypadku, kiedy pojazdem jeździ więcej osób. Kolejnym jego atutem jest monitorowanie i ostrzeganie dyspozytora

Stosując systemy z rozbudowanym *eco-drivingiem* skierowanym do flot ciężkich, można skutecznie walczyć z nieprawidłową eksploatacją pojazdów ciężarowych.

o dozwolonym czasie pracy, a także rozliczanie delegacji kierowców.

Możliwość **planowania tras** w systemie i przesyłania ich do kierowcy coraz częściej stanowi niezbędny element i podstawę do rozliczenia z podwykonawcą. System musi zatem posiadać odpowiednie mapy i router, czyli mechanizm wyznaczający trasę między punktami oraz podający odległość po drodze i czas przejazdu. Po zaplanowaniu trasa powinna być wysłana do nawigacji w pojeździe jako zlecenie lub co najmniej do aplikacji na telefonie kierowcy.

Dostawca usług i systemu monitorowania powinien zapewnić również odpowiednie **urządzenie,** które montuje się w pojeździe lub naczepie. Bardzo ważne jest, by było sprawdzone i pewne. Dobry lokalizator powinien posiadać następujące interfejsy:

- CAN/FMS do integracji z szyną pojazdu w celu analizy takich parametrów, jak prędkość, obroty, paliwo czy użycie retardera,
- złącze tachografu (może też być CAN),
- wyjście umożliwiające odcięcie zapłonu,
- szereg wejść pozwalających na monitorowanie przestrzeni ładunkowej czy wlewów paliwa,
- wejście do autoryzacji zapłonu za pomocą przycisku lub pilota bezprzewodowego.

Urządzenie musi być wyposażone we własną baterię, by awaria zasilania lub celowe odcięcie nie powodowało awarii lokalizatora. Jeżeli system ma oferować *eco-driving*, ten powinien być analizowany przez urządzenie, co zmniejsza ilość danych przesyłanych do serwera i umożliwia natychmiastowe informowanie kierowcy o popełnianych błędach za pomocą dźwięku lub aplikacji mobilnej.

Nie każdy system monitorowania floty zapewnia wszystkie wymienione elementy, dlatego właściciel floty powinien poszukać takiego dostawcy, który zapewni niezbędne funkcje i urządzenia. Nawet jeżeli w pierwszym kroku nie będzie chciał wykorzystywać pełnej funkcjonalności, warto wybrać taki, który umożliwi poszerzenie zakresu funkcji bez konieczności wymiany urządzeń, które wraz z instalacją stanowią znaczną część całkowitego kosztu takiego systemu.

Możliwość planowania tras w systemie i przesyłania ich do kierowcy coraz częściej stanowi niezbędny element i podstawę do rozliczenia z podwykonawcą.

BIO

Andrzej Nowak menedżer produktów do lokalizacji GPS. Od lat związany z systemami monitorowania GPS firm stosujących produkty Pulson i Omtech.

Usługi logistyczne i spedycyjno-transportowe

ZAGROŻENIA

W ostatnich latach na świecie nastąpił wzrost produkcji związanej z postępującą globalizacją. **Czynniki te mają duży wpływ na rozwój sektora logistyki kontraktowej i magazynowej oraz usług transportowo-spedycyjnych.**

Andrzej Żochowski

Firmy logistyczne funkcjonują coraz dynamiczniej, podnosząc efektywność świadczonych usług, aby nadążać za oczekiwaniami klientów. W wielu sytuacjach operatorzy logistyczni czy firmy kurierskie starają się przewidzieć zapotrzebowanie klientów, zanim klienci zwrócą się do nich o realizację określonych usług. Ponadto obserwujemy szybki wzrost nielegalnej migracji ludności, zwłaszcza z Bliskiego Wschodu. Wszystko to ma duży wpływ na bezpieczeństwo podczas wykonywanych operacji logistycznych w łańcuchu dostaw. Wraz z ich wzrostem zwiększa się skala wyzwań w zakresie zapewnienia bezpieczeństwa. Przewiduje się, że przyszłość w logistyce będzie należała do firm, które będą w stanie zapewnić klientom świadczenie kompleksowych usług logistycznych realizowanych w krótkim czasie, bez narażania na ryzyko uszkodzenia ładunków, kradzieży czy konsekwencji prawnych lub utraty reputacji. Odnosząc się do przytoczonej tezy, struktury bezpieczeństwa w sektorze logistyki będą musiały efektywnie zmierzyć się z wyzwaniami czy zagrożeniami, aby sprostać wymaganiom klientów.

Logistyka kontraktowa

• WEWNĘTRZNE KRADZIEŻE MAGAZYNOWE

Są najczęściej dokonywane przez nieuczciwych pracowników magazynowych – zarówno pojedyncze osoby, jak i działających zespołowo, np. w porozumieniu z kierowcami realizującymi usługi transportowe lub firmami zewnętrznymi wykonującymi usługi np. utylizacji odpadów lub ładunków uszkodzonych. W ostatnim czasie zauważalnym trendem jest wzrost kradzieży towarów przy „współpracy zespołowej" personelu, co przynosi olbrzymie straty. Takie działania są powiązane z wprowadzaniem do systemu komputerowego błędnych danych, aby maksymalnie opóźnić wykrycie tzw. braku w towarze, wysyłce lub dostawie u klienta.

Kolejnym specyficznym sposobem generowania strat w centrach logistycznych jest celowe uszkadzanie towarów i produktów. Wykorzystuje się obowiązujący standard, np. jakościowy, zgodnie z którym uszkodzenie towaru dyskwalifikuje go z dalszej dystrybucji. W rzeczywistości jednak towar ten jest pełnowartościowy i można go sprzedać nielegalnie, już poza firmą logistyczną. Towar taki jest „wyprowadzany" najczęściej z firmy logistycznej przez personel

zatrudniony w magazynie lub np. w ramach współdziałania z zewnętrzną firmą utylizacyjną. W tym przypadku również wprowadza się nieprawdziwe dane do magazynowych systemów zarządzania, aby formalnie „zamaskować" powstałą stratę. Finalnie firma logistyczna wypłaca odszkodowanie klientowi, nie mając świadomości, że towar został uszkodzony celowo.
Czynnikiem wpływającym na wzrost tego typu zagrożeń w sektorze logistyki kontraktowej i magazynowej jest postępujący brak pracowników wykwalifikowanych. Sytuacja ta wymusza konieczność zatrudniania „pracowników czasowych" poprzez agencje pracy czasowej. Niestety ta kategoria zatrudnianych nie jest formalnie związana z pracodawcą, dla którego świadczy usługi. Powoduje to, iż personel ten jest mniej zmotywowany do pracy. Nie traktuje zatrudnienia jako stałego, posiada mniejsze kwalifikacje i doświadczenie. Nie jest przy tym weryfikowany przez agencje pracy czasowej w aspekcie pozyskania referencji z poprzednich miejsc zatrudnienia.
• **CYBERATAK** na zasoby informatyczne firmy logistycznej – przykład z czerwca 2016 r. Zaatakowano wówczas wiele firm logistycznych i produkcyjnych w Europie, m.in. także w Polsce. Organizacje te nie przyznały się oficjalnie, że padły ofiarą takiego ataku. Jego skala spowodowała jednak ogromne straty w operacjach logistycznych, takich jak:
– utrata kontroli nad systemami bezpieczeństwa firm (systemy monitoringu wizyjnego, systemy kontroli dostępu, systemy zarządzania magazynami, systemy zarządzania ruchem pojazdów oraz pozostałe zasoby informatyczne firmy),
– utrata towarów i ładunków spowodowana celowym działaniem personelu firmy wykorzystującego negatywne skutki ataku i brak kontroli nad systemami operacyjnymi w organizacji, a także celowym działaniem klientów zgłaszających braki w tzw. dostawach towarów, którzy zostali poinformowani, iż organizacja uległa cyberatakowi,
– utrata reputacji firmy jako organizacji, która w ocenie klienta straciła wiarygodność z powodu gwałtownego spadku jakości usług powiązanej m.in. ze stratami towarów, przesyłek itp., czego efektem było przejście klientów do innych operatorów logistycznych czy firm kurierskich.

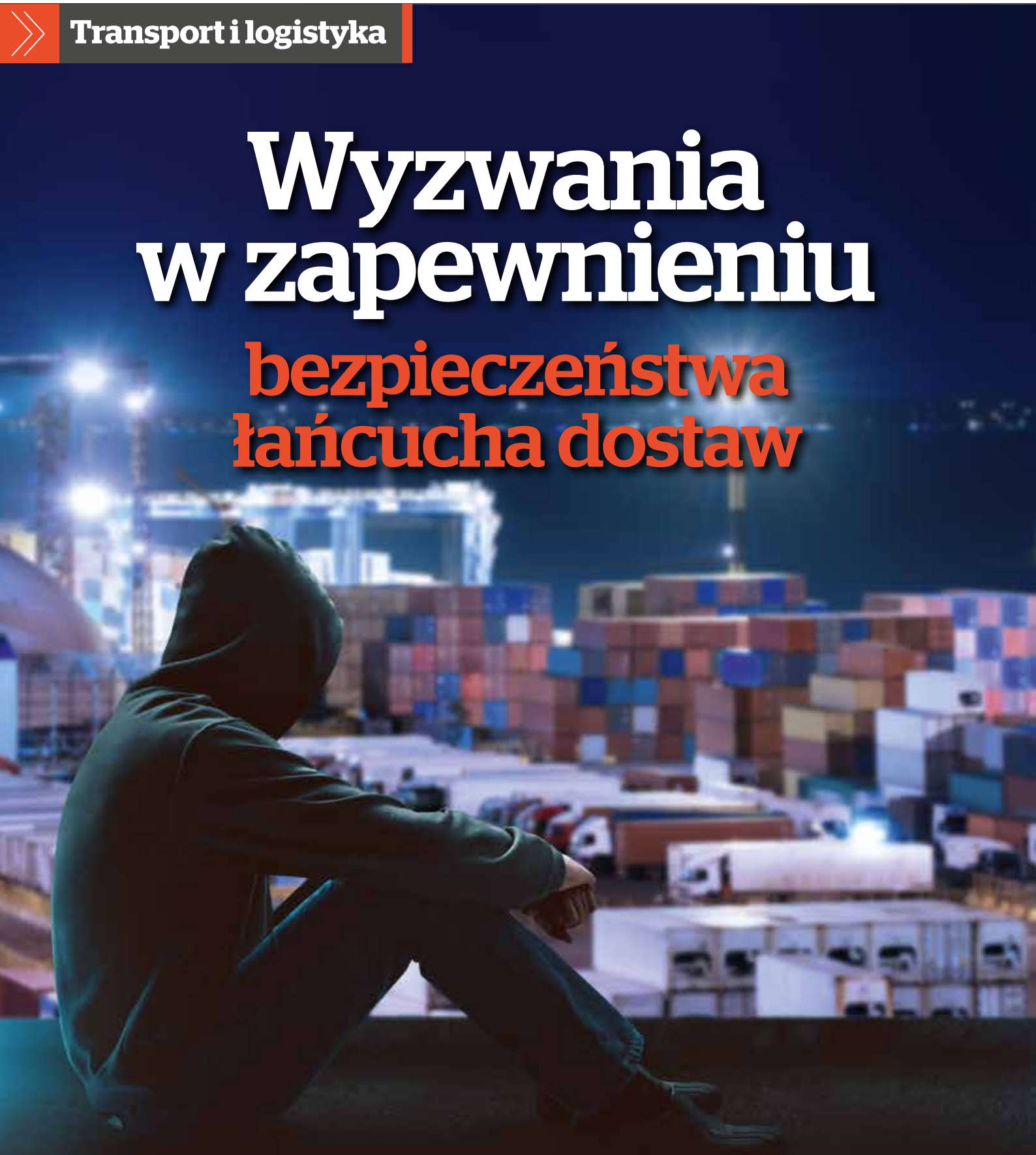
Usługi spedycyjno-transportowe

• **FAŁSZYWE FIRMY TRANSPORTOWE**
Funkcjonują na podstawie sfałszowanych dokumentów (KRS, licencje transportowe, polisy ubezpieczeniowe, dokumenty tożsamości i pojazdów) lub fałszywe firmy, które odkupiły firmę transportową działającą wcześniej legalnie na rynku logistycznym, posiadającą pozytywne opinie klientów. Po zakupie przestępcy – posługując się oryginalnymi dokumentami przejętej firmy – dokonują wyłudzenia ładunku od operatora logistycznego lub innej firmy, np. produkcyjnej. Firmy te są „podejmowane z rynku" przez klientów na podstawie zamieszczanego ogłoszenia na tzw. giełdach transportowych. W przestępczości tej przodują takie kraje, jak Polska, Węgry, Rumunia, Bułgaria, Ukraina i Czechy.
Przestępcy dokonujący tego typu kradzieży w ostatnich latach przeprowadzili bardzo duże zmiany w metodologii wyłudzania ładunków. Odstąpili od napadów na ciężarówki i rozpoczęli wyłudzanie ładunków, posługując się dokumentami sfałszowanymi. Pozwoliło to im na kradzieże droższych ładunków i większych wolumenów. Jednocześnie wykorzystali przepisy prawa, że wyłudzenie towarów na tzw. fałszywego przewoźnika ma zdecydowanie niższą „kwalifikację czynu przestępczego" w przypadku zatrzymania przez organy ścigania, ponieważ jest to tylko wyłudzenie ładunku i fałszowanie dokumentów, a nie np. czynna napaść, rabunek itp. Ponadto policja nie ma doświadczenia w ściganiu tego typu przestępstw, a prowadzone dochodzenia kończą się niewykryciem sprawców.
• **NIELEGALNI IMIGRANCI**
Nasilenie ruchów migracyjnych ludności przez Europę spowodowało w ostatnich latach nasilenie problemu dotyczącego osób usiłujących w sposób nielegalny przemieszczać się pomiędzy krajami w naczepach ciężarówek lub ich elementach konstrukcyjnych. Problem ten narasta wprost proporcjonalnie do rozwoju konfliktów zbrojnych w krajach Bliskiego Wschodu. Nielegalni imigranci wykorzystują sieci transportowe, głównie w Europie, do przemieszczania się.
Wynikiem takiej sytuacji jest zniszczenie przewożonych ładunków (np. żywności) lub zatrzymanie kierowcy i pojazdu przez służby celne i graniczne. W efekcie powstają straty po stronie zarówno klienta zlecającego przewóz ładunku, jak i firmy transportowej, która ponosi nie tylko szkodę z tytułu zniszczonego ładunku, ale także koszty prawne, sądowe itp. poniesione w celu odzyskania zatrzymanego pojazdu i uwolnienia kierowcy z aresztu.
• **PRZEMYT**
Polska jest krajem tranzytowym pomiędzy Europą Wschodnią a Zachodnią. Kraje Europy Wschodniej są największymi producentami podróbek papierosów, które przestępcy muszą przetransportować na Zachód. „Producenci" nielegalnych papierosów wykorzystują firmy spedycyjne i transportowe, ukrywając towar w opakowaniach innych przewożonych produktów. Dokumenty transportowe mają nieprawdziwe opisy (np. panele podłogowe, materiały reklamowe, części zamienne itp.).
Zatrzymanie pojazdu firmy transportowej przez służby celne lub graniczne skutkuje zatrzymaniem również kierowcy i przewożonych tym samym pojazdem ładunków innych klientów. Przynosi to wysokie straty finansowe firmie transportowej, kurierskiej, spedycyjnej oraz klientowi, który zlecił przewóz legalnych towarów. Firma transportowa ponosi straty finansowe z tytułu kosztów prawnych, sądowych itp. w celu odzyskania zatrzymanego pojazdu, ładunków innych klientów i uwolnienia z aresztu kierowcy.

BIO

Andrzej Żochowski
Związany z obszarem bezpieczeństwa od 20 lat. W przeszłości żołnierz zawodowy, na stanowiskach powiązanych z problematyką bezpieczeństwa instalacji militarnych. Przez ostatnich 10 lat pracuje dla korporacji jako *Country Security Manager* w obszarze produkcji i logistyki. Obecnie szef bezpieczeństwa w TNT Express Polska.

Wyzwania w zapewnieniu bezpieczeństwa łańcucha dostaw



Branża logistyczna jest jednym z obszarów najbardziej zagrożonych przestępczością. To skutek zarówno mnogości zagrożeń występujących w obszarach składowania i transportu oraz atrakcyjności produktów, jak i charakterystyki łańcucha dostaw. Produkty bardzo często pokonują dystans kilkunastu tysięcy kilometrów środkami transportu morskiego, lotniczego lub drogowego.

Robert Balcewicz

W transporcie międzynarodowym operatorzy logistyczni zazwyczaj współpracują z wieloma przewoźnikami, a produkty są składowane w magazynach o różnym standardzie bezpieczeństwa. Zagrożenie procederem przestępczym wzrasta wprost proporcjonalnie do atrakcyjności produktów. W związku z tym bardzo istotna jest **standaryzacja procesów bezpieczeństwa fizycznego, technicznego oraz proceduralnego** w całym łańcuchu dostaw. Jest ona możliwa dzięki implementacji międzynarodowych standardów bezpieczeństwa, takich jak **TAPA** (*Transported Asset Protection Association*) w obszarze **FSR** (*Facility Security Requirements*) lub **TSR** (*Trucking Security Requirements*). Brak jednolitego standardu bezpieczeństwa w całym łańcuchu dostaw jest bardzo dużym zagrożeniem.

W obszarze składowania produktów problem ten jest widoczny w parkach logistycznych typu *multitenant*, w których powierzchnia magazynowa jest wynajmowana przez kilku lub kilkunastu najemców w modułach od 2,5 tys. m² do nawet 30 tys. m². Operatorzy logistyczni w większości posiadają wewnętrzne piony bezpieczeństwa, które w odpowiedni sposób zabezpieczają wynajmowaną powierzchnię magazynową pod względem technicznym, fizycznym oraz proceduralnym, w tym odpowiednio implementując procedury zapobiegania stratom. Niemniej jednak, wynajmując np. 10 tys. m² w środkowej części budynku magazynowego o łącznej powierzchni 50 tys. m², możemy zabezpieczyć swoją powierzchnię zgodnie z najwyższymi standardami bezpieczeństwa, ale niestety mamy znikomy wpływ na sposób zabezpieczenia powierzchni magazynowej przez bezpośrednich sąsiadów.

W parkach logistycznych typu *multitenant* właściciele zawierają z najemcami różnego rodzaju umowy najmu – od rocznych do 7-letnich, najemcy składują różnego rodzaju produkty – od *High Value Goods* – np. elektronika, dobra luksusowe, kosmetyki czy alkohole, poprzez usługi IT (kolokacje), kończąc na branży FMCG. Ze względu na różne długości okresów najmu częste są przypadki, że sąsiednie pustostany pozostają niezabezpieczone. Różnorodność składowanych produktów powoduje natomiast, że poszczególne wynajęte powierzchnie są zabezpieczone w różny sposób, a czasami są nawet niezabezpieczone, jeżeli np. najemca w swoim procesie szacowania ryzyka uzna, iż produkty są na tyle nieatrakcyjne, że ryzyko włamania z kradzieżą praktycznie nie występuje.

Niestety w tej sytuacji nie są pomocni ani właściciele parków logistycznych, ani firmy zarządzające nieruchomościami – jakby nie rozumieli podstawowej zasady zabezpieczenia warstwowego czy też pierścieniowego w głąb (*Layered Protection also known as defense in depth*). **Pierwszy, zewnętrzny pierścień ochronny powinno stanowić ogrodzenie zewnętrzne parku wraz ze szczelnym systemem kontroli dostępu na bramach wjazdowych. Do drugiego, środkowego pierścienia ochronnego należy zaliczyć linię (obrys) budynku wraz z zewnętrznym obszarem przyległym. Wewnętrzny pierścień ochronny stanowi bezpośredni dostęp do powierzchni magazynowej ze składowanym towarem.**

Złamanie zasady ochrony warstwowej jest jednocześnie złamaniem drugiej podstawowej zasady ochrony obiektów **4D *(Deterrence, Detection, Delaying, Defense).*** Te dwie zasady zostały dokładnie opisane przez IFPO (*International Foundation for Protection Officers*) i leżą u podstaw zasad ochrony wszystkich obiektów.

Do większości parków logistycznych mających wielu najemców można się dostać swobodnie poprzez bramę wjazdową. Jeżeli zarządca czy właściciel parku logistycznego nie zadba o prawidłowe zabezpieczenie mechaniczne i elektroniczne elementów wspólnych infrastruktury parku, takie jak wejścia serwisowe na powierzchnię dachową, to sytuacja jest niebezpieczna. Powodem tego stanu rzeczy jest brak w strukturach organizacyjnych właścicieli parków logistycznych i firm zarządzających takimi parkami osób odpowiedzialnych za bezpieczeństwo, rozumiejących zagrożenia i potrafiących wypracować skuteczny model ochrony wynajmowanych obiektów.

W praktyce za bezpieczeństwo parku logistycznego odpowiada *property manager*, który zarządza 2–3 obiektami i wszystkimi serwisami na podległych nieruchomościach – od nadzoru nad serwisami sprzątającymi, do obsługi technicznej parku włącznie. W rezultacie kwestie bezpieczeństwa zostają przekierowane do zewnętrznych firm ochrony bez jednoznacznych wymagań i rekomendacji ze strony właściciela obiektu, w jaki sposób bezpieczeństwo parku powinno zostać zorganizowane. Nie jest również możliwe skuteczne rozliczanie zewnętrznych podwykonawców, stawianie wymagań z obszaru bezpieczeństwa podwykonawcom przez osoby niepracujące na co dzień w obszarze bezpieczeństwa, np. property managerów.

Transport i logistyka

Te elementy powodują, że pomimo zabezpieczenia wynajmowanej powierzchni zgodnie z obowiązującymi standardami wynajmujący nie może czuć się bezpiecznie w związku z brakiem jednolitego standardu bezpieczeństwa całego parku logistycznego.

Sytuację skutecznie wykorzystują zorganizowane grupy przestępcze. Każde włamanie do magazynu jest poprzedzone uzyskaniem przez grupę przestępczą dokładnych informacji odnośnie do systemu technicznej i fizycznej ochrony obiektu. Do włamań bardzo często dochodzi z sąsiadującej niezabezpieczonej lub słabo zabezpieczonej powierzchni. Popularną metodą jest również wykorzystywanie niezabezpieczonych elementów infrastruktury wspólnej, np. wejść serwisowych na powierzchnię dachu. Przestępcy, którzy są w stanie dostać się tam niepostrzeżenie, mają otwarty dostęp do towarów składowanych na regałach wysokiego składowania nawet pomimo prawidłowo zabezpieczonych klap dymowych.

Omawiając zagrożenia występujące w łańcuchu dostaw, nie można pominąć zagrożeń związanych z samym procesem transportu, np. zachowania przestępcze na drodze, współudział kierowców w procederze kradzieży czy próby wyłudzeń ładunków na podstawie fałszywych dokumentów. Dzisiaj praca dyspozytora lub kierownika zmiany magazynu nie polega już tylko i wyłącznie na sprawdzeniu imienia i nazwiska z awizacją oraz podstawienia samochodu pod odpowiednią rampę załadunkową. Biorąc pod uwagę współczesne zagrożenia związane z wyłudzeniami ładunków w transporcie krajowym lub międzynarodowym, osoby odpowiedzialne za wydanie ładunków po stronie operatora logistycznego powinny posiadać umiejętność weryfikacji dokumentów przedstawionych przez kierowcę zgłaszającego się do załadowania towaru. Autentyczność paszportów biometrycznych można zweryfikować za pomocą najprostszego urządzenia posiadającego łączność NFC oraz za pomocą bezpłatnej aplikacji NFC *Passport Reader*. W przypadku pozostałych paszportów, dowodów osobistych czy praw jazdy skutecznym sposobem jest porównanie przedstawionego do kontroli dokumentu z oficjalnymi bazami wzorców dokumentów, takimi jak http://www.consilium.europa.eu/prado/pl/prado-start-page.html lub http://www.edisontd.net/.

Największym i najtrudniejszym do wykrycia ryzykiem jest pojawienie się przestępcy posługującego się skradzionymi lub kupionymi autentycznymi dokumentami. Wówczas konieczna jest kontrola wizerunki i poproszenie kierowcy o wypełnienia krótkiej ankiety w języku, w którym wydane są dokumenty tożsamości, w celu potwierdzenia autentyczności właściciela dokumentów. Po poprawnej weryfikacji etapu dokumentacyjnego osoba odpowiedzialna za wydanie towaru powinna zweryfikować numer VIN znajdujący się w dowodzie rejestracyjnym i porównać jego poprawność z numerem wybitym na ramie naczepy ładowanego towaru. Wielu operatorów tworzy specjalne procedury wydania towaru oparte na wieloetapowym procesie weryfikacji przewoźników zgłaszających się po odbiór towaru.

Dzisiaj rynek transportowy jest rynkiem międzynarodowym, a kierowcy świadczący usługi transportowe reprezentują praktycznie wszystkie narodowości.

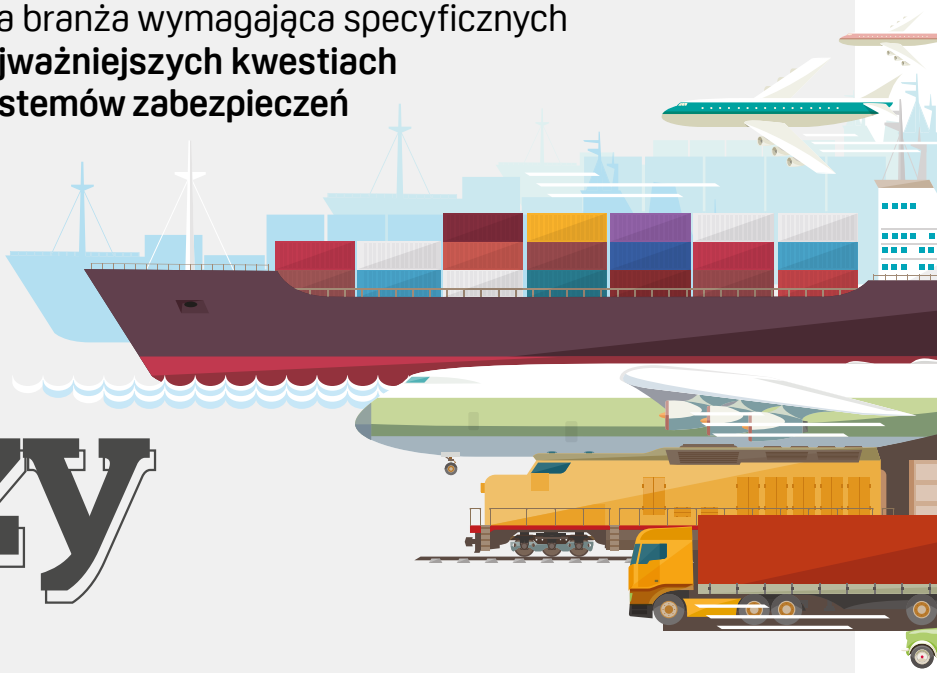
Opisane zagrożenia są bardzo dobrze znane osobom zajmującym się bezpieczeństwem w obszarze logistyki i funkcjonują w logistyce praktycznie od początku tej branży. Niestety obecnie występuje bardzo duża rotacja pracowników we wszystkich gałęziach gospodarki, w tym również w logistyce. Rotacja dotyczy zarówno pracowników magazynowych, jak i kierowców świadczących usługi na rzecz firm transportowych. Sytuacja taka sprzyja skutecznej infiltracji obiektów magazynowych oraz firm transportowych przez zorganizowane grupy przestępcze, poszukujące atrakcyjnych produktów w łańcuchach dostaw.

