



**POLSKA**

RYNEK  
SECURITY

→ 16

## Podsumowania i prognozy

Jak oceniają miniony rok i czego spodziewają się w 2020? Zapytaliśmy o to przedstawicieli najważniejszych firm działających na polskim rynku security.

NOWOCZESNE  
TECHNOLOGIE

→ 26

## Technologie przyszłości

Hiperautomatyzacja, blockchain, AI, chmura rozproszona czy pojazdy autonomiczne – to przykłady technologii, które całkowicie zmienią nasz sposób życia i pracy.

TEMAT  
NUMERU

→ 46

## Transport i logistyka

Prognozowany rozwój gospodarczy Polski nie będzie mógł się obyć bez inwestycji w segmentach transportu i logistyki. Jakie technologie pozwolą przedsiębiorcom osiągnąć wysoki poziom wzrostu?

# przyszłość security

w w w . a s p o l s k a . p l





# 24/7 VIVID COLOR CAMERA



# DEEP LEARNING

DVR



False  
Alarm Filter



Quick  
Target Search



Target  
Extraction



## WIĘCEJ NIŻ MOŻESZ ZOBACZYĆ TURBO HD 5.0

### HIKVISION NR 1 NA ŚWIECIE

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

### ColorVu

Obrazy w żywych kolorach przez całą dobę

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

### AcuSense

Inteligentna precyzja

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

# Drodzy Czytelnicy

Miniony rok należy zaliczyć do bardzo udanych – tak o 2019 wypowiadają się przedstawiciele najważniejszych firm w branży (s. 16). Jako czynniki wzrostu wskazywano głównie dobrą koniunkturę gospodarczą, inwestycje na rynku nieruchomości (zwłaszcza biurowych) oraz, paradoksalnie, wzrost płacy minimalnej pozytywnie wpłynęły na wyniki finansowe firm security obecnych na polskim rynku. Czy ten rok będzie lepszy? Firmy optymistycznie patrzą w przyszłość.

Jest ku temu powód. Inwestycje w transporcie i logistyce nie zwalniają. W ramach realizacji Programu Budowy Dróg Krajowych podpisano umowy na roboty budowlane o wartości blisko 70 mld zł. Transport kolejowy może liczyć na poparcie rządu i duży zastrzyk pieniędzy – ponad sto mld zł. Ten rok stoi pod znakiem przygotowań do największej inwestycji w kraju – Centralnego Portu Komunikacyjnego (s. 60), który ma rozwiązać problem wyczerpującej się już przepustowości lotnisk na terenie Europy Środkowo-Wschodniej.

Równoległe wciąż rośnie zapotrzebowanie na powierzchnie magazynowe. W tym obszarze poszukiwane są rozwiązania optymalizujące działalność (s. 68) i gwarantujące bezpieczeństwo pożarowe zgodnie z wymogami obowiązujących norm (s. 74). Security managerów czeka gorący okres dostosowywania modelu ochrony do zmieniających się możliwości budżetowych i otoczenia, który wymaga nowego podejścia do zarządzania bezpieczeństwem organizacji (s. 83).

Dużo miejsca w numerze poświęcamy nowoczesnym technologiom. Od nich zależy już niemal każda sfera naszego życia – pokazujemy, w jaki sposób nowoczesne rozwiązania „ulepszają” człowieka (s. 26) i jakie niosą wyzwania. Przybliżamy również wiedzę o blockchainie, coraz popularniejszej technologii, o której wiele się mówi w kontekście bezpieczeństwa i czekającej nas rewolucji autoryzacji danych (s. 32).

W nowy rok wkraczamy pełni werwy i entuzjazmu już jako grupa mediowa a&s Global. W odpowiedzi na zapotrzebowanie rynku rozszerzyliśmy zakres naszych działań o kompleksową działalność promocyjną, eventową i szkoleniową. Już dziś zapraszamy 4 czerwca na konferencję Warsaw Security Summit (s. 91), gdzie spotkają się wybitni specjaliści i uznani eksperci z Polski i zagranicy. Również w czerwcu zapraszamy zmagania z technologią podczas warsztatów strategiczno-terenowych Security BootCamp, na które zapraszamy szefów bezpieczeństwa z firm i instytucji z całego kraju!

**Marta Dynakowska**  
REDAKTOR NACZELNA

**Jan T. Grusznic**  
Z-CIA REDAKTORA NACZELNEGO

**Mariusz Kucharski**  
DYREKTOR ZARZĄDZAJĄCY

**a&s**  
POLSKA

www.aspolska.pl

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

Dyrektor zarządzający  
**Mariusz Kucharski**

Redaktor naczelna  
**Marta Dynakowska**

Z-ca redaktora naczelnego  
**Jan T. Grusznic**

Stały felietonista  
**Andrzej Popielski**

Dział marketingu i reklamy  
**Iwona Krawiec**

Dział eventów i konferencji  
**Jolanta A. Kucharska**  
**Aleksandra Czapska**

Projekt graficzny i skład  
**Bogusław Kalwala**

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

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

Korekta  
**Jolanta Kucharska**

Prenumerata  
www.aspolska.pl/prenumerata

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

a&s Polska jest częścią grupy wydawniczej a&s International.

© Copyright by a&s Polska

A&S POLSKA  
ZŁOTY PARTNER

**AXIS**  
COMMUNICATIONS

**BCS**

**HIKVISION**

**Linc**  
Polska Sp. z o.o.

**SCHRACK**  
SECONET

**TRUSTMAN**

A&S POLSKA  
SREBRNY  
PARTNER

**ahua**  
TECHNOLOGY

A&S POLSKA  
WYDANIE  
ONLINE

www.aspolska.pl/czasopismo

**BCS - NVR0402C-P-III**  
**BCS - NVR0802C-P-III**

**BCS**

dla profesjonalistów

Rejestratory mobilne przeznaczone są do użytku w środkach transportu. Znajdują zastosowanie w pojazdach komunikacji lądowej, wodnej, w pojazdach specjalnych jak samochody konwojowe, transport więzienny, karetki, taksówki oraz samochody ciężarowe każdego typu. Monitoring prowadzony z wnętrza pojazdu może okazać się kluczowy w przypadku próby kradzieży, wandalizmu i napadu. Współcześnie produkowane rejestratory mobilne obsługują kilka technologii komunikacji bezprzewodowej (**Wi-Fi, GPS**) oraz wykorzystują najwyższe standardy kodowania ruchomych obrazów (**H.265**), co sprawia, że otrzymujemy obraz w najwyższym standardzie. Ze względu na swoje zastosowanie, rejestratory mobilne są urządzeniami stosunkowo niewielkich rozmiarów, co sprawia, że nie zajmują dużo miejsca w samochodzie – a to czyni je jeszcze bardziej praktycznymi.

**BCS-DMMIP1501IR-E-Ai**



**NSS Sp. z o.o.**  
ul. Modułarna 11 (Hala IV), 02-238 Warszawa  
tel. +48 22 846 25 31, fax. +48 22 846 23 31 wew.140  
e-mail: info@bcscctv.pl NIP: 521-312-46-74

www.bcscctv.pl



8 Produkty numeru



14 Statystyki

16 Rynek security w Polsce – podsumowanie roku 2019

26 Technologie przyszłości – w służbie człowieka

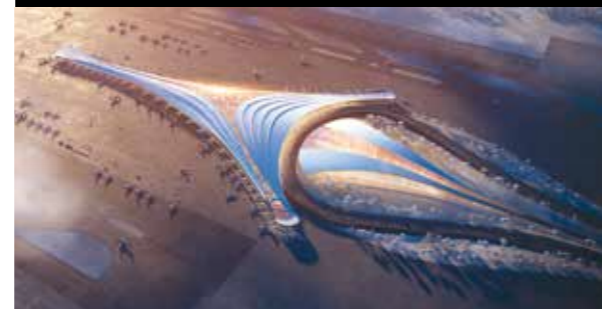
30 5 trendów technologicznych na rok 2020, które pomogą zmienić miasto w *smart city*  
**AXIS COMMUNICATIONS**

32 *Blockchain* – 5 faktów, o jakich powinieneś wiedzieć, a boisz się zapytać  
**JAN T. GRUSZNIC**

38 SLIM-DUAL-LUNA – dualna czujka ruchu z funkcją oświetlenia  
**SATEL**

40 FacePRO od Panasonic na stadionie w Brøndby  
**PANASONIC MARKETING EUROPE**

42 Nowoczesne systemy przyzywowe Schrack Seconet jako element wsparcia w opiece nad seniorami  
**PAWEŁ TOMASZEWSKI, SCHRACK SECONET POLSKA**



46 Rozwiązania transmisji usprawniające działanie kolei  
**A&S INTERNATIONAL**

52 Inteligentne pożegnanie z korkami  
**A&S INTERNATIONAL**

56 Transport przyszłości  
**RAPORT PWC**

60 Centralny Port Komunikacyjny – inwestycja na miarę przyszłości  
– **WYWIAD Z KONRADEM MAJSZYKIEM, DYREKTOREM KOMUNIKACJI I PR CPK**

64 *WinGuard PSIM+* Transport publiczny. Najwyższe standardy bezpieczeństwa w transporcie publicznym  
**C&C PARTNERS**

65 Kamery Hikvision w transporcie  
**HIKVISION POLAND**

66 smartGATE – innowacyjna usługa automatycznej kontroli procesów wjazdu i wyjazdu  
**SECURITAS POLSKA**

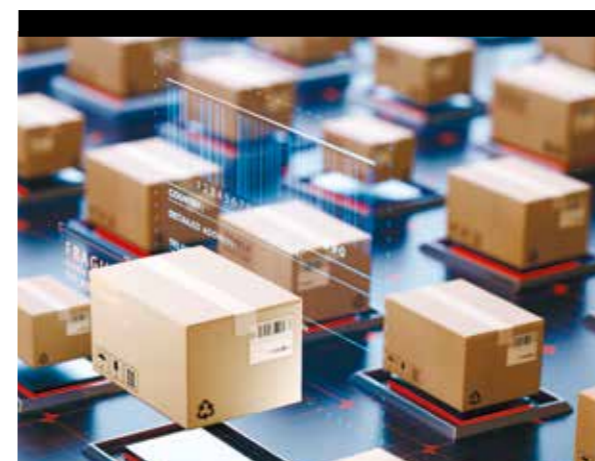
68 Optymalizacja nie może oznaczać ograniczeń  
**KRZYSZTOF WILCZYŃSKI**

69 Głos Branży

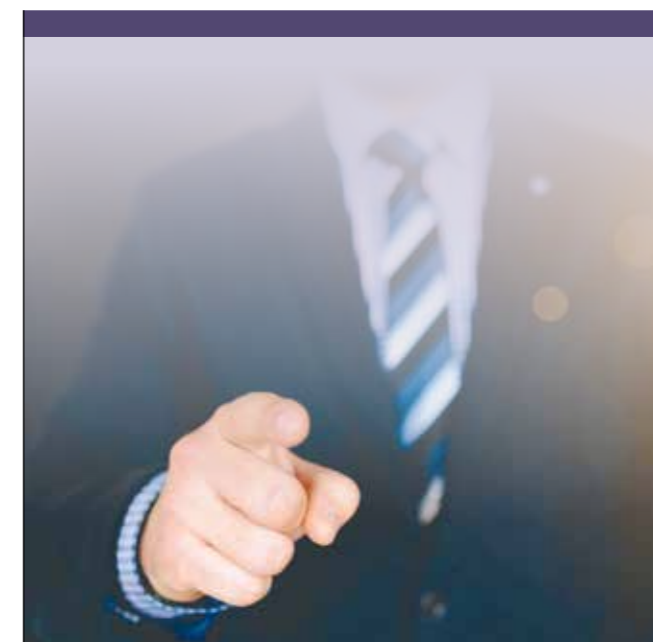


74 Norma NFPA 601 w kontekście bezpieczeństwa centrum logistycznego  
**ŁUKASZ STĘPIEŃ**

79 PROFILE FLEXIBLE – system sygnalizacji pożarowej firmy ZETTLER  
**JOHNSON CONTROLS INTERNATIONAL**



80 Komunikacja za pomocą systemów przyzywowych a ochrona prywatności i godności pacjenta  
**AGATA MARCINKOWSKA, ADRIANNA ŻYREK**



83 *New Security Concept* – nowe podejście do bezpieczeństwa z poziomu zarządzania organizacją  
**RAFAŁ ŁUPKOWSKI**



86 Śniadanie Ekspertów nt. bezpieczeństwa w handlu

88 Informacje branżowe i nowości firmowe



PRODUKT NUMERU

**AXIS COMMUNICATIONS** [www.axis.com/pl](http://www.axis.com/pl)

## AXIS Q1798-LE Sieciowa kamera 4K bez kompromisów

Kamera ma wyjątkowo światłoczuły przetwornik obrazu 4/3". Funkcja Lightfinder 2.0 pozwala na rejestrację obrazów w wysokiej jakości na potrzeby postępowania wyjaśniającego, nawet scen o słabym oświetleniu. Kamera ma rozdzielczość 10 Mpix przy

szybkości do 20 kl./s oraz 4K przy 30 kl./s. Nie wymaga dodatkowego oświetlenia: **AXIS Optimized IR** umożliwia detekcję w ciemnych scenach na odległość do 50 m. Jest wyposażona w obiektyw Canon o zmiennej ogniskowej **12-48 mm**, zapewniając doskonałe widoki szerokokątne o poziomym kącie widzenia **90°**, **4x zoom** i elektroniczną stabilizację obrazu (EIS). Idealnie nadaje się do dozoru rozległych, otwartych przestrzeni, np. na lotniskach, w portach i na stadionach. Dzięki funkcji Lightfinder 2.0 rejestruje obrazy o bardziej realistycznych i nasyconych kolorach i ostrzejsze obrazy poruszających się

obiektów. Dzięki funkcji Zipstream z kodowaniem **H.264** i **H.265** wymagania w zakresie przepustowości i zasobów pamięci masowej są dużo niższe. Nawet w nocy, gdy obraz ma wysoki poziom szumu, wymaga takiej samej przepustowości i zasobów pamięci, jak zwykłe kamery 1080p. Reasumując, zapewnia obrazy o wysokiej rozdzielczości, ma niewielkie wymagania w zakresie przepustowości sieci i umożliwia niespotykane oszczędności przestrzeni dyskowej. Obudowa kamery ma stopień ochrony **IP66**, **IP67** i odporności mechanicznej **IK10**, temp. pracy od **-40°C do 60°C**. Dzięki podpisanemu oprogramowaniu sprzętowemu i bezpiecznemu uruchamianiu można mieć pewność, że zainstalowano tylko autoryzowane i bezpieczne oprogramowanie.



**BCS** [www.bcsctv.pl](http://www.bcsctv.pl)

## Rejestrator BCS NVR6408R-4K-RR

**BCS NVR6408-4K-RR to najwyższej klasy rejestrator IP, który sprawdzi się wszędzie tam, gdzie jest konieczne zapewnienie najwyższej jakości obrazu**, np. w obiektach użyteczności publicznej, rządowych, hotelach, centrach handlowych czy instytucjach finansowych.

Zastosowanie 4-rdzeniowego procesora Intel umożliwia podgląd obrazu w rozdzielczości do 12 Mpix dla uzyskania dokładniejszej identyfikacji obiektów. Dzięki wsparciu dla standardu Onvif 2.4 rejestrator jest kompatybilny z urządzeniami innych producentów. Zastosowanie technologii Hotspare umożliwia wymianę uszkodzonego dysku bez

konieczności wyłączenia rejestratora poprawia jego niezawodność i odporność na ewentualne usterki dysków. Natomiast obsługa RAID 0/1/5/10 zapewnia bezpieczniejsze przechowywanie danych.

Rejestrator ma też funkcje zaawansowanej analizy obrazu: detekcji przekroczenia linii, wtargnięcia w strefę, pojawienia się i zniknięcia obiektu, rozpoznawania twarzy. Z kolei funkcja zliczania osób przechodzących przez wyznaczoną strefę może okazać się przydatna analitykom biznesowym do tworzenia raportów i statystyk. Rejestrator BCS NVR6408R-4K-RR współpracuje z kamerami typu *fisheye*, oferując



funkcje *dewarpingu* (w podglądzie, na żywo i odtwarzaniu) i obsługę mapy cieplnej. Współpracuje też z kamerami do identyfikacji tablic rejestracyjnych, dzięki czemu możliwa jest identyfikacja nadjeżdżającego pojazdu, ewentualne jego otwarcie oraz późniejsze łatwe wyszukanie nagrania na podstawie numerów rejestracyjnych.

**DAHUA TECHNOLOGY POLAND** [www.dahuasecurity.com/pl](http://www.dahuasecurity.com/pl)

## Kamera DH-IPC-HDBW5442EP-ZE z serii Pro dla wymagających

**Nowa kamera z serii Pro jest produktem dla wymagających użytkowników.** Jest wyposażona w przetwornik obrazu 1/1.8" CMOS o rozdzielczości **4 Mpix**, co przy zachowaniu dużej czułości gwarantuje obraz bogaty w szczegóły nawet w warunkach bardzo słabego oświetlenia. Możliwe jest to również dzięki wykorzystaniu obiektywu F.18 o zmiennej ogniskowej w zakresie **od 2,7 do 12mm**.



Wydajny procesor oraz pamięć RAM pozwalają na użycie najnowocześniejszej analizy obrazu.

Najnowszy model zawiera moduł analizy obrazu bazujący na algorytmach sztucznej inteligencji z takimi funkcjami, jak detekcja twarzy i generowanie metadanych na jej podstawie – pleć, okulary, zarost, maskowanie czy zliczanie osób w strefie (dostępne do tej pory wyłącznie w najwyższej serii kamer). Pojawiła się również funkcja *defog* wpływająca na poprawę obra-

zu. Kamera oferuje również funkcje, do których użytkownicy zdążyli się już przyzwyczaić – maska prywatności, przekroczenie linii, detekcja intruza lub zaginięcie obiektu. Zaawansowana analiza obrazu nie wpłynęła na wydajność kamery w zakresie generowania strumieni wizyjnych. Użytkownik nadal ma do dyspozycji trzy niezależne strumienie wizyjne z wykorzystaniem najnowszego kodowania **H.265**.

Smukła, estetyczna obudowa odporna na warunki atmosferyczne (**IP67**) oraz akty wandalizmu (**IK10**) to gwarancja, że kamera jest nie tylko wydajna, ale również pozwala na stabilną pracę w każdych warunkach.

**dahua**  
TECHNOLOGY

# Zobacz każdy szczegół w jego naturalnej postaci

Panoramyczny obraz 180° bez zniekształceń



### Cechy kamery

- Jedna obudowa - trzy przetworniki po 2 Mpx
- Jednolity obraz wysokiej jakości bez podziału sceny
- Panoramyczny obraz 180° bez zniekształceń w rozdzielczości 4K
- Łatwa instalacja
- Wysoki stopień ochrony IP67, IK10



CE FC ISO 9001:2000



**Dahua Technology Poland Sp. z o.o.**

ul. Salsy 2, 02-823 Warszawa  
tel. +48 22 395 74 00, fax +48 22 395 74 10  
e-mail: [biuro.pl@dahuatech.com](mailto:biuro.pl@dahuatech.com)  
[www.dahuasecurity.com/pl](http://www.dahuasecurity.com/pl)



PRODUKT NUMERU

**HIKVISION** [www.hikvision.com/pl](http://www.hikvision.com/pl)

## Kamery ANPR

**Kamery ANPR (Automatic Number Plate Recognition) odczytujące tablice rejestracyjne pojazdów są coraz powszechniejsze. Wspomagają zarządzanie dostępem do obiektów zarówno przemysłowych, jak i mniejszych: parkingi, biurowce, osiedla czy prywatne posesje.**

W obiektach handlowych, gdzie przepływ samochodów jest bardzo duży, automatyczne rozpoznanie numerów rejestracyjnych oznacza nie tylko bezpieczeństwo, ale także zarządzanie. Statystyki budowane na podstawie identyfikacji tablicy rejestracyjnej dają duże

możliwości marketingowe osobom odpowiedzialnym za strategię sprzedaży.

Firma Hikvision wprowadza na rynek dystrybucyjny kamerę **DS-2CD2A25G0/P-IZS**. Zastosowana technologia DarkFighter i duży przetwornik 1/1,8 cala zapewniają czytelny obraz w trudnych warunkach oświetlenia (ciemno, silne światła reflektorów). Obudowa kamery ma stopień ochrony **IP67** i klasę wytrzymałości mechanicznej **IK10**. Obiektyw o zmiennej ogniskowej 2,8-12 mm pomaga odpowiednio skadrować miejsce odczytu tablicy rejestracyjnej, co przy popraw-

nej konfiguracji pozwala osiągnąć skuteczność na poziomie 96%.

Kamera wyposażona w wyjścia przekątnikowe i slot na kartę **SD do 256 GB** może być instalowana jako urządzenie autonomiczne, wówczas listy pojazdów (biała lista, czarna lista – do 10 tys. tablic rejestracyjnych) tworzy bezpośrednio w pamięci kamery, która poprzez wyjścia przekątnikowe sama steruje bramą czy szlabanem.

Systemy monitoringu wizyjnego wykorzystujące kamery **ANPR Hikvision** mogą być zarządzane przez oprogramowanie klienckie **IVMS-4200** lub **Hik-Central**.



**LINC POLSKA** [www.linc.pl](http://www.linc.pl)

## Radar 360 Scan + Kamera Predator – niezawodne połączenie

**Ten praktyczny zestaw to kamera zintegrowana z radarem, automatycznie podążająca za celem wykrytym i śledzonym przez radar. Ponadto kamera jest wyposażona w oświetlacz (zakres do 250 m) oraz 30-krotny zoom optyczny.**

Rozwiązanie jest stworzone z myślą o projektach wymagających detekcji obiektów na krótkim i średnim dystansie, np. w obrębie ogrodzonego lub nieogrodzonego terenu. Szczególne zastosowanie znajduje w ochronie terenów otwartych, np. w miejscach wydobywania złóż naturalnych i ich składowania, na lotniskach, w ochronie granic państwa czy w projektach wojskowych. Średnica zasięgu do 400 m pozwala na śledzenie do 40 celów jednocześnie. Ponadto inteligentna funkcja alarmowania, tzw. **Time Share**, umożliwia dozór

oraz obsługę alarmów z wielu obiektów, proporcjonalnie lub wg priorytetów.