BIO

Robert Balcewicz
Związany z obszarem bezpieczeństwa od 16 lat, praktyk z wieloletnim doświadczeniem w obszarach zabezpieczeń technicznych, bezpieczeństwa fizycznego oraz proceduralnego.
Zwolennik ciekawych rozwiązań technicznych wspierających zarządzanie bezpieczeństwem w organizacjach.

Transport i logistyka to specyficzna branża wymagająca specyficznych rozwiązań z zakresu security. **O najważniejszych kwestiach opowiedzieli nam użytkownicy systemów zabezpieczeń i ich oferenci.**

Głos branży



Wizyjne systemy zabezpieczeń w transporcie i logistyce

Jakub Sobek
certyfikowany trener techniczny, Linc Polska

Kiedyś wizyjne systemy zabezpieczeń kojarzyły się głównie ze stacjonarnym zabezpieczeniem obiektów przemysłowych lub przestrzeni miejskiej. Wraz z rozwojem techniki i zmniejszeniem wielkości kamer zaczynają znajdować zastosowanie w nowych obszarach. Jednym z nich jest branża transportu i logistyki.

Przy zarządzaniu flotą pojazdów świadomość tego, co dzieje się z danym pojazdem lub kierowcą, jest bardzo istotna. Jednym z rozwiązań oferowanych dla tego segmentu są mobilne rejestratory wizyjne. Przy ich wyborze warto zwrócić uwagę na wiele aspektów. Przydatną funkcjonalnością jest np. jednoczesna możliwość rejestracji, wyświetlania i transmisji obrazu wraz z danymi GPS za pomocą modułów 3G/4G. Operator może zobaczyć na mapie, gdzie znajduje się dany pojazd. Obraz z kamer pokaże, co widzi kierowca, co dzieje się w jego kabinie lub w części załadunkowej ciężarówki. Nadajnik mobilny pozwala też na podłączenie przycisku napadowego, którego może użyć kierowca w sytuacji zagrożenia. Dzięki kamerom pracownik stacji monitoringu może zdalnie zdiagnozować sytuację (wideoweryfikacja) i szybko zareagować, np. wysłać grupę interwencyjną w miejsce wskazane przez dane GPS.

Dotychczas wiele rozwiązań mobilnych umożliwiało lokalną rejestrację obrazu. Należy jednak zwrócić uwagę na to, czy wybrane rozwiązanie jest przystosowane do zastosowań mobilnych, czyli do montażu w pojeździe. Istotna jest tutaj odporność na wstrząsy i spełnienie norm transportowych. Od pewnego czasu na rynku są także dostępne rozwiązania, które automatycznie rejestrują obraz w chmurze. Obraz jest lokalnie buforowany wyłącznie wtedy, gdy występuje problem z jego transmisją. Wiele osób obawia się przesyłania sygnałów wizji w czasie rzeczywistym. Należy jednak pamiętać, że wystarczająca jest przepustowość sieci na poziomie 50 Kb/s.

Zapis w chmurze to znaczące podniesienie bezpieczeństwa zapisywanych danych. W systemie webowym można na bieżąco monitorować stan wszystkich urządzeń. W momencie próby nieuprawnionego wyłączenia nadajnika od razu jest generowane zdarzenie alarmowe. Każda próba lokalnego manipulowania przy nagraniach jest niedozwolona, więc nawet gdyby kierowca chciał wykasować zapis wideo, będzie to niemożliwe. Każda próba zniszczenia takiego nadajnika czy jego kradzież nie pozbawiają nas zapisu, który jest bezpiecznie archiwizowany na dedykowanych serwerach.

W tym samym systemie mogą pracować kamery nasobne, w które zostaną wyposażeni pracownicy. Dzięki temu nawet wtedy, kiedy kierowca wysiada z pojazdu, można przez cały czas zapisywać obraz tego, co on widzi. Dzięki jednej platformie obrazy zarówno z nadajników mobilnych, jak i kamer nasobnych są łatwo dostępne w jednym miejscu.

Rozwiązania tego typu coraz częściej doceniają nie tylko firmy transportowe. Stają się również elementem wyposażenia grup patrolowych, pozwalając na pełną dokumentację podejmowanych interwencji, zapewniając przy tym większe poczucie bezpieczeństwa osobom z nich korzystającym. Kamera nasobna może także zawierać przycisk napadowy, pozwalający na wygenerowanie alarmu. Dwukierunkowa transmisja głosu uzupełnia komunikację pomiędzy użytkownikiem kamery a operatorem systemu.

Wyzwania przed operatorami logistycznymi

Krzysztof Wilczyński
Regional Security Coordinator,
CEVA Logistics Poland

W roku 2018 operatorów logistycznych czekają kolejne podwyżki cen usług ochrony. Dostawcy tłumaczą to zmianami w przepisach prawa oraz rynkiem pracy pracownika. Duża konkurencja powoduje, że w obszarach, w których jest to możliwe, firmy zaczną zastępować człowieka techniką, wcześniej pomijaną ze względu na ceny urządzeń. Przy obecnych kosztach ochrony fizycznej wydają się one już bardziej atrakcyjne. W tej sytuacji największym wyzwaniem dla firm branży logistycznej będzie utrzymanie obecnych kosztów ochrony.

Ważne jest przy tym, aby wprowadzone optymalizacje procesów nie pogarszały jakości usług (serwisu) i nie generowały większych strat inwentaryzacyjnych. Wieloetapowa analiza oraz skrupulatny dobór urządzeń pozwalają niemal zastąpić człowieka w rutynowych działaniach, wygenerować oszczędności względem lat poprzednich.

Firmy, szukając oszczędności, decydują się na integrację systemów zabezpieczeń z systemami magazynowymi, ponieważ monitoring wizyjny dawno już zmienił zakres swojej funkcjonalności. Obecnie obraz z kamer służy do rozpatrywania reklamacji, wyjaśniania błędów systemowych i pracowniczych. Inteligentne algorytmy analityki obrazu skonfigurowane z programem magazynowym skracają czas wyszukiwania zdarzeń oraz przyspieszają reakcję na bieżące nieprawidłowości. Dzięki temu można przy mniejszej liczbie pracowników zachować obecną jakość procesu.

Ogromny wpływ na bezprecedensowy wzrost sprzedaży urządzeń security miało uchwalenie przepisów o minimalnej stawce godzinowej: od 1 stycznia 2017 r. jest to 13 zł brutto. Wiele firm, chcąc optymalizować wydatki na fizyczną ochronę mienia, a jednocześnie podnosić poziom jego zabezpieczenia, systematycznie inwestuje w coraz nowsze rozwiązania tego typu.

Czołowi producenci z branży security, którzy kiedyś nie widzieli potencjału naszego kraju ze względu na wieczny pościg za najniższą ceną, obecnie wkraczają z innowacyjnymi systemami, znajdując bez problemu odbiorców końcowych.

Inwestując na bieżąco w innowacyjne technologie ochrony, możemy w łatwy sposób elastycznie dostosowywać naszą firmę do zmieniających się realiów rynku, wymagań klientów i nieoczekiwanych zagrożeń oraz szybko adaptować je do naszych potrzeb, aby zachować przez cały czas najwyższą jakość świadczonych usług.

Technologia jutra wspiera infrastrukturę drogową

Jan T. Grusznic
Sales Engineer,
Axis Communications

Na początku tego roku Axis Communications przedstawił 10 trendów technologicznych, które istotnie wpłyną na kierunek zmian w elektronicznych systemach zabezpieczeń. Jednym z nich jest zwiększająca się moc obliczeniowa urządzeń brzegowych, która sprzyja rozwiązaniu kwestii związanej z problematyką centralnego przetwarzania dużej liczby informacji, analizując dane w miejscu ich przechwytywania. Ponieważ kamery sieciowe, audio i inne czujniki – urządzenia znajdujące się na obrzeżach sieci – stają się coraz bardziej zaawansowane, zrównoważenie przetwarzania w chmurze, a także obliczeń brzegowych staje się nieodzowne w dostarczaniu niezawodnych i użytecznych danych.

Dobrym przykładem obrazującym to zjawisko jest realizacja programów Programu Operacyjnego Infrastruktura i Środowisko, które wśród priorytetów i działań wskazuje na usprawnienie przepustowości infrastruktury drogowej. Już teraz coraz większa liczba czujników instalowanych w pasie jezdni jest zastępowana kamerami z wbudowanymi aplikacjami, mającymi za zadanie analizę przepływności ruchu w miejscu ich instalacji. Kamery dostarczają raporty w czasie rzeczywistym o takich incydentach, jak zatrzymane pojazdy, niewłaściwa jazda (zbyt wolna lub w nieprawidłowym kierunku), przeciążenia, a nawet o pożarze.

Na bazie algorytmów rozpoznawania tablic rejestracyjnych realizowane są usługi zarządzania kontrolą wjazdu, automatycznych zgłoszeń o pojazdach znajdujących się na listach kontrolnych, rozliczeń opłat za korzystanie z odcinków płatnych lub miejsc parkingowych. Co prawda analiza jest wykonywana po stronie urządzeń brzegowych, jednak kluczowe staje się centralne przetworzenie rozproszonych danych pochodzących z kamer, aplikacji mobilnych, pętli indukcyjnych czy też sterowników automatyki. Dopiero połączone i przeanalizowane dane ze wszystkich elementów mogą być przedstawione użytkownikowi systemu – zarządcy, kierowcy, służbom utrzymania.

Dzięki standaryzacji, wykorzystaniu otwartych protokołów wymiany informacji, otwartej platformie i wysokiemu bezpieczeństwu produktów Axis tworzone dzisiaj systemy zarządzania transportem są przygotowane na wyzwania jutra.

Bezpieczeństwo to nie produkt, to proces

Tomasz Siwicki
Security Department Manager, kierownik Działu Bezpieczeństwa, GEFCO Poland

Jak stwierdził Bruce Schneier: *Bezpieczeństwo to nie produkt, to proces*, bezpieczeństwo transportu i logistyki nie jest problemem technologicznym, tylko problemem związanym z ludźmi i zarządzaniem.
W mojej ocenie największym wyzwaniem będzie właśnie zarządzanie ludźmi, przekonanie ich, że bezpieczeństwo to właśnie proces. Niestosowanie się do obowiązujących procedur oraz obniżanie wymaganego poziomu bezpieczeństwa powoduje, iż wzrasta liczba kradzieży, do których dochodzi w transporcie podczas postojów.
Kradzieże są coraz bardziej zuchwałe i są dokonywane również na parkingach, uważanych dotychczas za potencjalnie bezpieczne. Obecnie obserwujemy duży wzrost liczby kradzieży na parkingach w Europie Zachodniej. Przykładem może być Francja, gdzie identyfikuje się bardzo duży wzrost przestępstw popełnianych przez wyspecjalizowane gangi z Łotwy. Ten rok będzie wyzwaniem dla *security managerów* odpowiedzialnych za bezpieczeństwo łańcucha dostaw.

Kamery w służbie przemysłu transportowego i logistyki

Maciej Pietrzak
Sales Support Engineer, Dahua Technology Poland

Zakres i dostępność usług świadczonych przez firmy z branży transportu i logistyki stale rośnie. W zasadzie nie ma znaczenia rozmiar ładunku czy odległość, jaką musi pokonać. Liczba paczek wysyłanych pocztą lub za pośrednictwem firm kurierskich każdego roku się zwiększa. Nie bez znaczenia jest także stale rosnąca popularność e-commerce, jednego z ważniejszych motorów napędzających sektor logistyki. Wymusza to na przewoźnikach korzystanie z nowoczesnych technologii pozwalających sprostać wymaganiom. Firmy kurierskie muszą się skupić nie tylko na wydajności, ale również bezpieczeństwie – zarówno powierzonych im przesyłek, jak i pracowników oraz mienia.
Rozwiązania firmy Dahua Technology wspierają procesy mające na celu zapewnienie odpowiedniego poziomu bezpieczeństwa oraz usprawniają i automatyzują procesy przemysłowe.
W listopadzie 2017 r., na konferencji *Machine Vision Show* zorganizowanej przez Dahua Technology Poland, zostały zaprezentowane rozwiązania przeznaczone dla przemysłu. Kamery szybkoklatkowe pozwalające na odczyt nawet do 1000 kodów kreskowych na minutę, detekcja uszkodzeń lub innych anomalii, kamery 3D umożliwiające wymiarowanie gabarytów obiektu przemieszczającego się na taśmociągu to tylko wąski wycinek możliwości oferowanych przez kamery Machine Vision. Dzięki nim firma logistyczna jest w stanie szybciej sklasyfikować przesyłkę, określić jej wielkość i zadecydować o jej dalszej drodze, a wszystko bez udziału człowieka.
Nie bez znaczenia pozostaje aspekt bezpieczeństwa. Chcąc mieć wiedzę na temat tego, co dzieje się z przesyłką na terenie sortowni, należy zastosować kamery zapewniające obraz o wysokiej szczegółowości w każdych warunkach otoczenia. Te potrzeby mogą zaspokoić kamery stacjonarne i obrotowe PTZ Dahua Technology z ultraczułymi przetwornikami Sony Starlight, które oprócz wysokiej rozdzielczości 12 Mpix charakteryzują się możliwością pracy w każdych warunkach oświetleniowych.
Od czasu do czasu docierają do nas informacje o tym, że przesyłka zawierała niedozwolone substancje, które były przyczyną samozapłonu, co spowodowało szkody. Narzędziem pomocnym w detekcji tego typu zagrożeń może być kamera termowizyjna, która jest w stanie zainicjować alarm pożarowy, zanim dym zostanie wykryty przez czujki pożarowe. Kamera termowizyjna zastosowana w hali przemysłowej może służyć również do wczesnego wykrycia zużycia elementów mechanicznych maszyn pracujących w hali. Łożysko, którego oporność wzrosła w wyniku zużycia, emituje znaczną ilość ciepła, które może być wykryte przez kamerę termowizyjną.
Kluczowym elementem systemu bezpieczeństwa jest rejestrator lub oprogramowanie zarządzające. Warto zwrócić uwagę na fakt, że wszystkie wspomniane rozwiązania łączy oprogramowanie DSS Pro firmy Dahua Technology. Z poziomu oprogramowania można uzyskać dostęp do obrazu na żywo z dowolnej kamery w obiekcie oraz do materiału zarejestrowanego. Operator, mając kod kreskowy przesyłki, za pomocą oprogramowania może prześledzić całą jej trasę w sortowni. Dzięki temu przy ewentualnym uszkodzeniu paczki można szybko stwierdzić, czy miało ono miejsce w sortowni, czy też w dalszej drodze ładunku.
Zadaniem systemu dozoru wizyjnego jest nie tylko zapewnienie bezpieczeństwa i świadomości sytuacyjnej, dzisiaj ma on także kluczowy udział w procesach automatyzujących działanie przedsiębiorstwa. Mając to na uwadze, można być pewnym, że współpraca producentów rozwiązań wizyjnych oraz m.in. firm transportowych będzie przebiegała coraz ściślej.

Bezpieczny transport kolejowy

Paweł Augustowski
Project Engineer, Hikvision Poland

Polski transport kolejowy oraz produkcja pojazdów szynowych rozwijają się coraz szybciej, a co za tym idzie zapotrzebowanie na produkty z branży security wzrasta. Firma Hikvision posiada kompletną ofertę do rozwiązań mobilnych. Nasze urządzenia znalazły nabywców także wśród producentów krajowych.

Ostatnie lata stały pod znakiem ekspansji polskich producentów pojazdów na całą Europę. Konkurują nie tylko ceną, ale także jakością. Nakłady na bezpieczeństwo w Europie wzrastają z każdym rokiem i z każdym incydentem. Monitoring wizyjny w składach wpływa bezpośrednio na bezpieczeństwo pasażerów i kontrolę ruchu. Zastosowanie kamery z aplikacją zliczania osób w drzwiach wejściowych wagonu dostarczy danych do statystyk dotyczących liczby pasażerów podróżujących pociągiem w konkretnych godzinach. Taka informacja pozwoli zaplanować wielkość składów, które powinny być w danym dniu o konkretnej porze na wybranej trasie. Rozsądne gospodarowanie zasobami zapewnia oszczędności (fundusze można np. wykorzystać na nowy tabor) oraz efektywne planowanie zatrudniania obsługi.

Oferta urządzeń mobilnych Hikvision obejmuje m.in. pełną gamę rejestratorów i kamer przeznaczonych do tego typu rozwiązań. Projektowanie i produkcja ściśle spełniają wymogi inwestorów – kamery są odporne na wszelkiego rodzaju akty wandalizmu, obiektywy o szerokim kącie widzenia gwarantują brak martwych stref. Szeroki kąt widzenia jest bardzo ważny ze względu na ograniczoną wysokość montażu. Niezbędna jest funkcja WDR (*Wide Dynamic Range*) pozwalająca na widzenie szczegółów w scenach o różnym natężeniu światła – obszarach zarówno mocno oświetlonych, jak i zacienionych. Niezbędny do poprawnego działania kamery jest również promiennik IR.

Przyszłością rozwoju telewizji dozorowej jest przede wszystkim analityka wideo. Najważniejsze, aby operator monitoringu dostał precyzyjny sygnał o zdarzeniu (np. skład jedzie w niewłaściwym kierunku, kierowca jest zmęczony, pali papierosa), co bezpośrednio wpływa na bezpieczeństwo przewożonych osób. Jeszcze kilka lat temu tego typu rozwiązania mogliśmy sobie jedynie wyobrażać. W tej chwili to wszystko jest dostępne, a nawet więcej – jesteśmy gotowi do rozpoznawania i porównywania twarzy z bazą w centrum monitoringu, np. w celu znalezienia osób poszukiwanych.

Monitoring obiektów bez zasilania

Andrzej Nowak
menedżer produktów do lokalizacji GPS, Omtech

W branży transportowej wiele zagadnień związanych z bezpieczeństwem ładunku, pojazdu i ludzi można rozwiązać za pomocą kamer telewizji dozorowej, popularnych dzisiaj nadajników GPS, różnego rodzaju czujników instalowanych w przestrzeni bagażowej czy specjalnych urządzeń rozpoznających drogę, znaki drogowe i ostrzegających kierowców o nieprawidłowym zachowaniu. Wszystkie te rozwiązania łączy wspólna cecha: wymagają ciągłego zasilania i często złożonej instalacji.

Wyzwaniem jest np. zabezpieczenie kontenera morskiego, kolejowego wagonu towarowego lub kontenera na gruz. Tego rodzaju obiekty potrafią przede wszystkim „zaginąć". Przyczyną mogą być zarówno błędy ludzkie, np. pozostawienie podczas przeładunku czy odstawienie na bocznicę, jak i kradzież. Znane są przypadki, gdy zarządca floty nie potrafi zlokalizować setek wagonów, a koszt jednego wagonu towarowego znacznie przekracza milion złotych. W przypadku kontenerów morskich koszt każdego z nich nie jest już tak spektakularny, natomiast ich duża liczba i znacznie większe ryzyko ich zgubienia sprawia, że znalezienie odpowiedniego rozwiązania jest opłacalne.

Warto zwrócić uwagę na to, że te obiekty są pozbawione zasilania i jednocześnie pracują w trudnych warunkach, więc wykorzystanie delikatnych paneli fotowoltaicznych nie jest możliwe, nie wspominając o turbinach wiatrowych. Wydaje się, że jedynym rozwiązaniem pozostaje zatem zasilanie bateryjne lub akumulatorowe. Tutaj pojawiają się następujące wyzwania: urządzenie nie może być

Mobilne bezpieczeństwo

Marcin Morzyk
BCS

Nietrudno zbudować system telewizji dozorowej chroniący obiekty stacjonarne lub system monitoringu miast – oferta rozwiązań i urządzeń jest bogata. Zdarza się jednak, że po zabezpieczeniu budynków, np. hurtowni lub centrum logistycznego, konieczne jest również zabezpieczenie transportowanych towarów. Wówczas wybór odpowiedniego rozwiązania staje się bardziej skomplikowany. Wymagania monitoringu mobilnego są tak różne, jak różne są sposoby transportu. Projektując system, warto spojrzeć w przyszłość i wybrać rozwiązanie łatwo skalowalne, aby przy rozbudowie floty nie trzeba było wymieniać całego rozwiązania.

Podczas tworzenia systemu monitoringu obiektu, np. w hurtowni, trzeba uwzględnić pełną automatykę funkcji, pozwalającą minimalizować udział ludzi lub konieczność ich ingerencji w system. Oprócz standardowych kamer rejestrujących wjazd i wyjazd powinny się pojawić kamery ARTR rozpoznające tablice rejestracyjne, wówczas można awizować pojazdy i zdalnie nadawać im prawo wjazdu w danym dniu. Na podstawie informacji o wjeżdżających pojazdach zapisanych w karcie pamięci lub oprogramowaniu BCS Manager można również przygotować prosty raport wjazdów i wyjazdów z dowolnej kamery ARTR w systemie.

Zabezpieczając kolejny element naszego systemu – pojazdy dostarczające produkty, chcielibyśmy wiedzieć, gdzie nasz pojazd się znajduje, i widzieć obraz z kamer. Wówczas warto wybrać rejestrator mobilny z wbudowanym modemem 3G, 4G lub Wi-Fi oraz modułem GPS. Rejestratory mobilne występują w wersji HDCVI lub IP. Bardziej praktyczne wydaje się rozwiązanie IP ze względu na możliwość wykorzystania funkcji PoE i kamer z wbudowanymi mikrofonami. Zasilamy wówczas rejestrator, który ma szeroki zakres napięcia zasilającego (od 12 VDC do 36 VDC), a kamery podłączamy do wbudowanego w rejestratorze switcha PoE. Warto również zwrócić uwagę na możliwości odtwarzania nagranego materiału oraz sposoby archiwizacji nagrań. Tańsze rozwiązania mogą np. odtworzyć obrazy tylko z jednej kamery, co znacząco wydłuża czas wyszukiwania interesującego materiału. Konstrukcja rejestratora mobilnego powinna również zapewniać bezpieczeństwo danych, dlatego dysk powinien być instalowany w resorowanej kieszeni.

Budując system monitoringu wizyjnego, do którego chcemy dołączyć również mobilne rejestratory, musimy przewidzieć, jaki efekt chcemy osiągnąć. Warto wybrać producenta, który może zaoferować rozwiązanie kompleksowe.

duże, a wykorzystane elementy nie mogą być atrakcyjne dla postronnych osób. Co więcej, okres serwisowania nie może być zbyt krótki, ponieważ przeprowadzenie akcji dla całej floty jest dość złożone.

Z pomocą przychodzą nowoczesne lokalizatory GPS z transmisją komórkową, które wykorzystując akcelerometr, mogą służyć przez lata do lokalizowania obiektów. Niekwestionowanymi zaletami tego typu urządzeń są ich kompaktowe rozmiary, autonomiczne zasilanie, hermetyczna i odporna obudowa oraz brak konieczności częstego serwisowania. Istotna jest też łatwość wymiany i montażu takiego urządzenia, aby czynności te zajmowały jak najmniej czasu, nawet w niesprzyjających warunkach atmosferycznych w każdym terenie. Właśnie w tym celu urządzenia można wyposażyć w silne magnesy neodymowe, które umożliwiają montaż bez dodatkowych narzędzi w dowolnych warunkach. Lokalizatory tego typu mają za zadanie wskazać na mapie obiekt już po jego zatrzymaniu, dzięki czemu nie pobierają prądu na śledzenie bieżącej trasy i transmisję do serwera w czasie, kiedy obiekt jest w ruchu.

Kontener lub wagon towarowy miesięcznie przemieszczają się na długie dystanse. W każdym porcie może się zdarzyć, że się gdzieś „zawieruszy". Jego pozycję urządzenie może sprawdzić w dowolnej chwili, a jeśli zostanie przesunięty lub przewieziony, to po zatrzymaniu system znów będzie znał jego najnowszą lokalizację.

W szczególnych zastosowaniach, np. kolejnictwa towarowego, jest wymagana sprawozdawczość dotycząca przebiegu każdego wagonu. Jest to istotne ze względu na konieczność wykonywania przeglądów zależnych właśnie od przebiegu. W takim przypadku urządzenie może dodatkowo w pewnych odstępach czasu rejestrować lokalizację, zapisując ją w pamięci. Następnie po zatrzymaniu urządzenie przesyła na serwer w jednej paczce zarejestrowane pozycje wraz z tą po zatrzymaniu. To umożliwia operatorom wagonów wymaganą przepisami sprawozdawczość, a jednocześnie powoduje tylko nieznacznie większe zużycie prądu, dzięki czemu żywotność urządzenia nie spada drastycznie.

Zainteresowani takimi produktami na rynku polskim mogą znaleźć urządzenia zasilane dwiema lub trzema bateriami w rozmiarze D. Ich żywotność wg producenta wynosi nawet 36 miesięcy. Urządzenia mają wymiary ok. 160 x 80 x 65 mm.

BEZPIECZEŃSTWO POŻAROWE W METRZE

Metro, czyli miejski system kolei (podziemnych i nadziemnych), jest we współczesnych największych miastach nieodłącznym elementem organizacji transportu publicznego. Przewagą tego środka transportu w stosunku do innych jest jego wielokrotnie większa przepustowość.

Iza Trzeciak

W jedynym metrze w Polsce, w Warszawie, w godzinach szczytu pociągi kursują z częstotliwością ok. 20 na godzinę, czyli z każdej stacji pociąg odjeżdża co 3 min. Codziennie z warszawskiego metra korzysta ok. 550 tys. pasażerów. To dużo, choć w porównaniu do londyńskiego London Underground, które dziennie przewozi ok. 3,3 mln pasażerów, zaledwie niecałe 20%. W Polsce metro działa od 1995 r. (pierwszy odcinek pierwszej linii), Anglicy zaś mogą pochwalić się posiadaniem najstarszego metra na świecie.

Pierwszy odcinek London Underground oddano do użytku już w 1863 r. Obecnie tworzy go jedenaście linii, nad dwunastą trwają prace. Metro londyńskie ma już 154 lata, a jego długa i bogata historia jest jednocześnie dużą częścią światowej historii komunikacji zbiorowej.

Tragedia na King's Cross

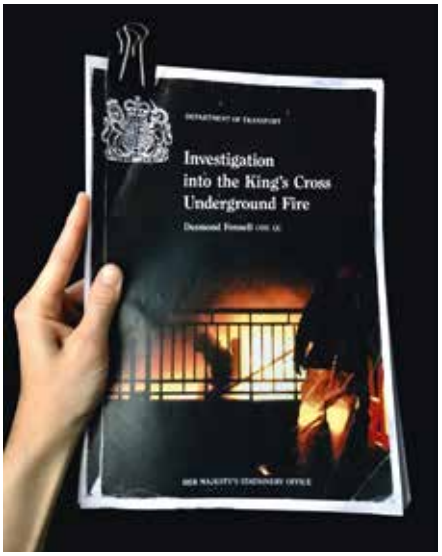
W bogatym doświadczeniu London Underground znajdują się również tragiczne wydarzenia, z których wnioski i przestrogi wyciąga cały świat. Ponad 30 lat temu miało miejsce wydarzenie, które zmieniło postrzeganie bezpieczeństwa pożarowego w obiektach infrastruktury metra. W pożarze, który wybuchł 18 listopada 1987 r. wieczorem na stacji King's Cross, zginęło 31 osób, w tym dowódca jednostki straży pożarnej. Wiele osób zostało poważnie rannych. Fotografia poparzonej twarzy jednego z ocalałych, Kwasi Afari Minta, w specjalnym opatrunku, obiegła świat i stała się symbolem tej tragedii. Po tym zdarzeniu pojawiły się wątpliwości, czy setki tysięcy pasażerów korzystających codziennie z metra mogą czuć się bezpiecznie.

Co się wydarzyło w ten listopadowy wieczór na stacji King's Cross? Odpowiedź na to pytanie znajduje się w oficjalnym raporcie [1] podsumowującym kilkumiesięczne dochodzenie. Jego autorem oraz kierującym pracami zespołu był Desmond Fennell. Wraz z zespołem biegłych i ekspertów przez prawie rok pracował nad wyjaśnieniem przebiegu tego pożaru. Śledztwo było prowadzone szczegółowo. Rozważono i wzięto pod uwagę wszelkie możliwe aspekty, które mogły doprowadzić do tak fatalnego splotu zdarzeń. Fennell ze swoim zespołem dokonał oględzin pogorzeliska, przesłuchał obsługę metra oraz świadków zdarzenia, przeanalizował reakcje personelu metra oraz służb ratunkowych, przyjrzał się modelowi zarządzania bezpieczeństwem w London Underground, wykorzystał rozwijającą się wówczas metodę FDS (*fire dynamics simulation*) do stworzenia komputerowego modelu tego pożaru, aż wreszcie – nie znajdując odpowiedzi na swoje wątpliwości – zbudował model schodów ruchomych nr 4 na stacji King's Cross na linii Piccadilly.

Po roku od tragedii, w listopadzie 1988 r. opublikowano raport *Investigation into the King's Cross Underground Fire* [1], w którym opisano przyczyny i przebieg pożaru oraz sformułowano wnioski i zalecenia, jak takich sytuacji uniknąć.

Jaka była przyczyna pożaru?

Można uznać, że odpowiedź na to pytanie była prosta, gdyż poznano ją już po oględzinach pogorzeliska. Otóż, pomimo zakazu palenia w metrze, który obowiązywał od lutego 1985 r. (po pożarze na stacji Oxford Circus), pasażerowie nie zaprzestali palenia papierosów. Powszechnym



zachowaniem było m.in. zapalanie papierosów zapałkami już na schodach ruchomych, przy opuszczaniu stacji. W listwach między schodami a balustradą znajdowały się ubytki, będące skutkiem intensywnego użytkowania (stale poruszające się stopnie pocierały o listwy, powoli je niszcząc). W schodach nr 4 ponad 30% długości tych listew było zniszczonych. Niezgaszona zapałka wpadła do środka schodów, gdzie trafiła na idealne podłoże. W układzie poruszającym schodami wskutek braku czynności konserwacyjnych nagromadziła się znaczna ilość zanieczyszczeń, m.in. kurz, drobne włókna i inne śmieci wymieszane ze smarem. Później, w trakcie oględzin pogorzeliska, znaleziono wiele zapałek w dolnej części schodów, a także ślady wielu mikropożarów, które dotychczas same gasły. **Inaczej stało się 18 listopada 1987 r. – wyrzucona płonąca zapałka zapaliła smar w układzie napędowym po prawej stronie schodów ruchomych nr 4, prowadzących do hali biletowej z linii Piccadilly na stacji King's Cross.**

Dalsze dochodzenie pozwoliło na ustalenie następującej kolejności zdarzeń: pożar rozpoczął się na wysokości mniej więcej 48. stopnia schodów ok. godz. 19.25. Oznaki pożaru – tj. płomień pod schodami czy też płonąca chusteczka na peronie – zauważyło kilkoro pasażerów i zgłosiło ten fakt obsłudze metra. Niestety, personel, po niezbyt wnikliwym rozeznaniu sytuacji, nie wezwał straży pożarnej ani nie podjął próby gaszenia. Nie wcisnął nawet przycisku alarmowego zatrzymania schodów, zrobił to kolejny pasażer. Do momentu zatrzymania schodów ogień rozprzestrzeniał się pod nimi w kierunku szczytu pochylni schodów oraz na ich lewą stronę. Po zatrzymaniu schodów jeden z pracowników metra zszedł z poziomu hali biletowej (gdzie miał swoje stanowisko pracy) na peron. Zobaczył dym i pojedynczy płomień i wreszcie podjął decyzję o zaalarmowaniu służb. Aby to zrobić, musiał wrócić na powierzchnię, ponieważ

W długiej historii London Underground są również tragiczne wydarzenia, z których wnioski i przestrogi do dziś wyciąga cały świat.

ROZGORZENIE CZY WSTECZNY CIĄG PŁOMIENI

Zjawisko rozgorzenia jest czasami mylone ze wstecznym ciągiem płomieni.

Rozgorzenie (*flashover*) - moment deflagracyjnego zapalenia się płomieniowego mieszaniny gazowej znajdującej się pod sufitem [2], nagłe ogarnięcie spalaniem powierzchni materiału palnego wewnątrz wydzielonej przestrzeni, pomieszczenia. Zjawisku temu towarzyszy wzrost ciśnienia po zapłonie do 1 kPa.

Wsteczny ciąg płomieni (*backdraft*) - deflagracja powstająca na skutek wprowadzenia tlenu do pomieszczenia wypełnionego nadmiarem produktów niezupełnego spalania i rozkładu termicznego. Wzrost ciśnienia po zapłonie osiąga wartość do 10 kPa [2].

ROZGORZENIE	WSTECZNY CIĄG PŁOMIENI
PODOBIEŃSTWA	
oba zjawiska prowadzą do fazy II pożaru (pożaru rozwiniętego)	
tworzą się w wyniku rozkładu termicznego gazów pożarowych, gromadzących się w górnej części pomieszczenia	
oba zjawiska charakteryzuje wyrzut płomieni na zewnątrz pomieszczenia	
RÓŻNICE	
zjawisko wyłącznie termiczne	zjawisko przepływowo-termiczne
zjawisko ciągłe	zjawisko chwilowe
zachodzi w warunkach dobrej wentylacji	zachodzi w warunkach ograniczonej wentylacji, przy niedostatku tlenu
moment deflagracyjnego zapalenia się płomieniowego mieszaniny gazowej znajdującej się pod sufitem	deflagracja powstająca na skutek wprowadzenia tlenu do pomieszczenia wypełnionego nadmiarem produktów niezupełnego spalania i rozkładu termicznego
gromadzące się gazy pożarowe pozostają w granicach wchodzących w zakres granic wybuchowości	gromadzące się gazy pożarowe w granicach przekraczających GGW
wzrost ciśnienia po zapłonie do 1 kPa	wzrost ciśnienia po zapłonie do 10 kPa

pod ziemią łączność radiowa nie działała. Straż pożarna otrzymała wezwanie ok. godz. 19.34. Należy podkreślić, że stacja cały czas była czynna i pasażerów przybywało – dopiero o godz. 19.40 wydano polecenie niezatrzymywania się pociągów na stacji King's Cross (w późniejszej fazie ludzi z peronu ewakuowano pociągami linii Victoria).

Po kilku minutach pożar spod schodów rozprzestrzenił się na ich powierzchnię (stopnie były wykonane ze sklejki drewnianej impregnowanej olejem), później objął elementy gumowe i lakierowane balustrady. O godz. 19.42 na miejsce dotarł pierwszy wóz pobliskiej jednostki straży pożarnej Soho, który zastał pożar już w stanie zaawansowanym. Jeden ze strażaków, dowódca jednostki, zszedł na peron, aby zrobić rozpoznanie, po czym wrócił na poziom hali biletowej i przekazał komunikat strażakowi kierującemu akcją: *make pumps 4 – persons reported.* Takie polecenie padające z ust strażaka świadczy o rozpoznaniu sytuacji wymagającej zadysponowania dodatkowych sił i środków. W tym wypadku wiązało się ze ściągnięciem dodatkowych czterech wozów gaśniczych oraz karetek pogotowia, gdyż należało spodziewać się rannych.

O tym, jak bardzo będą potrzebne, strażacy mieli przekonać się już za chwilę. Zaledwie po 3 minutach od przybycia strażaków cała hala biletowa wypełniła się intensywnym ciepłym powietrzem oraz gęstym, czarnym dymem. Zapadła ciemność. Kierujący akcją ratowniczo-gaśniczą rozkazał swojej załodze ewakuować ludzi i uciekać. O godz. 19.45 (na tej godzinie zatrzymał się zegar na szczycie schodów), zanim podano jakikolwiek środek gaśniczy, pożar przeszedł w fazę pożaru rozwiniętego – nastąpiło **rozgorzenie.** Płomienie wypełniły halę biletową, zabijając lub poważnie raniąc ludzi, którzy w tym momencie się tam znajdowali.

Zespołowi Fennella bardzo trudno było wyjaśnić, dlaczego pożar był tak dynamiczny i rozgorzenie nastąpiło tak szybko. Na dodatek zauważono, że w symulacjach komputerowych rozwoju tego pożaru płomienie zachowywały się inaczej, niż się spodziewano – nie unosiły się pionowo, jak podczas zwykłych obserwacji ruchu gorących gazów, tylko pełzały po schodach, jakby się do nich przylejały. Podejrzewano nawet, że w modelach matematycznych jest błąd, jednak nie udało się go znaleźć. Śledczy postanowili zbudować model schodów i zasymulować ten pożar, wiedząc już, co go spowodowało.

Zbudowano stanowisko w skali 1:3, używając dokładnie takich samych materiałów, z jakich zostały wykonane ruchome schody, oraz odwzorowując wszelkie warunki mogące mieć wpływ na przebieg pożaru. Podczas doświadczenia pierwsza zapalona zapałka, którą wrzucono w szczelinę przy balustradzie schodów, zapoczątkowała pożar. Przez pierwsze 6 min doświadczalny pożar zachowywał i rozwijał się normalnie. Jednak po upływie ok. 7,5 min płomienie przylgnęły do powierzchni schodów, a po 20 s od zanotowania tego faktu temperatura gwałtownie wzrosła do ok. 800°C. Po kilkunastu następnych sekundach badacze zaobserwowali rozgorzenie, wskutek którego makieta hali biletowej stanęła w płomieniach. Doświadczenie potwierdziło, że w symulacjach komputerowych nie było błędu.

Trench effect i wnioski

Z doświadczenia wyciągnięto cenne wnioski. Dowiedziono, że na tak dynamiczny i tragiczny rozwój pożaru na King's Cross złożyły się dwa kluczowe elementy. Nachylenie schodów o ok. 30° spowodowało „przyklejenie się" płomieni do schodów (jest za to odpowiedzialny efekt Coandy polegający na przyleganiu płynu do najbliższej powierzchni – w tym przypadku płomieni do nachylonych schodów), a fakt występowania balustrady z obu stron stworzył niejako tunel, w którym kumulowało się ciepło. Gdy ogień rozprzestrzeniał

się po pochylni schodów, tworzył przed nim niewidzialną warstwę ciepła i gazów, które z kolei nagrzewały drewniane stopnie. Potrzeba było zaledwie sekund, aby doszło do rozgorzenia. Katastrofalne skutki pożaru schodów na King's Cross były skutkiem połączenia efektu Coandy i rozgorzenia. Takie zjawisko było fenomenem, wcześniej nieobserwowanym, a poznanym i opisanym dopiero w raporcie Fennella. Nazwano go *trench effect*, co w języku polskim oznacza *efekt rynnowy* lub *efekt okopowy*.

Rozpoznając zjawisko efektu rynnowego, eksperci dopasowali ostatni element układanki. Wyjaśniono już przebieg zdarzeń i wskazano elementy, które miały wpływ na skutki. Mając tę wiedzę, Desmond Fennell zawarł w raporcie rekomendacje, których wprowadzenie w życie miało zapobiec podobnym zdarzeniom w przyszłości. Zawarł tam łącznie 157 (!) uwag i zaleceń, dotykając wszystkich aspektów, które składają się na bezpieczeństwo pożarowe w metrze: począwszy od wyposażania wskazanych miejsc w urządzenia przeciwpożarowe, zastosowanie w obiektach metra systemu łączności radiowej, wymiany drewnianych elementów schodów na stalowe, czytelnego oznakowania kierunków do wyjść ewakuacyjnych, wprowadzenia jasnego podziału obowiązków i odpowiedzialności, opracowania procedur alarmowych oraz programów szkoleń pracowników metra oraz wiele innych.

Implementacja zaleceń Fennella

Zmiany w kontekście bezpieczeństwa pożarowego w londyńskim metrze miały szeroki zakres i obejmowały m.in.:

- wymianę drewnianych schodów na metalowe,
- wprowadzenie nowych procedur awaryjnych i ewakuacyjnych,
- lepsze zapoznanie się służb ratowniczych z warunkami w metrze,
- opracowanie i wdrożenie nowych systemów zarządzania i audytów bezpieczeństwa,
- obowiązek uczestniczenia w szkoleniach z zakresu reakcji na zagrożenia dla wszystkich pracowników stacji,
- wyposażenie obiektów metra w system komunikacji.

Ponadto rozszerzono obowiązujące prawo dotyczące bezpieczeństwa pożarowego budynków, aby obejmowało również stacje podziemne.

Wnioski i rekomendacje, które sformułowano po tym zdarzeniu, są aktualne nie tylko w odniesieniu do metra w Londynie. Ślady tych doświadczeń są także w polskich przepisach określających wymagania w zakresie bezpieczeństwa pożarowego, jakie muszą spełniać obiekty metra.

Metro w polskich przepisach

Projekt budowlany metra wymaga uzgodnienia pod względem zgodności z wymaganiami ochrony przeciwpożarowej przez rzeczoznawcę ds. zabezpieczeń ppoż. Warunki techniczne, jakim powinny odpowiadać obiekty budowlane metra i ich usytuowanie, opisano w rozporządzeniu o tym samym tytule [3]. Przy projektowaniu należy ponadto uwzględnić odpowiednie wymagania bezpieczeństwa pożarowego określone w przepisach ppoż. [4] oraz w przepisach dotyczących warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie [5].

Przeglądając zapisy rozporządzenia [3], większość dotyczących bezpieczeństwa pożarowego znajduje się w załączniku nr 1 „Wymagania w zakresie zapewnienia

Tunele, stacje metra oraz budowle spełniające funkcję użytkową budynków powinny być wyposażone w instalację wentylacji pożarowej zapewniającą skuteczne usuwanie dymu w sposób zapobiegający zadymieniu stacji, wyjść ewakuacyjnych i pomieszczeń, w których znajdują się urządzenia bezpieczeństwa.

bezpieczeństwa pożarowego obiektów budowlanych metra". Poza załącznikiem zapisano tylko nieliczne warunki, np. dotyczące instalowania przeciwpożarowego wyłącznika prądu (odcinającego dopływ energii elektrycznej do wszystkich odbiorników na stacji metra, z wyjątkiem obwodów zasilających instalacje i urządzenia, których funkcjonowanie jest niezbędne w czasie pożaru i prowadzenia akcji ratowniczo-gaśniczej) oraz oświetlenia awaryjnego (w pomieszczeniach przeznaczonych na pobyt ludzi oraz w tunelach należy zapewnić oświetlenie awaryjne, a w pomieszczeniach użytkowanych przy wyłączonym oświetleniu podstawowym – oświetlenie dodatkowe służące uwidocznieniu przeszkód i dróg komunikacji ogólnej oraz podświetlane znaki ewakuacyjne).

Ewakuacja ze stacji metra

Podziemne budowle metra należy projektować w taki sposób, aby szerokości dróg komunikacyjnych stacji metra stanowiących drogi ewakuacyjne oraz łączna szerokość drzwi stanowiących wyjścia ewakuacyjne była wystarczająca, by ewakuacja stacji trwała nie dłużej niż 10 min, z zastrzeżeniem, że przewidywany czas ewakuacji (z wyłączeniem tuneli) nie może

być dłuższy od krytycznego czasu ewakuacji. Definicje tych pojęć są następujące:
Przewidywany czas ewakuacji – iloczyn obliczonego czasu niezbędnego do ewakuacji i współczynnika bezpieczeństwa ocenianego indywidualnie, lecz nie mniejszego niż 1,3.
Krytyczny czas ewakuacji – czas do osiągnięcia stanu krytycznego środowiska.
Stan krytyczny środowiska – wystąpienie w obiekcie budowlanym metra krytycznego dla życia i zdrowia ludzi warunku środowiskowego w wyniku przekroczenia jednego z następujących parametrów:
a) temperatury powietrza przekraczającej 60°C na wysokości mniejszej lub równej 1,8 m od poziomu drogi ewakuacyjnej,
b) gęstości strumienia promieniowania cieplnego o wartości 2,5 kW/m^2 przez czas ekspozycji dłuższy niż 30 s,
c) temperatury gorących gazów pożarowych powyżej 200°C na wysokości ponad 2,5 m od poziomu drogi ewakuacyjnej,
d) zasięgu widzialności mniejszego niż 10 m na wysokości mniejszej lub równej 1,8 m od poziomu drogi ewakuacyjnej,
e) zawartości tlenu poniżej 15%.

Stan krytyczny środowiska to nic innego, jak ogólnie znane, choć lekko zmodyfikowane na potrzeby metra „warunki bezpiecznej ewakuacji", które opisują m.in. Komenda Główna PSP [6] oraz SITP [7].
Do ewakuacji z podziemnych stacji metra dopuszcza się możliwość wykorzystania schodów ruchomych, jeżeli ich ruch jest zgodny z kierunkiem ewakuacji lub (w przypadku alarmu) następuje ich zatrzymanie, a ich maszynownia jest zabezpieczona stałym samoczynnym urządzeniem gaśniczym. Wtedy schody ruchome można uwzględnić przy obliczaniu szerokości dróg ewakuacyjnych.
Długość drogi ewakuacyjnej (z najdalszego miejsca, w którym może przebywać pasażer na peronie, do wyjścia w miejsce bezpieczne) nie powinna przekraczać 100 m. Miejscem bezpiecznym może być zabezpieczone przed zadymieniem wyjście ewakuacyjne, które prowadzi na drogę publiczną, inne miejsce poza terenem stacji metra lub na terenie obiektu budowlanego metra, w którym przez projektowy czas trwania pożaru nie powstanie stan krytyczny środowiska oraz toksyczność zagrażająca zdrowiu i życiu ludzi, zapewniające możliwość wyjścia z niego na poziom terenu.
Łączna szerokość w świetle wyjść ewakuacyjnych ze strefy biletowej nie powinna być mniejsza od łącznej szerokości w świetle schodów prowadzących do tych wyjść. Bramki i kołowroty kontroli biletowej powinny być zaprojektowane w taki sposób, aby zaprzestanie ich działania umożliwiało nieprzerwaną ewakuację pasażerów przejściem o szerokości w świetle bramki nie mniejszej niż 0,6 m. Obok bramek lub kołowrotów kontroli biletowej muszą znajdować się wyjścia o łącznej szerokości nie mniejszej niż 3,6 m, otwierane zgodnie z kierunkiem ewakuacji, wyposażone w urządzenia antypaniczne. Do szerokości wyjść ewakuacyjnych ze strefy biletowej zalicza się szerokości w świetle bramek i kołowrotów kontroli biletowej oraz szerokość zlokalizowanych przy nich wyjść ewakuacyjnych.

Wentylacja pożarowa w metrze

Dym – podstawowy nośnik ciepła w środowisku pożarowym – stanowi duże zagro-

żenie dla użytkowników z dwóch powodów: możliwości wdychania toksycznych związków chemicznych oraz ze względu na zaciemnienie przestrzeni objętej pożarem. Ograniczenie widoczności powoduje nieprzenikanie światła oraz łzawienie i pieczenie wywołane drażniącymi jego składnikami. W jej następstwie zwiększa się prawdopodobieństwo utraty orientacji w zadymionych pomieszczeniach. Znacznie utrudnia to ewakuację, dlatego obiekty metra wyposaża się w systemy wentylacji pożarowej, których celem jest usuwanie dymu oraz zapewnienie kontroli nad jego rozprzestrzenianiem.

Tunele, stacje metra oraz budowle metra spełniające funkcję użytkową budynków powinny być wyposażone w instalację wentylacji pożarowej zapewniającą skuteczne usuwanie dymu w sposób zapobiegający zadymieniu stacji, wyjść ewakuacyjnych i pomieszczeń, w których znajdują się urządzenia bezpieczeństwa. Tunele o długości powyżej 300 m powinny być wyposażone w mechaniczną instalację wentylacji pożarowej. [3] W załączniku do rozporządzenia zawarto wymagania dotyczące prędkości przepływu powietrza oraz klasy zastosowanych wentylatorów.

Urządzenia ppoż. i gaśnice

W rozporządzeniu w sprawie ochrony ppoż. budynków, innych obiektów budowlanych i terenów [4] znajdują się zapisy, zgodnie z którymi stacje metra i stacje kolei podziemnych wyposaża się w:

- system sygnalizacji pożarowej,
- dźwiękowy system ostrzegawczy,
- gaśnice co najmniej 2 kg (3 dm^3) na każde 100 m^2 strefy pożarowej (wynika to z klasyfikacji stacji metra jako strefy pożarowej ZL I),
- instalację hydrantową.

Ponadto zgodnie z rozporządzaniem [3] poniższe obszary powinny być wyposażone w stałe samoczynne urządzenia gaśnicze:

- podstacje trakcyjno-elektroenergetyczne,
- pomieszczenia, w których znajdują się urządzenia decydujące o bezpieczeństwie ruchu lub bezpieczeństwie pożarowym,
- pomieszczenia przeznaczone do prowadzenia usług, handlu i gastronomii usytuowane na podziemnej stacji metra, niewydzielone pożarowo z przestrzeni stacji przegrodami o klasie odporności ogniowej EI120/REI120 (odpowiednio – przegrody nienośne i nośne), jeżeli ich łączna powierzchnia na stacji przekracza 500 m^2 i na stacji występuje co najmniej jeden zespół takich pomieszczeń o łącznej powierzchni przekraczającej 200 m^2.

Procedury i szkolenia

Bezpieczeństwo pożarowe w metrze to nie tylko wyposażenie. Nieodłączne są szkolenia personelu, służby ratowniczej metra, procedury postępowania w różnych przypadkach, ćwiczenia, a także edukacja użytkowników. Metro posiada opracowaną instrukcję bezpieczeństwa pożarowego, w której podano zasady postępowania na wypadek pożaru bądź innego zagrożenia. Warto wspomnieć o akcjach informacyjnych w formie ulotek i plakatów skierowanych do pasażerów. Opisano w nich w prosty sposób, wraz z obrazkami, sposoby reagowania oraz zasady postępowania w nietypowych sytuacjach – przypadki pożaru na stacji i w tunelu, awarii pociągu, nieprawidłowego działania urządzeń i infrastruktury metra, zagrożenia terrorystycznego, napływu wody, zasłabnięcia pasażera, upadku pasażera czy przedmiotu na torowisko, wpadnięcia w przestrzeń pomiędzy peronem a pociągiem.

Podsumowanie

Bezpieczeństwo w każdym wymiarze, również pożarowym, jest składową doświadczeń przeszłości oraz dynamiki rozwoju zagrożeń i możliwości ich przewidywania, a także zapobiegania im. Tragiczne doświadczenia z dużą liczbą ofiar zmuszają do odpowiedzi na pytania, dlaczego tak się stało, co zawiodło, czy można było temu zapobiec, jakie działania należy podjąć, aby nie dopuścić do podobnych sytuacji w przyszłości. Dla bezpieczeństwa pożarowego obiektów metra takim doświadczeniem był pożar na King's Cross. Za wiedzę oraz bezpieczeństwo, które mamy dziś, trzydzieści lat temu zapłacono najdroższą cenę.

Literatura

[1] *Investigation into the King's Cross Underground Fire*, Desmond Fennell, Department of Transport, 1988 r.
[2] Materiały wykładowe z przedmiotu Teoria Pożarów, Wykład VI – Efekty nieliniowe pożaru – rozgorzenie (*flashover*) i ciąg wsteczny płomieni (*backdraft*), prof. nadzw. dr hab. Marek Konecki, Szkoła Główna Służby Pożarniczej, 2014 r.
[3] Rozporządzenie Ministra Infrastruktury z dnia 17 czerwca 2011 r. w sprawie warunków technicznych, jakim powinny odpowiadać obiekty budowlane metra i ich usytuowanie (Dz.U. 2011 nr 144, poz. 859).
[4] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. 2010 nr 109, poz. 719).
[5] Rozporządzenie Ministra Infrastruktury w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz.U. 2015 poz. 1422).
[6] Procedury organizacyjno-techniczne w sprawie spełnienia wymagań w zakresie bezpieczeństwa pożarowego w inny sposób niż to określono w przepisach techniczno-budowlanych, w przypadkach wskazanych w tych przepisach, oraz stosowania rozwiązań zamiennych, zapewniających niepogorszenie warunków ochrony przeciwpożarowej, w przypadkach wskazanych w przepisach przeciwpożarowych, KGPSP, 2009 r.
[7] „Podręcznik projektanta systemów sygnalizacji pożarowej", Izba Rzeczoznawców SITP oraz Instytut Techniki Budowlanej, edycja czerwiec 2010.