Dzięki wykorzystaniu technologii radarowej można, skanując chronioną powierzchnię w zakresie 360° z częstotliwością dwa razy na sekundę, wykrywać obiekty i śledzić ich ruch. W przypadku wykrycia zagrożenia możliwa jest **transmisja alarmów** do stacji monitorującej w celu ich weryfikacji i podjęcia odpowiedniej reakcji.

Zaawansowana technologia wykrywania za pomocą radaru nie jest zakłócana przez niekorzystne warunki atmosferyczne i środowiskowe, dlatego też **funkcja wykrywania i alarmowania** jest kontynuowana nawet w najtrudniejszych warunkach, np. deszcz, mgła czy śnieg, gwarantując wysoką skuteczność działania.



**OPTEX** [www.optex-europe.com/pl](http://www.optex-europe.com/pl)

## QXI – nowość w ofercie zewnętrznych czujek ruchu OPTEX

**QX Infinity (QXI) to nowa linia zewnętrznych czujek OPTEX. Obejmuje modele PIR i dualne (PIR+MW).** W skład serii **QXI** wchodzi czujki o kącie detekcji **120°** i zasięgu 12 m, dostępne są modele przewodowe oraz zasilane bateryjnie. Eleganckie i kompaktowe czujki **QXI** mają niewielkie wymiary. Są odpowiednie do każdego budynku mieszkalnego lub komercyjnego, zapewniając niezawodną detekcję ruchu, przy równoczesnym ignorowaniu ruchu małych zwierząt.

**Technologia QUAD w połączeniu z logiką AND** Czujki **QXI** mają precyzyjnie rozmieszczone podwójne wiązki **PIR** pracujące w logice **AND** (piroelement **QUAD** – cztery elementy światłoczułe). Wszystkie modele są wyposażone w cyfrowo wspomaganą technologię rozpoznawania sygnału, określaną jako **SMDA**. Analizuje

wzorec detekcji i zmiany w otoczeniu, np. warunki atmosferyczne i ruch roślinności, eliminując zakłócenia i przyczyniając fałszywych alarmów.

**Wybór wysokości montażu i wzorca detekcji** W przypadku montażu na wysokości **2,2-2,7 m czujka** zapewnia wielopoziomową detekcję, umożliwiającą ignorowanie niewielkich zwierząt. W przypadku obecności większych zwierząt czujkę montuje się na wysokości **0,8-1,2 m**.

**Łatwy montaż i konfiguracja** Jak zwykle firma **OPTEX** zadbała o wygodę instalatora. Zatraskowa pokrywa i zaprojektowanie miejsca na baterię w przedniej części czujki (w modelach bezprzewodowych) sprawiają, że detektory łatwo się montuje i konfiguruje.



Nowość

**Linc**  
Polska Sp. z o.o.

# TECHNOLOGIA RADAROWA W OCHRONIE



Pokrycie terenu od 100° H / 30° V



Zasięg detekcji 500 / 1000 m



Nie wymaga zezwoleń



Dokładność do 1 m



[WWW.LINC.PL/RADARY](http://WWW.LINC.PL/RADARY)



PRODUKT NUMERU

**SCHRACK SECONET POLSKA** [www.schrack-seconet.pl](http://www.schrack-seconet.pl)

## VISOCALL IP – system przyzywowy i komunikacji

**System przyzywowy i komunikacji szpitalnej VISOCALL IP optymalizuje proces opieki w służbie zdrowia.** System jest w pełni IP, co oznacza, że każde urządzenie zapewnia dwustronną cyfrową komunikację głosową IP i jest podłączone do przełącznika sieciowego. Rosnące potrzeby nowoczesnego szpitala wymagają inteligentnych rozwiązań w zakresie planowania, wdrażania i przyszłych remontów.

### System VISOCALL IP zapewnia:

- spełnienie RODO przez uszanowanie prywatności pacjentów, którzy mogą decydować, czy chcą rozmawiać z personelem w sposób dyskretny, czy głośnomówiący,
- możliwość prowadzenia rozmów przez każdego z pacjentów w tym samym czasie,
- optymalizację procesów z wykorzystaniem komu-



nikacji głosowej i odbieraniem przywołań na urządzeniach systemowych lub mobilnych, np. smartfonach, telefonach DECT/VoIP itp., → programowanie kierowanych do różnych osób i grup personelu przywołań specjalistycznych na terminalach przyłóżkowych bez konieczności modernizacji okablowania,  
→ integrację z urządzeniami medycznymi, systemami bezpieczeństwa, TV, radiem, automatyką budynkową,  
→ niskie koszty budowy i modernizacji (wykorzystanie infrastruktury LAN, standardowych przewodów sieciowych itp.).  
System działa sprawnie nawet w przypadku uszkodzenia serwera. Jest instalowany w największych i najnowszych szpitalach, m.in. w nowej siedzibie Szpitala Uniwersyteckiego Kraków-Prokocim (ok. 925 łózek), Wojewódzkim Szpitalu Zespolonym im. L. Rydygiera w Toruniu (ok. 670 łózek).

**TP-LINK** [www.tp-link.com.pl](http://www.tp-link.com.pl)

## TP-Link T2600G-28MPS (TL-SG3424P). Przełącznik zarządzalny 24x Gb PoE+, 4x SFP

**Przełącznik T2600G-28MPS to wydajny przełącznik zarządzalny L2+ przeznaczony do budowy profesjonalnych sieci w małych i średnich firmach.**

T2600G-28MPS został wyposażony w 24 porty PoE 10/100/1000 Mb/s zgodne ze standardami 802.3at/af, mogące łącznie dostarczyć 384 W mocy, co umożliwia podłączenie urządzeń typu punkty dostępowe, telefony IP oraz kamery IP. Urządzenie pozwala zasilić urządzenia odbiorcze do 30 W na każdy port. Takie funkcje, jak harmonogram PoE czy priorytet portów, pozwalają na efektywniejsze zarządzanie bu-



dżetem mocy przełącznika. Switch ma także cztery osobne sloty SFP umożliwiające bardziej uniwersalne wykorzystanie urządzenia w sieci. Tworzenie bezpiecznej sieci wspomagają liczne funkcje zarządzające – 802.1Q VLAN, izolacja portów, mirroring portów, STP/RSTP/MSTP, agregacja portów (LACP), funkcja kontroli przepływu 802.3x, ACL, funkcje L2+, tj. ro-

uting statyczny oraz Quality of Service (QoS, od L2 do L4). T2600G-28MPS jest prosty w obsłudze. Zarządzanie urządzeniem może odbywać się poprzez intuicyjny interfejs graficzny użytkownika w przeglądarce internetowej (GUI) lub interfejs linii poleceń (CLI). Transfer pakietów może być chroniony szyfrowaniem SSL lub SSH. Obsługa protokołów SNMP (1/2/3) oraz RMON umożliwia przełącznikowi przekazywanie istotnych informacji dotyczących statusu oraz wychwytywanie nieprzewidzianych zdarzeń. Produkt jest objęty 5-letnią gwarancją producenta.

**WINKHAUS** [www.winkhaus.com/pl-pl](http://www.winkhaus.com/pl-pl)

## ETB-IM. Klamka elektroniczna do drzwi wewnętrznych

**Nowa klamka elektroniczna ETB-IM, w pełni kompatybilna z systemem kontroli dostępu Winkhaus blueSmart, jest przystosowana do wszystkich popularnych drzwi wewnętrznych z drewna, stali lub tworzywa sztucznego.** Bezprzewodowa klamka elektroniczna ma szerokie zastosowanie, np. w drzwiach z zamkiem wpuszczanym, z funkcją zapadki lub samoryglującym się zamkiem automatycznym. Komunikacja jest realizowana szybko i bezdotykowo przy użyciu uprawnionych breloków do kluczy, kart identyfikacyjnych i kluczy blueSmart.

Elektroniczne sprawdzanie uprawnień odbywa się po zewnętrznej stronie drzwi, od wewnątrz wystarczy naciśnięcie klamki. Dzięki funkcji pojedynczego lub stałego otwarcia (ustawianej ręcznie lub automatycznie) można elastycznie zarządzać dostęпами w obiekcie.



Nowość

**Montaż klamki w drzwiach jest bardzo prosty:** bez okablowania, bez uszkodzenia skrzydła drzwiowego, a często także bez nawiercania. Równie szybko, za pomocą standardowych narzędzi można wymienić baterię i zmienić kierunek klamki.

**Od stycznia 2020 r. w ofercie Winkhaus jest dostępnych pięć modeli do drzwi standardowych, w tym trzy dopuszczone do stosowania w drzwiach ewakuacyjnych.** Wysokiej jakości uchwyty ze stali nierdzewnej i dyskretne obudowy z tworzywa w kolorze czarnym lub białym dobrze komponują się z niemal każdym budynkiem.

**Stosując elektroniczną klamkę ETB-IM, można szybko, w nieskomplikowany sposób rozbudować istniejący system dostępowy lub utworzyć nowy.**

ZINTEGROWANE SYSTEMY ZABEZPIECZEŃ

ICTProtegeGX<sup>®</sup>

ICTProtegeWX<sup>®</sup>

NAJWYŻSZY STOPIEŃ ZABEZPIECZENIA WG NORMY **EN 50131 GRADE 4**



[www.miwiurmet.pl](http://www.miwiurmet.pl)

urmet  
MIWI

MIWI URMET Sp. z o. o.

91-341 Łódź, ul. Pojezierska 90a | tel. 42 616 21 00 | [miwi@miwiurmet.pl](mailto:miwi@miwiurmet.pl)



# Statystyki



TEKST  
a&S International

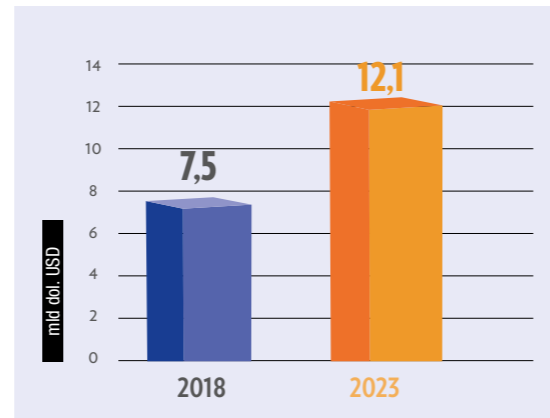
## Wzrost rynku kontroli dostępu

Przewiduje się, że rynek kontroli dostępu wzrośnie z 7,5 mld USD w 2018 r. do 12,1 mld USD do 2024 r., przy rocznym wskaźniku wzrostu (CAGR) na poziomie 8,24 proc. w latach 2018-2024. Wzrost ten jest spowodowany większym zainteresowaniem systemami kontroli dostępu wywołanym rosnącą przestępczością, postępem technologicznym i wdrażaniem w systemach zabezpieczeń technologii bezprzewodowej oraz współpracy systemów zabezpieczeń opartych na IoT z platformami przetwarzania w chmurze.

Oczekuje się, że kontrola dostępu jako usługa (ACaaS), wdrożenie rozwiązań mobilnych oraz postępująca urbanizacja w krajach wschodzących zapewnią graczom rynkowym ogromne możliwości rozwoju.

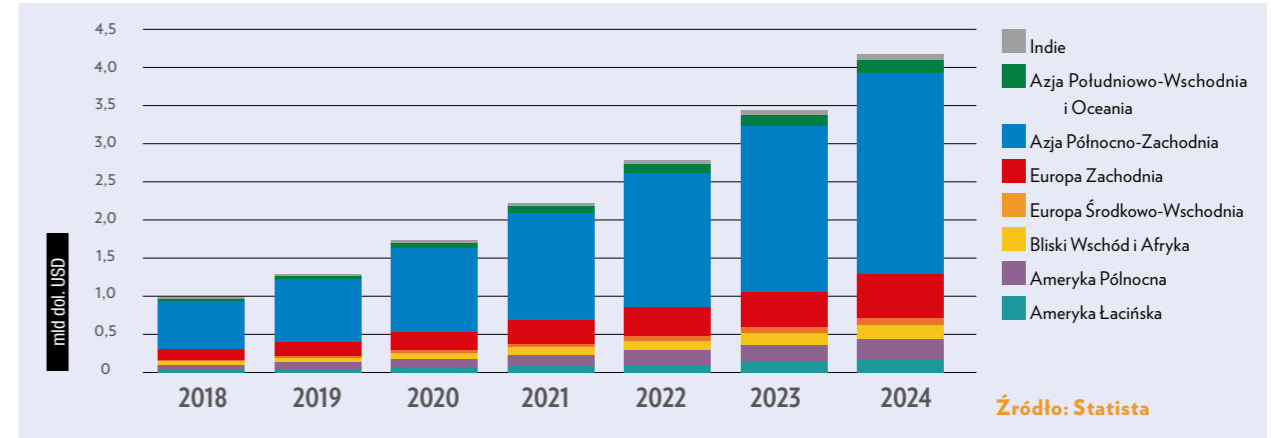
Czytniki kontroli dostępu w formie kart z paskami magnetycznymi, zbliżeniowych lub tzw. kart inteligentnych są bardziej niezawodne niż czytniki biometryczne czy zamki elektroniczne. Rosnące zapotrzebowanie na inteligentne i zbliżeniowe karty do nadzorowania i rejestrowania działań pracowników jest jednym z czynników napędzających ich rozwój.

## Wzrost rynku kontroli dostępu



Źródło: MarketsandMarkets

## Komórkowe połączenia IoT wg regionów



Źródło: Statista

## Połączenia IoT

Zwiększone zainteresowanie mobilnymi połączeniami IoT w samej Azji Północno-Wschodniej do 2024 r. przekroczy 4 miliardy marek. Rosnąca wykładniczo liczba podłączonych urządzeń oznacza cyfryzację podstawowych zasobów fabryk: budynków, wyposażenia, pojazdów i procesów. Aby unowocześnić swoją działalność, użytkownicy nie muszą czekać na technologię 5G – wielu z nich korzysta już z połączeń 4G. Stosując łączność mobilną we wszystkich strukturach fabryk, osiągają wysokie wyniki w produkcji.

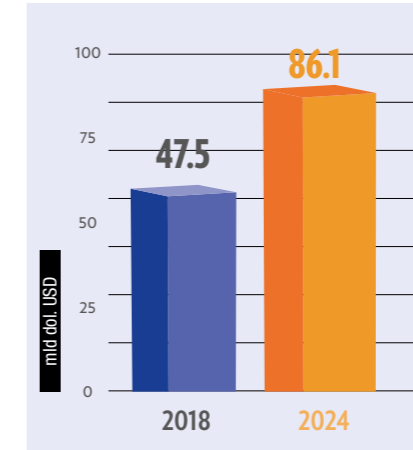
Jednak to 5G będzie motorem napędzającym inteligentne fabryki. Dzięki tej technologii będzie można uzyskać wydajniejszą łączność pomiędzy czujnikami elektronicznymi, scentralizować śledzenie towarów, przeprowadzać zdalną kontrolę jakości oraz zautomatyzować pracę w halach produkcyjnych. Inwestorzy będą mogli również łączyć różne budynki fabryki, a nawet obiekty firm zewnętrznych, tworząc ekosystem inteligentnych centrów produkcyjnych na całym świecie.

## Globalny rynek systemów dozoru wizyjnego do 2024 r. osiągnie wartość 86,1 mld USD

Globalny rynek systemów dozoru wizyjnego został w 2018 r. wyceniony na 47,40 mld USD, a oczekuje się, że do 2024 r. osiągnie wartość 86,1 mld USD, odnotowując roczny wskaźnik wzrostu (CAGR) na poziomie 10,3 % w okresie 2019-2024. Zastosowanie monitoringu wizyjnego w biznesie znacznie wzrośnie ze względu na zwiększone zapotrzebowanie na bezpieczeństwo fizyczne. Wykorzystanie usług w chmurze do scentralizowania danych będzie dodatkową korzyścią dla użytkowników.

W skali globalnej dążenie do poprawy bezpieczeństwa w różnych branżach znacznie przyczynia się do wzrostu rynku security. Zmienił się on w porównaniu do poprzedniej dekady głównie za sprawą szybkiego rozwoju oprogramowania do przechowywania i przetwarzania danych w chmurze. Dynamicznie rozwija się rynek usług VSaaS, głównie dzięki zwiększonej sprzedaży kamer IP. Znaczącymi czynnikami wpływającymi na ten rozwój są też m.in. ograniczenie kosztów IT, pojawienie się centrów danych oraz poprawa funkcjonalności związanych ze scentralizowanymi danymi. W ostatnich latach zapotrzebowanie na dozór wizyjny w segmencie komercyjnym znacznie wzrosło. Głównymi odbiorcami tych usług są segmenty bankowości i finansów, handlu detalicznego i hurtowego oraz mediów i rozrywki.

## Wartość światowego rynku systemów dozoru wizyjnego



Źródło: Mordor Intelligence

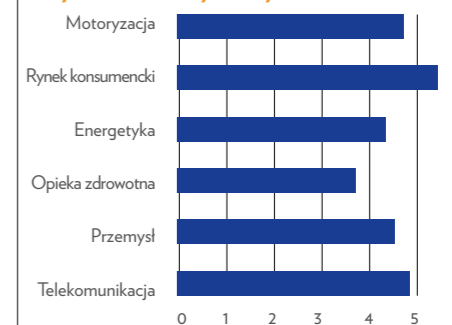
## 5G kluczem do realizacji pełnego potencjału IoT

Technologia 5G jest znacząca, ponieważ zapewnia trzy istotne korzyści: szybsze prędkości transmisji danych, mniejsze opóźnienia i zwiększoną łączność. Teraz możliwa będzie realizacja tego, czego nie można było osiągnąć za pomocą starszej technologii. Głównie dlatego, że 5G umożliwia zupełnie nowe zastosowanie, np. w samochodach bez kierowcy, rozrywce i wirtualnej rzeczywistości, grach wideo praktycznie bez opóźnień. Jeśli chodzi o przemysł, 5G

będzie kluczem do rozszerzenia i realizacji połączeń IoT pomiędzy czujnikami elektronicznymi. Wpływ technologii będzie odczuwalny w inteligentnych domach, inteligentnych miastach i inteligentnych branżach.

W pomiarach gotowości wdrożenia 5G wyniki były słabe ze względu na poziom rozwoju technicznego i złożoności wdrożenia. Jest to zrozumiałe, ponieważ potrzeba jeszcze wiele pracy, aby w pełni rozwinąć standard 5G, ułatwić wdrożenie i obniżyć koszty. Spośród rynków wertykalnych najniższą ocenę 5G uzyskało w służbie zdrowia, a także w przemyśle – w branżach, w których możliwości 5G, szczególnie ultraniezawodnej komunikacji o niskim opóźnieniu (URLLC), będą bardzo przydatne. □

## Gotowość rynków wertykalnych



Źródło: IHS Markit



CTMX	0.45	▲ +0.45%
FTR	-0.23	▼ -2.34%
CSCO	-1.01	▼ -1.89%
CHK	0.02	▲
AAPL	+2	
PRTO		
AMZN		
TSLA		
AVGO		
SIRI	0.65	





# RYNEK SECURITY W POLSCE PODSUMOWANIE ROKU 2019

**Największe wzrosty, najciekawsze realizacje, nowości rynkowe i nowatorskie technologie...**

**Jaki był miniony rok i czego spodziewamy się w 2020 r.?**

**Zapytaliśmy o to przedstawicieli najważniejszych firm na polskim rynku security.**

ABUS Polska

**Józef Grabowski**



Dla firmy ABUS rok 2019 był bardzo dobry. Na wszystkich polach działania osiągnęliśmy założone cele sprzedażowe, mocno je przewyższając. W zakresie zabezpieczeń mechanicznych w sektorze domów jednorodzinnych i obiektów komercyjnych uzyskaliśmy nieco ponad 20-proc. wzrost sprzedaży. Zauważamy pewien proces powrotu do zabezpieczeń mechanicznych, które w następnym etapie są uzupełniane o rozwiązania elektroniczne w myśl zasady „elektronika zawsze w parze z mechaniką, ale mechanika krok przed elektroniką”.

Był to dla nas kolejny rok, w którym zwiększyliśmy sprzedaż systemów klucza generalnego różnej wielkości. Największym systemem zrealizowanym w Polsce był system klucza dla szpitala w Krakowie-Prokocimiu. W tej dziedzinie wyraźnie zauważalny jest wzrost świadomości użytkowników oraz administratorów obiektów – zarówno komercyjnych, jak i użyteczności publicznej. W ubiegłym roku zaprezentowaliśmy również kilka innowacyjnych produktów, takich jak kłódka o wysokim poziomie zabezpieczeń otwierana odciskiem palca czy kamera w pełni bezprzewodowa z wbudowanym akumulatorem. Produkty te cieszyły się dużą popularnością. Na rok 2020 mamy nadal ambitne plany wzrostu sprzedaży na każdym rynku, na którym jako ABUS jesteśmy obecni. Chcemy osiągnąć dwucyfrowe wzrosty w dziale zabezpieczeń domowych, komercyjnych i bezpieczeństwa mobilnego. Nadal pozostajemy wierni naszemu modelowi bardzo bliskiej współpracy z partnerami lokalnymi, starając się jednak ich codzienną pracę usprawnić, oferując różnego rodzaju udogodnienia w sposobie zamawiania i obsługi zleceń.

Na ten rok zaplanowaliśmy prezentację kolejnych nowości, takich jak wkładki bębnekowe z elementami magnetycznymi, stanowiące skuteczną metodę ochrony przed nowoczesnymi sposobami nielegalnego kopiowania kluczy (m.in. druk 3D), nowe rozwiązania w dziale kamer i wiele innych ciekawych produktów. Portfolio firmy ABUS pozostaje bardzo szerokie, począwszy od kłódek i wkładek bębnekowych, przez kamery czy kaski rowerowe, kończąc na linii produktów JuniorCare, czyli produktach dbających o bezpieczeństwo dziecka.