BIO

Iza Trzeciak
Absolwentka Wydziału Inżynierii Bezpieczeństwa Pożarowego w Szkole Głównej Służby Pożarniczej. Założycielka bloga o ochronie przeciwpożarowej blog-ppoz.pl, na którym publikuje ciekawostki i problemy, z którymi spotyka się w codziennej pracy inżyniera bezpieczeństwa pożarowego.

Ochrona ppoż. w warszawskim metrze

Każdego dnia z komunikacji podziemnej korzysta ponad 0,5 mln pasażerów. Specyfika tego środka transportu wymusza stosowanie rygorystycznych zabezpieczeń pożarowych.

Metro Warszawskie

Dla Metra Warszawskiego opracowano warunki techniczne ochrony przeciwpożarowej zgodne z obowiązującymi przepisami określonymi w Rozporządzeniu Ministra Infrastruktury z 17 czerwca 2011 r. w sprawie warunków technicznych, jakim powinny odpowiadać obiekty budowlane metra i ich usytuowanie (Dz.U. 2011 nr 144 poz. 859). Stanowiły one wytyczne dla projektowych rozwiązań techniczno-funkcjonalnych. W aspekcie bezpieczeństwa pożarowego uwzględniono w nich m.in.:

- ograniczenie możliwości powstania i rozprzestrzeniania się ognia i zadymienia,
- stworzenie optymalnych warunków ewakuacji pasażerów,
- zapewnienie odpowiedniej liczby, rozmieszczenia i dostępności środków gaśniczych i ratowniczych,
- instalację sygnalizacji pożarowej i łączności usprawniających podejmowanie decyzji i prowadzenie działań ratowniczo-gaśniczych.

Metro zostało wyposażone w instalacje i urządzenia przeznaczone wyłącznie do celu ochrony ppoż. – system sygnalizacji pożarowej, sieć hydrantów, znaki informacyjne i bezpieczeństwa. Do celów ochrony ppoż. dostosowano także konstrukcję, elementy wystroju i układ funkcjonalny stacji oraz systemy zaopatrzenia w wodę, energię elektryczną, łączność i wentylację.

Wszystkie elementy budowlane i materiały wykończeniowe, izolacje termiczne, dźwiękochłonne oraz kable są niepalne lub nierozprzestrzeniające ognia, nie wydzielają też substancji toksycznych ani dymów gryzących wydzielających się pod wpływem wysokiej temperatury.

Równie ważnymi kwestiami są:

- wentylacja – zastosowano wentylatory rewersyjne odpro-

Liczba ROP-ów na stacjach
I linii:
580 szt.
II linii:
345 szt.
Ponadto cały tunel II linii zostanie wyposażony w liniowe czujki ciepła.

Liczba czujek na stacjach metra

I linii (21 stacji):
4436 szt.
II linii (7 stacji):
3668 szt.

wadzające dym i doprowadzające świeże powietrze do miejsc, w których znajdują się ludzie;
- sieć wodociągowa – wyposażona w hydranty ppoż. dostarcza wodę na potrzeby gaśnicze;
- oświetlenie awaryjne – zapewnione przez cały okres ewakuacji i akcji ratowniczej;
- nagłośnienie – selektywnie wykorzystywane do kierowania akcją gaśniczą.

Na każdej stacji II linii metra znajdują się ponadto specjalnej konstrukcji szyby windowe i windy (przedsionek ze szczelnymi drzwiami), które umożliwiają ekipom ratunkowym szybkie i bezpieczne dotarcie na miejsce zdarzenia.

Na wszystkich stacjach metra zastosowano system sygnalizacji pożarowej, zapewniający wczesne wykrycie pożaru oraz jego lokalizację. Do zabezpieczenia zarówno tuneli, jak i części stacji centralnego odcinka II linii metra wykorzystano liniowe czujki ciepła oraz stałe urządzenia gaśnicze wodne, przeznaczone do zwalczania pożarów w pierwszej fazie ich powstania i zapobiegające ich rozprzestrzenianiu się. Zastosowano je do zabezpieczenia trzech stacji metra, które – ze względu na budowę – są obiektami wielokondygnacyjnymi, zakwalifikowanymi do kategorii zagrożenia ludzi ZL I.

Na każdej stacji znajdują się ponadto stałe urządzenia gaśnicze gazowe, które umożliwiają automatyczne wykrycie i sygnalizację pożaru oraz rozpoczęcie akcji gaśniczej w chronionych przestrzeniach. Zgodnie z przepisami zainstalowano oddzielenie ppoż., tj. bramy i drzwi przeciwpożarowe oraz kurtyny dymowe stałe i automatyczne, które pozwalają kontrolować rozprzestrzenianie się dymu i ciepła. Dzięki temu jest możliwe wydzielenie stref gromadzenia się dymu oraz stref wolnych od zadymienia, co umożliwia przeprowadzenie bezpiecznej ewakuacji.

Systemy oraz urządzenia ochrony przeciwpożarowej są monitorowane i sterowane zarówno w miejsca ich usytuowania, czyli konkretnej stacji, jak i zdalnie z Centralnej Dyspozytorni zlokalizowanej na Stacji Techniczno-Postojowej Kabaty.

Na wszystkich stacjach regularnie przeprowadza się przeglądy oraz sprawdza działanie urządzeń i systemów służących do ochrony ppoż. Ponadto są prowadzone praktyczne ćwiczenia z oddymiana stacji i tuneli, w których uczestniczą służby metra, w tym Zakładowa Służba Ratownicza oraz Państwowa Straż Pożarna.

W sytuacjach zagrożenia w metrze obowiązują scenariusze pożarowe oraz procedury postępowania ujęte w Zakładowym Planie Ratowniczym, a pracownicy mają jasno określone wytyczne postępowania podczas konkretnego rodzaju zagrożenia.

Jedynym polskim miastem dysponującym siecią metra jest Warszawa. System składa się z dwóch linii: M1 – o długości 23,1 km (ponad 500 tys. pasażerów dziennie), oddawanej etapami w latach 1995-2008, oraz M2 (ponad 140 tys. pasażerów dziennie), której budowa trwa od 2010 r. Centralny odcinek II linii metra (o długości 6,1 km) uruchomiono w 2015 r. Obecnie trwa budowa kolejnych dwóch odcinków (każdy o długości ponad 3 km), które będą gotowe w 2019 r.

Schrack Seconet Polska
ul. Domaniewska 44a
02-672 Warszawa
http://schrack-seconet.pl

Platforma B5A/B6A systemu Integral IP

KOLEJNY ETAP EWOLUCJI

System sygnalizacji pożarowej Integral od momentu wprowadzenia na rynek jest stale rozwijany i rozbudowywany o nowe funkcje i możliwości. **Przyjęta przez Schrack Seconet koncepcja ewolucyjnego budowania spójnego i niezawodnego systemu bezpieczeństwa pożarowego doskonale się sprawdza i jest znakiem rozpoznawczym firmy, której działalność wyznacza najlepsze standardy w branży.**

Krzysztof Kunecki
dyrektor ds. technicznych,
Schrack Seconet Polska

Kolejnym etapom ewolucji technologicznej w roku 2018 będą podlegać zarówno komponenty sprzętowe (*hardware*), jak i oprogramowanie (*software*). Stały rozwój systemu dotyczy przede wszystkim zwiększania jego wydajności i niezawodności działania, a także realizacji coraz bardziej zaawansowanych i wymagających funkcji logicznych, które spoczywają na systemie bezpieczeństwa pożarowego. Gdy inni producenci w branży upraszczają swoje centrale, oddając pole zewnętrznym systemom sterowania i nadzoru, nowe komponenty Integrala są opracowywane z uwzględnieniem aktualnych potrzeb projektantów, instalatorów oraz użytkowników drapaczy chmur, potężnych i rozproszonych zakładów produkcyjnych czy zaawansowanych architektonicznie centrów handlowych.

Przy wprowadzaniu kolejnych generacji urządzeń bardzo ważne jest zapewnienie kompatybilności wstecznej, a więc możliwości pełnej współpracy nowych elementów z urządzeniami poprzednich generacji, co ma szczególne znaczenie przy rozbudowie i wieloletniej modernizacji istniejących instalacji sygnalizacji pożarowej. Ta filozofia niezmiennie przyświeca Schrack Seconet od momentu wprowadzenia na rynek pierwszego systemu sygnalizacji pożarowej. Proces wdrażania nowych rozwiązań został szczegółowo zaplanowany i skoordynowany: pierwszy etap zakłada zapewnienie nowym komponentom pełnej zgodności z istniejącymi produktami i wprowadzenie nowoczesnych technologii w zakresie *hardware'u;* kolejne etapy to z kolei rozwój oprogramowania i optymalizacja nowoczesnych funkcji, niezbędnych na danym etapie rozwoju. Nowe komponenty sprzętowe mają umożliwiać rozwój funkcjonalności systemowych przez wiele następnych lat. System jest budowany niejako „na wyrost", wyprzedzając technologicznie potrzeby bieżące, stąd jego dostosowanie do nowoczesnych wymagań stanowi w kolejnych latach cyklu życia produktu sumę skoordynowanych prac programistów i wymagań użytkowników. Jednym z kluczowych etapów rozwoju systemu sygnalizacji pożarowej, sterowania i zarządzania urządzeniami bezpieczeństwa pożarowego było wprowadzenie już w 2010 r.

bazy technologicznej w wersji Integral IP. Nazwa systemu z jednej strony podkreślała rolę komunikacji za pomocą m.in. protokołu TCP/IP w systemie bezpieczeństwa pożarowego, z drugiej zaś wyznaczała jego kierunek rozwoju na kolejne lata. Technologia IP umożliwiła wdrożenie nowej generacji sieci central Integral LAN pozwalającej na zastosowanie m.in. sieci kratowych (*mesh network*), stanowiła też bazę rozwijanej w kolejnych latach technologii Integral over IP, która służy do komunikacji z systemami zewnętrznymi w celu wizualizacji, integracji, zarządzania i zdalnego dostępu do central serii IP.
Wprowadzenie zaawansowanych możliwości logicznych i komunikacyjnych wersji Integral IP oraz wyposażenie jej w wysoko wydajną i elastyczną platformę obliczeniową pozwoliły na zbudowanie systemu zintegrowanego zarządzania bezpieczeństwem pożarowym (SIUP) SIS-FIRE, w którym to systemie Integral IP, wraz z modułami techniki pętlowej X-LINE, odgrywają w tym systemie kluczową rolę.
W ramach najnowszego w rozwoju systemu Integral IP, na przełomie lat 2017 i 2018, dotychczas oferowana platforma sprzętowa B5 została zastąpiona unowocześnioną platformą B5A (*A-Advanced*) dla modułowych central sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi Integral IP MX oraz analogicznie – platforma sprzętowa B6A zastąpiła wersję B6 dla central w wersji kompaktowej Integral IP CX.
Nowa platforma sprzętowa dla centrali Integral IP MX to przede wszystkim nowe główne komponenty systemu, do których należy unowocześniona karta głównego procesora B5-MCUA, zasilacz B8-PSU i magistrala systemowa B8-BUS. Odpowiednio dla centrali Integral IP CX podstawowymi składnikami platformy B6A są płyta główna B6-BCU-X2A oraz zasilacz B9-PSU. Podzespoły te w obu centralach stanowią „kręgosłup" systemu i decydują o jego wydajności oraz możliwościach związanych z zastosowaniem nowych kart rozszerzeń i powiązanych z nimi funkcji systemowych.
Wprowadzenie nowych elementów sprzętowych jest kolejną ewolucją w zakresie zwiększania odporności i niezawodności działania systemu na wypadek ewentualnej awarii systemu.
Tak jak dotychczas, Integral IP znacznie przewyższa swoimi funkcjami wymagania normy PN-EN 54-2.
Spośród licznych udoskonaleń wprowadzonych do systemu można wyróżnić następujące:

- karta głównego procesora central MX/CX została rozszerzona o port Ethernet, pozwalając na podłączenie rozwiązań techniki Intergral over IP bez potrzeby wyposażania centrali w dodatkową kartę sieciową. Funkcja ta umożliwia np. łatwiejsze podłączenie systemu zarządzania SIS-FIRE czy aplikacji do zdalnego dostępu, takich jak Integral Mobile, Integral MESSAGE. Ma też szczególne znaczenie dla nadzorowania central sterujących urządzeniami gaszenia Integral IP CXE, co stanowi nową, bardzo korzystną opcję dla użytkowników systemów sieciowych;
- nowa karta sterująca B8-BAF posiada dodatkowe trzy wyjścia przekaźnikowe i jedno wejście nadzorowane w porównaniu do poprzedniej wersji B5-BAF, co pozwala na optymalizację komponentów sprzętowych w ramach sterowania i nadzorowania urządzeń przeciwpożarowych;
- w zasilaczu B8-PSU, oprócz kolejnej optymalizacji funkcji redundancji systemowej, zastosowano nowe zabezpieczenia wyjść zasilających za pomocą kasowalnych bezpieczników elektronicznych, co pozwala na szybkie przywrócenie normalnego stanu pracy wyjścia w przypadku wystąpienia zwarcia w linii zasilającej bez potrzeby wymiany bezpieczników;
- system Integral IP został przygotowany pod względem sprzętowym do kolejnego etapu rozwoju w zakresie sieci central. W połowie 2018 r. zostanie wprowadzona nowa wersja oprogramowania, a wraz z nią sieć central nowej generacji Integral WAN (w miejsce dotychczasowej sieci SecoNET) do połączenia w system rozproszonych (niezależnych) instalacji sygnalizacji pożarowej z wykorzystaniem szybkich torów komunikacyjnych (do 2,5 Mb/s) bazujących na technologii IP. Aby umożliwić ten krok od strony sprzętowej, już teraz do centrali Integral IP MX wprowadzono nowe karty sieciowe typu B8-NET2-485 i B8-NET4-485 do połączenia central z wykorzystaniem przewodów miedzianych (skrętka) oraz nowe karty sieciowe z interfejsami światłowodowymi typu B8-NET2-FX4 i B8-NET-FX8 dla połączeń światłowodowych jedno- i wielomodowych. Konstrukcja interfejsów nowych kart światłowodowych w postaci gniazd współpracujących z modemami światłowodowymi typu SFP pozwala na wykonywanie w ramach jednej sieci (pierścień/sieć kratowa) połączeń mieszanych z wykorzystaniem torów światłowodowych jedno- i wielomodowych, a dodatkowo dla karty B8-NET2-FX4 także połączeń z wykorzystaniem kabli miedzianych. Podobnie unowocześniono centralę Integral IP CX, w której wprowadzono kartę światłowodową B9-NET-FX4.

Integral IP, oprócz funkcji detekcji i sygnalizacji pożaru, jest także systemem sterowania urządzeniami przeciwpożarowymi. Dzięki elastycznemu oprogramowaniu oraz redundancji komponentów sprzętowych pozwala na sterowanie praktycznie nieograniczoną liczbą urządzeń ppoż. w ramach układów sieciowych.
Zgodnie z nowymi dokumentami atestacyjnymi wydanymi przez VdS (Certyfikat Stałości Właściwości Użytkowych – CPR) oraz CNBOP (Świadectwo Dopuszczenia CNBOP) system Integral IP nie ma ograniczeń w odniesieniu do liczby sterowanych stref gaszenia dla central Integral IP MX/CX w ramach sieci Integral LAN. Stale rozbudowywane elastyczne oprogramowanie pozwala na realizację dowolnych algorytmów sterowania zarówno w przypadku systemów gaszenia, jak i innych sterowanych urządzeń ppoż., umożliwiając optymalne wykorzystanie systemu w obiekcie.
Nowa generacja urządzeń systemu Integral IP bazująca na platformie B5A i B6A to kolejny krok w ewolucji systemu bezpieczeństwa pożarowego, a wprowadzone unowocześnienia po raz kolejny zwiększają możliwości w zakresie detekcji pożaru, sterowania oraz zarządzania urządzeniami ppoż. Kolejne ważne kroki w rozwoju systemu są zapowiadane na lata 2019–2020.

Więcej nt. zintegrowanego systemu zarządzania SIS-FIRE w kolejnych wydaniach „a&s Polska".

DEKK FIRE SOLUTIONS
ul. Zielona 52, 05-500 Piaseczno
tel.: 22 244 22 00, faks: 22 24422 01
e-mail: info@dekk.pl

Jeśli masz wybór wybierz INERGEN®!

ZALETY SYSTEMU INERGEN – FIRE EATER®

- szybko i definitywnie gasi pożary;
- daje efekt gaszenia trójwymiarowego, co oznacza, że nawet „ukryte" pożary są szybko i skutecznie gaszone;
- brak zamglenia i szkodliwych produktów rozkładu;
- bezpieczny dla środowiska, ludzi i sprzętu;
- najefektywniejszy z gazów obojętnych;
- sprawdzony w działaniu podczas wielokrotnych testów i pożarów.

Pożary mogą powodować ogromne straty finansowe i materialne, a co gorsza, zagrażają zdrowiu i życiu ludzi. Szczególnymi obiektami są archiwa, magazyny, serwerownie i wiele innych, które muszą być chronione przed pożarem przez odpowiedni, bezpieczny system gaśniczy. Taką ochronę zapewni INERGEN®.

Ochrona przed przegrzaniem

Podstawową przyczyną pożarów w serwerowniach są przegrzane serwery. Po uwolnieniu INERGEN® nieznacznie obniża temperaturę w pomieszczeniu i redukuje poziom tlenu, zapobiegając przegrzaniu i ponownemu zapaleniu się ognia.

Dlaczego INERGEN®?

Podstawową zaletą jest duża skuteczność systemu przy równoczesnej elastyczności w projektowaniu instalacji. INERGEN® jest bezpieczny dla ludzi przy projektowanych stężeniach, bezpieczny dla środowiska, w przeciwieństwie do środków chemicznych. Niepowodowanie mikrokorozji czy szkodliwych substancji w połączeniu z dymem lub płomieniem są cechami, które istotnie wpływają na bezpieczeństwo chronionych materiałów i urządzeń.
INERGEN® należy do najnowocześniejszych systemów gaśniczych. Jest bezpieczny dla sprzętu, środowiska i ludzi, dlatego należy do najczęściej stosowanych skutecznych środków gaszących pożary w pomieszczeniach serwerowni. Gaśnicze działanie polega na redukowaniu tlenu w pomieszczeniu z 21% objętości do 14% i poniżej – pożar jest gaszony, a ludzie mogą oddychać. Zawiera poszczególne komponenty środowiska naturalnego, takie jak gaz szlachetny argon, azot oraz minimalną ilość dwutlenku węgla. Wysokość stężenia tego ostatniego składnika w procesie gaszenia umożliwia głębsze oddychanie, zapewniając organizmowi tlen.
INERGEN – Fire Eater nie powoduje zamglenia w pomieszczeniu w trakcie wyzwalania, nie pozostawia pozostałości po gaszeniu (aerozole). Dopuszczony w normie NFPA 2001 dłuższy czas wyzwolenia INERGEN-u nawet do 120 s świadczy o jego elastyczności i zarazem możliwości płynnego, spokojniejszego wypływu. Przy takiej swobodzie projektowania instalacji, połączonej z użyciem tłumików fali akustycznej system zapewnia najbezpieczniejszy proces wypływu, czego nie mają systemy bez takich możliwości. Możliwość zastosowania systemu wielostrefowego znacząco obniża koszty instalacji podczas zabezpieczania większej liczby pomieszczeń.
System ma bardzo prostą budowę, jest niezawodny, a ryzyko popełnienia błędów podczas montażu minimalne. Prosty montaż lub demontaż, możliwość szybkiej wymiany, łatwy pomiar ciśnienia sprawiają, że jest to rozwiązanie stosunkowo tanie i nieskomplikowane, a cena środka gaśniczego relatywnie niska. INERGEN był testowany w odniesieniu do ludzi. Dokumentacja techniczna potwierdza jego bezpieczeństwo dla człowieka.

Jak działa system?

Szybkość skutecznej akcji gaszenia jest ściśle związana z właściwym doborem systemu detekcji pożaru i przygotowaniem pomieszczenia do gaszenia. Gdy automatyczne detektory wykryją rozprzestrzeniający się pożar, centrala sterująca włącza sygnalizatory akustyczne i wizualne sygnały ostrzegawcze. Po upływie krótkiego czasu zwłoki na przygotowanie do wyzwolenia sygnał z centrali uruchamia zawór elektromagnetyczny, wyzwalając zestaw gaśniczy do chronionego pomieszczenia. Każdorazowo układ hydrauliczny z rurociągami i dyszami jest kalkulowany za pomocą profesjonalnych programów obliczeniowych, których poprawność została sprawdzona podczas wielu testów wyzwalania i pomiarów stężeń.

System gaśniczy INERGEN ma wiele zalet, m.in. zapewnia bezpieczeństwo ludzi i obszarów chronionych, ma prostą budowę zwiększającą sprawność układu. To coraz bardziej popularny i coraz częściej stosowany środek gaśniczy. Jest skuteczny i nie powoduje skutków ubocznych. Producent systemu Fire Eater przeprowadza testy rzeczywistego wyzwalania gazu potwierdzające jego cechy i właściwości.

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

PROJEKTUJEMY
zgodnie ze sztuką

SYSTEMY SYGNALIZACJI POŻAROWEJ

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

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

SYSTEM DETEKCJI GAZÓW SDG 6000

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.
85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.pl

Linc Polska
ul. Hallera 6/8, 60-104 Poznań
tel.: 61 839 19 00
info@linc.pl www.linc.pl

Termowizja FLIR

szybkie wykrywanie zagrożeń pożarowych

Kiedy mówimy o bezpieczeństwie, mamy na myśli subiektywnie odczuwany komfort i akceptowalny poziom ryzyka wystąpienia zagrożenia. **Oczywiście czym innym jest bezpieczeństwo osobiste człowieka, a czym innym bezpieczeństwo obiektów. Niemniej w obu przypadkach spokój może zostać zachwiany przez pożar.**

Zagrożenie stanowią np. składowiska odpadów komunalnych, węgla lub substancji chemicznych – zachodzące w hałdach procesy fizyczne i chemiczne często prowadzą do wzrostu temperatury do poziomu grożącego samozapłonem. Równie niebezpieczne sytuacje mogą nastąpić np. w wyniku błędu projektowego lub zaniedbania eksploatacyjnego w obiektach przemysłowych. Przykładowo, brak odpowiedniego chłodzenia instalacji energetycznych doprowadził do wielu pożarów, których efektem było m.in. skażenie środowiska naturalnego.

Jak ustrzec się przed potencjalnym pożarem? Najprostszym rozwiązaniem jest pomiar temperatury i alarmowanie o jej wzroście. Tak proste techniki wydają się oczywiste w przypadku stałych konstrukcji. A co zrobić, gdy następują dynamiczne zmiany w środowisku? Pożary na składowiskach odpadów czy w pojemnikach na śmieci są częstym i znanym problemem dla specjalistów zajmujących się gospodarką odpadami. Ukryte źródło ciepła, wynikające z rozkładu biologicznego lub utleniania chemicznego, powoduje wzrost temperatury. Jeżeli masa odpadowa nie może rozproszyć ciepła szybciej, niż jest ono wytwarzane, może wystąpić samozapłon.

Przykładem wzorcowego rozwiązania problemu jest niemiecka sortownia i spalarnia śmieci w Ludwigslust. W 2014 r. doszło tam do pożaru, który rozproszył się tak szybko, że nie można go było opanować. Kataklizm spowodował szkody o wartości około 95 tys. euro. Zastosowanie kamer dozorowych oraz czujek dymu w systemie wykrywania płomienia okazało się – ze względu na długi czas wykrywania – bezskuteczne. Postanowiono więc przetestować technikę termowizyjną. Zainstalowano dwie kamery z serii FC-R marki FLIR w celu monitorowania całego pola składowania odpadów o wymiarach 25 x 25 m. Te stałopozycyjne kamery radiometryczne oprócz obserwacji terenu umożliwiają dokładny, bezdotykowy pomiar temperatury. To sprawia, że są idealnym rozwiązaniem do wczesnego wykrywania gorących miejsc i pożarów.

Obie kamery mierzyły na bieżąco rzeczywistą temperaturę stosów odpadów. Ilekroć dochodziło do osiągnięcia krytycznego progu temperatury (w tym przypadku 65°C), odpowiednio skalibrowana i skonfigurowana kamera wysyłała alarm kierowany bezpośrednio do pomieszczenia kontrolnego, gdzie operatorzy mogli decydować o zastosowaniu dalszych środków zaradczych. Dzięki wdrożeniu na stałe systemu monitoringu, opartego na radiometrycznych kamerach termowizyjnych, w sortowni odpadów udało się ograniczyć do minimum ryzyko wystąpienia pożaru.

Należy podkreślić bardzo istotny fakt, że kamery z serii FC-R marki FLIR są nie tylko narzędziem radiometrycznym, ale także mogą być elementem systemu monitoringu wizyjnego. Łączą one bowiem dwie funkcje: pomiar i obserwację. Niechłodzony mikrobolometryczny przetwornik obrazu o wysokiej czułości termicznej (<50 mK), dostępny w dwóch rozdzielczościach, 4-krotny zoom elektroniczny oraz szeroki wybór obiektywów to tylko niektóre cechy tej serii kamer. Ponadto przetwornik FLIR jest objęty 10-letnią rękojmią, co świadczy o jego wysokiej jakości. Kamery z serii FC-R mają wyjście analogowe i IP oraz obsługują standard ONVIF, dzięki czemu łatwo je zintegrować z rozwiązaniami firm trzecich.

Ponadto są wytrzymałe i odporne na warunki atmosferyczne, mogą pracować na zewnątrz obiektów. Możliwości ich zastosowań są praktycznie nieograniczone.

CZASOPISMO RYNKU SECURITY

a&S POLSKA

PRENUMERATA 2018

zamów online:

www.aspolska.pl/prenumerata

Drony w przestworzach

Wraz z szybkim rozwojem i wprowadzaniem takich technologii, jak sztuczna inteligencja (*artificial intelligence,* AI) czy głębokie uczenie się (*deep learning*) **bezzałogowe statki powietrzne zdobywają coraz większą popularność w branży zabezpieczeń.**

Prasanth Aby Thomas
a&s International

Amerykańska Federalna Administracja Lotnictwa już zaproponowała rygorystyczny zakres dobrych praktyk dotyczący dronów stosowanych komercyjnie, chociaż wiele krajów musi dopiero zaakceptować szybki wzrost ich popularności. Nie powstrzymuje to jednak przemysłu dronowego przed rozwojem oraz nadążaniem za innowacjami. Firmy inwestują w ten sektor, eksperymentując ze sprzętem i oprogramowaniem, a także z ich możliwościami. Brak przepisów nie powstrzymuje również użytkowników przed szerszym wykorzystaniem tych latających maszyn. Drony są coraz chętniej stosowane przez różne branże – pozwalają rozwiązać niektóre problemy, dotychczas żmudne, kosztowne albo wręcz niemożliwe, począwszy od ochrony, skończywszy na rolnictwie, produkcji i sprzedaży. Według raportu firmy badawczej Markets and Markets wartość globalnego rynku dronów ma wzrosnąć do 21 mld dol. w roku 2022 – przy wskaźniku wzrostu CAGR ok. 16% w latach 2016–2022.

ROŚNIE ZNACZENIE SZTUCZNEJ INTELIGENCJI W DRONACH

Postęp w dziedzinie sztucznej inteligencji sprawia, że drony latają bezpieczniej i są wydajniejsze. Wraz z rozwojem technologii i postępującą redukcją kosztów autonomiczne drony stają się coraz bardziej popularne. Mogą wykonywać powierzone zadanie bez udziału nawigatora, są więc rozwiązaniem atrakcyjnym dla klientów oczekujących automatyzacji procesów oszczędzającej koszty pracy i inne koszty operacyjne.

Zwiększająca się liczba dronów wywołuje też obawy, czy podczas pracy nie będą się ze sobą zderzać. Obawy te były jednym z głównych czynników spowalniających rozwój i adaptację autonomicznych dronów.

Z problemem próbują zmierzyć się innowacyjne firmy, które oferują rozwiązania umożliwiające tym urządzeniom nawigowanie w przestworzach. Należy do nich firma Iris Automation z San Francisco. Firma wprowadziła rozwiązanie, które pozwala dronom widzieć otoczenie.

Skonstruowaliśmy system unikania kolizji „wyczuj i unikaj", dzięki któremu drony przemysłowe widzą świat tak, jak pilot – mówi A. Harmsen. – *Nasz system obejmuje odwzorowanie 3D i dynamiczne śledzenie ruchomych obiektów z dużych odległości, co zapewnia dronowi bezpieczny lot w krajowej przestrzeni powietrznej, potencjalnie poza polem widzenia.*

Rozwiązanie oparto na widzeniu komputerowym. Wykorzystano w nim najnowsze przełomowe osiągnięcia wbudowanych systemów obliczeniowych i kamer.

Firma opracowała autorskie algorytmy, które umożliwiają systemowi pracę na zewnętrz, w środowisku niezabudowanym. Algorytmy te pracują na pokładzie drona w czasie rzeczywistym. A. Harmsen twierdzi, że wbudowanie tej funkcjonalności w moduł o masie 300 g oraz sprzedaż w rozsądnej cenie zmienią funkcjonowanie w całej branży.

Rdzeniem rozwiązania Iris Automation jest oprogramowanie sterowane przez zintegrowany procesor graficzny (GPU). Oprogramowanie potrafi rozpoznać, podzielić na segmenty i sklasyfikować obiekty w otoczeniu. Możliwe jest także całkowite i z zachowaniem pełnej geometrii odwzorowanie środowiska w postaci wewnętrznego modelu świata.

Zdolność projekcji w czasie pozwala systemowi na ocenę, czy możliwa jest kolizja z jakimkolwiek obiektem – dodaje A. Harmsen. – *W efekcie system może podjąć działanie unikowe. Oczywiście, wiele z tego nie byłoby możliwe bez zastosowania deep learning i sztucznej inteligencji.*

Sztuczna inteligencja w widoczny sposób zrewolucjonizowała branżę dronów. Wcześniej podążały one za znacznikami GPS lub wykonywały polecenia pilota, zdalnie manipulującego drążkiem sterowniczym. Oparte na sztucznej inteligencji rozwiązanie Iris Automation pozwala dronom widzieć świat w taki sposób, w jaki widzi go pilot, mogą więc podejmować decyzje w czasie rzeczywistym. Dzięki temu można uchronić maszynę przed ewentualną kolizją.

Klasyfikacja pracy dronów w bezpieczeństwie

Dążenie do najwyższej wydajności branża security zawsze opierała na technologii, zwłaszcza zaawansowanej elektronice, czujnikach oraz wideo. Kilka firm prezentowało w ostatnich latach innowacyjne podejście do bezpieczeństwa, jednak branża ta w dużej mierze wymaga bezpośredniego zaangażowania człowieka. Pojawienie się dronów ma to przynajmniej częściowo zmienić. Dzięki szybkości, zdolności manewrowania, rozmiarom i wbudowanym technologiom doskonale zastępują obsługę naziemną w monitorowaniu rozległych terenów. W krótkim czasie kontrolują duże obszary i docierają do miejsc trudno dostępnych dla ludzi. Nie potrzebują wieloosobowej obsługi, minimalizując konieczność angażowania znacznych sił do monitorowania obiektu. Według raportu PwC wartość rynku zastosowań dronów w branży security sięga 10,5 mld dol. Co ciekawe, w tym raporcie podzielono drony dozorowe na dwa typy w zależności od tego, czy ich rejon monitoringu ma charakter liniowy, czy monitorują pewien obszar. W monitoringu liniowym – nadzorowaniu autostrad, wybrzeży lub obszarów nadgranicznych używa się stałopłatów. Mogą wypatrywać prób nielegalnego przekroczenia granicy, przemytu lub śledzić wędrówki dzikiej zwierzyny. Do monitorowania obszarowego częściej wykorzystuje się drony z wieloma śmigłami ze względu na lepsze możliwości manewrowania i zawisania w powietrzu, zauważają autorzy raportu. Bezzałogowe statki powietrzne przesyłają strumień danych w czasie rzeczywistym, podążając za obiektami lub intruzami w bezpiecznej odległości szybko kontrolują znaczny obszar, ale też robią zdjęcia, na których widać, czy np. wycięto las lub zabrano hałdę żużla, kontynuują autorzy. Dron ma tę przewagę nad konkurencyjnymi kamerami stacjonarnymi, że intruz nie może się przed nim ukryć, może też rejestrować obszary normalnie niewidoczne. Mogą też wykonywać zdalny zwiad miejsca wypadku, aby sprawdzić, czy teren jest bezpieczny dla zespołu interwencyjnego. To znacznie poprawia skuteczność grup reagowania.

Wg Markets&Markets wartość globalnego rynku dronów ma wzrosnąć do 21 mld USD w 2022 r. przy skumulowanym rocznym wskaźniku wzrostu CAGR ok. 16% w latach 2016–2022.

Inne zastosowania dronów w kontekście security wykracza poza podstawowy monitoring. Mogą zapewniać bezpieczeństwo obiektom kluczowym, takim jak porty czy lotniska. Przykładowo w Abu Zabi w Zjednoczonych Emiratach Arabskich firma zarządzająca portami uzupełnia swój system ochrony dronami. Oprócz zastosowań z zakresu security bezzałogowe statki powietrzne są przydatne w weryfikacji jakości pracy załogi.

Praca autonomiczna

Godny uwagi rozwój branży doprowadził do opracowania dronów autonomicznych. W uproszczeniu są to samodzielnie latające drony, które przemieszczają się w ra-

mach przypisanego im obszaru. To pierwszy krok w kierunku automatyzacji działań mających na celu poprawę bezpieczeństwa. Wiele firm opracowało autonomiczne drony przeznaczone dla sektora security. Jedną z nich jest Nightingale Security. Według Cary Savasa, wiceprezesa ds. marketingu firmy, ich produkt może wykonywać wiele zadań obsługiwanych przez ludzi, robiąc to i taniej, i szybciej. *Pracownicy ochrony mają ograniczone możliwości* – dodaje C. Savas. – *Na przykład jest im trudno szybko skontrolować duże obszary albo miejsca odległe. Szybkie reagowanie jest po prostu w większości rozległych obiektów niemożliwe. Są też inne czynniki zmniejszające efektywność, np. zwolnienia chorobowe, dni wolne od pracy, wakacje, kradzieże itd. Są to ludzkie sprawy, które wpływają na każdą branżę, jednak uznałem za stosowne zwrócić na nie uwagę przy porównywaniu ludzi i robotów. Roboty nie mają wakacji.* Pomysł Nightingale Security obejmuje wyspecjalizowane drony z wbudowanymi funkcjami, które są kluczowe dla zadań ochrony.

Drony są wyposażane w jeden lub większą liczbą czujników, np. RGB, IR, termowizyjny, lidarowy i czujnik materiałów niebezpiecznych. Kolejne są opracowywane i intensywnie wdrażane. Rozwiązanie zawiera również stację bazową, która jest nie tylko lądowiskiem. Wewnątrz przemysłowej obudowy odpornej na warunki otoczenia znajdują się element ładujący oraz komputer sieciowy służący do zarządzania autonomiczną pracą drona. Najważniejszym elementem autonomicznego robota wciąż pozostaje oprogramo-

AUTONOMICZNY DRON DOZORUJĄCY STOSOWANY WEWNĄTRZ BUDYNKÓW

Większość dronów jest przeznaczona do ochrony na zewnątrz budynków. Coraz częściej odgrywają ważną rolę w branży zabezpieczeń. Mając unikatowe możliwości, takie jak docieranie do miejsc niedostępnych dla ludzi i kontrola dużych obszarów trudnych do monitorowania, stają się ulubionymi urządzeniami specjalistów ds. bezpieczeństwa. Trend ten wzmacniają postępy w produkcji dronów. Rozwój technologii – sztuczna inteligencja, *deep learning* i *machine vision* – sprawia, że są inteligentniejsze, sprawniejsze i, co ma największe znaczenie, bardziej autonomiczne. Kilka firm wprowadziło na rynek autonomiczne drony do celów dozorowych. W znacznej mierze są one przeznaczone do pracy na zewnątrz budynków. Pojawiła się jednak firma, która twierdzi, że jako jedyna może zaoferować autonomicznego drona dozorowego do pracy wewnątrz budynków – Arctic Robotics z Vantaa w Finlandii produkuje w pełni autonomiczną platformę dronów do pracy w budynkach służącą do ochrony i proaktywnego monitoringu, która pomaga zmniejszyć koszty i poprawić jakość systemów zabezpieczeń. Niko Oksanen, prezes i współzałożyciel firmy, wyjaśnia, dlaczego to rozwiązanie jest unikatowe i może odmienić branżę zabezpieczeń. *Jesteśmy jedyną firmą oferującą w pełni autonomiczne rozwiązanie pozwalające na lot wewnątrz budynków, w którym dron stanowi jedynie platformę. Wykorzystanie naszych usług w chmurze do kontroli maszyn i zarządzania flotą umożliwi przeglądanie nagrań na żywo lub zarejestrowanie z dowolnej przeglądarki internetowej, a całe rozwiązanie można łatwo zintegrować z istniejącym systemem pomieszczeń kontrolnych* – podkreśla N. Oksanen.

Dron zdolny do poruszania się wewnątrz budynku wykorzystuje system nawigacyjny 2D oparty na lidarze[1]. Jest w pełni zautomatyzowany i przemieszcza się po wyznaczonych trasach. Pauli Isoaho, dyrektor techniczny i współzałożyciel Arctic Robotics, dodaje, że dron wykorzystuje obracający się lidar do pomiaru odległości od ścian, a także sonar do unikania przeszkód. *Stosujemy też sonary i lidary do mierzenia odległości od podłogi i sufitu* – wyjaśnia P. Isoaho. – *Nasz system zawiera automatyczną stację ładującą i usługę w chmurze. Nie budujemy ram drona sami, lecz tworzymy algorytmy nawigacji i jesteśmy właścicielem pełnego rozwiązania. Zatem nasza praca to w 80 proc. oprogramowanie, natomiast w 20 proc. sprzęt.*

[1] Lidar (LIDAR – Light Detection and Ranging) – urządzenie działające podobnie jak radar, ale zamiast światła wykorzystuje mikrofale.

wanie. Dziś drony są produkowane przez wiele firm, ale wykorzystanie takiego rozwiązania na skalę komercyjną wymaga przede wszystkim oprogramowania opartego na sztucznej inteligencji, które umożliwi pracę flocie dronów i sieci stacji bazowych. Oprogramowanie to w rzeczywistości „mózg" całego rozwiązania. Nowinki sprzętowe zdecydowanie determinują sposób funkcjonowania branży zabezpieczeń, natomiast tak naprawdę innowacje w oprogramowaniu zdecydują o stopniu inteligencji tych maszyn.

Połączenie dronów i robotów dla poprawy bezpieczeństwa

Monitoring podniebny może okazać się niewystarczający. Podejmowane są próby połączenia możliwości dronów z autonomicznymi robotami-strażnikami. Działająca w Singapurze firma OTSAW Digital stworzyła O-R3 – autonomicznego robota do pracy w terenie z wbudowanym modułem sterującym dronem. *O-R3 to pierwszy na świecie autonomiczny robot-strażnik, który łączy nadzór naziemny z powietrznym dzięki zintegrowanemu systemowi UGV-UAV* – wyjaśnia Ling Ting Ming, prezes OTSAW Digital. – *Stwarza to możliwości obserwacji w pełnym zakresie 360° bez martwych stref. Ponadto obecność O-R3 „robi wrażenie" i skutecznie zniechęca potencjalnych przestępców.*
Dubaj już podjął decyzję o wykorzystaniu O-R3, przed końcem tego roku roboty powinny pojawić się na ulicach tego miasta. Nie zastąpią one pracowników ochrony, ale będą ich wspierać.

W kierunku bardziej inteligentnych dronów

Wraz z dalszym rozwojem technologii dronów branża zabezpieczeń z pewnością będzie jednym z sektorów odnoszących największe korzyści. Oprócz większej autonomii i proaktywnemu stawianiu czoła zagrożeniom, drony są na najlepszej drodze do objęcia kluczowej roli w przetwarzaniu danych. Widzenie maszynowe (*machine vision*) umożliwi im wykonywanie takich zadań, jak wykrywanie nieuprawnionych wejść na teren obiektu. Biometryczne systemy rozpoznawania twarzy pomogą nawet zidentyfikować intruza. Zdaniem Waltera Lee, ambasadora marki i dyrektora ds. relacji z rządem w globalnym dziale bezpieczeństwa w NEC, sztuczną inteligencję (AI) i drony łączą silne współzależności. Są dwie główne płaszczyzny wykorzystania AI w dronach. Na poziomie lotu i na poziomie operacyjnym może być pomocna w kontrolowaniu wzorców poruszania się, koordynacji pracy roju dronów, widzeniu otoczenia, reagowaniu na warunki pogodowe itd. Na poziomie zabieranego na pokład osprzętu sztuczna inteligencja pomaga wprowadzać takie technologie, jak analityka obrazu czy różnorodne czujniki.
Drony potrafią widzieć i odczuwać otoczenie, co poprawia skuteczność ochrony i dozoru – wyjaśnia W. Lee. Specjalnością NEC jest sztuczna inteligencja i technologie biometryczne. To ważny segment zastosowań w przypadku dronów w aspekcie działań antyterrorystycznych. Wkrótce drony staną się nieodłącznym narzędziem sektora bezpieczeństwa. Przy obserwowanym tempie rozwoju technologii najbliższa przyszłość zapowiada się więc interesująco.

Wkrótce drony staną się nieodłącznym narzędziem sektora bezpieczeństwa. Nie zastąpią one pracowników ochrony, ale będą ich wspierać.

„ŻYWOTNOŚĆ" BATERII JEST DUŻĄ PRZESZKODĄ W ROZWOJU TECHNOLOGII DRONÓW

Dostępne w sprzedaży drony zdobywają coraz większą popularność w kolejnych sektorach wertykalnych. Z pomocą kilku nowych *start-upów* i nowinek technologicznych użytkownicy poznali ich szczególne zalety i możliwości przydatne w konkretnych branżach. Stąd też można spotkać te urządzenia np. w zastosowaniach security do autonomicznego dozoru wybranych obszarów; w rolnictwie do przeglądu upraw, a nawet w pracach badawczych do zbierania informacji.

Jedną z poważniejszych przeszkód na drodze rozwoju tego sektora jest niski czas życia baterii zasilających drony. Lot dostępnych w handlu dronów trwa średnio 10-20 minut, co sprawia, że stają się mało przydatne podczas intensywnej pracy. Na przykład w zastosowaniach security nadzorowanie ogromnych obszarów nie jest możliwe bez baterii o odpowiedniej żywotności.

Pojawiło się rozwiązanie. Elistair, francuska firma z Lyonu, projektuje i produkuje przewodowe stacje dla dronów, zapewniające większe bezpieczeństwo, nieograniczoną autonomię i szybki transfer danych niezbędnych do pracy dronów. Guilhem de Marliave, prezes i założyciel Elistair, wyjaśnia, że rozwiązanie zapewnia łatwy dostęp do nieograniczonej ilości danych wprost z dronów. Głównym rynkiem zbytu produktu są firmy zajmujące się stałym dozorem przestrzeni powietrznej, telekomunikacją *pop-up* oraz kontrolą przemysłową w trudnym środowisku.

Flagowy produkt Elistair, SAFE-T, to inteligentna stacja przewodowa dla dronów cywilnych, dostarczająca operatorom i użytkownikom dronów większe możliwości – zapewnia G. de Marliave. Mikroprzewód zapewnia stałe zasilanie i szybki transfer danych. W efekcie rozwiązanie umożliwia nieograniczony, bezpieczny, globalny dostęp do obrazów z powietrza w czasie rzeczywistym. SAFE-T stanowi doskonałe rozwiązanie dla licznych zastosowań w obszarze dozoru, kontroli, telekomunikacji i TV programowej. Urządzenie można łatwo transportować i używać w każdym terenie. Jest niewielkie i zdolne do pracy w kilka sekund.

Nie ulega wątpliwości, że łączący przewód ogranicza wielkość obserwowanego obszaru. Jednak dzięki bezpośredniemu i nieprzerwanemu zasilaniu przez mikroprzewód dron zyskuje możliwość długotrwałej pracy.

Spójrzmy na to z góry

Rozwój w obszarze kamer będzie kontynuowany zgodnie z trendem obserwowanym na rynku już od kilku lat. Generowany obraz będzie miał coraz lepszą jakość i wyższą rozdzielczość, a ceny kamer zaczną sukcesywnie spadać. Kamera termowizyjna stanie się przy tym naturalnym elementem wyposażenia drona.

Jakub Sobek

Na numer alarmowy przychodzi połączenie. Dyspozytorka słyszy w słuchawce roztrzęsiony głos kobiety:
– Chciałam zgłosić zaginięcie córki. Musicie ją odnaleźć. Ona na pewno jest przerażona!
– Proszę spokojnie powiedzieć, kiedy nastąpiło zaginięcie dziecka i gdzie może się obecnie znajdować? Im więcej poda pani szczegółów, tym bardziej ułatwi nam pani pracę.
– Córka oddaliła się od domu około godziny temu. Wyszła w kierunku lasu i pewnie tam zabłądziła.

Po ustaleniu wszystkich szczegółów została podjęta decyzja o rozpoczęciu akcji poszukiwawczej. Na zewnątrz temperatura dochodziła do -8°C, a wkrótce miał zapaść zmrok. Z opisu wynikało, że dziecko miało na sobie kurtkę, jednak nie był to strój przystosowany do długiego przebywania na mrozie. W takiej sytuacji każda minuta była na wagę złota. Dziecko z powodu wychłodzenia organizmu mogło bowiem zapaść w hipotermię zagrażającą życiu.
Po krótkiej odprawie ze strażakami i policją rozpoczęły się poszukiwania. Zastosowano standardowe środki: przeszukiwania wytypowanego wcześniej terenu w szyku tyraliery oraz wykorzystanie przewodników z psami tropiącymi. Dowódca zlecił też użycie drona z kamerą termowizyjną do patrolowania większego obszaru z powietrza. Po godz. 18.00 poinformował, że niebawem zapadnie zmrok, a wtedy poszukiwania staną się jeszcze trudniejsze. Temperatura spadła do -15°C. W pewnej chwili operator drona zauważył pod drzewem nietypowy obiekt. Zbliżył się niego i obniżył pułap lotu – okazało się, że była to poszukiwana dziewczynka. Słysząc nadlatujący dron, zaczęła machać w jego kierunku, co upewniło operatora. Odczytano bieżącą pozycję GPS drona i drogą radiową przekazano ją do wszystkich uczestników poszukiwań. Operator zauważył na obrazie z kamery zamarznięte jezioro w pobliżu drzew i ostrzegł, aby poruszać się po tym terenie ze szczególną ostrożnością. Wszystko zakończyło się *happy endem*. Tym razem udało się dotrzeć na czas.

Dodatkowe oko

W przypadku takiej akcji poszukiwawczej kamera termowizyjna umieszczona na dronie okazała się nieoceniona. Pozwoliła na wytypowanie celu, jego weryfikację i dokładną lokalizację. To jedno z takich rozwiązań, jakie w ostatnich latach staje się coraz bardziej powszechne.
Czy połączenie kamery pracującej w zakresie podczerwieni ze statkiem bezzałogowym jest najlepszym narzędziem? W jakich jeszcze sytuacjach można je wykorzystać i jakie są ograniczenia takiej technologii?
UAV (*Unmanned Aerial Vehicle* – bezzałogowy statek powietrzny) wyposażony w kamerę nie jest niczym nowym. Dron może być nośnikiem dowolnego czujnika, począwszy od tradycyjnych sensorów światła widzialnego, przez skanery LIDAR, czujniki skażenia radiologicznego, chemicznego, biologicznego, skończywszy na kamerach termowizyjnych. Umieszczenie na dronie kamery termowizyjnej znacznie rozszerza możliwości jego zastosowania. Jest wiele dostępnych kamer, więc wybór właściwego rozwiązania, które musi być uzależnione od rodzaju prowadzonej misji, nie zawsze jest łatwy.

Trzeba pamiętać, że kamery pracujące w zakresie IR (niewidzialnym dla człowieka) są wyposażone w różnego typu przetworniki obrazu. Najczęściej dzielimy je ze względu na długości fal, które wykorzystują przy tworzeniu obrazu: bliska podczerwień (SWIR) zakres 1–2,5 µm oraz średnia (MWIR) 3–5 µm i daleka podczerwień (LWIR) 7,5–14 µm (termowizja).
Długości fal, w jakich operują kamery SWIR, nie są widoczne dla ludzkiego oka, ale zasada ich działania jest podobna do klasycznych kamer światła widzialnego, które korzystają z odbitego światła emitowanego przez inne źródła (np. słońce). Dlatego na obrazach z kamer SWIR i w wyniku odbić światła można zaobserwować cienie i lokalne różnice w kontraście. Są to przeważnie czarno-białe wysokiej rozdzielczości.
Detektory SWIR są zbudowane w technologii InGaAs (arsenek galu indu). Obecnie najczęściej stosuje się je w obszarach wojskowych, ponieważ są alternatywą dla kamer noktowizyjnych i oferują wysoką rozdzielczość. Dodatkowo pozwalają zauważyć np. światło lasera o długości fal 1550 nm.
Detektory pracujące w zakresie MWIR i LWIR wykorzystują promieniowanie IR emitowane przez wszystkie występujące w przyrodzie obiekty. Mogą widzieć w zupełnej ciemności, w przypadku zapylenia, zamglenia i zadymienia oraz w czasie opadów. Zasadnicza różnica między tymi dwiema technologiami polega na tym, że kamery MWIR bazują najczęściej na chłodzonych przetwornikach obrazu, a kamery LWIR – na przetwornikach niechłodzonych.
Przetwornik MWIR wykonany w technologii np. InSb jest chłodzony przez aktywny układ mechaniczny wykorzystujący hel.

Chłodzenie przetwornika do ujemnej temperatury jest wymagane w celu zmniejszenia poziomu szumów indukowanych cieplnie na przetworniku poniżej poziomu sygnałów pochodzących z obrazowanych obiektów. Ten precyzyjny układ mechaniczny zużywa się wraz z upływem czasu, a gaz ulatnia się z niego mimo dokładnego uszczelnienia. Z tego powodu w zależności od konkretnego rodzaju przetwornika wymaga on serwisowania co 10–13 tys. godz. pracy, polegającego na wymianie chłodziwa. Przetworniki MWIR są droższe od przetworników LWIR, a trzeba też uwzględnić koszty obsługi serwisowej.

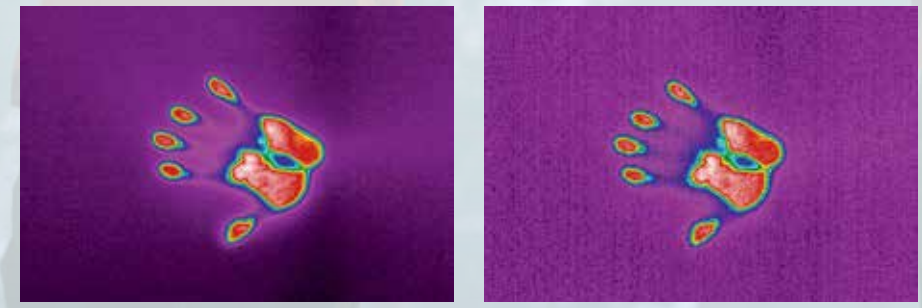
W związku z tym nasuwają się pytania, czy stosowanie chłodzonych przetworników ma sens i w jakich przypadkach warto z nich korzystać. Technologia ta ma wiele zalet, a jakość obrazu jest na najwyższym poziomie. Jeśli dla użytkownika kamery termowizyjnej jest ważna wysoka czułość termiczna, to taka kamera jest świetnym rozwiązaniem. Kamery MWIR ponadto pozwalają na precyzyjny pomiar temperatury szybko poruszających się obiektów, nawet niewielkich, a także badanie rozkładów temperatury w specyficznych zakresach sygnału. W przypadku latających statków bezzałogowych o masie startowej do 25 kg stosowanie technologii MWIR należy raczej do rzadkości. Przy obecnych kosztach jest onazarezerwowana głównie do profesjonalnych zastosowań, gdzie cel misji jest bardzo wymagający. Dron wyposażony w taką kamerę może prowadzić obserwację na dalekich dystansach, dzięki temu możliwe jest wykonywanie zwiadu powietrznego przy bardzo wysokim pułapie lotu.