Wszystkie produkty z naszej oferty mają wspólny mianownik: BEZPIECZENSTWO. W roku 2020 pozostajemy wierni naszej filozofii – *Chcemy uczynić życie odrobinę bardziej bezpieczne.*

Axis Communications Poland

**Dagmara Pomirska**



Zdaniem Axis Communications w 2019 r. byliśmy świadkami kolejnego technologicznego kroku naprzód, przy czym z naszej perspektywy, jako innowatora i podmiotu wdrażającego nowe technologie, istotne było to, że skupiliśmy się na rozpatrywaniu i testowaniu tych idei i rozwiązań, które dobrze rokowały w kategoriach tworzenia wartości dodanej i pozytywnego wpływu na daną organizację czy obywateli. To był imperatyw i pewien filtr, poprzez który obserwowaliśmy i odsiewaliśmy trendy technologiczne pod kątem ich efektywnego zastosowania przemysłowego, społecznego, ekologicznego.

Okazało się, że eksperci Axis Communications bardzo trafnie wytypowali trendy, które miały kształtować branżę security w 2019 r. Kilka kluczowych kierunków pojawiło się już w zestawieniu trendów w roku poprzednim, ale ze względu na swój potencjał i nośność naturalnie rozwijały się także w kolejnym. Były to m.in. sztuczna inteligencja – także dla sektora zabezpieczeń, chmury obliczeniowe, ruch w kierunku urządzeń brzegowych, personalizacja i prywatność.

Jednym z ważniejszych wyzwań, także w branży zabezpieczeń, było i nadal jest cyberbezpieczeństwo. Rzecz w tym, że problemy te nigdy nie zostaną całkowicie rozwiązane, ponieważ cyberprzestępcy zawsze będą próbować wykrywać i wykorzystywać luki w zabezpieczeniach. Dlatego w Axis nieustannie pracujemy nad coraz lepszymi cyberbezpieczeniami, informując partnerów o ewentualnych lukach. Wiemy, że nasza praca w tym zakresie nigdy się nie skończy.

Ważnym trendem w 2019 r. był ruch ku budowaniu systemów zintegrowanych, które umożliwiają faktyczne wdrażanie inteligentnych rozwiązań. Zaawansowane systemy wykorzystujące sztuczną inteligencję niebawem mogą odgrywać centralną rolę w monitorowaniu stanu termoizolacji, energooszczędności czy efektywności energetycznej różnych obiektów. Będą też istotnym wsparciem w rozwiązywaniu wielu problemów ekologicznych, przyczyniając się do zrównoważonego rozwoju. W roku 2020 będziemy kontynuowali prace nad rozwojem technologicznym naszych produktów i wdrażaniem nowych rozwiązań. Będziemy je pokazywać podczas licznych wydarzeń branżowych, m.in. w trakcie kolejnej edycji Axis Partners Day 2 kwietnia br. Kontynuować będziemy również bardzo popularny cykl porad na FB – Espresso z Bogumiłem. Rok 2020 zapowiada się bardzo interesująco i dla naszej firmy, i całej branży zabezpieczeń.

AxxonSoft Polska

Paweł  
Trojak

Według danych na koniec 2019 r. już ponad 2100 obiektów budowlanych w Polsce było strzeżonych i zarządzanych przez produkty AxxonSoft. Rośnie także średnia wartość nabywanych od nas licencji, co przekłada się na rekordową sprzedaż nieprzerwanie już od 7 lat. Podobny trend zauważamy w większości naszych 50 biur na świecie.

Szczególnie cieszą mnie fantastyczne wyniki, jakie osiągamy w krajach będących pod naszą opieką – w Czechach i na Słowacji, a „tygrysem sprzedaży” w 2020 r. zapowiadają się Węgry. Doskonale prezentują się także wyniki w USA oraz na zachodzie Europy, gdzie przodują Niemcy, Wielka Brytania i Włochy. Ogólnosiwiatowy wzrost sprzedaży AxxonSoft wyniósł rok do roku aż 44%.

Są dwa główne czynniki tej hossy: coraz większa liczba urządzeń instalowanych w obiektach budowlanych (zwłaszcza kamer i urządzeń kontroli dostępu) oraz rosnąca potrzeba integracji, a także wizualizacji urządzeń i systemów. AxxonSoft, jako jeden z liderów wśród dostawców platform integrujących, jest naturalnym beneficjentem tego trendu. Naszą pozycję pomogły umocnić nowości w ofercie, a rok 2020 zapowiada się pod tym względem wręcz ekscytująco. Z niecierpliwością czekamy na zapowiadane technologie będące aktualnie w opracowaniu. Największym dla nas wyzwaniem było i wciąż pozostaje podążanie za tempem rozwoju rynku i zapotrzebowaniem na nasze produkty. Za sukcesem handlowym musi jednocześnie iść wysokiej jakości wsparcie techniczne i obsługa sprzedażowa, a nadążanie za tak szybkim rozwojem jest niezwykle trudne. Do zespołu AxxonSoft Polska dołączyły w 2019 r. dwie nowe osoby, wciąż widzimy potrzebę zatrudnienia kolejnych. Ważnym krokiem było dla nas uzyskanie certyfikatu CNBOP na System Integrujący Urządzenia Przeciwpowarowe, długo oczekiwany przez wielu naszych klientów i biura projektowe.

Jeśli chodzi o wydarzenia branżowe, rynek wyraźnie podążył w kierunku profilowanych konferencji, gdzie można pozyskać praktyczną wiedzę, a „służbowa turystyka imprezowa” bez wartości merytorycznych wyraźnie zanika. Rynek dojrzał w tym względzie. Natomiast w AxxonSoft uważamy, idąc nieco pod prąd, że imprezy targowe wciąż mają sens, i bierzemy udział we wszystkich znaczących expo na świecie, włączając w to nasz rodzimy Securex.

Naszym celem na najbliższy rok jest otwarcie nowych biur w krajach Europy Środkowo-Wschodniej oraz utrzymanie znakomitego trendu i dobrej opinii o naszych produktach.

W połowie roku spodziewamy się premiery nowych rozwiązań, które pozwolą umocnić naszą pozycję wśród liderów rynku PSIM/VMS.

BCS

Artur  
Stępowski

Miniony rok był wyjątkowy, osiągnęliśmy większy wzrost sprzedaży niż notowany w ostatnich latach. Nastąpił on we wszystkich liniach produktowych BCS CCTV, co ma kluczowe znaczenie przy budowaniu i utrzymaniu stabilności marki. Otwarcie na rynki zagraniczne dały szansę polskiej marce BCS zaistnieć w świadomości klientów z takich krajów, jak Litwa, Czechy, Słowacja, Cypr, Portugalia.

W roku 2019 działania zespołu były skupione na udoskonalaniu jakości obsługi klientów BCS. Nasza filozofia opiera się na przekonaniu, że w pierwszej kolejności powinniśmy doceniać i wspierać swoich Partnerów, poszerzając z nimi współpracę. Rozszerzyliśmy linie produktowe, umożliwiając dostęp klientom BCS do różnych technologii. Równocześnie w trosce o najwyższy poziom obsługi nasz dział handlowy został rozbudowany i wyposażony w dodatkowe narzędzia ułatwiające bieżącą współpracę z dystrybutorami. Zadbaliśmy też o wsparcie posprzedażowe, skupiając się na aspektach związanych z obsługą serwisową. Czas realizacji napraw został skrócony do 2-3 dni roboczych, a ich liczba znacząco zmniejszona dzięki rozbudowie działów jakości i wsparcia technicznego. Głównym celem zespołu BCS będzie utrzymanie wysokiego poziomu satysfakcji dystrybutorów, instalatorów, inwestorów oraz klientów końcowych, korzystających z naszych rozwiązań.

Wprowadziliśmy na rynek wiele nowości, które spotkały się z dużym zainteresowaniem i zostały bardzo dobrze przyjęte. Inteligentne rejestratory serii BCS Line AI wyposażone w funkcje zaawansowanej analizy obrazu pojawiły się w ofercie na początku ub.r., pokazując kierunek, w którym podążają nowoczesne rozwiązania na rynku CCTV/VSS. Nowe funkcje, takie jak klasyfikacja obiektów wraz z gromadzeniem dodatkowych informacji nt. osób czy samochodów widocznych na obrazie z kamer, były do tej pory niedostępne na rynku cywilnym. Dzięki tym funkcjom i możliwości filtrowania zarejestrowanego materiału można na podstawie metadanych łatwo i szybko odszukać interesujące nas zdarzenie, bez konieczności żmudnego przeszukiwania ogromnych nagrań wideo. Kontynuując rozwój w obszarze urządzeń AI, do oferty urządzeń inteligentnych zostały dodane kamery BCS Line AI o nowych możliwościach weryfikacji alarmów. Funkcje ochrony obwodowej uzupełnione o rozpoznawanie obiektów pozwalają dokładnie określić, na jakiego typu zdarzenia ma reagować system monitoringu wizyjnego. Nowe kamery wyposażone w analizę identyfikacji twarzy potrafią porównać wykrytą twarz z zapisaną w bazie danych. Kamery z funkcją liczenia ludzi i tworzenia raportów z tego typu zdarzeń pozwalają na wkroczenie systemów telewizji przemysłowej na zupełnie nowe obszary rynku.

Równolegle z dostarczeniem innowacyjnych urządzeń rozbudowywaliśmy polskie oprogramowanie BCS Manager. Chcąc dać możliwość zapoznania się z naszymi rozwiązaniami klientom, którzy dotychczas nie mieli przyjemności pracować na produktach BCS, dodaliśmy do naszego oprogramowania obsługę protokołu ONVIF. Zostały także zaimplementowane natywne protokoły największych światowych producentów. Jednocześnie BCS Manager, oprócz obsługi produktów linii BCS Line i BCS Point, obsługuje nowe linie produktowe BCS Basic i BCS View. Opracowaliśmy od podstaw nowatorskie rozwiązania techniczne umożliwiające integrację z zewnętrznymi urządzeniami lub systemami kasowymi w trybie „live”. Dzięki tej opcji obsługa elektronicznego paragonu (POS) została tak zmodyfikowana, że BCS Manager widzi cały proces tworzenia paragonu w czasie rzeczywistym, z prezentacją anulowanych pozycji włącznie. Wyróżnianie słów kluczowych, przeglądanie zarchiwizowanych paragonów połączone z możliwością nagrywania obrazu bezpośrednio na PC, wybór budowy systemu jako lokalny lub klient-serwer to tylko część właściwości, które w przyszłości umożliwią nam współtworzenie rynku ochrony w Polsce i za granicą.

Rok 2019 pokazał, czego możemy spodziewać się w roku 2020 i w dalszych latach. Główny nacisk jest kładziony na rozwiązania związane z szeroko pojętą sztuczną inteligencją. Rozwój oprogramowania z inteligentnym przeszukiwaniem danych, automatycznymi kopiami bezpieczeństwa, rozproszoną infrastrukturą, własną chmurą będzie wpisany w trend tego rozwoju.

Bosch Building Technologies

Krzysztof  
Góra

Rok 2019 możemy zaliczyć do udanych w każdym z możliwych aspektów. Przede wszystkim osiągnęliśmy rekordowe wyniki sprzedaży. Szczególnie cieszy mnie fakt, że są to organiczne wzrosty w każdej z oferowanych przez nas grup produktowych, składających się na kompletne rozwiązania safety & security marki Bosch. Udało nam się to osiągnąć, wyposażając kilkaset budynków w Polsce w dedykowane platformy bezpieczeństwa obejmujące telewizję dozorową, kontrolę dostępu, system sygnalizacji pożarowej, dźwiękowy system ostrzegawczy, system sygnalizacji włamania i napadu oraz zarządzający całością rozwiązania Bosch Integration System. To zasługa bardzo zmotywowanego i zaangażowanego zespołu Bosch Building Technologies oraz kompetentnych, lojalnych i rozumiejących rynek projektowy partnerów handlowych. Korzystając z okazji chciałbym przekazać wyrazy uznania i podziękowań zarówno moim kolegom z firmy, jak i naszym partnerom handlowym. To zaszczyt i przyjemność pracować w takim gronie.

W roku 2020 nasze działania będą koncentrowały się wokół nowych produktów i rozwiązań. Będzie to dla nas rok przełomowy pod tym względem w zakresie telewizji dozorowej, systemów sygnalizacji pożarowej i dźwiękowych systemów ostrzegawczych. Wprowadzamy na rynek nowości, które diametralnie zmienią naszą ofertę. Zapewniam, że będzie o nas głośno, a to wymaga starannego zaplanowania i realizacji wielu działań.

Branża security jest ściśle powiązana z rynkiem budowlanym. W przypadku firm takich jak nasza, koncentrujących się na projektach, szczególne znaczenie ma budownictwo komercyjne. Prognozy dla tej części rynku niosą ze sobą pewne ryzyko. Jeżeli spowolnienie rzeczywiste nastąpi, to nie powinno się ono jeszcze w tym roku odbić na wynikach firm naszej branży. Mamy bowiem wiele propozycji dla rynku budowlanego, takich jak inwestycje w obszarze transportu, przemysłu, służb mundurowych i kilku innych. Jestem przekonany, że branża może z uzasadnionym optymizmem planować ambitne cele na rok 2020.

Trendem wyraźnie zauważalnym w roku 2019, który nas bardzo cieszy, jest rosnąca świadomość konieczności zapewnienia bezpieczeństwa danych w systemach safety i security. Urządzenia z naszej branży są dziś przede wszystkim elementami sieci IT. W przypadku, gdy producent nie zapewni odpowiedniego poziomu zabezpieczeń swoim urządzeniom, mogą być one najsłabszym elementem sieci IT, a co za tym idzie stać się przedmiotem ataków hakerskich. Coraz częściej spotykamy się z inwestorami świadomymi tego faktu na tyle, aby nie przyjmować naiwnej argumentacji niektórych producentów, że wydzielenie na potrzeby systemów zabezpieczeń dedykowanej sieci IT oddala zagrożenia atakami hakerskimi na tyle, aby nie skupiać się na poziomie zabezpieczeń zainstalowanych kamer.

Dahua Technology Poland

Artur  
Prusinowski

Rok 2019 był dla zespołu Dahua Technology Poland bardzo udany. Po spektakularnym sukcesie w 2018 r. musieliśmy po raz kolejny stanąć na wysokości zadania, aby ponownie zrealizować wszystkie ambitne cele. Godny podkreślenia jest fakt, iż umocniliśmy się jako lider w obszarze CCTV (VSS) dzięki utrzymaniu wysokiej dynamiki wzrostu sprzedaży. Jednocześnie z działaniami aktywnymi sprzedaż szeroko pojętych rozwiązań telewizji dozorowej wprowadziliśmy na rynek nowe rozwiązania z zakresu kontroli dostępu oraz nowej generacji systemów wideodomofonowych.

Nowe linie produktowe pozwalają spokojnie patrzeć w przyszłość. Rośnięmy, poszerzając ofertę oraz wprowadzając innowacje w obszarze sztucznej inteligencji, która jest już dostępna w większości oferowanych przez nas urządzeń do monitoringu wizyjnego. Dahua Technology jako pierwsza firma w Polsce wprowadziła do masowej sprzedaży tak doskonałe algorytmy AI dostępne dla każdego uczestnika rynku.

Oczywiście wspomniany sukces mógł być możliwy wyłącznie dzięki wspaniałemu zespołowi ludzi oraz lojalności Partnerów biznesowych. Raz jeszcze serdecznie dziękuję Wszystkim za ciężką pracę w 2019 roku. Razem możemy więcej!

Rok 2020 dla Dahua Technology Poland będzie obfitował w wiele aktywności, które przygotowaliśmy już teraz, aby utrzymać pozycję lidera CCTV (VSS). Ponadto rok 2020 będzie to czas dużych inwestycji, jakie zaplanowaliśmy w Polsce. Jeszcze w pierwszym kwartale zwiększymy powierzchnię naszego biura w Warszawie z 700 do ponad 1000 m<sup>2</sup>. W nowej części będzie mieściła się siedziba działu R&D dla całego regionu CEE&Nordic. Zadaniem nowej komórki organizacyjnej będzie dostosowanie rozwiązań oferowanych w tej części Europy do lokalnych potrzeb. W imieniu zespołu oraz swoim gorąco zachęcam do śledzenia naszych aktywności w mediach społecznościowych oraz aktywnego udziału w wydarzeniach, które będziemy realizować z dobrze znanym Państwu rozmachem i jakością merytoryczną na najwyższym poziomie.

Ela-compil

Norbert  
Bartkowiak

Rok 2019 śmiało możemy zaliczyć do bardzo udanych. Ela-compil zrealizowała wszystkie priorytetowe założenia, szczególnie w kategoriach sprzedaży i rozwoju naszego flagowego produktu – systemu GEMOS oraz zacieśniania współpracy z Gretsch-Unitas, koncernem, do którego należymy. Jesteśmy także dumni z rosnącej popularności naszego drugiego rozwiązania – centrali FPM+. Sterowanie urządzeniami przeciwpożarowymi za pomocą dedykowanej centrali staje się już standardem, liczba projektów bazujących na FPM+ rośnie z roku na rok. Dużą satysfakcją sprawia nam fakt, że klienci w swoich kolejnych inwestycjach postanawiają zastosować ten sam standard.

Największym sukcesem firmy w 2019 r. była nowa odsłona systemu GEMOS w opcji MOSAIC. Coraz częściej GEMOS jest stosowany w obiektach o bardzo dużej powierzchni i znacznym stopniu rozproszenia. Dotychczasowe podejście do wizualizacji obiektu przestaje być efektywne, ponieważ obszerne plany z mnóstwem informacji stają się nieczytelne. Tym bardziej, gdy stosuje się podział planu i nawigację pomiędzy wieloma mniejszymi jego wycinkami. Takie podejście jest jednak mniej przyjazne dla użytkownika w porównaniu z filozofią MOSAIC – nowym sposobem wyświetlania planów w systemie GEMOS. Został on opracowany z myślą o tym, aby pomóc wizualizować cały plan naraz przede wszystkim wtedy, gdy ma on duże rozmiary. Zamiast wyświetlania wszystkiego jednocześnie MOSAIC dynamicznie wizualizuje zawartość planu w zależności od stopnia przybliżenia, priorytetu czy preferencji użytkownika. Operator może swobodnie nawigować na jednej dużej mapie, nie musząc wybierać i przeladowywać kolejnych planów.

Dużym wyzwaniem w 2019 r. były zmiany wewnątrz naszego koncernu Gretsch-Unitas, które zaowocowały powierzeniem nam dodatkowych zadań na polu R&D. Zmiany były wynikiem fuzji spółek zależnych pod szyldem GU i związanych z nią zmian kadrowych.

W bieżącym roku skupimy się na dalszym rozwoju i ekspansji na rynku. Wykorzystamy sprzyjającą nam koniunkturę i rosnącą na rynku świadomość zarządzania bezpieczeństwem w nowoczesnych budynkach. Jednym z najpopularniejszych haseł w 2019 r. było *smart city/smart home*, ale nie jako jednoroczna moda, a długotrwały proces. Wartość rynku inteligentnych urządzeń domowych nieprzerwanie rośnie i ta tendencja będzie się utrzymywała. W konsekwencji koncepcja *smart city/smart home* stanie się bardziej powszechna.

Rysując perspektywę polskiego rynku security w 2020 r., muszę wspomnieć o szansie, jaką daje analiza danych w kontekście generowania coraz większej ich liczby przez kilkanaście różnych systemów jednocześnie. Bez systemu integrującego i analizującego nie będzie można funkcjonalnie zabezpieczyć budynków. W najbliższych latach wzrośnie popularność otwartych systemów integrujących systemy zabezpieczeń, a także rozwiązań, które mogą być łatwo skalowalne i umożliwiać automatyzację procesów. Przyszłość należy do integracji i rozwiązań klasy PSIM (*Physical Security Information Systems*).

Problemem, z jakim aktualnie się mierzymy, jest brak odpowiednio przeszkolonej kadry wśród pracowników ochrony. Nowoczesne rozwiązania, takie jak GEMOS (czyli zintegrowane systemy ochrony), wymagają specjalistycznych programów, umiejętności analizy sytuacji i podejmowania właściwych działań. Na pewno czeka nas zmiana w podejściu do szkolenia kadr (podniesienie kwalifikacji pracowników) i dotychczasowego wizerunku pracownika ochrony.

Genetec

Jakub  
Kozak

Rok 2019 był bardzo udany dla Genetec – globalnie i w krajach Europy Środkowo-Wschodniej, w tym w Polsce. Udało się nam zrealizować wszystkie założone cele, zarówno te sprzedażowe, jak i związane z rozwojem technologii oraz budowaniem i wzmocnieniem kanału sprzedaży. Genetec osiągnął pozycję światowego lidera w sprzedaży systemów VMS. Zdajemy sobie sprawę, że uzyskanie tej pozycji, choć niezwykle ważne, nie jest dla nas celem samym w sobie.

Najważniejszym zadaniem, jakie sobie stawiamy, jest umożliwienie wiodącym światowym organizacjom zwiększenia efektywności operacyjnej, sprawności w przetwarzaniu dużych zbiorów danych i oczywiście ich bezpieczeństwa. Warto też podkreślić, że Genetec Security Center jest dziś platformą o zdecydowanie większych możliwościach niż typowy system VMS. W Genetec mówimy o naszym głównym produkcie jako o zunifikowanej platformie bezpieczeństwa właśnie dlatego, że funkcjonalność Genetec Security Center to zarówno system monitoringu wizyjnego, jak i system kontroli dostępu, ANPR oraz wielu innych elementów systemu bezpieczeństwa.

Rynek Europy Środkowo-Wschodniej jest stosunkowo nowym obszarem działania dla Genetec. Na tym etapie wyzwaniem jest możliwe szybkie utworzenie skutecznego kanału sprzedaży i dotarcie do wszystkich głównych, potencjalnych odbiorców naszych systemów. Kilkanaście ostatnich miesięcy było dla nas okresem niezwykle wyjątkowej pracy w tym zakresie.

W Polsce coraz więcej firm poszukuje rozwiązań stabilnych, skalowalnych i otwartych – niekiedy w najniższej cenie. W dalszym ciągu polski rynek należy uznać za nieco bardziej zachowawczy niż pozostałe rynki światowe. Widać to wyraźnie na przykładzie podejścia klientów do rozwiązań w chmurze. Klienci preferują systemy *on-premise* (lokalnie), choć rozwiązania Genetec w zakresie cyberbezpieczeństwa są na najwyższym poziomie i wiele światowych organizacji, które zabezpieczamy, w pełni ufa bezpieczeństwu systemów pracujących w chmurze. W Genetec pamiętamy, że system bezpieczeństwa musi być przede wszystkim sam w pełni zabezpieczony. W języku angielskim brzmi to *security of security system*. Innym trendem wartym odnotowania jest wzrost świadomości problematyki prywatności i ochrony danych osobowych. Genetec jako jedna z pierwszych firm nie tylko zwróciła uwagę na tę kwestię, ale także zaproponowała gotowe rozwiązanie – Privacy Protector pozwalające na zapewnienie bezpieczeństwa bez narażania na szwank prywatności osób postronnych. W roku 2020 planujemy dalszy dynamiczny rozwój. Będziemy też zdecydowanie bardziej widoczni w działaniach marketingowych na rynku – również w ścisłej współpracy z „a&s Polska”.

Polski rynek security najprawdopodobniej będzie coraz bardziej cenil wartość stabilności systemów zabezpieczeń, wysokiego poziomu cyberbezpieczeństwa i otwartości na integrację z innymi rozwiązaniami. Oczywiście cena zakupu zawsze będzie istotnym kryterium wyboru, ale klienci na pewno zaczną też zwracać uwagę na niższy całkowity koszt posiadania oraz wysoką wartość użytkową swoich systemów.

Hikvision Poland

Artur  
Jajszcak

Wydaje się, że tylko chwila minęła od podsumowania roku 2018, a już nadszedł czas na podsumowanie 2019. Dla naszej firmy był on szczególnie pod wieloma względami, wypełniony licznymi wyzwaniami mającymi istotny wpływ na wyniki końcowe.

Ubiegły rok, jubileuszowy z okazji 5-lecia działalności Hikvision w Polsce, był dla nas bardzo udany. Kolejny raz z rzędu zanotowaliśmy bardzo wysoki wzrost sprzedaży, udało się wypromować z sukcesem wiele nowych produktów i rozwinąć sprzedaż nowych linii produktowych. Wzorem lat ubiegłych bardzo mocno skoncentrowaliśmy się na edukacji naszych klientów, przeprowadzając ogromną liczbę szkoleń w całym kraju. Szkoliliśmy dystrybutorów, instalatorów i klientów końcowych. Byliśmy obecni na największych wydarzeniach branżowych, np. Warsaw Security Summit 2019, kolejny już raz w ramach TruckShow odwiedziliśmy wybrane miasta w całej Europie.

We wrześniu przeprowadziliśmy się do nowego biura w warszawskim kompleksie Business Garden, dzięki czemu jesteśmy w stanie zaoferować naszym gościom wszelkie niezbędne wygody w czasie szkoleń, spotkań biznesowych czy też prezentacji w naszym showroomie. Z okazji wspomnianego jubileuszu 5-lecia działalności Hikvision w Polsce zorganizowaliśmy loterię, jej zwycięzcom przekazaliśmy pięć samochodów marki Fiat Fiorino. Loteria była w ocenie naszych klientów i nas samych jedną z najatrakcyjniejszych akcji promocyjnych w branży w minionym roku. Potwierdzają to nie tylko opinie rynku, ale także ogromna liczba rejestracji, przewyższająca wielokrotnie nasze oczekiwania. W listopadzie na zakończenie obchodów jubileuszu zaprosiliśmy przedstawicieli naszych dystrybutorów na oficjalne otwarcie nowego biura firmy oraz uroczystą galę uroczynową. Była to też okazja do podziękowań naszym Partnerom za dotychczasową współpracę i wyróżnień szczególnie zaangażowanych w promowanie naszej marki w Polsce. Poprzedni rok oceniamy jako bardzo udany i dla nas, i dla całej branży. Większość naszych Partnerów odnotowała bardzo wysokie wzrosty sprzedaży nie tylko naszych produktów, ale także wszystkich kluczowych marek posiadanych w swojej ofercie. Rynek okazał się bardzo chłonny, co pozwala na optymizm patrząc w przyszłość. Przed nami nowy rok 2020, w którym zamierzamy dalej zwiększać aktywność na wszystkich polach naszej działalności w Polsce. Zespół Hikvision Poland wciąż się powiększa, dzięki czemu będziemy w stanie realizować więcej szkoleń i angażować się w kolejne najważniejsze wydarzenia branżowe. Nie zabraknie również kolejnych spektakularnych promocji dla naszych klientów, w tym zakresie z pewnością będzie to jeszcze ciekawszy rok. Jeśli rynek zachowa dotychczasową stabilność i chłonność, mamy przed sobą kolejny bardzo udany rok dla całej branży. Hikvision będzie kontynuować swoją strategię z poprzedniego roku, ponieważ okazała się bardzo skuteczna. A oczekiwania wobec firmy są jeszcze większe.

Linc Polska

Harald  
Dingemans

Podczas każdego spotkania i rozmowy z klientem staramy się wsłuchiwać w jego oczekiwania i sugestie oraz wyciągać wnioski. To właśnie one stanowią dla nas drogowskaz do dalszych działań na kolejne miesiące, a nawet lata. Konsekwencją takiej strategii było uzupełnienie w 2019 r. naszego portfolio o nowe produkty, pozwalające zbudować funkcjonalny system zabezpieczeń z wykorzystaniem wyłącznie oferowanych przez nas rozwiązań.

W ubiegłym roku kluczowym obszarem naszego działania były systemy zdalnej weryfikacji wizyjnej. Wcześniej skupialiśmy się tylko na sprzedaży wideonadajników, teraz oferujemy szeroki asortyment kamer, algorytmy analizy wizyjnej, czujki PIR czy urządzenia audio pozwalające na zdalną reakcję. Nasi klienci nie muszą się już martwić o integrację tych rozwiązań, są one przez nas sprawdzone i przetestowane. Tak budowane systemy pozwalają na wielowarstwową ochronę, a połączenie kilku technologii znacznie podnosi poziom zabezpieczenia danego obiektu.

Sytuacja na polskim rynku ochrony odzwierciedla zmiany w wysokości płacy minimalnej. To, co kiedyś nazywaliśmy trendem, obecnie jest już faktem. Coraz częściej ochrona fizyczna jest uzupełniana lub zastępowana rozwiązaniami technicznymi. Prosty rachunek ekonomiczny przemawia za tą zmianą, a klienci przekonali się już, że nowoczesne rozwiązania potrafią skutecznie zabezpieczyć dany obiekt. Odpowiedzią naszej firmy na te zmiany jest autorskie rozwiązanie iTower – mobilna wieża do monitoringu wizyjnego. Ten w pełni autonomiczny system można uruchomić w każdym miejscu i po paru minutach od jego dostarczenia dany obiekt jest już monitorowany. Mam nadzieję, że wkrótce w całej Polsce będzie działało coraz więcej takich mobilnych wież.

Nad technologiami w chmurze pracowaliśmy już w latach ubiegłych i na nich chcemy się skupić również w 2020 r. Widzimy ich wielki potencjał zarówno pod kątem zarządzania systemami rozproszonymi, jak i w perspektywie ich możliwości, np. kontekstowej analizy obrazu przez systemy AI. Rozumiemy, że każdy chce korzystać z nowoczesnych rozwiązań, ale technologia nie ma nas angażować, ale wspierać. Nie może budować ograniczeń, ale musi otwierać nowe możliwości każdego dnia. Nowoczesne technologie w chmurze pozwolą nam oferować właśnie takie rozwiązania.

Patrząc z perspektywy czasu, myślę, że rok 2019 był dla nas bardzo dobry. Umocniliśmy naszą pozycję w segmentach, w których byliśmy obecni. Konsekwentnie poszerzaliśmy obszar działalności, realizując m.in. nowoczesne wdrożenia oparte na technologiach radarowych. Jestem przekonany, że rozwiązania te, ze względu na oferowaną funkcjonalność połączoną z atrakcyjną ceną, w najbliższym czasie zyskają na popularności. W naszym portfolio mamy już radary do monitoringu na krótkim zasięgu – marki Scan 360, średnim – marki Magos oraz takie, które pozwalają na detekcję na dystansie kilku kilometrów – marki Blighter. Produkty te stanowią dla nas kolejny element budowania systemów wielowarstwowych. Radary pozwalają nie tylko na ochronę terenu samego obiektu, lecz także przestrzeni powietrznej, np. w celu detekcji nadlatujących dronów.

Stale monitorujemy pojawiające się nowe zagrożenia i szybko na nie reagujemy, dostosowując naszą ofertę do zmieniających się potrzeb. Tego wymagają od nas klienci, a my stawiamy na silne partnerstwo z nimi i w bieżącym roku, i w przyszłości.

MIWI-URMET

Jacek  
Karcewicz

Rok 2019 był dla firmy MIWI-URMET pracowity i bardzo udany. Wykorzystaliśmy koniunkturę w branży budowlanej w kraju, w zakresie zarówno budownictwa mieszkaniowego, jak i pozostałych segmentów rynku budowlanego. To był dobry rok dla firmy przede wszystkim w zakresie sprzedaży zintegrowanych systemów KD i CCTV, systemów wideodomofonowych i automatyki bramowej.

Realizacja niektórych dużych projektów będzie kontynuowana w roku bieżącym, co jest dobrym prognostykiem na przyszłość. Nasi główni partnerzy i dostawcy wprowadzili sporo nowości, dzięki czemu staliśmy się jeszcze bardziej konkurencyjni na krajowym rynku security. Informacje o nowościach w ofercie systematycznie przedstawialiśmy w pismach branżowych. Nasi partnerzy biznesowi, głównie integratorzy i projektanci instalacji niskoprądowych, mogli zapoznać się z naszą nową ofertą na zorganizowanych licznych konferencjach, prezentacjach i szkoleniach. W roku 2019 zrealizowaliśmy wszystkie najważniejsze cele. Za największy sukces uważamy rozwój współpracy z dotychczasowymi kluczowymi klientami oraz pozyskanie wielu nowych obiecujących partnerów.

W bieżącym roku, mimo mniej optymistycznych prognoz dotyczących wzrostu gospodarczego, branża security powinna nadal dynamicznie się rozwijać. Związane jest to m.in. z wyższą świadomością rosnących zagrożeń bezpieczeństwa wśród inwestorów oraz większą dostępnością systemów i urządzeń z tego segmentu rynku (malejące ceny, nowe technologie zwiększające ich funkcjonalność i wydajność). Na pewno będzie kontynuowany trend związany z integracją systemów zabezpieczeń, rozwijana inteligentna analityka wideo. Będzie to również miało wpływ na dalszy rozwój i zapotrzebowanie na systemy KD.

Systemy z branży security, kojarzone dotychczas głównie z ochroną, będą coraz częściej stosowane w innych celach i obszarach (np. marketingowych – algorytmny analizy obrazu umożliwiające zliczanie i przemieszczanie osób i przedmiotów; transport i smart city – usprawnienie ruchu drogowego; wspomaganie zarządzaniem obiektami – rezerwacja miejsc; przemyśl – kontrola procesów technologicznych, serwisowanie sprzętu itp.). Nadal ważnym zagadnieniem pozostanie cyberbezpieczeństwo będące ważnym zadaniem dla producentów urządzeń i systemów zabezpieczeń. Firma MIWI-URMET jest przygotowana na wszystkie wymienione wyzwania. Nowoczesne systemy zabezpieczeń już wprowadziliśmy do naszej oferty, przewidujemy dalszy rozwój w tym zakresie w 2020 r. Nowością w ofercie będzie zaawansowany technologicznie system sygnalizacji pożarowej.

Dynamicznie zmieniająca się oferta i duża liczba nowych rozwiązań na rynku security powodują, że integratorzy i administratorzy systemów oczekują jeszcze silniejszego wsparcia ze strony dystrybutorów. Wychodząc naprzeciw tym oczekiwaniom, oferujemy naszym klientom szkolenia, zapewniamy wsparcie techniczne na każdym etapie, m.in. projektowe i pomoc przy uruchamianiu systemów. Przewidujemy, że wspólnie z naszymi partnerami osiągniemy wszystkie cele założone na rok 2020, które są jeszcze bardziej ambitne niż w latach poprzednich.

NEDAP

Anna  
Twardowska

Wyniki sprzedaży Nedap Security Management w Polsce sukcesywnie rosną, a ubiegłoroczne przerosły nasze założenia. Ugruntowaliśmy stabilną pozycję na rynku i zdobyliśmy kolejnych kluczowych klientów w sektorach prywatnym i publicznym. Działamy w kilku segmentach rynku, najwięcej projektów realizujemy w zakresie budynków użyteczności publicznej, produkcji, nieruchomości i transportu. Możliwość realizowania ambitnych i ciekawych projektów napędza nas do ciągłego rozwoju.

Rok 2019 to także przeniesienie siedziby w Polsce do nowego większego biura, które świętowaliśmy wraz z klientami i partnerami. Nowa powierzchnia biurowa pozwoliła nam na stworzenie profesjonalnego demo roomu, w którym prezentujemy nasz system kontroli dostępu w integracji z rozwiązaniami naszych firm partnerskich w zakresie biometrii, VMS (Video Management System), depozytorów kluczy, systemów lokalizacji i czytników wielozakresowych. Wieloletnia współpraca z partnerami technologicznymi przynosi efekty w postaci możliwości zaoferowania unikatowych i technologicznie zaawansowanych rozwiązań dostosowanych do indywidualnych potrzeb naszych klientów.

Rozwijamy także naszą sieć partnerską, wprowadziliśmy wiele zmian w programie partnerskim. Nasi partnerzy mają możliwość zdobywania wiedzy podczas certyfikowanych szkoleń, w zakresie zarówno technicznym, jak i sprzedażowym.

To był dla nas bardzo dobry rok. Praca nad naszymi projektami jest zadaniem długofalowym, już teraz widzimy, że dywersyfikacja rynków i procesowanie wielu projektów na różnym etapie realizacji zapewni nam stabilny rozwój w tym roku. Patrzymy bardzo pozytywnie na rok 2020 i zakładamy kolejny przyrost wyników finansowych.

Polon-Alfa

Robert  
Pestka

Początek roku skłania zazwyczaj do posumowań poprzednich dwunastu miesięcy. Jaki był miniony czas? Czy zrealizowane zostały wszystkie plany? Czy pojawiły się nowe wyzwania?

Rok 2019 w firmie POLON-ALFA S.A. to m.in. nieustające umacnianie silnej pozycji na rynku zabezpieczeń przeciwpożarowych, niezwykły dynamiczny wzrost sprzedaży produkowanych urządzeń na rynku krajowym oraz zdecydowana ekspansja na czasami bardzo egzotyczne rynki zagraniczne. W podsumowaniu sprzedaży niekwestionowanym liderem kolejny rok pozostaje system sygnalizacji pożarowej oparty na centrali o architekturze rozproszonej POLON 6000. To właśnie rekordowy wzrost sprzedaży tego systemu był jednym z elementów wpływających na ekspresowe wręcz tempo zakończenia budowy nowych hal produkcyjno-magazynowych. W naszym odczuciu był to właśnie jeden z największych sukcesów ubiegłego roku. Uruchomienie nowych linii produkcyjnych oraz magazynów w nowo oddanych budynkach, których łączna powierzchnia ma ponad 8200 m<sup>2</sup>, w znaczący sposób usprawniły cykl produkcyjny. Nowe moce produkcyjne przyniosły wzrost zatrudnienia – począwszy od stanowisk produkcyjnych, przez inżynierskie, na kadry menedżerskiej kończąc. Duże zainteresowanie, nie tylko na lokalnym rynku, możliwością podjęcia pracy w POLON-ALFA jest najlepszym dowodem na to, że firma jest rzetelnym pracodawcą, zapewniającym duże możliwości rozwoju.

Rok 2019 to również wzmożona działalność marketingowo-szkoleniowa. Aktywne uczestnictwo przedstawicieli firmy w wielu ważnych, krajowych i zagranicznych targach, sympozjach, seminariach i spotkaniach branżowych utwierdziło naszych Partnerów oraz obecnych i przyszłych Klientów w słuszności wyboru systemów sygnalizacji pożarowej sygnowanych logo POLON-ALFA.

Niewątpliwie bardzo ważnym wydarzeniem dla całej polskiej branży security są organizowane już od dwudziestu sześciu lat Ogólnopolskie Warsztaty „Sygnalizacji i Automatyka Pożarowa SAP”. Tegoroczna edycja z tematem wiodącym „Dobre praktyki w zakresie bezpieczeństwa” zgromadziła rekordową liczbę 450 uczestników. W 2019 roku przeprowadziliśmy w siedzibie firmy i najważniejszych miastach kraju szkolenia z zakresu wszystkich produkowanych urządzeń. Uczestniczyło w nich kilkuset projektantów, instalatorów, konserwatorów oraz rzeczoznawców ds. zabezpieczeń przeciwpożarowych.

Co czeka nas w roku 2020? Nieustająca praca nad nowymi kierunkami sprzedaży, odpowiadanie na ciągle rosnące potrzeby Klientów i oczywiście nowe produkty. W najbliższym czasie wejdą do oferty: nowa Centrala Automatycznego Gaszenia IGNS 2500, Pożarowy Zasilacz Buforowy z serii PZB-6000, konwencjonalne i adresowalne Sygnalizatory Akustyczne – Optyczne SAB-6000 i inne.

Zapraszamy do kontaktu z firmą POLON-ALFA oraz do uczestnictwa w organizowanych przez nas szkoleniach i warsztatach.

Roger

Grzegorz  
Wensker

Rok 2019 był bardzo dobry dla sektora budownictwa, w szczególności budownictwa powierzchni biurowych pod wynajem. Koniunktura ta skutkowała m.in. dużym zapotrzebowaniem na różnego rodzaju systemy elektroniczne stosowane w tego typu budynkach. Ważną rolę odgrywają tu systemy kontroli dostępu i automatyki budynkowej.

Do tej pory w zasadzie cały rynek rozwiązań kontroli dostępu dla biznesu był zdominowany przez rozwiązania renomowanych firm zachodnich, takich jak Bosch czy Honeywell, które nie miały liczącej się lokalnej konkurencji. Wydaje się, że w 2019 r. sytuacja ta zmieniła się za sprawą systemu RACS 5. W roku 2016 firma Roger wprowadziła do oferty system kontroli dostępu i automatyki budynkowej RACS 5, zaprojektowany w oparciu na wieloletnim doświadczeniu firmy zdobytym w trakcie projektowania i sprzedaży prostszych funkcjonalnie rozwiązań kontroli dostępu przeznaczonych dla małych i średnich obiektów. System RACS 5 był projektowany z myślą o wykorzystaniu w dużych obiektach i zakwalifikowaniu go do klasy tzw. Enterprise – systemów przeznaczonych dla biznesu. Jego powstanie było możliwe nie tylko dzięki rozwojowi potencjału inżynierskiego firmy, ale także dzięki wzrostowi możliwości komponentów elektronicznych, przede wszystkim mocy obliczeniowej i możliwości procesorów stosowanych w urządzeniach elektroniki budynkowej.

Z oczywistych względów decyzja o wyborze nowego systemu przeznaczanego do wykorzystania w inwestycjach budowlanych o budżetach na poziomie dziesiątków czy setek milionów złotych nie jest łatwa i z reguły odbywa się na drodze ewolucji, jeśli oczywiście poziom techniczny i funkcjonalny produktu oraz jego niezawodność będą w miarę wpływu czasu dowodziły jego przydatności dla tego typu zastosowań. Tak też działo się z systemem RACS 5, który z roku na rok zdobywał kolejnych zadowolonych odbiorców, a opinia o jego walorach rozchodziła się wśród projektantów budynków. Na jego sukces złożyło się również to, że jest on produktem krajowym. Polityka firmy Roger dopuszczająca dostosowywanie jego funkcjonalności do indywidualnych wymagań inwestycji istotnie ułatwiała pozyskanie kolejnych projektów. Można powiedzieć, że rok 2019 był pod pewnym względem przełomowy, gdyż w tym roku system RACS 5 został zastosowany do kontroli ponad 17 tys. przejść, w dużej mierze znajdujących się w nowo budowanych biurach. Można zaryzykować stwierdzenie, iż stał się znaczącym konkurentem produktów zachodnich.

Przewiduje się, że pomimo już obserwowanego i prognozowanego na rok 2020 spowolnienia gospodarczego wywołanego czynnikami o charakterze zarówno globalnym, jak i lokalnym, rynek budownictwa biurowego będzie nadal generował bardzo dobre wyniki, chociażby z tego powodu, że inwestycje budowlane realizowane w 2020 r. zostały już wcześniej zaplanowane i zabudżetowane, a bieżące negatywne trendy w gospodarce nie będą miały na niego istotnego wpływu.

SATEL

Agnieszka  
Pitrus

Rok 2019 już za nami. W SATEL był to, jak zawsze, czas wyjątkowej pracy i podejmowania nowych, ciekawych wyzwań. Wyśięk przyniósł oczekiwane efekty – znacznie rozszerzyliśmy naszą ofertę produktową, weszliśmy na kolejne rynki: australijski i irlandzki, zintensyfikowaliśmy działania edukacyjne skierowane do profesjonalistów.

Niezmiennie od lat opinie użytkowników naszych urządzeń są dla nas istotnym czynnikiem podczas podejmowania decyzji dotyczących oferty SATEL. Badania satysfakcji klienta wyraźnie pokazują, że szeroka funkcjonalność, wygoda obsługi i jakość, a przy tym ciekawy design to stałe oczekiwania rynku. Dynamicznie rośnie popyt na systemy bezprzewodowe, funkcje smart home oraz integrację SSWiN z KD i automatyką budynkową.

Systemy SATEL od lat skutecznie wykrywają próby włamania, a także zdarzenia losowe: pożar, zalanie czy pojawienie się szkodliwych gazów. Centrale INTEGRA oferują również wygodne sterowanie podstawowymi funkcjami automatyki budynkowej. W roku 2019 poszliśmy o krok dalej – wprowadziliśmy moduły do realizacji wspomnianych zaawansowanych funkcji smart home w standardzie KNX. Warto podkreślić, że funkcje automatyki mogą być wygodnie obsługiwane przy użyciu manipulatora dotykowego tudzież aplikacji mobilnej służących do sterowania SSWiN. To znacznie wpływa na ekonomiczność całej instalacji.