Najbardziej popularne obecnie są kamery termowizyjne pracujące w zakresie LWIR. Przetworniki te są oparte na matrycy typu FPA (*Focal Plane Array*). W ostatnich latach zanotowano ogromny rozwój kamer pracujących w tej technologii. Znaczącą rolę odegrała szczególnie dostępność nowych materiałów do ich produkcji. Wyraźna poprawa w odczytywaniu sygnałów pochodzących z matryc, ulepszenie cyfrowej obróbki tych sygnałów, technologia wytwarzania FPA oraz zmniejszenie ich rozmiarów – wszystko to sprawia, że obecnie na rynku są dostępne miniaturowe kamery o rozdzielczościach zaczynających się od 80 x 60 pikseli. Można też kupić kamery, które mają kilkanaście megapikseli. Przetworniki o takiej rozdzielczości są obecnie wykorzystywane w najbardziej zaawansowanych aparaturach badawczych, stosowanych w astronomii, m.in. w teleskopie Hubble'a czy teleskopie Jamesa Webba, który zastąpi teleskop Hubble'a na początku 2019 r. W teleskopie Webba przetwornik będzie prowadzić obserwacje w zakresie aż do 28 µm, co pozwoli na obrazowanie odległych galaktyk, tworzących się w kosmosie gwiazd, komet o słabym świetle czy obiektów w pasie Kuipera. Nowy teleskop już wkrótce pokaże kosmos w „nowej odsłonie" właśnie dzięki termowizji.

Przetworniki LWIR są najczęściej wykonywane z dwóch różnych materiałów półprzewodnikowych. Na rynku są dostępne przetworniki zbudowane z amorficznego krzemu A-Si oraz z tlenku wanadu VO_x. Wiele kamer termowizyjnych instalowanych na zewnątrz pomieszczeń jest narażonych na bezpośrednie działanie promieni słonecznych. Kamery wykonane w technologii VOx są odporne na degradację obrazu spowodowaną długą, bezpośrednią obserwacją słońca. Z kolei przetworniki A-Si doświadczają znaczącej degradacji obrazu i mogą na nich powstawać trwałe uszkodzenia spowodowane wystawieniem na działanie promieni słonecznych.

W przetworniku można ponadto zastosować kolejne mechanizmy ochronne. W czujniku VO_x umieszcza się rezystory, które pochłaniając promieniowanie IR, zmieniają swoją rezystancję. Dzięki procesom zachodzącym wewnątrz detektora energia pochodząca z promieniowania słonecznego jest rozpraszana, aby nie powodowała nieodwracalnego uszkodzenia rezystorów. W kamerze umieszcza się także tzw. *shutter*, czyli mechaniczny układ pozwalający na kalibrację kamery metodą FFC (*Flat Field Calibration*). Kalibracja występująca w kamerze co pewien czas zapewnia wyczyszczenie z obrazu tzw. powidoków widzianych na obrazie, spowodowanych obserwacją w świetle słonecznym. Wszystko to dzieje się w ułamku sekundy. W przetwornikach A-Si czasem potrzeba natomiast kilkudziesięciu minut lub godzin, aby rozproszyć powstały na obrazie efekt.

Ze względu na to, że kamery LWIR są praktycznie bezobsługowe i nie wymagają okresowego serwisowania, są stosowane w wielu obszarach, m.in. ręcznych kamerach pomiarowych wykorzystywanych w badaniach termograficznych, kamerach dozorowych w zastosowaniach security, a także kamerach coraz częściej stosowanych w dronach.



Ślad cieplny dłoni zobrazowany za pomocą kamery termowizyjnej chłodzonej (po lewej) i niechłodzonej (po prawej). *Źródło:* **FLIR.com**

Termowizja w misji powietrznej

Ze względu na koszty i dostępność technologiczną w misjach powietrznych będą używane kamery LWIR. Drony obecnie znajdują zastosowanie w wielu obszarach. Korzystają z nich zarówno amatorzy, jak i profesjonaliści. Często od skuteczności odpowiednio dobranej technologii może zależećludzkie życie. Termowizja może być przydatna w różnego rodzaju zadaniach. Jednym z najczęstszych zastosowań dronów i termowizji są loty inspekcyjne, których zadaniem jest zobrazowanie anomalii temperaturowych na badanym obszarze. Często można np. zauważyć uszkodzone lub przegrzewające się elementy na działającym panelu fotowoltaicznym. W takiej sytuacji dron pozwala na przeprowadzanie inspekcji dużego obszaru, np. farmy solarnej czy kominów przemysłowych, w krótkim czasie, znacząco usprawniając dotychczasowe metody kontroli. Zadania, które do tej pory były niebezpieczne i uciążliwe dla człowieka, mogą być wykonane szybciej, dokładniej, a co najważniejsze bez ponoszenia zbędnego ryzyka.

W przytoczonej na początku historii kamera termowizyjna znalazła zastosowanie w misji poszukiwawczo-ratunkowej. Aby w takich działaniach była skutecznie wykorzystywana, trzeba mieć pełną świadomość zarówno

Zdjęcie wykonane za pomocą kamery termowizyjnej w trakcie inspekcji paneli fotowoltaicznych. *Źródło:* **TEAX**

Osoba zauważona podczas prowadzenia misji poszukiwawczej jesienią. *Źródło:* **zbiory prywatne autora**

jej możliwości, jak i ograniczeń. Wielu ludziom wydaje się, że promieniowanie termiczne przenika przez pewne powierzchnie. Ten brak wiedzy często sprawia, że możliwości tych kamer są źle oceniane. Trzeba wiedzieć, kiedy i gdzie kamera termowizyjna będzie pomocna. Kiedy poszukiwane są osoby zaginione lub zwłoki, z upływem czasu temperatura ciała będzie się obniżała, zmniejszy się kontrast termiczny z otoczeniem i zasadność wykorzystania termowizji. W przypadku poszukiwań osób po zejściu lawiny śnieżnej technologia ta napotyka pewne ograniczenia. Nie ma bowiem możliwości, aby zauważyć osobę, która leży pod grubą warstwą śniegu, ponieważ obraz z kamery odwzorowuje temperaturę powierzchni śniegu. Aby pojawiła się szansa zlokalizowania takiej osoby, nad powierzchnią śniegu musi wystawać przynajmniej fragment ciała lub poprzez szczeliny w śniegu musi wydostawać się np. znacznie cieplejsze wydychane powietrze. Jeśli te warunki nie zostaną spełnione, termowizja nie będzie pomocna. Podobne ograniczenia występują, gdy np. w celu znalezienia zwłok przeszukiwane są zbiorniki wodne lub rzeki. Jeśli ciało znajduje się pod wodą, nie ma możliwości jego dostrzeżenia, gdyż zawsze na obrazie będzie widoczna jedynie temperatura powierzchni wody.

Połączenie drona z kamerą termowizyjną przyniesie najlepsze efekty, gdy poszukiwania będą prowadzone na łąkach, polach, w lesie, na obszarach górzystych czy pustyniach. Jedyne ograniczenia wyraźnego zauważenia obiektu pojawiają się, gdy osoba przebywa w gęstym lesie, kamera termowizyjna nie widzi bowiem tego, co znajduje się pod grubą warstwą liści na drzewach.

Nie bez znaczenia pozostaje skład załogi obsługującej drona podczas misji poszukiwawczej. Akcja jest najskuteczniejsza, gdy grupa składa się z czterech osób: operatora drona, operatora kamery, mechanika oraz dowódcy załogi koordynującego wszystkie działania oraz pozostającego w bezpośrednim kontakcie z koordynatorem całej akcji poszukiwawczej lub ratowniczej.

Szczególnie istotnym czynnikiem decydującym o sukcesie misji jest zapewnienie dobrych warunków pracy operatorowi kamery termowizyjnej. Trudno np. obserwować obraz IR, gdy na monitor świeci słońce, a obraz jest widoczny w niskim kontraście. Operator kamery powinien pracować w namiocie lub pojeździe, aby zewnętrzne oświetlenie nie wpływało na jakość obrazu widocznego na ekranie. Jakość wyświetlacza ma znaczenie także w przypadku, gdy obraz jest wyświetlany np. w skali szarości. Istotne jest właściwe odwzorowanie czerni oraz skali szarości. Operator kamery termowizyjnej powinien odbyć szkolenie. Tylko znajomość zasad fizyki umożliwi zrozumienie możliwości i ograniczeń termowizji oraz pozwoli na poprawne wnioskowanie z obrazów widocznych na ekranie. Przykładowo, kiedy do dyspozycji mamy kamerę o rozdzielczości 640 x 480 pikseli o poziomym kącie widzenia 45° i lecimy dronem na wysokości 60 m, cel wielkości człowieka na ekranie monitora wynosi ok. 50 pikseli. Gdyby kamera miała niższą rozdzielczość 320 x 240 pikseli, to przy tym samym kącie widzenia i wysokości lotu operator na ekranie musiałby zauważyć 17 pikseli. To pokazuje, w jakim skupieniu musi pracować i jak ważne jest jego doświadczenie, aby w trakcie lotu nie pominąć ważnego obiektu.

> Dron może być nośnikiem dowolnego czujnika, począwszy od tradycyjnych sensorów światła widzialnego, przez skanery LIDAR, czujniki skażenia radiologicznego, chemicznego, biologicznego, skończywszy na kamerach termowizyjnych.

Co będzie dalej

Kamery termowizyjne w połączeniu z dronami będą wykorzystywane coraz częściej. Rozwój zarówno technologii kamer, jak i dronów będzie kreować nowe zastosowania. W odniesieniu do misji poszukiwawczych jest kilka kierunków, w których jest jeszcze dużo do zrobienia.

Autonomiczne loty pojedynczych dronów i ich rojów, które komunikując się ze sobą, mogą synchronicznie wspólnie przeszukiwać jeszcze większe obszary, znacząco ułatwią prowadzenie akcji poszukiwawczych i skrócą czas potrzebny na przeszukanie terenu. Ponadto rozwój analizy wideo pozwoli w przyszłości na automatyczne typowanie celów poszukiwanych obiektów. Operator drona będzie otrzymywał pojedyncze obrazy pochodzące z dronów w celu dokonania ich wideoweryfikacji.

Wiele dronów ma jeszcze dość restrykcyjne ograniczenia, jeśli chodzi o lot w trudnych warunkach atmosferycznych. To także pewien czynnik, który ogranicza ich wykorzystanie w sytuacji, gdy mogą być najbardziej potrzebne. Pokonanie tej przeszkody sprawi, że będą coraz częściej wykorzystywane, bez względu na warunki atmosferyczne.

Jest jeszcze jeden czynnik, który spędza sen z powiek użytkowników dronu – czas lotu. Mechanik co kilkanaście, kilkadziesiąt minut musi wymieniać baterie, co przerywa lot i zabiera cenny czas.

Literatura:
http://www.flir.com/science/display/?id=65982; **http://www.**photonics.ucla.edu/host/ieee_photonics_la/documents/James_Beletic_OPN.pdf; **http://www.**petriefied.info/AirbornelR.pdf

Drony
nowe zagrożenie dla mienia i infrastruktury

Na rynku globalnym notowuje się olbrzymi wzrost popularności i zastosowań dronów (bezzałogowych statków powietrznych), począwszy od zabawek dla dzieci, poprzez drony dokonujące inspekcji obiektów czy robiące zdjęcia krajobrazowe, skończywszy na rozwiązaniach wojskowych.

dr Radosław Piesiewicz

Mimo wielu użytecznych zastosowań nietrudno sobie wyobrazić także wykorzystanie dronów w działalności niepożądanej, takiej jak naruszanie prywatności, terrorystycznej, szpiegowskiej lub przemytniczej. Mogą bowiem być użyte do podglądania osób, podsłuchiwania polityków czy biznesmenów, planowania rabunku ludzi majętnych czy wręcz przeprowadzenia ataku z użyciem broni ostrej lub ładunków wybuchowych na wybrane osoby czy obiekty – to w sferze prywatnej. W sferze publicznej mogą stanowić zagrożenie terrorystyczne (dron może przenieść średnio kilkukilogramowy ładunek) dla obiektów publicznych i infrastruktury krytycznej (elektrowni, lotnisk, portów, rafinerii itp.). Mogą również służyć do przemytu narkotyków czy broni przez granice, zagrażać obiektom wojskowym lub być wykorzystywane w celach szpiegowskich.

Jeszcze kilka lat temu drony były techniką zarezerwowa-

ną wyłącznie dla wojska. Dziś są w zasięgu „każdego Kowalskiego". W Polsce, oprócz osób prywatnych, używają ich zwykle firmy z branży filmowej i reklamowej, a także coraz częściej dostawcy usług monitorowania w rolnictwie, energetyce czy geodezji. Rynek bezzałogowych statków powietrznych, wg raportu Markets and Markets" z października 2015[1] , jest szacowany na 14,9 mld USD w 2020 r. przy aktualnej wartości na poziomie 10 mld USD i dynamice wzrostu na poziomie 8% CAGR.

W ostatnim czasie w mediach pojawiają się z dużą częstotliwością doniesienia o naruszeniu prywatności, działalności przestępczej czy stanowiącej niebezpieczeństwo dla transportu publicznego oraz wskazujące na możliwą działalność szpiegowską z użyciem dronów. Można wymieniać wiele, chociażby przerzut telefonów i narkotyków do więzienia w Wielkiej Brytanii[2], wtargnięcie na teren lotniska w Cork w Irlandii i zablokowanie ruchu lotniczego[3] czy użycie dronów przez ISIS do ataków w Iraku[4]. Wykorzystanie dronów do aktów terrorystycznych w Europie czy USA nie należy już do tematów *science fiction*, lecz stanowi realne zagrożenie[5].

Pojawiło się nowe zagrożenie, musi się więc znaleźć skuteczna na nie odpowiedź.

Nie istniały dotychczas skuteczne metody detekcji dronów. Technologie wojskowe nie były projektowane pod kątem tak małych, plastikowych obiektów latających, poruszających się na niewielkich wysokościach. Technologii cywilnych nie było. Systemy do wykrywania i neutralizacji dronów zaczynają się dopiero pojawiać. Firmy, które prezentują stosowne technologie, można wymienić na palcach jednej ręki. Jedna z tych firm pochodzi z Polski.

System skuteczny w wykrywaniu dronów musi opierać się na zastosowaniu wielu sensorów. Aby działał w dzień i w nocy, w każdych warunkach atmosferycznych (mgła, chmury, deszcz, śnieg), musi zawierać co najmniej trzy różne czujniki: radary, kamery wizyjne i detektory akustyczne. Istotne jest też, żeby nie miał luk w pokryciu przestrzennym, tj. aby zapewniał pełną ochronę obiektu czy instalacji w formie parasolowej. Drony mogą poruszać się bardzo nisko przy ziemi lub latać wysoko. Dron może pojawić się z dowolnego kierunku, z każdej wysokości.

Po stronie neutralizacji można stosować zagłuszarki sygnałów (*jammery*) lub metody kinetyczne oraz drony przechwytujące. Efektem jest albo przechwycenie drona, albo jego odesłanie z powrotem do operatora lub wymuszenie lądowania. W przypadku metod kinetycznych, najbardziej drastycznych, dron zostaje zniszczony, np. poprzez zestrzelenie.

Niektóre z pojawiających się systemów detekcji i neutralizacji dronów zostały oparte na integracji gotowych rozwiązań z obszaru wojskowego, co czyni je ekstremalnie drogimi i tym samym dostępnymi wyłącznie dla wąskiego grona odbiorców, tj. głównie wojskowego. Inne systemy zostały natomiast opracowane na bazie tanich, masowych sensorów komercyjnych, głównie prostych kamerek wizyjnych, i nie integrują sensora radarowego, który jest najważniejszym elementem z punktu widzenia skuteczności wykrywania dronów – pozwala na działanie niezależnie od warunków atmosferycznych, w dzień i w nocy oraz z dużej odległości, tj. przekraczającej kilkaset metrów.

> Mimo wielu użytecznych zastosowań nietrudno sobie wyobrazić wykorzystanie dronów także w działalności niepożądanej, takiej jak naruszanie prywatności, terrorystycznej, szpiegowskiej lub przemytniczej.

Opracowanie sensora radarowego jest jednak skomplikowane i czasochłonne, wymaga zaawansowanej wiedzy z zakresu elektroniki, informatyki i przetwarzania sygnałów.

Biorąc pod uwagę nowe, dotychczas niewystępujące zagrożenia bezpieczeństwa infrastruktury, obiektów oraz osób prywatnych, które wynikają z szerokiego oraz dynamicznie rosnącego stosowania i dostępności dronów, popyt na systemy wykrywające i neutralizujące te zagrożenia będzie ogromny. Przewidywane są cztery główne segmenty wykorzystania systemów antydronowych:

1. monitorowanie i ochrona infrastruktury krytycznej w dużych przedsiębiorstwach instytucjonalnych (porty morskie, lotnicze, kolejowe, rurociągi, energetyczne linie przesyłowe, elektrownie, rafinerie itp.);
2. zastosowanie przez służby państwowe do monitorowania granic, obiektów rządowych, baz wojskowych, ambasad;
3. ochrona terenu średnich firm i fabryk, w szczególności przed szpiegostwem za pomocą dronów;
4. monitorowanie i ochrona przestrzeni prywatnej i osobistej (domy, prywatne posesje).

1) www.marketsandmarkets.com

2) www.thesun.co.uk
3) www.newstalk.com
4) http://heavy.com/news
5) www.washingtonpost.com

BIO

Radosław Piesiewicz
Prezes firmy Advanced Protection Systems z Gdyni, specjalizującej się w produkcji sensorów i systemu SafeSky do wykrywania i neutralizacji dronów.

Drony w bezpieczeństwie biznesu

Jeszcze nie tak dawno drony kojarzyły się z widowiskowymi atakami głównie amerykańskich sił zbrojnych na bojowników w Iraku czy Afganistanie. **Oczywiście dron może zostać użyty jako sprzęt do zabijania, i taki był pierwotny cel jego twórców, którzy opracowali go na potrzeby wojska. Ale może również służyć do zadań cywilnych.**

Sebastian Błażkiewicz
SASMA Europe

Postęp w dziedzinie budowy dronów jest dziś tak duży, że trudno sobie wyobrazić firmę profesjonalnie zajmującą się ochroną osób i mienia oraz ogólnie kwestiami bezpieczeństwa, która nie korzystałaby z najnowszych tego typu rozwiązań. W jakich obszarach zastosowań dron może wspierać pracę osoby odpowiedzialnej za bezpieczeństwo? Jest ich wiele, a ogranicza nas tylko nasza wyobraźnia… i prawo. Należy pamiętać, że każdy kraj ma własne regulacje dotyczące użycia dronów i trzeba się

Dron to narzędzie pracy osoby odpowiedzialnej za bezpieczeństwo w XXI wieku, narzędzie o ogromnym potencjale i wielu możliwych zastosowaniach.

z nimi zapoznać, by nie mieć problemów z lokalną jurysdykcją – w niektórych krajach można w miarę sprawnie poradzić sobie z tym ograniczeniem, w innych korzystanie z drona jest limitowane i należy uzyskać odpowiednie pozwolenia czy też licencję na jego użycie.

Na początek drobny przykład. Klient miał problem z udokumentowaniem nielegalnego wydobycia żwiru na terenie swojej kopalni. Za pomocą drona ten problem udało się rozwiązać bardzo szybko i skutecznie. Ale to tylko jedna z wielu potencjalnych możliwości wykorzystania tego urządzenia. Kilka kolejnych obszarów zastosowania dronów wyposażonych w kamerę CCTV w ochronie mienia i osób:

- audyty bezpieczeństwa – dron doskonale wspiera pracę ochrony fizycznej podczas wszelkich audytów, zwłaszcza dużych obszarów (centra logistyczne, fabryki, obiekty przemysłowe),
- detektywistyka biznesowa – może np. prowadzić obserwację określonego terenu czy osoby, poruszając się niezauważony,
- rozpoznanie pirotechniczne – przyspiesza wszelkie sprawdzenia terenów rozległych,
- nadzór i kontrola – za pomocą drona można monitorować pracę ochrony, a także działanie całego systemu bezpieczeństwa,
- fizyczne testy penetracyjne obiektów,
- szkolenia – dron może zostać użyty do zarejestrowania np. ćwiczeń czy ewakuacji; uzyskany za jego pomocą film służy jako materiał szkoleniowy,
- rozpoznanie terenu – dron wyposażony w kamerę 4K (opcjonalnie termowizyjną) jest nie do zastąpienia w prowadzeniu działań operacyjnych,
- *Loss Prevention* – minimalizacja strat,
- bezpieczeństwo łańcucha dostaw,
- bezpieczeństwo imprez masowych.

Drony, dzięki oprogramowaniu wspomagającemu monitoring wizyjny, mogą realizować:

- automatyczne śledzenie wybranej osoby czy samochodu,
- poruszanie się po wcześniej zaprogramowanej trasie,
- automatyczny powrót do punktu startu w przypadku utraty sygnału,
- obserwację określonego terenu.

Oprócz zastosowań z zakresu *security* doskonale sprawdzą się też w obszarze *safety:*

- poszukiwaniu zaginionych osób,
- patrolowaniu lasów (pożary),
- patrolowaniu kąpielisk i dużych akwenów wodnych.

Użycie dronu mogą ograniczać głównie niesprzyjające warunki atmosferyczne, np. silny wiatr. Zaawansowane technicznie urządzenia mogą pracować podczas opadów deszczu i śniegu. Kolejnym ograniczeniem jest czas pracy wynoszący 20–25 minut na jednej baterii, dlatego należy mieć ich zapas.
Ważną cechą dronów jest także możliwość wykorzystania ich wewnątrz obiektów, dzięki sensorom oraz oprogramowaniu ryzyko wypadku czy też zderzenia zostało zminimalizowane. Możliwość wyposażenia w kamerę o rozdzielczości 4K z transmisją obrazu w czasie rzeczywistym oraz wykonywanie zdjęć o wysokiej rozdzielczości, duża prędkość (do 60 km/h) i fakt, że z wysokości 100 m dron pracuje bezgłośnie, dopełniają uniwersalność tych latających bezzałogowców.

W jakich obszarach zastosowań dron może wspierać pracę security managera? Jest ich wiele, a ogranicza nas tylko nasza wyobraźnia... i prawo. Każdy kraj ma własne regulacje, z którymi się trzeba zapoznać.

Od pewnego czasu drony są także na wyposażeniu SASMA. Z całą pewnością można stwierdzić, że jest to narzędzie pracy osoby odpowiedzialnej za bezpieczeństwo w XXI wieku o ogromnym potencjale.

PRZYSZŁOŚĆ W MONITORINGU 2018

Monitoring sygnałów alarmowych oraz dozór wizyjny powinny podążać za rosnącymi oczekiwaniami klientów. Ich rozwój jest pochodną wyścigu technologicznego konkurujących firm oraz gwałtownego wzrostu cen ochrony fizycznej.

Krzysztof Ciesielski

Monitoring alarmowy i dozór wizyjny staną się kluczowymi usługami ochrony osób i mienia. Coraz częściej będziemy rozmawiać o tzw. zdalnym dozorze wizyjnym prowadzonym przez Internet w odległym centrum dozoru. Dotychczas byliśmy przyzwyczajeni, że odbywa się na miejscu, w chronionym obiekcie.

Czynniki kształtujące rozwój

Do najważniejszych czynników, które będą kształtować monitoring alarmowy i dozór wizyjny w najbliższych latach, należą:

- poszukiwanie nowych form ochrony, które będzie można oferować jako ekwiwalent ochrony fizycznej,
- taniejąca i łatwo dostępna technologia, która umiejętnie zastosowana przyniesie więcej korzyści,
- lepsze i bardziej dostępne łącza cyfrowe do transmisji danych (w tym do transmisji sygnałów wizyjnych), dzięki którym usługi zdalnego nadzoru nad bezpieczeństwem będą bardziej efektywne,
- stopniowa zmiana struktury klientów – dominującą rolę zaczną odgrywać klienci biznesowi, stawiający konkretne zadania przed firmami ochrony,
- trudności w znalezieniu fachowców – technika zabezpieczeń szybko zmierza w kierunku IT i wymaga większych kwalifikacji niż dotychczas; biegli w IT przechodzą z firm ochrony do informatycznych, gdzie mają lepiej płatną pracę.

Rozwój usług monitoringu i dozoru wizyjnego będzie się sprowadzał do praktycznego i skutecznego zastosowania technologii w ochronie, ale jednak z udziałem człowieka. Chodzi o takie zastosowanie technologii, aby mogła realnie wesprzeć lub zastąpić nadmiarowych pracowników ochrony. Będzie to możliwe dzięki wprowadzaniu większej centralizacji nadzoru i zarządzania bezpieczeństwem, w czym kluczową rolę odegra możliwość tańszego i szybszego przesyłania większej ilości danych.

Ważnym czynnikiem rozwoju techniki w branży ochrony będą cieszące się coraz większą popularnością rozwiązania w chmurze. Branża ochrony w Polsce to w większości (ok. 70%) małe i średnie przedsiębiorstwa, dla których jedyną właściwą drogą rozwoju jest zastępowanie starej infrastruktury nowymi rozwiązaniami i usługami w chmurze zarówno w formie SaaS (*Security as a Service*), jak i IaaS (*Infrastructure as a Service*).
To trend ogólnoświatowy. Należy zwrócić na to szczególną uwagę, gdyż wiele firm popełnia strategiczny błąd, decydując się na wprowadzenie już dzisiaj przestarzałych rozwiązań. Oczywiście umiejętność oceny, co jest obecnie właściwym i przyszłościowym rozwiązaniem, nie jest sprawą łatwą, ale kluczową. Ci, którzy dobrze wybiorą, wygrają.

Prognozowane trendy

Przewiduję, że monitoring alarmowy będzie podążał w następujących kierunkach:

- rozwój zdalnego dozoru wizyjnego, czyli wykorzystanie transmisji obrazów wideo z chronionych obiektów do weryfikacji zdarzeń i działań prewencyjnych,
- wykorzystanie technologii VoIP/SIP do łączności głosowej z monitorowanym obiektem,
- zastąpienie starych mediów transmisji sygnałów alarmowych (UKF, łącza komutowane) nowymi rozwiązaniami, głównie IP,
- integracja systemów monitoringu z systemami zarządzania przedsiębiorstwem,
- pogłębiona integracja systemów zabezpieczeń z innymi systemami w obiektach klienta,
- zastosowanie automatycznej analizy danych, w tym analityki wizyjnej,
- wykorzystywanie technologii termowizyjnej i radarowej w ochronie zewnętrznej,
- zastosowanie aplikacji mobilnych i dostępu przez www zarówno dla klientów, jak i pracowników firm ochrony.