W ubiegłym roku Dział Badań SATEL uzyskał akredytację KNX Association. Nowo powstałe Akredytowane Laboratorium Testów KNX jest jednym z szesnastu na świecie i pierwszym w Europie Wschodniej uprawnionym do testowania współdziałania i funkcjonalności urządzeń KNX oraz ich oprogramowania. To dla nas duże wyróżnienie, potwierdzające gruntowną wiedzę specjalistów SATEL w zakresie systemów KNX.

Wiosną 2019 r. z sukcesem wprowadziliśmy także dwukierunkowy system bezprzewodowy ABAX 2. Rozwiązania radiowe cieszą się rosnącą popularnością m.in. ze względu na łatwy montaż, bez naruszania konstrukcji budynku. Nasz najnowszy system wyróżnia się na rynku, m.in. wyjątkowo długą (nawet do 8 lat) pracą urządzeń bez konieczności wymiany baterii, a także imponującym, sięgającym aż 2 km zasięgiem działania.

W naszej ofercie pojawiła się nowa linia czujek ruchu SLIM LINE. To seria 10 urządzeń – PIR oraz dualnych – o dużym obszarze detekcji i kącie widzenia 90°. Jedną z czujek, SLIM-PIR-LUNA, została wyróżniona w konkursie „Dobry Design 2020”.

Debiut miały również dwa nowe zasilacze buforowe: APS-1412 i APS-724 o dużej sprawności energetycznej (>90%) i bardzo dobrych stabilnych parametrach zasilania. Oprócz nich zaprezentowaliśmy także nowe moduły komunikacyjne: GSM-X LTE i GPRS-A LTE, obsługujące transmisję danych w technologii LTE. Co przed nami?

W 2020 roku SATEL obchodzi 30-lecie działalności. To dodatkowy impuls do mierzenia się z kolejnymi wyzwaniami, zdobywania nowych rynków i wprowadzania kolejnych urządzeń, z dbałością o najwyższą jakość, funkcjonalność i konkurencyjność naszych produktów.

Schrack Seconet Polska

Grzegorz  
Ćwiek

Miniony rok był dla nas wyjątkowy pod wieloma względami. W 2019 roku rozpoczęliśmy bowiem kolejną dekadę obecności marki w Polsce, miał to być też rok rozstrzygnięcia wielu ważnych kontraktów, o które staraliśmy się od lat. Wiosną zapowiedzieliśmy także przygotowania do zmian osobowych w Zarządzie Spółki. Choć ogłosiliśmy je na rok przed wdrożeniem, nie byliśmy pewni, jak zostaną odebrane przez rynek i naszych Klientów czy Partnerów oraz jaki będzie miało to wpływ na naszą bieżącą działalność.

Po 12 miesiącach wyjątkowej pracy okazało się, że nasze starania zaowocowały najlepszym w historii firmy wynikiem sprzedaży, pozytywnym rozstrzygnięciem kluczowych dla nas konkursów ofertowych oraz niezliczonymi wyrazami wsparcia i kontynuacji zaufania. Do tego odnotowaliśmy rekordową liczbę uczestników naszych imprez szkoleniowych i znacznie zwiększone zainteresowanie przystąpieniem do naszej sieci partnerskiej. Można zatem powiedzieć, że stabilność i przewidywalność naszej organizacji, wspierana otwartą i szczerą komunikacją z rynkiem oraz niezmiennie wysoką jakością produktów i usług (realizowanych zarówno przez nas, jak i Autoryzowanych Partnerów), to fundamenty naszego wielkiego sukcesu w roku 2019.

Na przestrzeni trzynastu lat mojej obecności w firmie jako prezesa Zarządu ubiegły rok był dziesiątym kolejnym rokiem nieprzerwanego wzrostu wyników sprzedaży i zarazem dwunastym rokiem wzrostu wyników firmy. Niewiele firm na rynku może pochwalić się taką statystyką i niewielu członków zarządu ma w swojej karierze możliwość wspierania tak dynamicznego rozwoju firmy i zespołu, z którym pracuje. W tym roku zarówno nas, jak i naszych Autoryzowanych Partnerów czeka wiele wyzwań. Po pierwsze skupiamy się na zadaniach realizacyjnych, ponieważ w roku 2019 wyposażyliśmy w systemy bezpieczeństwa pożarowego, dźwiękowe systemy ostrzegawcze i systemy komunikacji (przyzywowe) blisko 1000 obiektów budowlanych. W tym samym czasie zbudowaliśmy potężny portfel zamówień na rok 2020 i lata kolejne, co sprawia, że poziom zaangażowania zarówno naszego zespołu, jak i naszej sieci partnerów osiąga niespotykane dotąd rozmiary.

Dynamicznie zaangażowaliśmy się też w rozwój rynku systemów zintegrowanych, na którym mamy już ogromne doświadczenie. Realizujemy projekty o niezwykle dużym stopniu zaawansowania technicznego i organizacyjnego. Staliśmy się zdecydowanym liderem w tym obszarze i takiej pozycji będziemy bronić. Ponadto przygotowujemy się do wprowadzenia do sprzedaży kolejnej generacji systemów sygnalizacji pożarowej (pierwszy kwartał 2021) i już teraz nad tym pracujemy. Niezmiennie wprowadzanie nowych produktów będzie realizowane w sposób ewolucyjny – czyli taki, do którego przyzwyczailiśmy już naszych klientów w ponad 50 krajach świata. Wyzwaniem nie tylko dla nas, ale także całego rynku mogą być coraz bardziej zmienne warunki działalności gospodarczej, zawirowania na rynku inwestycyjnym, na które wpływ ma ryzyko wynikające ze zmian politycznych (zbliżające się wybory prezydenckie w Polsce), prawno-ekonomicznych (lokalnie – zmiany w prawie pracy, alokacji środków budżetowych, sądownictwie oraz globalnie – np. wybory prezydenckie w USA czy wyjście Wlk. Brytanii z UE i związana z tym niepewność co do inwestycji realizowanych przy udziale kapitału brytyjskiego).

Cały czas obserwujemy także niedostatek wykwalifikowanych pracowników, co miało wpływ na spowolnienie tempa realizacji wielu znaczących projektów inwestycyjnych w całym kraju. Ta tendencja będzie się utrzymywać, ale moim zdaniem w dłuższej perspektywie przyniesie to korzyści dla naszej branży.

Trudno przewidzieć, jaki będzie rozwój rynku security w Polsce w 2020 r. Perspektywa ma przynajmniej dwie warstwy: ekonomiczną i techniczną. W warstwie ekonomicznej z pewnością uwidocznią się dalsze opóźnienia w realizacjach inwestycji budowlanych wynikające z niedostępności pracowników na rynku pracy. Spowodują także ochłodzenie koniunktury w gospodarce polskiej i europejskiej (spodziewane i chyba już widoczne w innych branżach), które odczujemy nieco później i nieco łżej. Patrząc z kolei na warstwę techniczną możliwości rozwojowych, choć wielu producentów zapowiedziało na ten rok premierę nowości produktowych, nie należy się spodziewać wejścia na rynek przełomowych technologii czy rozwiązań. Z pewnością dobrym miejscem, by przekonać się o kierunkach rozwoju rynku w najbliższym czasie, będą targi Securex 2020. Obecni tam wystawcy z pewnością będą prezentowali swoje najnowsze rozwiązania, nakreślając tym samym nowy obraz rynku. Nas z pewnością tam nie zabraknie. Gorąco zapraszamy do kontynuacji rozmów na ten temat właśnie w Poznaniu. Tymczasem w imieniu swoim, koleżanek i kolegów z firmy – życzę Państwu wszystkiego dobrego w nowym roku i zapraszam do kontaktu z nami.

Securitas

Krzysztof  
Bartuszek

Zasadniczo rok 2019 mógłbym podsumować podobnie jak kilka poprzednich lat. Wiele nadziei na pozytywne zmiany, a w rzeczywistości wiele wyzwań, czyli ciężka praca w trudnych warunkach, która mimo wszystko na koniec dnia daje dużo satysfakcji. Z perspektywy Securitas – zrealizowaliśmy założone cele.

Od wielu lat świadomie stosujemy strategię zakładającą rozwój naszych usług na trzech poziomach. W naszym przypadku rok to nie okres rewolucji, ale świadoma ewolucja, trwająca od kilkunastu lat. Po pierwsze – naszym kapitałem są ludzie. W dalszym ciągu uważamy, że mimo stosowania zaawansowanych technologii to oni determinują efektywność usług z zakresu szeroko rozumianego bezpieczeństwa. Oczywiście zmienia się profil pracownika, jego zadania, tak jak zmieniają się potrzeby klientów, zagrożenia i chronione obiekty. Inwestujemy w naszych pracowników, szkolimy ich, podnosimy kwalifikacje, zachęcamy do poszukiwania nowych rozwiązań oraz wprowadzamy narzędzia, które pracownikom ułatwiają pracę, a zarządzającym umożliwiają digitalizację i optymalizację procesów. Drugim trendem, z którym się utożsamiamy i w który stale inwestujemy, są zintegrowane systemy bezpieczeństwa, a więc przede wszystkim obszar zabezpieczeń technicznych. Coraz doskonalsze rozwiązania techniczne mają być „supercami”, którymi możemy wesprzeć naszych pracowników, a co za tym idzie efektywniej realizować zadania na rzecz klientów. Trzecią platformą rozwoju to usługi inteligentne – czyli nasza przyszłość. Sztuczna inteligencja, predykcja, robotyka – to tylko kilka hałset kryjących się za tym nurtem. W roku 2019 na każdym z tych pól zrobiliśmy postępy, mamy kilka ciekawych wdrożeń. I to cieszy. Co ważne, z każdym kolejnym rokiem do naszych wizji udaje się nam przekonać coraz więcej klientów, a to cieszy podwójnie.

Wspomniałem o nadziejach i wyzwaniach, a tych nam na pewno nie brakuje. Oczywiście koszty rosną, ale z tym muszą mierzyć się wszyscy, więc w tej kwestii nie ma co narzekać – jak co roku trzeba zakasać rękawy i ciężko pracować. Boli nieco fakt, że nasza branża jest mocno zróżnicowana, a modele biznesowe są niestety nie zawsze do końca uczciwe, a co za tym idzie, często walczyliśmy nie pomysłami, ale ceną. W 2019 r. spore nadzieje wiązałyśmy z zapowiadaniem ozusowaniem zleceń, co według nas byłoby transparentnym rozwiązaniem, wyrównującym szanse i niepozostawiającym niedomówień w obszarze zatrudnienia pracowników. Cały czas czekamy również na nowelizację ustawy o ochronie osób i mienia, która ma już swoje lata. Myślę, że dobrze by było, gdyby nowe przepisy uwzględniły chociaż postęp technologiczny, jaki nastąpił, a może również uregulowałyby kwestie osób niepełnosprawnych w ochronie. Na razie wszystko wskazuje na to, że nasze nadzieje i wyzwania będą aktualne również w roku 2020, a w wymiarze wzrostu plac i kosztów – także w kolejnych latach. Jako Securitas będziemy podążać wcześniej obraną drogą, gdyż wierzymy, że zmiany i wyzwania to nie tylko zagrożenia, ale przede wszystkim szansa na rozwój i innowacyjność dla całej branży.

Suma

Robert  
Stanosz

Rok 2019 był dla naszej firmy 30. rokiem działalności. Te lata doświadczeń spowodowały, że szerzej spoglądamy na branżę security, na kolejne „rewolucje i wyzwania”. Wejście firmy w czwartą dekadę działalności skłania do podsumowań.

W minionym roku dała się zaobserwować dojrzałość rynku do usług jakościowych i zwiększone chęci do ich zakupu. Dziś pod otoczką marketingu tysiące firm sprzedaje „zaawansowane technologie”, których wynik działania wnosi niewielką wartość dla inwestycji. Klienci zaczynają to zauważać, dostrzegają, że są różne „lody truskawkowe”. To polaryzuje rynek na firmy zorientowane na produkty, eksperymentujące z technologią i takie firmy, które poszukują dojrzałych rozwiązań. To ciekawe doświadczenie, gdy spotykamy się pod wspólnym mianownikiem nowoczesnych rozwiązań. Ogromnym wyzwaniem jest wskazanie i pomoc klientowi w dostrzeżeniu różnic pomiędzy dojrzałymi rozwiązaniami, a tymi najpopularniejszymi na rynku – szczególnie gdy rywalizację sprowadza się do gry cenowej.

Rok 2020 rozpoczęliśmy właśnie od dopasowania naszej struktury organizacyjnej do potrzeb klientów, jakie obserwujemy od pewnego czasu. Oprócz znanej dystrybucji i szkoleń dla firm instalacyjnych, które prowadzimy od ponad 15 lat, rozszerzyliśmy nasze działania o centrum kompetencji. Zaoferowaliśmy naszym Partnerom wspólne działania z inwestorem w trakcie inwestycji, szkolenie kadr firm instalacyjnych oraz ich wsparcie w projektowaniu i we wskazaniu inwestorom ich kompetencji. W dalszym ciągu planujemy pozostanie w głównym nurcie specjalizacji w zakresie obsługi rynków wertykalnych i poszerzaniu oferty specjalistycznej. Naszym priorytetem będzie bliska współpraca z Partnerami i inwestorami, a celem zaoferowanie inwestorowi korzyści z synergii całego kanału: od sprzedaży, przez integrację, po eksploatację.



# Technologie przyszłości – w służbie człowieka

HIPERAUTOMATYZACJA, BLOCKCHAIN, BEZPIECZEŃSTWO AI, CHMURA ROZPROSZONA I URZĄDZENIA AUTONOMICZNE TO GŁÓWNE ZAGADNIENIA, O KTÓRYCH ZROBI SIĘ GŁOŚNO W TYM ROKU. BĘDĄ ONE DOMINOWAĆ W TEGOROCZNYCH TRENDACH TECHNOLOGICZNYCH.

# P

Poprawianie człowieka przywołuje wizje futurystycznych cyborgów, ale ludzie ulepszają części ciała od setek lat. Okulary, aparaty słuchowe i protetyka przekształciły się w implanty ślimakowe, soczewki kontaktowe. Nawet laserowa chirurgia oka stała się powszechna. A gdyby naukowcy mogli ulepszyć mózg, aby zwiększyć pamięć, lub wszczepić chip do dekodowania wzorów neuronowych? Co będzie, jeśli egzozoskielety staną się standardowym mundurem dla osób pracujących w przemyśle samochodowym, umożliwiając im podnoszenie nadludzkich ciężarów? A jeśli lekarze będą mogli wszczepiać czujniki, aby śledzić, jak leki przemieszczają się w ciele?

Technologia jest teraz na progu wychodzenia poza ulepszenia, które zastępują ludzkie możliwości, w ulepszenia, które tworzą nadludzkie zdolności. Wpływ tych zmian na świat i biznes sprawia, że poprawianie ludzi jest jednym z 10 strategicznych trendów technologicznych wg Gartnera, które będą stwarzać szanse rozwoju w ciągu najbliższych od pięciu do dziesięciu lat. Trendy są oparte na idei „inteligentnych przestrzeni zorientowanych na człowieka”, co oznacza rozważenie, w jaki sposób te technologie wpłyną na ludzi (tj. klientów, pracowników) i miejsca, w których żyją (tj. dom, biuro, samochód).

– Te trendy mają głęboki wpływ na nas i miejsca, w których mieszkamy – powiedział Brian Burke, wiceprezes ds. badań w firmie Gartner, podczas Gartner 2019 IT Symposium/Xpo™ w Orlando na Florydzie. – Zamiast tworzyć nowe technologie, a następnie badać potencjalne ich zastosowania, organizacje muszą najpierw wziąć pod uwagę kontekst biznesowy i ludzki.

Trendy te nie istnieją w oderwaniu, liderzy IT muszą zdecydować, która kombinacja trendów najbardziej sprzyja innowacji i jest zgodna z ich strategią. Dla przykładu sztuczną inteligencję (AI) w postaci uczenia maszynowego (ML) z hiperautomatyzacją i przetwarzaniem brzegowym można łączyć, aby stworzyć wysoce zintegrowane inteligentne budynki i przestrzenie miejskie. Z kolei te kombinacje technologii umożliwiają dalszą demokratyzację technologii.



## TREND 1. Hiperautomatyzacja

Automatyzacja wykorzystuje technologię do automatyzacji zadań, które kiedyś wymagały udziału ludzi. Hiperautomatyzacja zajmuje się zastosowaniem zaawansowanych technologii, w tym sztucznej inteligencji (AI) i uczenia maszynowego (ML) w celu coraz większej automatyzacji procesów i wspomagania ludzi. Obejmuje ona szereg narzędzi, które można zautomatyzować, ale odnosi się również do wyspecjalizowanej automatyzacji, tj. odkrywania, analizowania, projektowania, automatyzacji, pomiaru, monitorowania, ponownej oceny. Hiperautomatyzacja często powoduje powstanie cyfrowego bliźniaka organizacji. Ponieważ żadne pojedyncze narzędzie nie może zastąpić człowieka, hiperautomatyzacja obejmuje dziś kombinację narzędzi, w tym zrobotyzowaną automatyzację procesów (RPA), inteligentne oprogramowanie do zarządzania przedsiębiorstwem (iBPMS) i sztuczną inteligencję, której celem jest podejmowanie decyzji w coraz większym stopniu opartych na sztucznej inteligencji.

Chociaż nie jest to główny cel, hiperautomatyzacja często skutkuje stworzeniem cyfrowego bliźniaka organizacji (DTO), umożliwiając wizualizację interakcji funkcji, procesów i kluczowych wskaźników wydajności, aby uzyskać lepszą wartość. DTO staje się następnie integralną częścią procesu hiperautomatyzacji, zapewniając w czasie rzeczywistym ciągłą analizę otoczenia organizacji, znacząco stymulując możliwości biznesowe.



## TREND 2. Wszechdoświadczenie

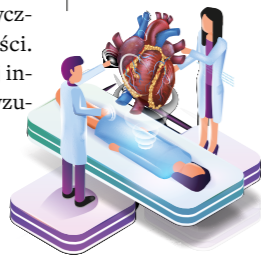
Wszechdoświadczenie zastępuje ludzi znajdujących się na technologii na technologię rozumiejącą ludzi. W tym nurcie tradycyjna idea komputera ewoluje od jednego punktu interakcji, obejmując interfejsy wielosensorowe i wielowymiarowe, takie jak urządzenia do noszenia i zaawansowane czujniki elektroniczne.

Domino's Pizza np. stworzyła coś więcej niż posiłek zamawiany przez aplikację, wprowadziła bowiem autonomiczne pojazdy, rozwiązania umożliwiające śledzenie zamówionej pizzy i komunikację opartą na zaawansowanych technologicznie głośnikach. W przyszłości trend ten stanie się tzw. doświadczeniem ambientowym, ale obecnie wszechdoświadczenie koncentruje się na przeżyciach, które wykorzystują rozszerzoną rzeczywistość (AR), wirtualną (VR), rzeczywistość mieszaną, wielokanałowe interfejsy człowiek-maszyna i technologie sensoryczne. Połączenie tych technologii może być wykorzystane do prostej nakładki AR lub wciągającej rzeczywistości VR.



### TREND 3. Demokratyzacja

Demokratyzacja technologii oznacza zapewnienie ludziom łatwego dostępu do wiedzy technicznej lub biznesowej bez obszernego (i kosztownego) szkolenia. Koncentruje się na czterech kluczowych obszarach: tworzeniu aplikacji, danych i analizie, projektowaniu i wiedzy. Często jest określany jako „dostęp obywatelski” (powszechny dostęp do informacji), co doprowadziło do wzrostu liczby osób zajmujących się danymi i programistami. Demokratyzacja pozwoliłaby np. twórcom oprogramowania generować modele danych bez posiadania specjalistycznej wiedzy, jaką posiadają specjaliści. Zamiast niej polegałoby na sztucznej inteligencji generującej kod i automatyzującej proces testów.



### TREND 4. Ulepszanie człowieka

Ulepszanie ludzi polega na wykorzystaniu technologii w celu poprawy poznawczych i fizycznych doświadczeń danej osoby. Fizyczne ulepszanie zmienia zdolność fizyczną poprzez wszczepienie lub umieszczenie technologii wewnątrz lub na ciele. Przykładem mogą być branża motoryzacyjna lub górnicza, w których używa się ubrań, aby poprawić bezpieczeństwo pracowników. W innych branżach, np. w handlu detalicznym, urządzenia noszone na ciele są używane do zwiększenia wydajności pracowników.

Augmentacja fizyczna dzieli się na cztery główne kategorie: augmentacja sensoryczna (słuch, wzrok, percepcja), ulepszenie funkcji biologicznych poprzez zastosowanie dodatków (egzoszkielety, protetyka), ulepszenie mózgu (implanty w leczeniu napadów) i ulepszenie genetyczne (gen somatyczny i terapia komórkowa).

Wspomaganie poznawcze zwiększa zdolność człowieka do myślenia i podejmowania lepszych decyzji, np. poprzez wykorzystywanie informacji i aplikacji w celu poprawy uczenia się lub zdobywania nowych doświadczeń. Zwiększanie zdolności poznawczych obejmuje również pewną technologię z kategorii ulepszania mózgu, ponieważ są to implanty fizyczne, które zajmują się rozumowaniem poznawczym. Ulepszanie człowieka ma szereg implikacji kulturowych i etycznych, np. użycie technologii CRISPR do wzmocnienia genów ma znaczące implikacje etyczne.

### TREND 5. Przejrzystość i identyfikowalność

Ewolucja technologii powoduje kryzys zaufania. Ponieważ konsumenci stają się bardziej świadomi sposobu gromadzenia i wykorzystywania ich danych, organizacje dostrzegają również rosnącą odpowiedzialność za ich przechowywanie i gromadzenie. Ponadto AI i ML są coraz częściej wykorzystywane do podejmowania decyzji, wyręczając w tym ludzi, przyczyniając się do ewolucji kryzysu zaufania, co wzmaga zapotrzebowanie na wyjaśnienie działania AI i zarządzanie AI. Ten trend wymaga skoncentrowania się na sześciu kluczowych elementach zaufania: etyce, uczciwości, otwartości, rozliczalności, kompetencjach i spójności.

Na całym świecie jest wprowadzane ustawodawstwo, podobne do rozporządzenia o ochronie danych osobowych (RODO), nadające kierunek ewolucji i ustanawiające podstawowe zasady postępowania.

### TREND 6. Wzmocnienie brzegu sieci

Przetwarzanie brzegowe to topologia, w której przetwarzanie informacji, ich gromadzenie i dostarczanie są umieszczone bliżej źródeł informacji, kierując się zasadą, że utrzymanie lokalnego i rozproszonego ruchu zmniejszy opóźnienia. Obejmuje to całą technologię w Internecie Rzeczy (IoT). Wzmocnienie brzegowe przyczynia się do tworzenia podstaw inteligentnych przestrzeni, przybliżając kluczowe aplikacje oraz usługi bliżej ludzi i urządzeń, które ich używają.

Do 2023 r. na brzegu sieci może być ponad 20 razy więcej inteligentnych urządzeń niż w zwykłych urządzeniach IT.



### TREND 7. Chmura rozproszona

Chmura rozproszona oznacza dystrybucję publicznych usług chmurowych do lokalizacji poza fizycznymi centrami danych dostawcy chmury, które są nadal kontrolowane przez dostawcę. W chmurze rozproszonej dostawca chmury jest odpowiedzialny za wszystkie aspekty architektury usług: dostarczania, operacji, zarządzania i aktualizacji. Ewolucja od scentralizowanej chmury publicznej do rozproszonej chmury publicznej wprowadza nową erę przetwarzania w chmurze.

Chmura rozproszona umożliwia lokalizację centrów danych w dowolnym miejscu. Rozwiązuje to zarówno problemy techniczne, takie jak opóźnienie, jak i wyzwania regulacyjne, takie jak suwerenność danych. Oferuje także zalety obu usług: chmury publicznej i prywatnej chmury lokalnej.



### TREND 8. Urządzenia autonomiczne

Urządzenia autonomiczne, w tym drony, roboty, statki i maszyny, wykorzystują sztuczną inteligencję do zadań zwykle wykonywanych przez ludzi. Ta technologia działa na podstawie danych zebranych w sposób półautonomiczny lub w pełni autonomiczny, w różnych środowiskach, w tym w powietrzu, na morzu i na lądzie. Chociaż obecnie autonomiczne urządzenia funkcjonują głównie w zamkniętych obiektach, takich jak kopalnie lub magazyny, ostatecznie ewoluują, aby funkcjonować w otwartych przestrzeniach publicznych. Autonomiczne urządzenia przejdą również z funkcjonowania samodzielnego do współpracujących rojów, takich jak roje dronów używane podczas Zimowych Igrzysk Olimpijskich w 2018 roku.

Urządzenia autonomiczne nie mogą jednak zastąpić ludzkiego mózgu i działają najskuteczniej w oparciu na wąsko zdefiniowanym, dobrze sprecyzowanym celu.



### TREND 9. Praktyczny blockchain

Blockchain jest rodzajem rozproszonej księgi rachunkowej, z rozwijającą się chronologicznie uporządkowaną listą podpisanych kryptograficznie, nieodwołalnych zapisów transakcyjnych udostępnianych wszystkim uczestnikom sieci. Pozwala również stronom na prześledzenie historii zasobów od początku ich powstania, co jest korzystne dla tradycyjnych aktywów, ale może też być wykorzystane do innych zastosowań, takich jak śledzenie chorób przenoszonych przez żywność, aż do pierwotnego dostawcy. Umożliwia także dwóm lub więcej stronom, które się nie znają, bezpieczną inte-

rakcję w środowisku cyfrowym i wymianę wartości bez potrzeby powiadomiania scentralizowanego organu.

Kompletny model *blockchain* składa się z pięciu elementów: współdzielonej i rozproszonej księgi rachunkowej, niezmiennej i identyfikowalnej księgi rachunkowej, szyfrowania, żetonizacji i mechanizmu rozproszonego publicznego konsensusu. *Blockchain* pozostaje jednak niedojrzały w przypadku wdrożeń korporacyjnych z powodu szeregu problemów technicznych, w tym słabej skalowalności i interoperacyjności.

*Blockchain*, który pojawia się już w eksperymentalnych i małych projektach, będzie w pełni skalowalny do 2023 r.

Obecnie korporacyjne łańcuchy bloków przyjmują praktyczne podejście i wdrażają tylko niektóre elementy pełnego łańcucha. W ten sposób uniezależniają księgę rachunkową od poszczególnych aplikacji i uczestników, a replikując ją w sieci rozproszonej, tworzą wiarygodny zapis istotnych wydarzeń. Każdy z uprawnionym dostępem widzi te same informacje, a integrację upraszcza wspólny łańcuch bloków. Konsensus jest obsługiwany przez bardziej tradycyjne modele prywatne.

### TREND 10. Bezpieczeństwo AI

Ewolujące technologie, takie jak hiperautomatyzacja i urządzenia autonomiczne, oferują możliwości transformacji w świecie biznesu. Tworzą jednak również luki w zabezpieczeniach i nowe potencjalne punkty ataku. Działy bezpieczeństwa muszą sprostać tym wyzwaniom i mieć świadomość, jak sztuczna inteligencja wpłynie na poziom zabezpieczenia ich firm. Bezpieczeństwo AI ma trzy kluczowe perspektywy:

1. Ochrona systemów wykorzystujących AI – zabezpieczanie danych treningowych AI, koncepcji szkoleniowych i modeli ML.
2. Wykorzystanie sztucznej inteligencji do poprawy bezpieczeństwa – używanie ML do zrozumienia wzorców, odkrywania ataków i automatyzacji części procesów cyberbezpieczeństwa.
3. Przewidywanie wykorzystywania AI przez atakujących – identyfikacja ataków i obrona przed nimi.

Opracowano na podstawie Raportu Gartner

*Gartner jest wiodącą firmą badawczą i doradcą założoną w 1979 r. Wychodzi znaczenie poza standardowe badania technologiczne, aby zapewnić kierownictwu wyższego szczebla w przedsiębiorstwach niezbędne informacje biznesowe, porady i narzędzia, których potrzebują, aby osiągnąć najważniejsze cele i zbudować organizację przyszłości.*



# 5 trendów technologicznych na rok 2020 które pomogą zmienić miasto w *smart city*

Coraz więcej mówi się o rozwoju miast w kontekście ich przemiany w smart city. Najważniejszym aspektem tej transformacji jest technologia – to właśnie ona może sprawić, że aglomeracje staną się bezpieczniejsze, a ich mieszkańcy bardziej mobilni. W roku 2020 kluczowe znaczenie w tym zakresie będzie miała przede wszystkim analiza na krawędzi sieci oraz wykorzystanie chmur prywatnych i hybrydowych.

Rozpatrując trendy technologiczne, które mogą odegrać najważniejszą rolę w nowym roku, oprócz technologii na pierwszy plan wysuwają się także kwestie regulacyjne związane z bezpieczeństwem i prywatnością. Istotne będą również możliwości urządzeń, w tym rosnąca moc obliczeniowa. Przedstawiamy pięć najważniejszych elementów, które będą kształtowały obraz smart city w 2020 r.

## 1 NA KRAWĘDZI SIECI

Obecnie do sieci są już podłączone miliardy urządzeń, a liczba ta z roku na rok stale się powiększa. Wraz z nią rośnie także dynamika obliczeń i analiz wykonywanych na krawędzi sieci (w jej urządzeniach brzegowych). Wynika to głównie z charakteru i wymagań urządzeń, które – aby spełniać swoje zadania – muszą dziś mieć możliwość natychmiastowej, samodzielnej reakcji. Oczywistym tego przykładem są autonomiczne auta. By skutecznie dostrzegać potencjalne ryzyko, np. obiekt znajdujący się na drodze, muszą podejmować decyzje w ułamku sekundy. Nie byłoby to możliwe, gdyby dane wysyłane z samochodu musiały trafiać najpierw do centrum danych. Proces przetwarzania i analizy byłby wówczas zbyt długi, uniemożliwiając skuteczną reakcję w odpowiednim czasie.

Podobnie jest w przypadku innych urządzeń, np. kamer monitoringu. – *Aby miasto mogło stać się prawdziwym smart city, systemy wizyjne powinny umożliwiać natychmiastowe reakcje, a nie być tylko wsparciem, np. w postępowaniu dowodowym. Przejście do działań praktycznych będzie możliwe tylko wtedy, kiedy kamery same będą dokonywały analizy potencjalnych zagrożeń i automatycznie informowały o nich odpowiednie służby* – podkreśla Konrad Badowski, Business Relationship Manager w Axis Communications.

## 2 WIĘKSZA MOC OBLICZENIOWA

Aby przejście na krawędź sieci było możliwe, niezbędna jest także optymalizacja sprzętu i oprogramowania. Tym samym coraz więcej urządzeń będzie musiało dysponować zwiększoną mocą obliczeniową. Bardziej popularna stanie się także koncepcja wbudowanej w urządzenie sztucznej inteligencji wykorzystującej uczenie maszynowe. Już w tej chwili coraz więcej firm zauważa, że to element niezbędny do ich rozwoju. Wyzwaniem może się jednak okazać opracowanie nowych, „łżejszych” modeli, które będą potrzebowały mniej pamięci i mocy obliczeniowej. W kontekście miast może to pomóc w podniesieniu

poziomu ich bezpieczeństwa, a także mobilności mieszkańców. Już dziś w transporcie publicznym kamery wyposażone we własne procesory i aplikacje mogą analizować zachowanie kierowcy, np. autobusu. Z kolei takie kamery zainstalowane na zewnątrz pojazdu komunikacji miejskiej mogą działać jak cyfrowe lusterka, pomagając prowadzącemu w umiejmiejnym i bezpiecznym wykonaniu np. skomplikowanego manewru. W niedalekiej przyszłości kamery będą także samodzielnie analizowały, czy podnoszone ze sklepowych półek produkty nie są kradzione, lub informowały o ewentualnych nieprawidłowościach w dostawie przesyłek. Umożliwiają to procesory nowej generacji, np. Artpec 7 od Axis Communications, które znacznie poprawiły możliwości analityczne oraz ułatwiają optymalizację cyberochrony w systemach zabezpieczeń.

## 3 KROK W KIERUNKU BEZPIECZEŃSTWA

Podniesienie poziomu zaufania do technologii to jeden z kolejnych kluczowych trendów, ale również wyzwanie. Ważne jest bowiem, by mieć pewność, że organizacje gromadzą i wykorzystują dane w sposób odpowiedzialny, a urządzenia są zabezpieczone przed cyberprzestępcami. Właśnie krawędź sieci w niedalekiej przyszłości okaże się punktem, w którym konieczne będzie zadbanie o bezpieczeństwo.

Zasadnicze znaczenie ma w tym kontekście zabezpieczenie całego łańcucha dostaw. Osadzenie chipów szpiegowskich w sprzęcie jest raczej odległe. Łatwiej zainstalować oprogramowanie szpiegujące we wprowadzonym na rynek urządzeniu, a później dokonywać jego aktualizacji, niż robić to na etapie jego produkcji. Przy zwiększonej liczbie danych przetwarzanych w urządzeniach bezpieczeństwo cyfrowe stanie się elementem krytycznym. Podstawą bezpiecznego systemu jest zarządzanie zarówno poszczególnymi urządzeniami, jak i całym cyklem życia danego rozwiązania oraz wszystkimi jego elementami: sprzętem, oprogramowaniem i użytkownikami. W kontekście smart city, oprócz cyberbezpieczeństwa, istotne będą także kwestie związane z prywatnością. – *Już teraz prędko rozwija się technologia pozwalająca na respektowanie prawa do pozostania anonimowym, także w kontekście monitoringu miejskiego. Technologie obróbki obrazu pozwalają na poprawienie rejestrowanego materiału wideo tak, aby np. maskowały sylwetki ludzi, zapewniając tym samym zgodność z przepisami. Istnieje także możliwość udostępnienia takiego monitoringu – nagrań bezpiecznych dla danych osobowych – podmiotowi zewnętrznemu* – podkreśla K. Badowski. Ze względu na wagę kwestii związanych z ochroną prywatności można się spodziewać, że tego typu rozwiązania technologiczne będą rozwijane także w kolejnych latach.

## 4 REGULACJE A TECHNOLOGIA

Prawne uregulowanie nowych technologii jest często trudne, jeśli wręcz niemożliwe. O wiele prościej mówić o próbie uregulowania konkretnych przypadków ich użycia. Przykładowo, rozpoznawanie twarzy w trakcie odprawy lotniskowej może znacznie przyspieszyć ten proces i być ułatwieniem nieszkodliwym, a wręcz pożądanym. Użycie tego samego narzędzia w celu monitorowania obywateli może jednak budzić wątpliwości związane z ingerencją w prywatność. Choć technologia jest dokładnie taka sama, cel użycia okazuje się inny.

Rozporządzenie RODO, które weszło w życie w 2018 r., w dużym stopniu zmieniło postrzeganie prywatności i podniosło świadomość związaną z ochroną danych osobowych. Regulacje wciąż będą starały się nadążać za postępem technologicznym, ale najważniejsza będzie ich analiza pod kątem konkretnych przypadków, tak by móc tworzyć prawo dopasowane do określonych zastosowań urządzeń, z korzyścią dla obywateli.

## 5 RÓŻNORODNOŚĆ SIECI

Bezpośrednim skutkiem zawiłości związanych z regulacjami prawnymi, prywatnością i bezpieczeństwem na przełomie ostatnich dwóch dekad jest zauważalne odchodzenie od całkowicie otwartej sieci. Wprawdzie Internet i usługi w chmurach publicznych wciąż pozostają częścią tego, w jaki sposób przesyłamy, analizujemy i przechowujemy dane, jednak coraz bardziej popularne staną się chmury hybrydowe i prywatne. Zauważalny jest wzrost liczby „inteligentnych wysp”, gdzie systemy dla konkretnych aplikacji mają bezpośrednie połączenia z innymi systemami współzależnymi.

Wprawdzie niektórzy wskazują, że odejście od otwartych modeli jest niepożądane, przekonujące mogą się okazać argumenty dotyczące bezpieczeństwa i ochrony danych. Jedną z wymienianych dotychczas korzyści otwartości sieci była możliwość uczenia maszynowego, przy założeniu że komputery mogą się uczyć tylko na wielkich zbiorach danych. Obecnie modele sieciowe dopasowane do konkretnych aplikacji korzystają jednak z relatywnie niewielkiej ich liczby.

Przykładowo, w Axis Communications model wizyjnego monitorowania ruchu ulicznego składający się z 7000 przykładowych zdjęć pozwolił na zmniejszenie liczby fałszywych alarmów w wykrywaniu wypadków przez kamery aż o 95 proc. □

Axis Communications Poland

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







TEKST  
Jan T. Grusznic

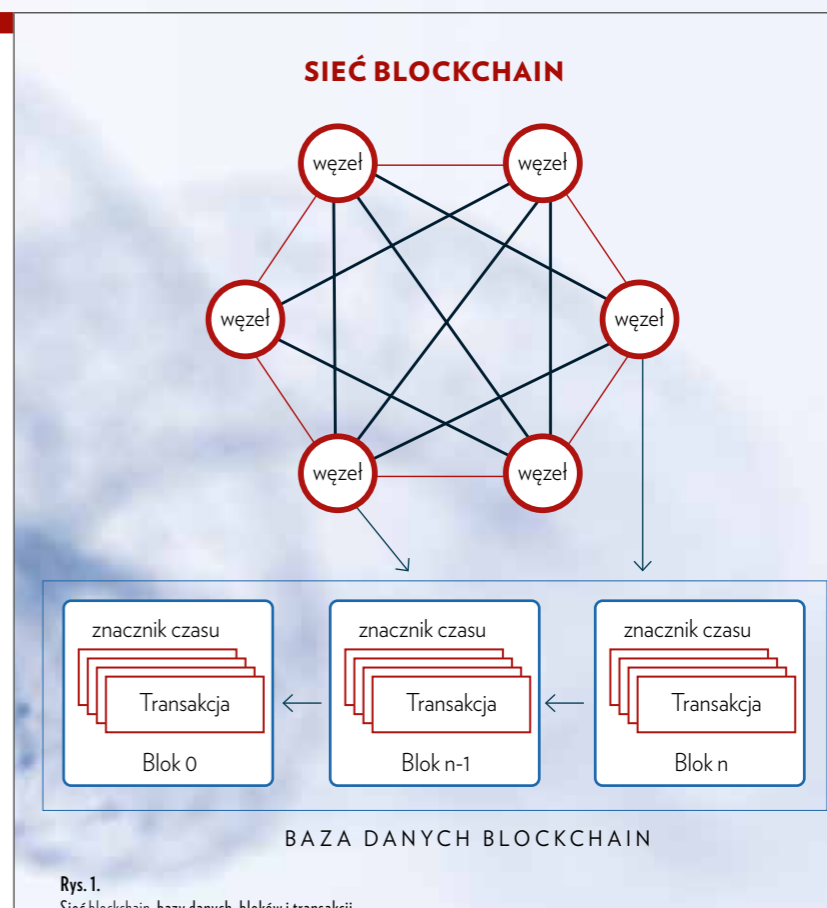
TECHNOLOGIA BLOCKCHAIN ZAPEWNE ZREWOLUCJONIZUJE NASZ SPOSÓB ŻYCIA I PRACY. MA ONA POTENCJAŁ, BY ZAPEWNIĆ WIĘKSZĄ KONTROLĘ NAD NASZĄ OPIEKĄ ZDROWOTNĄ CZY LEPSZY WGLĄD W POCHODZENIE I JAKOŚĆ SPOŻYWANEJ PRZEZ NAS ŻYWNOŚCI ORAZ KUPOWANYCH PRODUKTÓW. TRANSAKCJE FINANSOWE BĘDĄ REALIZOWANE SZYBCIEJ, A PRZY TYM STANĄ SIĘ PRZEJRZYSTE I BEZPIECZNE. BIZNES BĘDZIE PROWADZONY Z WIĘKSZĄ EFEKTYWNOŚCIĄ I MNIEJSZYM RYZYKIEM. NIEPOWTARZALNE ATRYBUTY TECHNOLOGII BLOCKCHAIN ZAPEWNIĄ NOWĄ INFRASTRUKTURĘ, NA KTÓREJ ZOSTANIE ZBUDOWANA NOWA GENERACJA USPRAWNIONYCH APLIKACJI BIZNESOWYCH. NALEŻY SIĘ SPODZIEWAĆ, ŻE BLOCKCHAIN ZREWOLUCJONIZUJE ZWŁASZCZA TE BRANŻE, KTÓRE WYMAGAJĄ WYSOKIEGO POZIOMU BEZPIECZEŃSTWA I INTEGRALNOŚCI DANYCH – RÓWNIEŻ NASZĄ. DLATEGO WARTO WIEDZIEĆ O NIEJ NIECO WIĘCEJ.

# BLOCKCHAIN

## 5 FAKTÓW O JAKICH POWINIENIEŚ WIEDZIEĆ, a boisz się zapytać

### 1. Czym jest?

*Blockchain* (zwany też łańcuchem bloków) jest współdzieloną, rozproszoną i odporną na błędy bazą danych, która utrzymuje rekordy w blokach (rys. 1). Bloki są połączone ze sobą w formie łańcucha, każdy z nich przetrzymuje identyfikator (*hash*) swojego poprzednika. Każdy blok zawiera od kilku do kilku tysięcy zweryfikowanych transakcji (wartość zależna od stosowanego rozwiązania), znacznik czasu wskazujący moment jego utworzenia oraz liczbę losową (*nonce*) dla operacji kryptograficznych wykonywanych w celu potwierdzenia poprawności bloku. Sieć *blockchain* składa się z tzw. węzłów, które utrzymują łańcuch bloków w sposób rozproszony (sieć *peer-to-peer*). Wszystkie węzły mają dostęp do bloków, ale nie mogą ich całkowicie kontrolować. Jedną z najważniejszych zalet tej technologii jest właśnie niezmiennosc i przejrzystość – bloki są dostępne dla wszystkich użytkowników łańcucha, ale nie jest można ich usunąć lub modyfikować. *Blockchain* pozwala stronom na interakcje bez obecności zaufanej strony trzeciej (pośrednika). Każda z interakcji jest rejestrowana w bazie danych,





zapewniając pożądaną wymogi bezpieczeństwa. Gdy użytkownik łańcucha bloków nawiązuje kontakt z innym użytkownikiem, przesyła on swoją „transakcję” do sieci *blockchain*. Węzły w sieci sprawdzają, czy interakcje są poprawne, i konstruują nowy blok poprawnych transakcji w tzw. procesie kopania (walidacja bloku). Jeśli nowy blok zostanie uznany za ważny, jest dołączany do bazy danych łańcucha bloków i nie może być później usunięty lub zmieniony. Zarówno transakcje, jak i bloki są podpisywane, dlatego też nie można ich cofnąć lub usunąć w przyszłości.