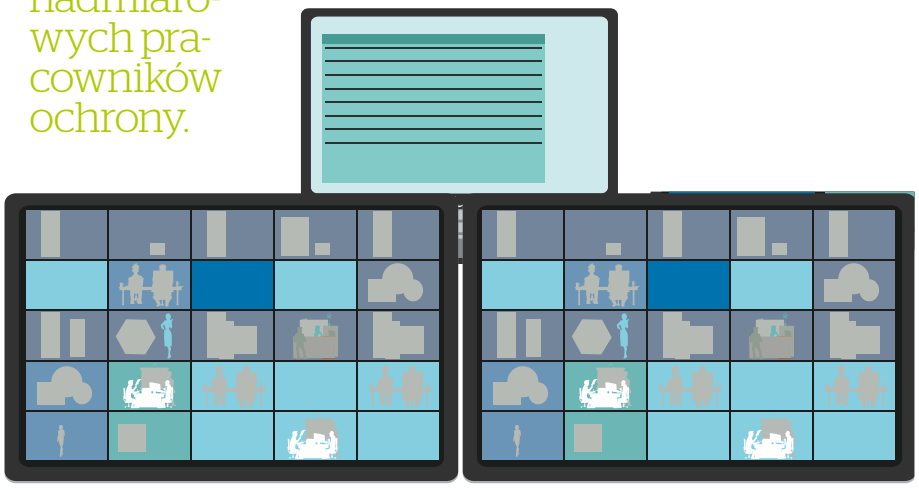
Współczesny monitoring alarmowy i zdalny dozór wizyjny w większości przypadków będzie odpowiedzią na te trendy. Konsekwencją jego rozwoju stanie się konieczność optymalizowania kosztów usług realizowanych przez centra monitorowania, w szczególności kosztów osobowych związanych z obsługą sygnałów oraz kosztów utrzymania coraz bardziej zaawansowanej infrastruktury. W tym obszarze należy się spodziewać następujących rozwiązań:

- automatyzacja i usprawnianie procesu obsługi sygnałów,
- automatyczne przekazywanie informacji o alarmach z wykorzystaniem rozwiązań mobilnych i integracyjnych,
- zastosowanie rozwiązań optymalnie wykorzystujących łącza telekomunikacyjne,
- zwiększenie niezawodności i bezpieczeństwa centrów monitorowania,
- wprowadzanie inteligentnych algorytmów weryfikujących fałszywe alarmy,
- umożliwienie klientowi samodzielnego dokonywania drobnych zmian konfiguracyjnych usługi,
- zastosowanie rozwiązań w chmurze w celu optymalizacji kosztów infrastruktury.

Czy rozwój pójdzie jednym nurtem?

Uważam, że będziemy mieli niebawem do czynienia z dwoma nurtami. Mimo że będą one podążać w tym samym kierunku, będą się od siebie wyraźnie różnić szerokością i tempem.

Chodzi o takie zastosowanie technologii, aby mogła realnie wesprzeć lub zastąpić nadmiarowych pracowników ochrony.



• SZEROKI, ALE WOLNIEJSZY

Szerszym nurtem podążą firmy ochrony dysponujące dużymi centrami monitorowania alarmów i dozoru wizyjnego – powyżej 50 tys. monitorowanych obiektów. W Polsce działają trzy takie firmy i potencjalnie stać je na utrzymanie standardów oraz rozwój technologiczny. To one będą realizować duże, ambitne kontrakty, często ogólnopolskie. Tworzą prywatne chmury do usług monitoringowych. Ich rozwój będzie wiązał się z rosnącymi oczekiwaniami klientów biznesowych, którzy stawiają przed ochroną duże oczekiwania, ale zależy im też na jak najniższej cenie.
Znaczącym problemem dużych centrów monitorowania alarmów jest ograniczona zdolność modernizacji i podążania za nowymi trendami w technologiach monitoringu. Przy dużej skali monitorowanych obiektów trudno wdraża się nowe rozwiązania – co może powodować oddawanie niektórych obszarów mniejszym firmom, które lepiej i szybciej dostosują się technologicznie, np. korzystając z gotowych rozwiązań chmurowych.

• WĘŻSZY, ALE SZYBSZY

Węższym, ale na pewno szybszym nurtem będą podążać mniejsze firmy. W Polsce są to firmy obsługujące ok. 10 tys. monitorowanych obiektów. Lokalne centra monitoringu zaczynają się umacniać. Dzięki możliwości bezpośredniego i dobrego kontaktu z klientem sukcesywnie odzyskują obszary, które próbowały zająć duże ogólnopolskie firmy z branży ochrony. Wśród nich pojawiają się prawdziwe perełki.

Powstają też nowe firmy ochrony, które specjalizują się w zdalnym dozorze wizyjnym. Rozwijają się bardzo szybko, oferując nowoczesne i dobrze skalkulowane usługi ochrony. Jest to możliwe m.in. dzięki technologiom dostępnym w chmurze – rozpoczęcie działalności nie wymaga dużych nakładów w sprzęt. To już nowa filozofia działania, nowe podejście do biznesu. Firmy te będą coraz bardziej skutecznie „podgryzać" lokalne „tuzy monitoringu", które uważają, że ich siłą jest „zasięg" patroli interwencyjnych, zapominając o postępie technologicznym.

Nie zdziwi, gdy w tym wyścigu wygra technologia i nowe, świeże podejście, gdyż wielu firmom zarządzanym przez starsze pokolenie właścicieli brakuje pomysłów na biznes.

Czy konsolidacja rynku ochrony wpłynie na monitoring?

Z pewnością tak. Należy jednak pamiętać, że konsolidacja usług monitoringu jest znacznie trudniejsza i rządzi się nieco innymi prawami niż innych usług ochrony. Obok klasycznych problemów biznesowych pojawiają się spore problemy techniczne. Ich rozwiązanie jest kluczowe i możliwe, lecz niejednokrotnie nieopłacalne lub brakuje wiedzy, jak je rozwiązać. Dlatego często w przypadku konsolidacji firm ochrony nie likwiduje się zastanych, lokalnych centrów monitoringu – wynika to głównie z barier technologicznych, braku odpowiednich narzędzi informatycznych i know-how. Nie osiąga się wtedy pożądanego w konsolidacji, optymalnego efektu skali.

Kwestią nie do pominięcia w tym aspekcie jest przyszłość patroli interwencyjnych firm ochrony.

Rola firm telekomunikacyjnych i *self monitoring*

Coraz częściej operatorzy telekomunikacyjni dochodzą do wniosku, że skoro podstawą usług monitoringu są ich sieci i transmisja danych, to dlaczego nie mieliby świadczyć usług monitoringu. Posiadana infrastruktura w połączeniu z milionami klientów, którym wystarczy jedynie zaoferować usługę dodatkową, stają się ciekawym kierunkiem rozwoju firm telekomunikacyjnych. Tym bardziej że na łączach operatorzy zarabiają coraz mniej i poszukują możliwości oferowania usług dodatkowych.

Obecnie bezpośredni udział firm telekomunikacyjnych w rynku monitoringu nie jest jeszcze bardzo widoczny. Operatorzy obecnie dostarczają rozwiązania firmom ochrony, jeszcze nie proponują ich klientom końcowym. Jednak ich rola w bezpośrednim świadczeniu usług monitoringu będzie szybko rosła.

Operatorzy GSM sprzedali już każdemu Polakowi co najmniej jedną kartę SIM do prowadzenia rozmów i teraz oferują tzw. karty M2M (*machine to machine*), których rynek jest wielokrotnie większy niż rynek rozmów. Kiedy popyt wśród agencji ochrony na karty SIM (M2M, Internet) nie będzie spełniał oczekiwań operatorów, zaczną poszukiwać innych sposobów ich sprzedaży. Zjawisko to można już obserwować.

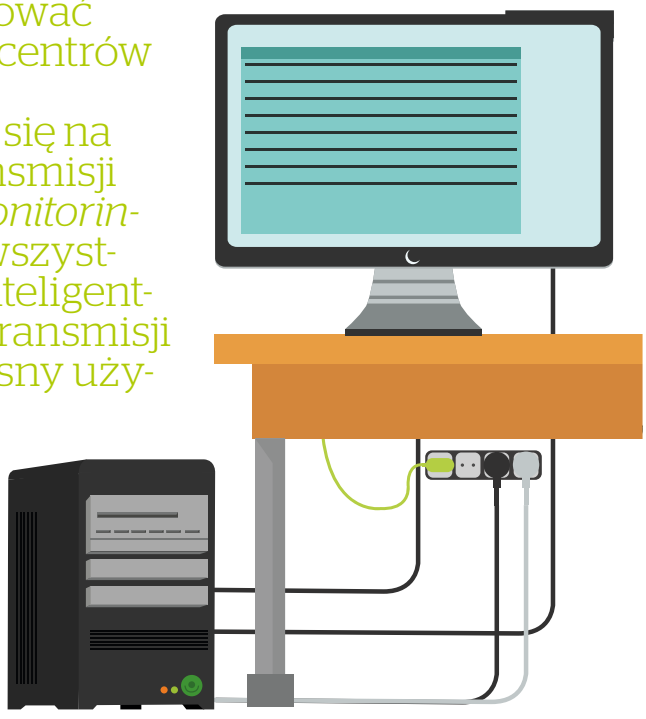
Z dość dużym prawdopodobieństwem można założyć, że operatorzy GSM raczej nie będą budować alarmowych centrów odbiorczych, umożliwiających świadczenie usług ochrony na podstawie odebranych sygnałów (choć oczywiście nie można tego wykluczyć). Skoncentrują się na usługach transmisji wideo, *self monitoringu*, a przede wszystkim na tzw. inteligentnym domu i transmisji wideo na własny użytek klientów.

Czy policja zastąpi patrole firm ochrony?

To dość kontrowersyjne pytanie, a odpowiedź na nie z pewnością zelektryzuje sporą część czytelników. Nie wykluczam takiej możliwości, a może się to stać szybciej, niż sądzimy... Choć oczywiście nie stanie się tak w 100%. Dlaczego policja może przejąć pracę części patroli firm ochrony? Oto okoliczności, które sprzyjają takiemu scenariuszowi:

- Średnia liczba fałszywych alarmów, jakie są odbierane i obsługiwane w centrach monitoringu, jest na poziomie ok. 95%. Oznacza to, że 95 na 100 wyjazdów grup interwencyjnych jest niepotrzebnych. To są gigantyczne koszty dla firm ochroniarskich ponoszone bezzasadnie, więc wcześniej czy później klienci nie będą za to chcieli płacić. Tym bardziej że te usługi wciąż drożeją.
- Jeżeli fałszywe alarmy zostaną ograniczone (do czego się zmierza dzięki zastosowaniu lepszej technologii), to *de facto* patrole interwencyjne firm

Operatorzy GSM raczej nie będą budować alarmowych centrów odbiorczych. Skoncentrują się na usługach transmisji wideo, *self monitoringu*, a przede wszystkim na tzw. inteligentnym domu i transmisji wideo na własny użytek klientów.



ochrony nie będą miały co robić, ponoszenie kosztów większej liczby patroli interwencyjnych też nie będzie miało sensu. W ten sposób koło się zamyka.

Dla klientów indywidualnych świadczenie usług patroli interwencyjnych może stać się nieopłacalne. Mając pewność, że alarmy są prawdziwe, bo zostały zweryfikowane, zgłoszenia będzie mogła obsłużyć policja (zgłoszenie klienta). I tu *self monitoring* będzie również miał coraz większe znacznie. To dość kontrowersyjna teza, ale redukcja liczby patroli interwencyjnych, próby łączenia czy wzajemnego zlecania wyjazdów itp. jest już widoczna.

Jest jednak obszar dla patroli interwencyjnych, których z pewnością nie da się zastąpić policją. Są to wyspecjalizowane usługi dla biznesu i sektora publicznego oraz większych klientów indywidualnych, tzw. VIP-ów. Coraz częściej patrole interwencyjne w połączeniu z usługami zdalnego dozoru wideo będą wykorzystywane jako ekwiwalent stacjonarnych pracowników ochrony.

Warto wspomnieć, że pojawiają się koncepcje związane z utworzeniem ogólnopolskiej, państwowej agencji ochrony, która obsługiwałaby firmy i instytucje państwowe, a także obiekty wojskowe. Potencjalnie jest możliwe, że taka firma nie będzie tworzyła sieci patroli interwencyjnych, lecz będzie wspierała się interwencjami służb publicznych. Wpłynęłoby to na drastyczną redukcję patroli interwencyjnych firm ochrony. Gdyby proces taki miał nastąpić, będzie trwał dłużej niż perspektywa roku 2020.

Jakie problemy będą występować?

Głównym problemem komplikującym biznes ochrony, w tym usługi monitoringu sygnałów alarmowych i zdalnego dozoru wizyjnego, będzie niedobór odpowiednio wykwalifikowanych pracowników. Takich, którzy nowe tendencje – zarówno w obszarze technicznym, jak i organizacyjnym – będą potrafili zauważyć, zagospodarować, a następnie wdrożyć i na tym zarabiać. Firmom, które nie mają obecnie dobrze działających działów technicznych i odpowiedniego know-how, będzie trudno zbudować to od podstaw.

Rosnące zarobki to dobre zjawisko pod każdym względem. Jednym z jego skutków jest wzrost kosztów ochrony fizycznej, na którą będzie stać coraz mniej klientów. Zamiast nich pojawia się technologia.

Z pewnością dla wielu problemem okaże się brak świadomości zmian, jakie właśnie obserwujemy – zarówno w obszarze technologicznym, jak i biznesowym. Sporo firm uważa, że dysponuje nowoczesną technologią, mimo że to rozwiązania przestarzałe i nieefektywne. Firmy, które zamykają się na nowe rozwiązania, z pewnością czeka zimny prysznic…

Stosowanie nowych technologii, takich jak współczesny monitoring alarmowy i zdalny dozór wizyjny wymaga oprócz odpowiedniego know-how, którego nie da się po prostu kupić. Potrzebne jest doświadczenie, którego nabiera się z czasem i wraz z liczbą monitorowanych obiektów. Firmy, które próbują odważnie podchodzić do biznesu, mogą początkowo spotkać się z negatywnymi skutkami nieumiejętnego zastosowania nowoczesnej techniki, np. analityki wideo, transmisji dużej liczby danych itp., lecz mimo to warto w nią inwestować.

Istotnym problemem jest zmiana świadomości zamawiających usługi. Pomijam kwestie stawek. Chodzi głównie o to, że świadomość nowych rozwiązań stosowanych w ochronie jest jeszcze niewielka wśród klientów – głównie w obszarze zamówień publicznych, ale również klientów indywidualnych i małego biznesu. Coraz częściej będziemy obserwować, że powielane od lat SIWZ-y nie będą pasować do rzeczywistości. Mentalność będzie trudno zmienić, ale to proces nieunikniony.

Podsumowanie

Na rynku ochrony osób i mienia czekają nas bardzo interesujące czasy. Wiele firm rezygnuje z prowadzenia biznesu w tym obszarze, zamiast nich pojawiają się nowe, które wykorzystują nowe technologię i świeże, współczesne podejście do tego biznesu. Duzi gracze poszukują i inwestują w nowe technologie. Dla mniejszych firm dostępne są rozwiązania w chmurze, z których coraz odważniej zaczynają korzystać. Rozwój technologiczny w tej branży jeszcze nigdy nie był taki dynamiczny, a zaawansowane rozwiązania tak skuteczne i dostępne.

Warto też odnieść się do konsolidacji firm branży ochrony. To zagadnienie wielopłaszczyznowe, z którym mamy też do czynienia w innych branżach. Nie demonizowałbym tego zjawiska. Trzeba nauczyć się podejmować decyzje biznesowe na chłodno i zapomnieć o „etosie ochrony".

Jeżeli firma zbuduje mocne podwaliny technologiczne i organizacyjne, to albo będzie przynosiła duże zyski właścicielom, albo stanie się łakomym kąskiem dla większego. W obu przypadkach właściciel zyskuje, a chyba o to chodzi w biznesie. Dlatego warto inwestować w nowe rozwiązania i *know-how,* podnosząc tym wartość firmy. Wiele z nich jeszcze „stoi na peronie", obserwując odjeżdżający pociąg. W najbliższych 2–3 latach jeszcze będzie miała szansę wsiąść. Później może być problem z dogonieniem liderów zarówno ogólnopolskich, jak i lokalnych.

Ostatnim elementem tej układanki jest człowiek. Rosnące zarobki to dobre zjawisko pod każdym względem. Jednym z jego skutków jest wzrost ceny ochrony fizycznej, na którą będzie stać coraz mniej klientów. Zamiast nich pojawia się technologia. Niezależnie z której strony podejdziemy do tematu, na pierwszy plan wysuwa się technologia… ▮

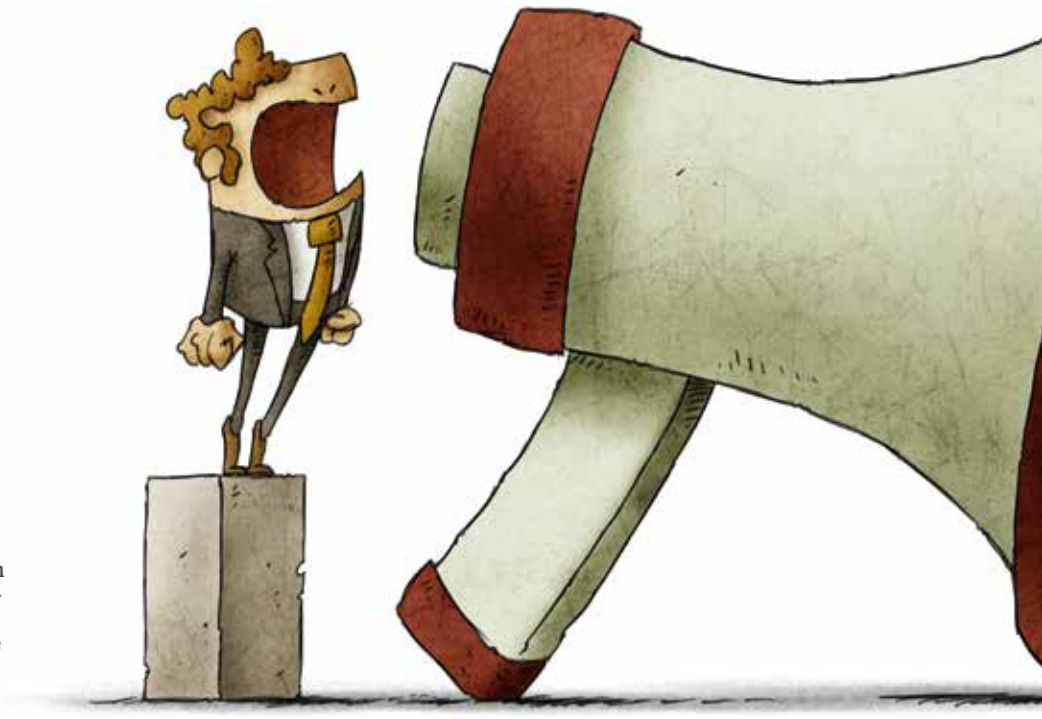
BIO

Krzysztof Ciesielski
Doświadczony ekspert od ponad 20 lat związany z branżą ochrony i zabezpieczeń elektronicznych. Specjalizuje się w nowoczesnych rozwiązaniach w chmurze w monitoringu sygnałów i zdalnym dozorze wizyjnym.

PROBLEMY W OCHRONIE

Z PUNKTU WIDZENIA KLIENTA

Rynek ochrony w Polsce jest bardzo rozdrobniony. Wynika to m.in. z tego, iż wiele firm powstało pod kątem konkretnego klienta. **Oferowanie usług o nieodpowiedniej jakości przy silnej konkurencji powoduje, że część z nich pozostaje podmiotami niszowymi.**



BIO

Krzysztof Wilczyński
Związany z obszarem bezpieczeństwa od 2002 r. Ma bogate doświadczenie w sektorze produkcyjnym, obiektach handlowych, jednostkach wojskowych i placówkach dyplomatycznych oraz przy zabezpieczaniu imprez masowych. Obecnie zajmuje się branżą logistyczną.

Krzysztof Wilczyński

Duże ogólnopolskie spółki – pomimo wprowadzenia stawki minimalnej za godzinę – wciąż konkurują ze sobą tylko ceną za usługę. Marzenia klientów o tym, że nagle w ochronie pojawią się rośli panowie z wysokim ilorazem inteligencji nie zmaterializowały się. Oprócz podwyżek kosztów ochrony wynikających ze zmian w prawie nic się nie zmieniło. Firmy poważanie traktujące swoje bezpieczeństwo są zmuszone zatrudniać security managerów, ponieważ koncesjonowani dostawcy usług patrzą tylko przez pryzmat własnegobiznesu, nie zwracając uwagi na potrzeby klienta. A przecież Henry Ford kiedyś powiedział: *Bacz wpierw na oddawanie usług, zanim spojrzysz na zysk.*

Wielokrotnie badałem koszty usług ochrony, przygotowując szczegółową specyfikację zamówienia, aby móc porównać stawki poszczególnych firm. W czasie spotkań z usługodawcami wyrażałem potrzebę spojrzenia na obiekt świeżym okiem i zaproponowanie bardziej wydajnego modelu ochrony niż obecnie funkcjonujący. Wszyscy uznawali, iż to, co sam wyszczególniłem, jest najlepsze. Nie mieli uwag, dostali gotowca.

Brak jest odpowiedniego nadzoru nad usługą. I nie mam na myśli nadzoru nad pracownikami (ponieważ logiczne jest, iż pracodawca odpowiada za swoich pracowników), ale całościowy nadzór nad realizacją usługi. Po pewnym czasie okazuje się, iż jest nawet problem z zakupem toneru do drukarki, zresztą po co pracownikowi ochrony drukarka – pewnie i tak się nie nauczy obsługi albo zaraz ją uszkodzi. Nie wiem, dlaczego cały czas bez wpisania do umowy szczegółowych zapisów firmy nie wyposażają pracowników w podstawowe narzędzia pracy, a nawet jeśli w umowie jest wpisany laptop, to okazuje się, iż nie ma pakietu Office lub posiada tak stare oprogramowanie, że może służyć tylko jako eksponat.

> Firma, która rośnie dzięki rozwojowi i ulepszeniom, nie zginie. Ale kiedy przestaje być twórcza i tylko produkuje – już po niej.

Drugą ważną kwestią jest brak proaktywności ze strony dostawców, uprzedzania oczekiwań klientów. Każdy klient życzyłby sobie, aby usługa była realizowana kompleksowo, a przedstawiciele firm, idąc z duchem czasu, obniżali koszty klienta, wprowadzając innowacyjne rozwiązania. Niestety to tak nie działa. Oprócz osób ze strony klienta, które analizują corocznie dane, koszty ochrony i nowe dostępne rozwiązania na rynku, nikt nie wychodzi naprzeciw – bo po co? Im więcej ludzi, tym więcej godzin, a im więcej godzin, tym więcej kasy, więc po co coś zmieniać. Lepiej wmawiać klientowi, iż obecnie jest świetnie i już nic nie da się zrobić pod kątem optymalizacji kosztów.

Cytowany już Henry Ford powiedział: *Firmy, które rosną dzięki rozwojowi i ulepszeniom, nie zginą. Ale kiedy firma przestaje być twórcza, kiedy uważa, że osiągnęła doskonałość i teraz musi tylko produkować – już po niej.* A przecież czasem wystarczyłoby zmienić zapisy procedury – tylko tyle albo aż tyle. Często zdarza się, iż ochrona realizuje wiele czynności, które niczego nie wnoszą, albo tworzy dużo różnych raportów, w większości powielających te same dane lub archiwizowane w różnej formie tylko po to, aby pokazać, że coś robi. Czasy, gdy pracowitość pracowników ochrony postrzegano przez godziny spędzone w pracy, już dawno minęły i nie wrócą. Teraz ważne są efekty pracy. Jest duża różnica pomiędzy udawaniem, że się pracuje a samą pracą. Nie wnosi żadnej wartości dodanej grupka ładnie ubranych osób czy profesjonalnie opracowana dokumentacja obiektowa, skoro roczne braki inwentaryzacyjne przekraczają przyjęty budżet.

Ostatnie zagadnienie dotyczy zasady odpowiedzialności. Czytałem wiele umów z firmami ochrony. Większość z nich jest napisana w taki sposób, iż w chwili wielkiej próby, tj. faktycznie poniesionej straty przez klienta, dostawca i tak za nic nie odpowiada. Po co więc ochrona? Chyba tylko dla niższej składki własnego ubezpieczenia. Zawsze jest to samo tłumaczenie – taką mamy polisę z ubezpieczycielem. Bez odpowiedzialności nie ma zaufania i profesjonalnej usługi.

Mam nadzieję, że stale rosnące koszty pracy spowodują, iż firmy zaczną w końcu proponować klientom rozwiązania szyte na miarę. Na początek proponuję, aby w umowach realizowały zapisy zawarte w ofertach, by nie stały się jak obecnie tylko pustymi sloganami.

PRACOWNIK I JEGO KOMPETENCJE CYFROWE

jako obiekt ochrony informacyjnej

Żyjemy w XXI wieku niesieni informacyjną III falą rozwoju społecznego, której podstawowymi atrybutami są cyfryzacja wiedzy i informatyzacja systemów przetwarzania, jako wsparcie dalszego rozwoju i doskonalenia człowieka.
A jak on sam się w tym wszystkim odnajduje?

Marek Blim

Wszak coraz częściej mówimy o wykluczeniu informatycznym sporej części naszej społeczności niezbyt umiejącej nadążyć za rozwojem I&CT, więc może trzeba uporządkować oraz uzupełnić wiedzę i kompetencje cyfrowe pracowników. Najpierw określmy, na jakim poziomie są one obecnie klasyfikowane w Polsce w porównaniu do społeczeństw Unii Europejskiej. Kompetencje cyfrowe [1] to podstawowe umiejętności pozwalające na komunikowanie, pozyskiwanie informacji oraz tworzenie treści w środowisku cyfrowym. *Do bardziej zaawansowanych kompetencji cyfrowych, cenionych wśród pracodawców, należą kompetencje odnoszące się m.in. do specyficznych zastosowań ICT (Information and Communication Technologies – technologie informacyjno-komunikacyjne) w różnych obszarach działalności pracowniczej i biznesowej, np. zarządzanie finansami, kontaktami z klientem i procesami logistycznymi, komunikacja w zespołach, kontakty z instytucjami publicznymi* – twierdzi Anna Majos, młodszy analityk DELab UW [1].