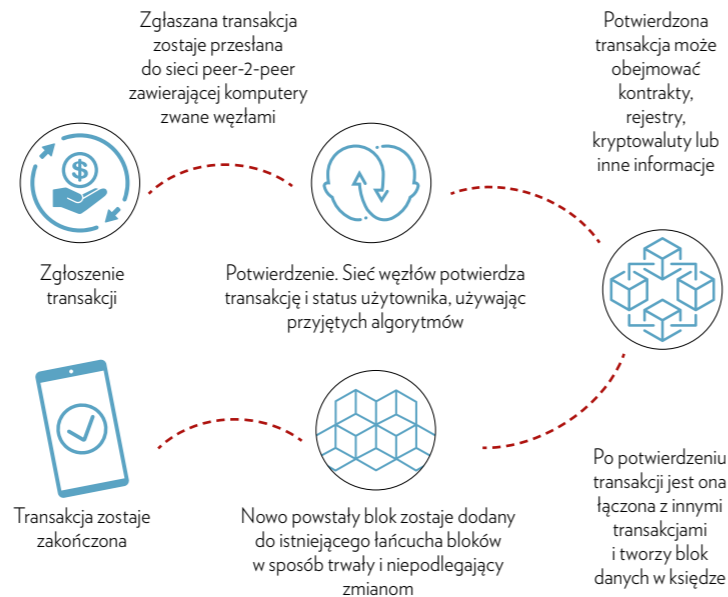
Technologia *blockchain* ma trzy generacje, które wspierają odpowiednio transakcje pieniężne, aktywa oraz inteligentne umowy (*smart contracts*). Pierwsza została opublikowana przez Satoshi Nakamoto w 2009 r. i ograniczała się do transakcji pieniężnych. Znamy ją jako kryptowalutę bitcoin, która jest pierwszą tak szeroko wykorzystaną aplikacją opartą na koncepcji łańcucha bloków. Druga generacja miała szersze zastosowanie i dotyczyła nie tylko pieniędzy, ale i aktywów – użytkownicy mogą wymieniać dowolne aktywa, np. towary, nieruchomości, a nawet głosy. Trzecia wprowadziła inteligentne kontrakty. Inteligentna umowa jest kontraktem programowalnym, sprawdzanym przez wszystkich w sieci, a zatem zmusza obie strony komunikacji do jego ścisłego przestrzegania. Możliwości łańcucha bloków trzeciej generacji zostały znacznie zwiększone, co przyczyniło się do ich popularności na całym świecie i wzrostu zainteresowania ich aplikacjami.

## 2. Jak działa?

*Blockchain* to prosty, aczkolwiek pomysłowy sposób przekazywania informacji z punktu A do punktu B, w pełni zautomatyzowany i uznawany za bezpieczny. Jedna strona transakcji inicjuje proces poprzez utworzenie bloku. Jest on weryfikowany przez tysiące, być może nawet miliony komputerów rozmieszczonych w sieci. Zweryfikowany blok jest dodawany do łańcucha, który jest przechowywany w całej sieci, tworząc nie tylko unikalny rekord, ale także niepowtarzalny zapis o unikalnej historii (rys. 2). Falszowanie pojedynczego rekordu oznaczałoby zafalszowanie całego łańcucha w milionach przypadków, co jest bardzo mało prawdopodobne. Łańcuch bloków korzysta z różnych algorytmów w celu osiągnięcia porozumienia w sprawie nowego stanu dla łańcucha bloków. Główną ideą zastosowania algorytmu zgody jest wykorzystanie grupy osób zaangażowanych w system do podejmowania decyzji, zamiast korzystania z zaufanej strony trzeciej.

Wspomniany inteligentny kontrakt to tak naprawdę zestaw programowalnych funkcji, przechowywanych w łańcuchu bloków i automatycznie egzekwujących warunki bez potrzeby korzystania z zaufanych pośredników. Funkcjonalność inteligentnego kontraktu wzorowana jest na tradycyjnych umowach zawierających warunki, a każda ze stron jest zobowiązana przestrzegać zapisanych w nich postanowień. Inteligentny kontrakt automatyzuje zadania samoczynnie potwierdzając warunki, uruchamiając kolejne kroki po wykonaniu postanowień umowy. Wszystko odbywa się bez potrzeby istnienia centralnego organu

## JAK DZIAŁA BLOCKCHAIN



Rys. 2. Uproszczony schemat działania blockchain

lub systemu prawnego. Korzystając z tego rozwiązania, można zdefiniować bardziej złożone transakcje określone warunkami zapisanymi w łańcuchu. W rezultacie pozwala to rozwijać aplikacje w bardziej różnorodnych obszarach aniżeli sam transfer walut cyfrowych, np. łańcuch dostaw, zarządzanie procesami biznesowymi lub opieka zdrowotna.

## 3. Dlaczego powstał?

Chmura zmieniła sposób interakcji między ludźmi. Codziennie wymieniamy się setkami danych, plików, zawieramy umowy, wykonujemy transakcje. Korzystamy przy tym z różnych aplikacji na wielu urządzeniach i w każdej sieci, która zapewni nam dostęp do zasobów. Takie rozdrobnienie wymaga rozproszonych mechanizmów kontroli. Tymczasem większość obecnych praktycznych rozwiązań z zakresu utrzymania bezpieczeństwa jest scentralizowana i nieefektywna. Centralizacja sprzyja powstawaniu pojedynczych punktów awarii. Bezpieczeństwo zapewniane przez osoby (firmy) trzecie może być zagrożone, gdy ulegną atakowi i zostaną skompromitowane. Do tego możliwe jest wykasowanie interakcji w centralnym systemie (np. po udanej próbie ataku).

*Blockchain* z natury jest rozproszony, dlatego też usługi bezpieczeństwa oparte na łańcuchach bloków mogą być wdrażane właśnie w ten sposób. Decyzje dotyczące kolejnych bloków w łańcuchu są podejmowane w drodze zdecentralizowanego konsensusu, większością głosów

(co znacząco utrudnia skompromitowanie, chyba że atakujący ma kontrolę nad całym systemem) i porozumienia między węzłami. Każda transakcja i blok są podpisane w taki sposób, aby nie można było później zaprzeczyć przeprowadzeniu transakcji (niezmiennosc). Każda transakcja jest przejrzysta dla wszystkich uczestników łańcucha.

## Decentralizacja

Zanim pojawiły się bitcoin i BitTorrent, byliśmy bardziej przyzwyczajeni do scentralizowanych usług: centralna jednostka przechowuje dane i musimy współdziałać wyłącznie z tą jednostką, aby uzyskać potrzebne informacje. Popularnym przykładem takiej centralizacji są banki. Przechowują one wszystkie twoje pieniądze, i jedynym sposobem, w jaki możesz coś zapłacić, jest przejście przez bank. Innym jest przeszukiwanie zasobów sieci: gdy szukasz czegoś w Google, wysyłasz zapytanie do serwera, który następnie zwraca odpowiednie informacje – typowe rozwiązanie klient-serwer.

Systemy scentralizowane sprawdzają się od wielu lat, jednak mają kilka luk. Przede wszystkim dane są przechowywane w jednym miejscu. To sprawia, że są one celem potencjalnych ataków. Aktualizacja oprogramowania centralnego serwera zatrzymuje na pewien czas pracę systemu. Awaria scentralizowanej jednostki powoduje, że nikt nie jest w stanie uzyskać dostępu do informacji. A gdy centralny komputer padnie ofiarą udanego ataku i część danych zostanie zmieniona w sposób trudny do wykrycia, to dalsze operacje będą opierały się na błędnych informacjach w systemie.

W zdecentralizowanym systemie informacje nie są przechowywane przez jeden podmiot. W rzeczywistości każdy w sieci jest właścicielem informacji. W zdecentralizowanej sieci, chcąc nawiązać kontakt ze swoim przyjacielem, możesz to zrobić bezpośrednio, bez przechodzenia przez osoby trzecie. To była główna idea bitcoinów. Ty i tylko ty jesteś odpowiedzialny za swoje pieniądze. Możesz je wysłać do kogo chcesz, bez konieczności przechodzenia przez bank.

## Przejrzystość

Przejrzystość to najbardziej interesująca i zarazem źle rozumiana cecha *blockchain*. Jedni twierdzą, że łańcuch bloków zapewni ci prywatność, inni, że jest przejrzysty. Oba stwierdzenia są prawdziwe, a wpływa na nie sposób wykonywania zapisów transakcji.



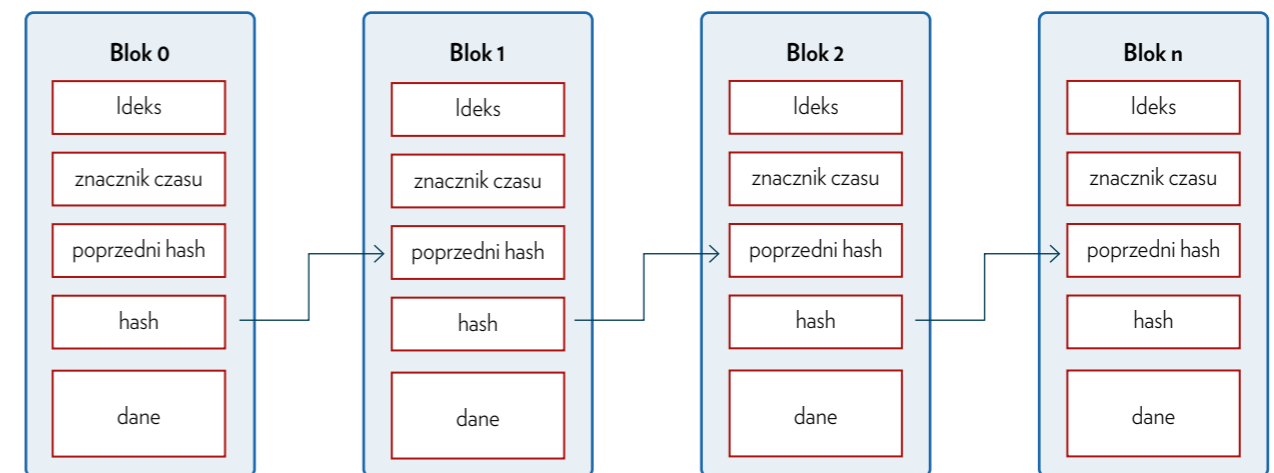
Tożsamość osoby jest bowiem ukryta poprzez zapis ciągu znaków i reprezentowana tylko przez jej adres publiczny. Zatem historia transakcji danej osoby, przedstawiana jest jako ciąg „1MF1bhsFLkBzzz9vp-FYEmvT2TbyCt7NZJ wysłał 1 BTC”, nie zaś „Jan wysłał 1 BTC”. Tak więc wprowadzenie tożsamości osoby jest bezpieczne, ale nadal widoczne są wszystkie transakcje, dokonane przez jej adres publiczny.

Ten poziom przejrzystości nigdy wcześniej nie istniał w ramach np. systemu finansowego. Patrząc wyłącznie z poziomu kryptowalut, znając adres publiczny instytucji, można po prostu wrzucić go do wyszukiwarki i przyjrzeć się wszystkim transakcjom, w które była ona zaangażowana. Fakt ten zmusza korporacje do szczerości, za jaką nigdy wcześniej nie miały do czynienia. Jestem pewny, że większość z tych firm nie będzie przeprowadzać wszystkich transakcji z wykorzystaniem kryptowalut. Jednocześnie ta cecha poważnie przyczynia się do lepszego zarządzania łańcuchem dostaw i była długo poszukiwana na rynku.

## Niezmiennosc

Wyobraźmy sobie, jak wiele przypadków fraudów można zdusić w zarodku, jeśli ludzie wiedzą, że nie mogą prowadzić kreatywnej księgowości i manipulować rachunkami firmowymi. W technologii *blockchain* wynika to z hashowania, czyli tworzenia czegoś na wzór sum kontrolnych dla danych transakcyjnych i całego bloku. W prostych słowach ujmując, hashowanie oznacza pobranie danych wejściowych o dowolnej długości i wydanie ciągu znaków o stałej długości.

## POWIĄZANIE BLOKÓW W SIECI BLOCKCHAIN



Rys. 3. Przykład powiązania bloków w sieci blockchain



→ Funkcja hashująca to specjalna klasa funkcji, która ma różne właściwości czyniące ją idealną w kryptografii, a najważniejszą z nich jest „efekt lawinowy”. Polega on na tym, że nawet niewielka zmiana w danych wejściowych (np. zmiana wielkości litery) powoduje poważną zmianę w danych wyjściowych. Ta właściwość została wykorzystana w *blockchain*: każdy blok (oprócz bloku genesis, pierwszego w łańcuchu), zawierający dane ma swój hash oraz hash bloku poprzedzającego, który łączy go z poprzednim blokiem, tworząc w ten sposób łańcuch (rys. 3).

Ten, wydawać by się mogło, trywialny zabieg sprawia, że łańcuchy bloków są tak zadziwiająco niezawodne. Atak na blok 1 i próba ingerencji w dane zmieni bowiem hash, przechowywany również w bloku 2. Próba zmiany wartości hash w bloku 2 spowoduje zmianę wartości hash dla niego samego (przy obliczaniu wartości hash każdego nowego bloku brana jest pod uwagę również wartość hash z poprzedniego bloku) i w konsekwencji brak zgodności ze wskaźnikiem hash przetrzymywany przez blok następny. Brak ciągłości jest natychmiast wykrywany, a dzięki replikacji bazy (każdy bowiem węzeł w systemie zdecentralizowanym ma kopię łańcucha bloków danych) jest możliwe przywrócenie stanu sprzed ataku. Właśnie w ten sposób łańcuchy blokowe uzyskują niezmiennność.

#### 4. Potencjalne rynki

Jako pierwsza potencjał łańcucha bloków rozpoznała branża finansowa. Od 2014 r. widać wysyp start-upów, które rozwijają technologie kryptowalut opartych na technologii *blockchain*. Powstała nowa branża FinTech (od słów *finance* i *technology*), a w branży ubezpieczeniowej – InsurTech. W energetyce dostrzeżono zalety *blockchain* do rozliczania transakcji kupna-sprzedaży energii pomiędzy małymi producentami, np. gospodarstwami domowymi (prosumentami) a ich klientami, odbiorcami energii, także rozproszonymi, np. elektrycznymi samochodami.

Trwają prace nad wykorzystaniem łańcucha bloków do podpisu cyfrowego w administracji państwowej czy jako księgi rachunkowej w bankowości. Transakcje te mogą odbywać się poza funkcjonującym od wieków systemem – bez udziału instytucji zaufania publicznego, bezpośrednio pomiędzy stronami transakcji. Przykładów zastosowania technologii *blockchain* jest bardzo dużo



i wciąż pojawiają się nowe pomysły. Szansę na jej rozwój dostrzeżono m.in. w takich obszarach jak płatności oraz pożyczki *peer-to-peer*<sup>1)</sup>, Internet Rzeczy<sup>2)</sup>, systemy głosowania<sup>3)</sup>, transport<sup>4)</sup>, hazard i systemy gier<sup>5)</sup>, digitalizacja dokumentów<sup>6)</sup>, identyfikacja i śledzenie dóbr luksusowych<sup>7)</sup>, usługi rządowe<sup>8)</sup>, zautomatyzowane łańcuchy dostaw<sup>9)</sup>, składowanie danych<sup>10)</sup>, tożsamość i jej weryfikacja<sup>11)</sup>.

Wśród obiecujących zastosowań technologii *blockchain* znajdują się usługi monitorowania sieci i ogólnie pojętego bezpieczeństwa obejmujące uwierzytelnianie, poufność, prywatność, integralność i pochodzenie. Obecnie usługi te są świadczone przez zaufanych zewnętrznych brokerów lub przy użyciu nieskutecznych metod rozproszonych. Zatem bezpieczeństwo jest i będzie głównym wyzwaniem dla obec-

- <sup>1)</sup> globalna sieć przekazów pieniężnych i pożyczek, eliminująca pośredników, np. Abra, BTC Jam  
<sup>2)</sup> śledzenie stanu, historii, wymiana zdarzeń, np. Filament  
<sup>3)</sup> rozproszone, niezaprzeczalne, automatyczne zliczanie głosów z pełną historią, np. FollowMyVote  
<sup>4)</sup> wynajem przejazdów, prywatni kierowcy, współdzielenie przejazdów, przewóz osób i rzeczy. Dzięki *blockchain* i przezroczystości możliwe ominięcie pośredników i regulacji państw (tzw. Uber Killer), np. Arcade City  
<sup>5)</sup> anonimizacja graczy, przekazy wygranych, osiągnięcia, własne waluty w grach komputerowych, systemy przewidywania (np. ruchu przeciwnika), np. Augur, Deckbound  
<sup>6)</sup> składowanie odpowiedników w formie inteligentnych kontraktów, składowanie skanów, odpowiedników w formie plików danych, gwarancja niezaprzeczalności, np. składowanie paragonów w *blockchain* w celach gwarancyjnych, Colu  
<sup>7)</sup> śledzenie dzieł sztuki, diamentów, zegarków, dóbr kolekcjonerskich, np. Everledger, BlockVerify, Chainlink  
<sup>8)</sup> podatki, składki, hipoteki, akty własności, księgi wieczyste, rejestry (PESEL, NIP itp.), recepty, np. BitNation, ShoCard  
<sup>9)</sup> inteligentne kontrakty – automatycznie zawierane i wykonywane kontrakty, których nikt nie kontroluje, ale każdy (w obrębie *blockchain*) im ufa, np. UbiMS, Mirror  
<sup>10)</sup> zaufane, rozproszone, odporne na awarie i próby wpływnia na integralność danych systemy składowania danych, np. NXT, PeerNova  
<sup>11)</sup> rozproszone systemy identyfikacji osób, cyfrowe podpisy, autoryzacje, reputacja, np. Uniquld, OneName, WorldTable

nych zastosowań. Technologia *blockchain* może je zagwarantować, rozwiązując wiele tradycyjnych problemów, zapewniając w pełni rozproszone, w miarę możliwości bezpieczne i oparte na konsensusie rozwiązanie (rys. 4).

#### 5. Blockchain w branży zabezpieczeń technicznych

Trwały sposób śledzenia zmian danych w czasie oraz ich niezmiennność jest najbardziej interesującą cechą omawianej technologii, która mogłaby znaleźć zastosowanie w naszej branży. W zabezpieczeniach technicznych łańcuch bloków może zapobiegać manipulowaniu dowodami wideo i kontrolą dostępu, a także systemami zarządzania tożsamością. Ze względu na możliwość śledzenia interakcji z plikami cyfrowymi *blockchain* może określić, czy plik został naruszony, a następnie dostarczyć informacji o miejscu i czasie naruszenia. Z powodzeniem może być wykorzystywany do weryfikacji treści wideo z wielu źródeł, np. publiczne telefony komórkowe i kamery nasobne, wykorzystywane w postępowaniach sądowych.

Oprócz danych wideo *blockchain* mógłby być również użyty do weryfikacji autentyczności urządzeń podłączonych do systemów dozorów wizyjnych, zwłaszcza gdy myśli się np. o korzystaniu z prywatnych instalacji. Już teraz władze miast planują powszechniejsze wykorzystanie istniejących kamer prywatnych zainstalowanych na osiedlach, stacjach benzynowych, w sklepach, centrach handlowych czy placówkach oświatowych. Te prywatne systemy dozorowe są ważnym elementem ekosystemu monitoringu, ponieważ pozyskany z nich materiał ma często decydujące znaczenie w procesie dochodzeniowym. Tymczasem zapis wideo z tych systemów jest przechowywany lokalnie i udostępniany organom ścigania tylko na żądanie. Jediną for-

mą zabezpieczenia przed manipulacją jest tzw. znakowanie wodne, dostarczone przez producenta urządzenia w celu potwierdzenia autentyczności zapisanego obrazu. Niestety rozwiązania te nie dają gwarancji, że uzyskany materiał wizyjny nie został zmieniony cyfrowo, budząc wątpliwości co do jego wiarygodności. Już dawno pojawiła się potrzeba opracowania rozwiązania technologicznego, które może zapewnić dowód integralności informacji z systemu dozoru wizyjnego wymienianych między urządzeniami obsługiwanych przez podmioty o różnym poziomie zaufania.

*Blockchain* może poważnie namieszać również w systemach kontroli dostępu. Głównym powodem jest historia wszystkich zarejestrowanych transakcji przechowywana w niezawodnej, zabezpieczonej przed manipulacją bazie danych, co znacznie zmniejsza ryzyko nadużycia. Interesujące jest również zarządzanie prawami dostępu oparte na podejściu rozproszonym, gdy uprawnieni użytkownicy mogą przyznawać lub odbierać dostęp innym użytkownikom. Pozwala wyeliminować administratora systemu, osobę trzecią pośredniczącą we wszystkich transakcjach. Udzielanie tymczasowego dostępu do wybranych przejść jest możliwe dzięki egzekwowaniu przepisów (inteligentny kontrakt). *Blockchain* może np. zapewnić unikatowe hasła dla gości każdej z firm budynku biurowego. Dziś jest to zazwyczaj realizowane przez wydawanie kart zbliżeniowych z nadanymi takimi samymi uprawnieniami.

Pozostając przy systemach kontroli dostępu, warto wspomnieć o systemach biometrycznych. Wkrótce identyfikacja biometryczna będzie powszechną metodą weryfikacji tożsamości, zgodnie z którą wiele protokołów zabezpieczeń utworzy unikalny identyfikator, który będzie mógł być indeksowany w łańcuchu bloków. Co prawda w łańcuchu nie będą przechowywane żadne dane, ale pozwoli to użytkownikowi udowodnić, że jest tym, za kogo się podaje oraz określić, jakie dane, na jak długo i z kim dzieli. Systemy kontroli dostępu bazujące na takim rozwiązaniu będą prawdziwą rewolucją w branży.

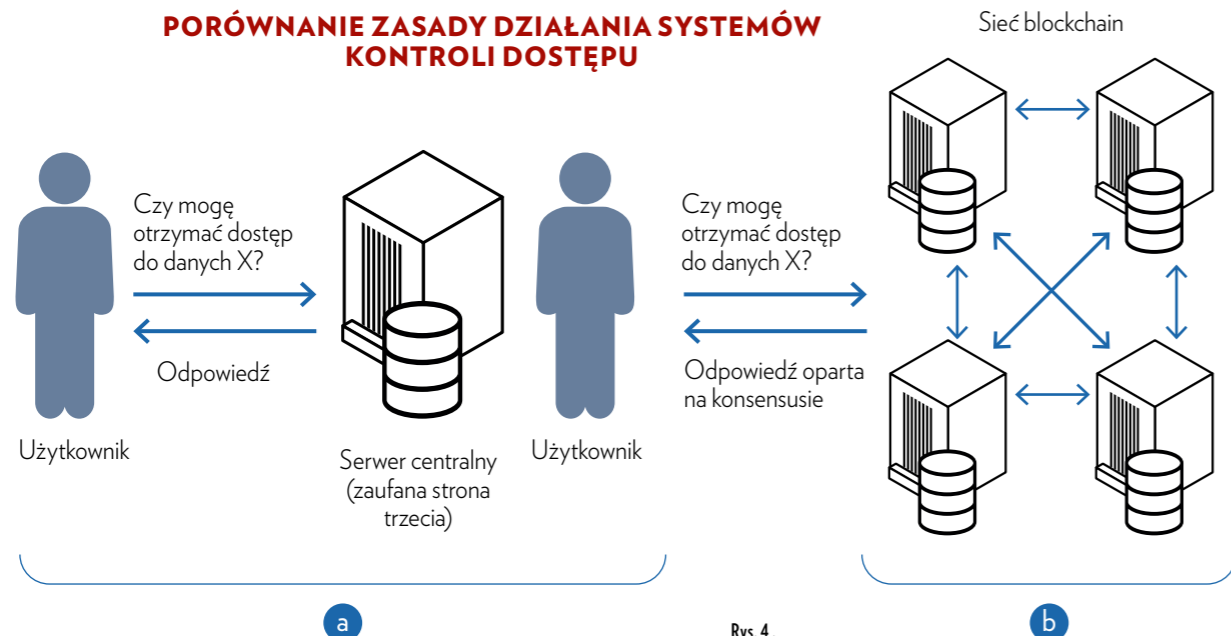
*Blockchain* jest wykorzystywany przez globalne organizacje poszukujące technologii stanowiących podstawę ich systemów zabezpieczeń. W miarę jak korzyści płynące z łańcucha bloków staną się powszechniejsze, inni również zaczną go stosować do ochrony integralności swoich danych operacyjnych i bezpieczeństwa. Także nasza branża. □

B I O

Jan T. Grusznic

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

#### PORÓWNANIE ZASADY DZIAŁANIA SYSTEMÓW KONTROLI DOSTĘPU



Rys. 4.