Chcąc uwypuklić poziom kompetencji cyfrowych polskich pracowników MŚP na tle UE, przedstawiono dane pochodzące z bazy danych Eurostatu w podziale na trzy grupy funkcjonalne:
– UE15 (tzw. stara Unia, czyli kraje, które przystąpiły do Unii Europejskiej przed 2004 r.),
– NMS12 (*New Member States* – kraje, które przystępowały do Unii od 2004 r. – bez Polski),
– Polska, jako wyodrębniona kategoria informacyjna.

Wykresy przedstawiają kompetencje odpowiednio: w uję-

BAZA DANYCH STATYSTYCZNYCH UE (EUROSTAT) W OBSZARZE KOMPETENCJI CYFROWYCH WYRÓŻNIA CZTERY KATEGORIE [2]

komunikacja, do której należą:
- zdolność do porozumiewania się w środowiskach cyfrowych,
- działanie za pośrednictwem narzędzi internetowych,
- współpraca za pomocą narzędzi cyfrowych,
- interakcja i uczestniczenie w społecznościach i sieciach,
- świadomość międzykulturowa,

informacja, do której należą osoby wykazujące zdolność do:
- znalezienia odpowiednich informacji w Internecie oraz ich identyfikowania, lokalizowania, pobierania, przechowywania, organizowania i analizowania,

rozwiązywanie problemów:
- zdolność do zarządzania plikami,
- umiejętność zmieniania ustawień oprogramowania,
- korzystanie z usług online,

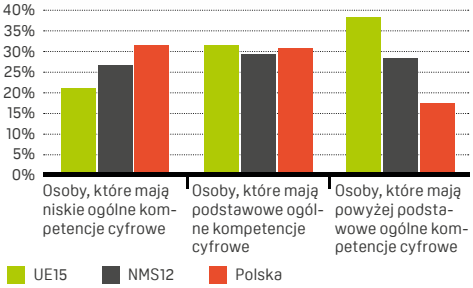
umiejętności w zakresie wykorzystania programów, które obejmują:
- zdolność do korzystania z edytorów tekstu, arkuszy kalkulacyjnych i programów do edycji multimediów,
- zdolność do tworzenia i edytowania nowej zawartości,
- zdolność do łączenia i ponownego wyszukania dotychczasowej wiedzy i treści,
- zajmowanie się oraz stosowanie praw własności intelektualnej i licencji.

ciu ogólnym oraz dane wybrane w zakresie wykorzystania oprogramowania w odniesieniu do poziomu ponadpodstawowego, tzn.

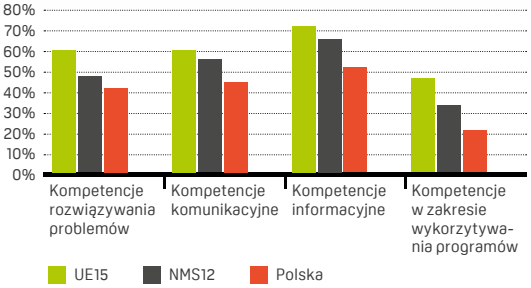
– tworzenie prezentacji lub dokumentów tekstowych, zdjęć, tabel i wykresów,
– używanie zaawansowanych funkcji arkusza kalkulacyjnego do porządkowania i analizowania danych,
– napisanie kodu w języku programowania.

Podstawowym problemem w ocenie kwalifikacji i kompetencji polskich pracowników MŚP staje się nie ocena statystyczna (Eurostat), ale codzienne porównania skuteczności działania. Wśród polskich pracowników przeważają osoby posiadające niskie lub podstawowe kompetencje cyfrowe. Co trzeci polski zatrudniony ma niskie ogólne kompetencje cyfrowe, w UE jest to co piąta osoba. Polscy pracownicy znacznie rzadziej niż pracownicy UE15 mogą wykazać się ponadpodstawowymi kompetencjami cyfrowymi (18–38%).

Poziom ogólnych kompetencji cyfrowych



Poziom ponadpodstawowych kompetencji cyfrowych



Dlaczego w sposób szczególny zwracamy na to uwagę? Ponieważ efektem tych zaniedbań jest łatwość przekonania polskiego pracownika do mimowolnego przekazania osobie nieuprawnionej wielu istotnych tajemnic firmy (*spear-phishing*), a droga do tego prowadzi przez zaniedbania w ochronie danych osobowych pracowników.

Literatura

[1] Majos A., *Kompetencje cyfrowe pracowników MŚP. Polska na tle UE.* Biuletyn Euro-Info, 1/2017

[2] https://stat.gov.pl/statystyka-miedzynarodowa/instytucjeorganizacje-miedzynarodowe/ess-eurostat/

Intersec Dubai 2018

XX edycja

Ponad 1300 wystawców z 59 krajów, 60 tys. m² powierzchni wystawienniczej, w tym 15 pawilonów krajowych. Jedne z największych targów security na świecie odbyły się 21-23 stycznia w Dubaju.

Mariusz Kucharski
korespondencja z Dubaju

Podczas XX edycji Intersec Dubai zaprezentowano produkty ponad 5 tys. marek. O wielkości rynku security na Bliskim Wschodzie stanowią liczby – podczas pierwszej edycji targów prezentowało się zaledwie 61 wystawców, a cały rynek zabezpieczeń w tym regionie był wyceniany na 52 mln USD. Obecnie jego wielkość szacuje się na 12,2 mld USD, przy rocznym tempie wzrostu na poziomie 33 procent!

Ten potencjał dostrzegają firmy z całego świata, licząc na wykrojenie dla siebie jak największego kawałka bliskowschodniego budżetu na rozwiązania z zakresu security. W wejściu na ten rynek pomaga wiele krajowych organizacji branżowych, które zorganizowały własne pawilony wystawiennicze. Na taką formę promocji rodzimych firm zdecydowały się m.in. silne gospodarczo Niemcy, Włochy, USA i Kanada, azjatyckie potęgi Chin, Korei Południowej czy Indii oraz (po raz pierwszy) Rosja, a nawet małe Czechy, które zgromadziły w swoim pawilonie 12 wystawców.

Polska nie miała własnego pawilonu, nasz rynek reprezentowały cztery firmy. Jak mówili nasi rozmówcy, na ten rynek zdecydowanie warto wejść nie tylko ze względu na jego dynamiczny rozwój, ale także gotowość do wdrażania najnowocześniejszych rozwiązań i chęć inwestycji w innowacje. To właśnie tutaj, w Dubaju, spełniają się marzenia o najwyższych budowlach czy najnowocześniejszych rozwiązaniach architektonicznych, a także najbardziej zaawansowanych i innowacyjnych rozwiązaniach z dziedziny zabezpieczeń.

Robert Pestka
dyrektor ds. handlowych, Polon-Alfa

W targach Intersec w Dubaju uczestniczyliśmy po raz pierwszy. Organizacja, odwiedzający i ogromne zainteresowanie produktami Polon-Alfa spełniły nasze oczekiwania. Jestem przekonany, że przyniesie to wymierne korzyści dla naszej firmy i naszych partnerów handlowych z Bliskiego Wschodu.

W Dubaju zaprezentowaliśmy zarówno nowości, jak i wyroby znane już na rynku europejskim. Nasze produkty podlegają ciągłemu procesowi rozwoju. Motywują nas klienci, z którymi rozmawiamy m.in. na targach. Jesteśmy otwarci na ich potrzeby, wsłuchujemy się w oczekiwania, nasze wyroby są najwyższej jakości i znajdują kolejnych odbiorców.

W Dubaju mieliśmy okazję przeprowadzić wiele rozmów i prezentacji. Teraz nadszedł czas wytężonej pracy, mającej na celu podtrzymanie kontaktów – spotkania i przygotowanie ofert. Jestem optymistą co do rezultatów, tym bardziej że już pozyskaliśmy pierwsze zamówienia.

Wśród odwiedzających zaciekawienie budził fakt, że jesteśmy firmą z Polski i produkujemy w Polsce. Dla klientów z Bliskiego Wschodu ma to znaczenie. To, że jesteśmy krajem europejskim, daje gwarancję jakości i bezpośrednio przyczynia się do pozytywnego postrzegania marki już na samym początku.

Mamy bogate doświadczenie związane z organizacją i uczestnictwem na targach czy konferencjach, więc jesteśmy w tym zakresie samowystarczalni . Uważam jednak, że dla każdej firmy ekspozycja w pawilonie krajowym byłaby ułatwieniem wejścia na dany rynek.

Zygmunt Rafał Trzaskowski
dyrektor generalny, Hertz Systems

Widząc potencjał i zapotrzebowanie na nasze rozwiązania, postanowiliśmy po raz kolejny zaprezentować swoje autorskie projekty na Bliskim Wschodzie. Na Intersec debiutowaliśmy w 2017 r. Tym razem zdecydowaliśmy się powiększyć zarówno stoisko, jak i prezentowany asortyment.
Organizator targów łączy swoje doświadczenie europejskie z kulturą Bliskiego Wschodu, co sprawia, że czujemy się tu bardzo dobrze i widzimy realne szanse sprzedażowe. Jeżeli chodzi o frekwencję, wydaje się nam, że globalnie była niższa od ubiegłorocznej, chociaż nam udało się nawiązać więcej kontaktów niż w roku ubiegłym. Potwierdza to słuszność promocji naszych rozwiązań w tym rejonie świata.
Na tym rynku jesteśmy już rozpoznawalną marką i jeszcze przed targami mieliśmy umówionych wiele spotkań z klientami poznanymi rok wcześniej oraz z kontrahentami, z którymi nawiązaliśmy kontakty dzięki stałej współpracy z partnerami z regionu. Podczas targów wiele osób wspominało ubiegłoroczne spotkanie i gratulowało rozwoju naszego systemu.
System antydronowy, nasz innowacyjny produkt, jest rozwiązaniem pożądanym przez wiele instytucji rządowych i nie tylko. Rynek dostawców i odbiorców jest daleki od nasycenia. Daje nam to przewagę produktową nad innymi firmami, które oferują produkty bardziej powszechne.
Temat pochodzenia naszej firmy pojawiał się w rozmowach bardzo często, a większość odwiedzających była zadowolona, że produkt ma pochodzenie europejskie, a nie np. azjatyckie.

Zorganizowanie polskiego pawilonu na takich targach byłoby bardzo pomocne. Byłaby to promocja nie tylko konkretnych firm, ale również polskiej myśli inżynieryjnej i innowacyjności. Europejski rodowód ma na Bliskim Wschodzie niebagatelne znaczenie. Z punktu widzenia wystawcy koszty stoiska w pawilonie narodowym byłyby zapewne niższe, o wzajemnym wsparciu poprzez networking nie wspominając...

Radosław Pasierb
inżynier serwisu, Ambient-System

W targach w Dubaju uczestniczyliśmy po raz drugi. Widać już efekty naszej obecności – nawiązaliśmy kontakty z wieloma potencjalnymi partnerami, z którymi rozmawiamy na temat przyszłej współpracy.
Odwiedzający reprezentowali właściwie każdy segment rynku – począwszy od niewielkich firm instalatorskich szukających nowego produktu, po duże firmy zainteresowane dystrybucją w swoich obszarach działania.
Każdy nowy rynek wymaga wypromowania marki w najlepszy możliwy sposób. Międzynarodowe targi z sekcjami tematycznymi są doskonałym miejscem służącym promocji własnych produktów, nawiązaniu nowych i podtrzymywaniu już nawiązanych kontaktów biznesowych. Każdy z naszych rozmówców interesował się pochodzeniem firmy i krajem produkcji. Zauważyliśmy, że klienci z Bliskiego Wschodu doceniają europejskie produkty, utożsamiając je z wysoką jakością wykonania i ciekawym designem. Jesteśmy dumni z naszej oferty. Nie ukrywam, że możliwość ekspozycji w polskim pawilonie ułatwiłaby promowanie polskich marek poza granicami kraju.

Maciej Żółciński
członek zarządu, TM Technologie

Na Intersec prezentowaliśmy naszą ofertę po raz pierwszy. Do tej pory uczestniczyliśmy w targach w Polsce (Targi Światło, Warszawa i Energetab, Bielsko-Biała) i za granicą (Light & Buliding, Frankfurt i Interlight, Moskwa).

Same targi zostały zorganizowane perfekcyjnie, „po niemiecku" – gratulacje dla organizatorów, Messe Frankfurt. Byliśmy też pozytywnie zaskoczeni frekwencją na naszym stoisku, a duże zainteresowanie wzbudzało nasze europejskie pochodzenie.
Już widać, efekty naszej obecności w Dubaju – zaraz po targach odbyliśmy spotkania z zainteresowanymi firmami.
Sami zorganizowaliśmy swój pobyt na targach i wybudowaliśmy stoisko, ale na pewno dla wielu innych polskich firm wystawianie się w polskim pawilonie byłoby pomocne.

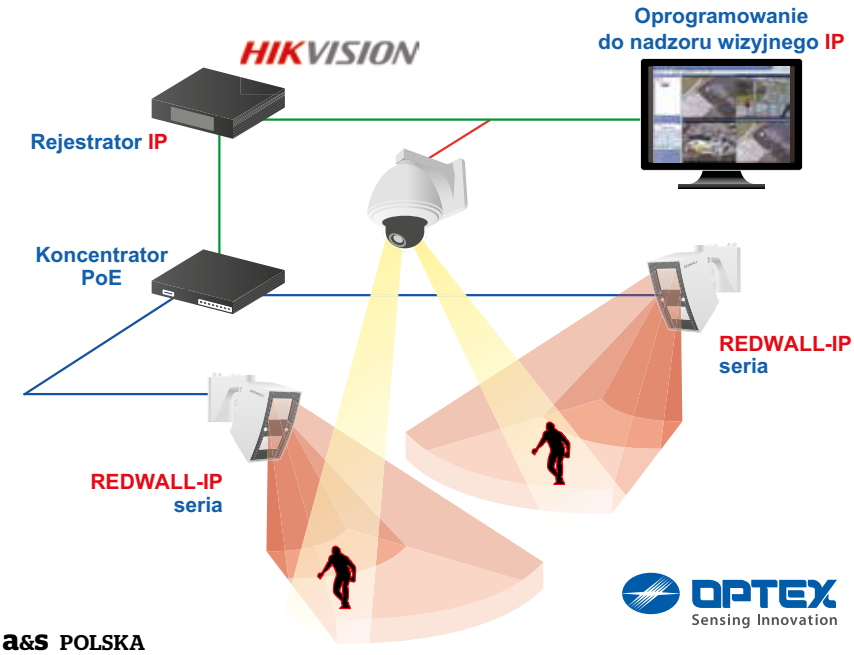
Zarządzanie treścią na wyświetlaczach Digital Signage

Dahua Technology wprowadza na rynek nowe rozwiązania Digital Signage. Autorskie oprogramowanie Media Publish System (MPS) do zarządzania i publikacji treści na wyświetlaczach umożliwia wyświetlanie filmów, zdjęć itp. na różnego typu nośnikach, w tym na monitorach LCD lub ścianach diodowych.

Do sprzedaży zostaną też wprowadzone wyświetlacze LCD – naścienne lub w formie totemu informacyjnego (na razie w wersji do użytku wewnętrznego) z wbudowanym odtwarzaczem SoC (*System on Chip*) opartym na systemie Android. Do urządzeń bez wbudowanego SoC (np. ściany wideo i projektów) firma proponuje zewnętrzny odtwarzacz o wysokich parametrach wyświetlania w rozdzielczości 4K.
Oprogramowanie MPS umożliwia także dodawanie strumieni wizyjnych z kamer Dahua lub innych kompatybilnych z protokołem ONVIF, a następnie wstawienie do wcześniej utworzonego szablonu i wyświetlenie w danym harmonogramie.
Tworzenie nowej treści i zarządzanie nią oraz tworzenie nowych harmonogramów odbywa się poprzez prosty interfejs w przeglądarce, z podziałem na typy użytkowników i lokalizacje. Wszelkie pliki są zachowywane w bazie danych serwera, co pozwala na zdalny dostęp z sieci lokalnej lub publicznej (wymagane publiczne IP serwera) po uwierzytelnieniu w systemie.

Inf. Dahua Technology

Skuteczna ochrona obwodowa dzięki integracji Optex i Hikvision



Optex – największy na świecie producent czujek zewnętrznych oraz Hikvision – międzynarodowy lider wśród dostawców produktów i rozwiązań monitoringu wizyjnego, opracowali zintegrowane rozwiązanie do ochrony obwodowej.

W rozwiązaniu tym czujki Optex z serii REDWALL wspierają działanie kamer IP i rejestratorów Hikvision. Połączenie detekcji ruchu w kamerze z zewnętrzną czujką ruchu zmniejsza liczbę fałszywych

Innowacyjna PanoVIX od IntelliVIX

PanoVIX jest innowacyjnym rozwiązaniem składającym się z kamery panoramicznej o kącie widzenia 180º oraz dedykowanego jej oprogramowania. Obraz z 4 kamer o rozdzielczości 3 Mpix jest składany z wykorzystaniem technologii łączenia obrazu (*Stitching Technology*), dzięki czemu powstaje obraz panoramiczny bez żadnych zniekształceń i martwych stref.
Rozwiązanie umożliwia powiększenie pola widzenia i rejestrację obrazu, a także udostępnia wirtualną kamerę PTZ. Ponadto PanoVIX pozwala na zastosowanie różnych funkcji analizy obrazu. Kamera PanoVIX ma kompaktowe wymiary (średnica 250 mm, wysokość 89,2 mm) i jest łatwa w instalacji.
Dzięki wbudowanej grzałce, wiatrakowi chłodzącemu i konstrukcji zapobiegającej skraplaniu się wody może pracować na zewnątrz. Idealnie sprawdzi się w monitorowaniu obszarów o dużej powierzchni, takich jak parkingi, lotniska, porty morskie, stadiony czy granice państwa.

Inf. IntelliVIX

alarmów wywoływanych przez zmiany oświetlenia, opady atmosferyczne czy owady. Ma to znaczenie szczególnie w rozbudowanych systemach, w których operator musi reagować na sygnały z wielu źródeł. Oprogramowanie Optex zainstalowane w rejestratorach NVR Hikvision aktualizuje się wraz z *firmware*, dzięki czemu ustawienia integracyjne nie są tracone.

Urządzenia wykorzystujące tę integrację:
- HIKVISION I-SERIES NVR Firmware
- DZ_K51_EN_STD_ V3.4.93_170502

Wspierane wersje *software* Optex:
- Redscan RLS-3060L/SH v7.13+
- Redscan RLS-2020I/S v1.43+
- PIE-1 v1.2.0+

Informacje na temat czujek REDWALL-IP oraz współpracujących urządzeń Hikvision: optex@optex.com.pl

Skok w nowy rok

Branża ochrony wciąż rośnie w siłę. Wzrasta rola zabezpieczeń technicznych. W 2017 r. wartość rynku security przekroczyła 10 mld zł, i to mimo wzrostu płac, które można było stopniowo i mniej boleśnie podnosić od lat, co poprawiłoby przy okazji autorytet branży.

Zawsze mówiłem, że ekonomia nie zauważa hamującego bodźca, jakim jest chciwość. To widać szczególnie na przełomie roku, gdy niektórzy podniecają się firmowymi fuzjami – kto kogo przejmie – a które dotyczą nielicznych właścicieli biznesów security: fizycznych, technicznych i dystrybutorskich. A tak chciałbym wiedzieć, co firmy, zwłaszcza polskie, wniosą ciekawego na rynek. I nie mam na myśli implementacji tego, co wymyślono gdzie indziej.

Od pół roku trwa budowa najdłuższego tunelu drogowego w Polsce, i to nie na południu kraju, ale w Warszawie. Taka inwestycja korzysta z wielu urządzeń i technologii zabezpieczeń technicznych oraz architektury specjalnej. Pierwszy raz przekonałem się o tym, gdy 11 lat temu pisałem reportaż do „Systemów Alarmowych" o tunelu drogowym biegnącym przez środek Katowic (DTŚ – Drogowa Trasa Średnicowa). Wentylacja, różne czujniki i kamery, pomieszczenia ucieczkowe… Tunel pod Ursynowem jest większym wyzwaniem technicznym. Prawie 2,4 km to jak na Polskę imponująca długość. Czy wszystko mi się podoba? Nie. Ma nim jeździć podobno do 7,5 tys. samochodów na godzinę (180 tys. na dobę), a 15-metrowe – niewysokie w porównaniu do domów mieszkalnych – kominy wlotowe i wylotowe umiejscowiono na krańcach tunelu. Na dodatek nie chcą w nich zamontować elektrofiltrów. To się nazywa cios w bezpieczeństwo publiczne. I to w sytuacji, gdy zaczęto podawać dane smogowe i wzrosła świadomość zagrożeń. Mieszkańcy wywalczyli na razie to, że przez rok sytuację będą monitorować czujniki wzdłuż trasy. Jest jakiś mądrzejszy decydent?

Trwa serial o budowli ochronnej, także w naszych felietonach, pod nazwą mur Trumpa. Odnotujmy zmiany koncepcji. Imponująca jego długość 3300 km – bo tyle ma granica USA z Meksykiem – już uległa drastycznemu skróceniu. Departament Bezpieczeństwa Publicznego przekazał senatorom plan inwestycji. Ma w ciągu 10 lat kosztować 18 mld dolarów. Trump zakładał 8, które miał zapłacić Meksyk. Na biednego nie trafiło. Projekt przewiduje budowę nowych zapór na odcinkach 560 km oraz wymianę starych barier różnego typu na długości ok. 1050 km. Skracając pierwotną długość, zauważono, że granica ma wiele trudnych do przekroczenia naturalnych miejsc, gdzie bez pomocy władz można skręcić kark lub utonąć. Prezydent już wystąpił do Kongresu o finanse na budowę 120 km pierwszej fazy muru – to 1,6 mld dolarów – na styku Teksasu z Meksykiem. Senatorowie z opozycyjnej Partii Demokratycznej nazwali to marnotrawieniem pieniędzy podatników.

Odnotuję nowelizację kodeksu karnego zakładającego poszerzenie granic obrony koniecznej, już obowiązującą. Temat jest niełatwy, a ocena sytuacji często zależy od niewymiernych okoliczności. Jak np. udowodnić, że strzelający na własnym podwórku do nieuzbrojonego, uciekającego włamywacza był w panicznym strachu na widok jego pleców i rażąco nie przekroczył granic obrony koniecznej? Nowelizacji zarzuca się nieprecyzyjne określenia skutkujące różnymi interpretacjami. Nie jesteśmy mistrzami świata w konstruowaniu dobrego prawa.

Były dyrektor wykonawczy serwisu Facebook wypowiedział się kąśliwie o ekspracodawcy. Uważa on bowiem, że firma dysponująca tak gigantycznymi pieniędzmi nie powinna udawać, że nie ma wpływu na losy świata i jego bezpieczeństwo, a także na to, że kształtuje sposób myślenia. Co robi Facebook, kiedy coraz więcej ziemi znika pod wodą? Wymyśla nowy rodzaj lajków. Facebook – według niego – rozrywa więzi społeczne i jest wciąż bezradny wobec mowy nienawiści. Firma odpowiedziała, że krytykujący odszedł z niej sześć lat temu, sama widzi problem i pracuje nad poprawą.

Spodnie z niespodzianką! Jeden z ciekawszych przemytów w ubiegłym roku. W pewnym bagażu gdańscy celnicy odkryli sadzonki roślin mięsożernych z rodzaju *Nepenthes* – dzbaneczniki. Towar został zgłoszony do odprawy jako odzież męska (spodnie). Podpowiedź dla ambitnych hodowców: w lecie dzbanecznik może być także muchołapką.

BIO

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

8.06.2018 r.

DRUGA MIĘDZYNARODOWA KONFERENCJA

Warsaw Security Summit

Spotkanie liderów rynku security

organizator:

a&S POLSKA

Więcej informacji na:

www.WarsawSecuritySummit.eu

DAHUA

WIODĄCY DOSTAWCA ROZWIĄZAŃ BEZPIECZEŃSTWA

Przez lata firma Dahua Technology była postrzegana jako wiodący dostawca rozwiązań monitoringu z aplikacjami dedykowanymi dla wielu gałęzi rynku światowego takich jak Smart City, inteligentny transport, budynki inteligentne, monitoring mobilny itp. Dedykowane rozwiązania Dahua Technology oraz duże doświadczenia projektowe są wciąż dużą wartością dla Klientów.



Smart City

- Wysoki poziom zabezpieczenia bez tzw. martwych stref
- Efektywne zabezpieczenie granic z technologią termowizyjną
- Szybka odpowiedź na bieżące problemy
- Scentralizowane zarządzanie w tym współdzielenie danych na poziomie miasta, raportowanie stanu ruchu ulicznego, wskazówki dla ruchu itp.

Budynki inteligentne

- Integracja systemów budynkowych w celu redukcji kosztów utrzymania
- Elastyczne i skalowalne systemy dopasowane do potrzeb użytkowników
- Systemy otwarte i kompatybilne z większością standardów przemysłowych
- Zawierające monitoring wizyjny, kontrolę dostępu, systemy wideodomofonowe, systemy alarmowe oraz Inteligentne zamki.

Inteligentny Transport

- Pełne rozwiązanie, redukujące korki w ruchu ulicznym oraz ratujące życie
- Pomoc przy rozładowywaniu dużego ruchu ulicznego
- Wysokiej jakości projektowanie systemów z możliwością elastycznego rozmieszczania
- Zawiera rozpoznawanie tablic rejestracyjnych / sterowanie światłami / pomiar prędkości / systemy parkowania

Monitoring mobilny

- Wiele aplikacji dla autobusów miejskich, szkolnych, samochodów policyjnych, transportu kolejowego itp.
- Wysokiej jakości monitoring w czasie rzeczywistym oraz przy lokalnej rejestracji
- Pewny system zarządzania VMS zwiększający sprawność opieki nad pojazdami
- Śledzenie i lokalizacja pojazdów, monitorowanie i ściąganie informacji poprzez GPS, 3G / 4G / Wi-Fi

CE FC UL RoHS ISO 9001:2000

www.dahuasecurity.com/pl

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