(a) Tradycyjna centralizowana kontrola dostępu (b) Kontrola dostępu oparta na łańcuchu bloków

#### LITERATURA

- Sara Rouhani, Vahid Pourheidari, Ralph Deters "Physical Access Control Management System Based on Permissioned Blockchain", University of Saskatchewan, IEEE Xplore Digital Library, 2019
- Alem Fitwi, Yu Chen, Sencun Zhu "A Lightweight Blockchain-based Privacy Protection for Smart Surveillance at the Edge", 1st International Workshop on Lightweight Blockchain for Edge Intelligence and Security (LightChain, colocated with IEEE BlockChain Conference), 2019
- https://www.lazarski.pl/pl/wydzialy-i-jednostki/instituty/wydzial-ekonomii-i-zaradzania/centrum-technologii-blockchain/
- http://twojblockchain.pl/czym-jest-blockchain/
- https://www.asmag.com
- John Velissarios, Justin Herzig, Didem Unal "BELIEVE IT OR NOT, Blockchain's potential starts with security", Accenture 2019
- https://magoo.github.io/Blockchain-Graveyard/
- https://thenextweb.com
- https://www.darkreading.com
- Tara Salman, Student Member, IEEE, Maede Zolanvari, Student Member, IEEE, Aiman Erbad, Member, IEEE, Raj Jain, Fellow, IEEE, and Mohammed Samaka, Member "Security Services Using Blockchains: A State of the Art Survey", IEEE, 2018
- M. Pilkington, "Blockchain Technology: Principles and Applications" in Research Handbook on Digital Transformations, 2016
- https://tokeneo.com/
- https://blockgeeks.com
- Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008
- https://andersbrownworth.com/
- "Genetec shares its top physical security trends predictions for 2020", Genetec Inc., 2020
- https://www.axis.com/blog/secure-insights/technology-trends/

# SLIM-DUAL-LUNA – dualna czujka ruchu z funkcją oświetlenia

**Czujki ruchu, wraz z postępującym rozwojem technologicznym, charakteryzują się coraz lepszymi parametrami detekcji i zwiększoną odpornością na niepożądane alarmy. Czy oprócz podstawowej funkcji, jaką jest wykrywanie potencjalnych intruzów, mogą oferować inne ciekawe funkcje?**

W ostatnim kwartale 2019 r. firma SATEL wprowadziła na rynek serię dziecięciu czujek ruchu - SLIM LINE. Jedną z nich jest SLIM-DUAL-LUNA spełniająca wymagania normy EN 50131 dla Grade 2, wyposażona w czujnik PIR i mikrofalowy (MW) oraz zestaw białych diod LED do realizacji funkcji oświetlenia.

## Skuteczna detekcja ruchu

Niezawodne wykrywanie intruzów przy zminimalizowaniu ryzyka występowania niepożądanych alarmów w niemal każdych warunkach cieplnych to cecha charakteryzująca całą rodzinę SLIM LINE. Jest wynikiem zastosowania najnowszych technologii, soczewki szerokokątnej o unikalnej konstrukcji, zaawansowanego algorytmu detekcji oraz funkcji dynamicznej kompensacji temperatury otoczenia. SLIM-DUAL-LUNA to czujka dualna zapewniająca skuteczne wykrywanie ruchu na obszarze o wymiarach 20 x 24 m. Można ją z powodzeniem instalować w pomieszczeniach, gdzie występują nagłe zmiany temperatury lub np. przeciągi. Dodatkowym atutem jest włączana opcjonalnie kontrola strefy podejścia.

## Wygodna konfiguracja

SLIM-DUAL-LUNA posiada rozbudowane menu konfiguracyjne. Można się po nim poruszać i zmieniać ustawienia za pomocą przycisków umieszczonych na płycie elektroniki lub zdalnie – pilotem OPT-1 – bez otwierania obudowy, co eliminuje konieczność sięgania do już zainstalowanej czujki, gdy zajdzie potrzeba zmiany ustawień.

## Różne parametry pracy czujki

Czujka może pracować w różnych trybach. W podstawowym alarm jest zgłaszany, gdy oba czujniki wykryją ruch w czasie krótszym niż 3 s. W zaawansowanym czujka zareaguje także w dwóch innych przypadkach:

- gdy czujnik MW wykryje ruch, a czujnik PIR zarejestruje jedynie drobne zmiany w polu widzenia (niezglaszane jako ruch),
- gdy tylko czujnik MW wykryje ruch - 16 razy w ciągu 15 minut, niezależnie od czujnika PIR.

Możliwe jest także, aby pracował tylko jeden z czujników (tryby: PIR i MW). W SLIM-DUAL-LUNA można ustawić

dwa zestawy parametrów pracy czujki (tryby pracy i czułości czujników). Przeląca się między nimi, podając masę na zacisk SENS. Dzięki temu, np. gdy system jest w stanie czuwania, może być używana konfiguracja eliminująca niepożądane alarmy, natomiast przy sterowaniu oświetleniem (system rozbrojony) może pracować tylko jeden z czujników.

Do wyboru jest także kolor, jakim wskaźnik LED sygnalizuje alarm, wykrycie ruchu lub awarię – dostępnych jest 7 barw. Wskaźnik można załączyć na stałe za pomocą zworki lub zdalnie, podając masę na zacisk LED.

## Źródło światła

Czujka SLIM-DUAL-LUNA, dzięki funkcji oświetlenia, sprawdza się m.in. w pomieszczeniach niewymagających do sprawnego przemieszczania się załączania innych źródeł światła. Białe diody w czujce mogą być załączane:

- przez aktywację ruchem na zaprogramowany czas (do wyboru 5 / 15 / 30 / 60 / 90 lub 180 s),
- zdalnie poprzez podanie masy na zacisk LUNA, np. przy naruszeniu innej czujki, zgodnie z timerem lub zegarem astromonicznym,
- przez aktywację ruchem i sterowanie zdalnie.

Można też wskazać, czy światło ma gasnąć natychmiast, czy ściemniać się powoli.

## Siostry LUNA

Opisywana czujka występuje również w wersji SLIM-DUAL-LUNA-PET odpornej na ruch zwierząt (masa < 20 kg). Jeśli w danej lokalizacji nie ma konieczności montażu czujki dualnej, można sięgnąć po modele bez czujnika MW: SLIM-PIR-LUNA-PET lub SLIM-PIR-LUNA. Ta ostatnia z wymienionych otrzymała wyróżnienie w kategorii „Nowoczesne technologie” konkursu „Dobry Design 2020”.

## SATEL

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



OD 1990 ROKU  
DBAMY O **BEZPIECZEŃSTWO I KOMFORT**  
LUDZI NA CAŁYM ŚWIECIE



... to już **30 lat!**

Dziękujemy, że jesteście z nami.

Dowiedz się więcej:  
www.satel.pl/30lat



# FacePRO od Panasonic na stadionie w Brøndby

Brøndby IF to założony w 1964 r. jeden z najlepszych klubów piłkarskich duńskiej Superligi. Lokalna społeczność Brøndby stanowi sporą grupę fanów silnie związanych z klubem. Entuzjazm czasami przeradza się jednak w niedopuszczalne zachowania niektórych kibiców, takie jak odpalanie rakiet świetlnych na trybunach, niezgodne z przepisami Duńskiego Związku Piłki Nożnej i może narazić klub na kary.



Przez tego typu zachowania klub zaczął mierzyć się m.in. ze spadkiem liczby kibiców przychodzących z rodzinami, a także z zagrożeniem bezpieczeństwa. Na tzw. czarnej liście znalazło się prawie 100 zidentyfikowanych osób powodujących problemy. Listy przekazywano w formie fizycznej ochroniarzom na wejściach, którzy musieli (ręcznie) sprawdzić każdą osobę wchodzącą na stadion. Proces potwierdzania był bardzo czasochłonny i nie zawsze skuteczny, dlatego klub musiał znaleźć sposób na jego usprawnienie. Aby odpowiedzieć na wyzwania stojące przed klubem i zwiększyć bezpieczeństwo kibiców, zapobiegając wejściu na rozgrywki osób z czarnej listy, przy jednoczesnym przestrzeganiu przepisów UE o ochronie danych osobowych (tzw. RODO), postanowiono zastosować rozwiązanie Panasonic FacePRO. Zainstalowanie systemu rozpoznawania twarzy FacePRO firmy Panasonic przy wejściach na stadion pomaga

skutecznie i przede wszystkim szybko identyfikować osoby znajdujące się na czarnej liście. Dzięki zastosowaniu FacePRO są one automatycznie rozpoznawane w tłumie. Alerty o ich obecności są wysyłane do operatorów, którzy dokładnie weryfikują dopasowanie twarzy wykonane przez system z osobami z czarnej listy przed wysłaniem powiadomienia do ochroniarzy. System wykorzystuje funkcję Best-Shot firmy Panasonic, która automatycznie wybiera najlepsze klatki twarzy do analizy nawet w trudnych warunkach oświetleniowych. Umożliwia to przetwarzanie dużej liczby obrazów twarzy bez przeciążania sieci i przyczynia się do redukcji kosztów całego systemu. Oprogramowanie umożliwia precyzyjną identyfikację konkretnej osoby nawet wtedy, gdy jej twarz jest odwrócona pod kątem, a także gdy jest częściowo zasłonięta przez okulary przeciwsłoneczne czy maskę. System jest w stanie zidentyfikować osoby nawet mimo zachodzących procesów starzeniowych (do 10 lat).

Jedną z najważniejszych kwestii, którą należało uwzględnić przy wdrożeniu, była zgodność z przepisami RODO Unii Europejskiej. Rozwiązanie Panasonic FacePRO jest w tym zakresie bardzo

elastyczne i można je skonfigurować tak, aby system automatycznie usuwał lub przechowywał dane w zależności od potrzeb. Aby spełnić wymagania Brøndby IF, dane z kamery są szyfrowane, a klatki, na których znajdują się osoby spoza czarnej listy, nigdy nie są przechowywane. Kadry osób mających zakaz wejścia na stadion są z kolei szyfrowane i gromadzone wyłącznie na serwerze niemającym dostępu do Internetu i innych systemów zewnętrznych, co spełnia wymagania postawione Brøndby IF przez Duńską Agencję Ochrony Danych.

Zauważyliśmy znaczne zmniejszenie liczby flar używanych na stadionie podczas naszych meczów. Zainstalowanie systemu to niesamowity sukces, w naszej ocenie rozwiązaniem Panasonic są niezbędnym narzędziem w celu utrzymania bezpieczeństwa – podsumowuje wdrożenie Mickel Lauritsen, szef ochrony w Brøndby IF. □

#### Panasonic Marketing Europe

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



axxonSOFT  
EXPERIENCE THE NEXT®



OTWARTA PLATFORMA INTEGRUJĄCA  
SYSTEMY BEZPIECZEŃSTWA

# Nowoczesne systemy

## przyzywowe Schrack Seconet jako element wsparcia w opiece nad seniorami

**OSTANIE DZIESIĘCIOLECIE TO OKRES CHARAKTERYZUJĄCY SIĘ ZNACZNYM WZROSTEM POPULACJI OSÓB STARSZYCH. W OBLICZU ROSNĄCEJ LICZBY SENIORÓW W POLSKIM SPOŁECZEŃSTWIE NALEŻY ROZWAŻYĆ ZASTOSOWANIE SZCZEGÓLNYCH ROZWIĄZAŃ POPRAWIAJĄCYCH KOMFORT ŻYCIA, KTÓRE ZNIWELUJĄ PROBLEMY, JAKIE NAPOTYKAJĄ OSOBY STARSZE ZAMIESZKUJĄCE W INSTYTUCJONALNYCH PLACÓWKACH OPIEKI.**

T E K S T  
**Paweł Tomaszewski**

Zwrot w kierunku nowoczesnych technologii w kontekście starzejących się społeczeństw wynika po pierwsze z szerokiego spektrum możliwości, jakie oferują, a po drugie z uwagi na efektywność kosztową – redukcji kosztów związanych z hospitalizacją lub opieką długoterminową świadczoną przez wykwalifikowany personel.

Działanie każdego domu pomocy społecznej (DPS) objęte jest Rozporządzeniem Ministra Polityki Społecznej z 23 sierpnia 2012 r. w sprawie domów pomocy społecznej (Dz.U. z 2009 r. nr 175, poz. 1362, z późn. zm.). Warto wiedzieć, że aby DPS spełniał warunki stawiane w ustawie, musi zostać wyposażony m.in. w system przyzywowo-alarmowy i system alarmu przeciwpożarowego.

Firma Schrack Seconet, działająca na rynku polskim od ponad 30 lat (posiada ponad 6 tys. obiektów referencyjnych), oferuje certyfikowany system przyzywowy i komunikacji VISOCALL IP, system lokalizacji SecurWATCH, a także systemy sygnalizacji pożarowej INTEGRAL IP. Wyżej wymienione systemy należy stosować w DPS-ach w celu zapewnienia odpowiedniego poziomu bezpieczeństwa pensjonariuszy. Schrack Seconet jest również producentem systemu sygnalizacji pożarowej INTEGRAL IP. Centrale sygnalizacji pożarowej Integral IP oparte zostały na wydajnej, innowacyjnej i przełomowej technologii, oferując tym samym większą elastyczność w montażu i eksploatacji.

### System przyzywowy i komunikacji VISOCALL IP

Nowoczesne systemy są dziś niezbędnym elementem wyposażenia domów seniora. W tych miejscach nie brakuje osób, które mają wyraźne problemy z samodzielnym funkcjonowaniem. Aby im pomóc i jednocześnie zagwarantować im bezpieczeństwo, montuje się system przyzywowy, który pozwala na szybsze dotarcie z pomocą do osób, które rzeczywicie jej w danym momencie potrzebują. Systemy przyzywowe to także rozwiązania o nowoczesnej stylistyce, produkowane z materiałów przeznaczonych do stosowania w tego typach obiektach.

System VISOCALL IP bazujący na technologii IP realizuje różnorodne scenariusze opieki. W pokojach montowane są specjalne przyciski, których naciśnięcie sprawia, że wysyłany jest sygnał do miejsca przebywania personelu. Na ekranie wyświetla się informacja, z której sali nadany został sygnał – lekarz czy pielęgniarka od razu wiedzą, kto potrzebuje pomocy. Po nadaniu sygnału personel niezwłocznie może udać się do sali. System dostarcza informacje o bieżących potrzebach pacjentów, jak również pozwala na ich późniejszą analizę.

Istnieje możliwość przystosowania systemu z funkcją lub bez komunikacji głosowej, z możliwością przywołania personelu pielęgniarskiego, rozmawiania z personelem w sposób dyskretny lub głośnomówiący, także przez wszystkie osoby w pokoju w tym samym czasie, ogłaszania komunikatów o obchodach lub zagrożeniach, a także dostęp do wszystkich nowoczesnych mediów, takich jak telewizja, radio, telefon i Internet.

System optymalizuje także czas pracy poprzez zamontowanie urządzeń systemu przyzywowego w punktach pielęgniarskich, salach, gabinetach, pokojach personelu itp. Dzięki temu personel może w dowolnym czasie zarządzać przywołaniami zgodnymi z priorytetami, wyświetlić rzeczywisty opis pomieszczeń, akceptować lub przypominać o przywołaniach, a także zdalnie je kasować po zakończeniu rozmowy, ma również wgląd do aktualnych zdarzeń i lokalizacji osób na oddziale.

Szybka komunikacja i łatwość korzystania to najważniejsze cechy systemów przywoławczych, których adaptacja do istniejącej infrastruktury jest niezwykle prosta. Profesjonalne systemy przyzywowe podnoszą jakość obsługi i w znaczny sposób wpływają na koszty w przyszłości dzięki kompatybilności rozwiązań.

Systemy przyzywowe mają wiele zalet. Łatwa instalacja, a także prosta obsługa pozwala na korzystanie z nich praktycznie każdym, nawet najbardziej schorowanym pacjentem lub osobom niepełnosprawnym. Są również niezwykle elastyczne, tzn. można je dowolnie skonfigurować lub dodać nowe funkcje, np. przywołania salowej, opiekuna – zwiększa to efektywność działania urządzeń. Dopasowując je do zmieniających się oczekiwań i potrzeb odbiorców, można zapewnić bezpieczeństwo i uwagę niemal każdej osobie. W obiektach o podwyższonym standardzie dzięki zastosowaniu technologii IP, każdy osoba może rozmawiać w tym samym czasie, a terminale pacjentów (słuchawki) mogą dodatkowo pełnić funkcję telefonu lub też za ich pomocą można słuchać i zmieniać programy radiowe.

Dzięki temu rozwiązaniu pacjenci czują się bardziej bezpiecznie, warunki są bardziej komfortowe, a uniwersalność tego systemu optymalizuje czas opieki i ułatwia pracę personelowi.

### SecurWATCH IP

SecurWATCH IP to obszerny system lokalizacji działający w czasie rzeczywistym (*real time location system*, RTLS), który niezawodnie lokalizuje osoby w niebezpieczeństwie – zarówno w budynkach, jak i na zewnątrz. Najnowocześniejsza technologia zapewnia niespotykaną dotąd skuteczność. Dzięki temu interaktywnemu systemowi pensjonariusze mogą poruszać się swobodnie, jednocześnie znajdując się w niezawodnej strefie bezpieczeństwa.

Nasze rozwiązanie daje także możliwość nadzorowania pacjentów w przypadku próby opuszczenia obiektu, np. z demencją, dzięki integracji z systemami lokalizacji za pośrednictwem transpondera w formie bransoletki lub zegarka na rękę, zabezpieczonych specjalnym rodzajem zapięcia, które może zostać rozpięte tylko przez opiekuna.

Integracja systemu z systemem lokalizacji zapewnia:

- zwiększone bezpieczeństwo podopiecznych dzięki opasce alarmowej na rękę, wyposażonej w opatentowane zapięcie i otwieranej za pomocą klucza magnetycznego,
- odbieranie sygnałów alarmowych z podaniem identyfikacji i lokalizacją osoby,
- lokalizację wartościowych przedmiotów w obrębie budynku,
- dokumentację wszystkich zdarzeń.

Dzięki naszemu systemowi IP i możliwości bezprzewodowego połączenia alarmowego poprawiamy poczucie bezpieczeństwa pacjenta, także w nagłych sytuacjach, takich jak upadek – osoba może wezwać pomoc przyciskiem alarmowym transpondera na rękę i wtedy opiekunowie wiedzą, kto wywołał alarm i gdzie dana osoba się znajduje.

### Integracja z systemem sygnalizacji pożarowej INTEGRAL IP

Dziś na wyposażeniu domów opieki nad osobami starszymi znajdziemy nie tylko systemy przeciwwłamaniowe, przyzywowe czy monitoringu. Trudno jest myśleć o bezpieczeństwie bez uwzględnienia możliwości zaistnienia pożaru i doboru pod tym względem odpo-



wiedniego systemu przeciwpożarowego. Nie wystarczy już samo rozmieszczenie wszelkiego rodzaju czujek czy urządzeń gaśniczych. Potrzebne jest rozwiązanie, które będzie zarządzało wszystkimi urządzeniami podłączonymi do wspólnej sieci. Taką możliwość oferują nowoczesne centrale przeciwpożarowe, które zwiększają bezpieczeństwo w razie wystąpienia pożaru.

Ustawa o ochronie przeciwpożarowej określa ochronę przeciwpożarową jako realizację przedsięwzięć mających na celu zabezpieczenie życia, zdrowia i mienia lub środowiska przed pożarem, klęską żywiołową bądź innym miejscowym zagrożeniem poprzez zapobieganie ich powstaniu i rozprzestrzenianiu się, zapewnienie sił i środków do ich zwalczania, a także prowadzenie działań ratowniczych.

Centrale przeciwpożarowe pozwalają usprawnić pracę samych urządzeń, ale też informować na bieżąco o zagrożeniach z dokładnym uwzględnieniem miejsca wystąpienia ognia i dymu. Za ich pomocą możemy sterować systemami zabezpieczeń, m.in. bramami pożarowymi, klapami oddymiającymi, ale też wysłamy informację o pożarze do odpowiednich służb. To pozwala na szybszą reakcję, a tym samym ponoszenie mniejszych strat. Centrale pozwalają też na automatyczne bądź ręczne uruchomienie urządzeń przeciwpożarowych, sygnalizatorów akustycznych i optycznych, wysterowanie systemu oddymiania, kontrolę wewnętrzną układów własnych i obwodów w urządzeniu. Dzięki temu możemy wychwycić także ewentualne nieprawidłowości w funkcjonowaniu samej centrali.

W ofercie producenta znajdziemy trzy typy centrali przeciwpożarowych o nazwach: Integral IP MXF, Integral IP CXF oraz Integral IP BXF. Dostępne są też zewnętrzne panele wskazań i obsługi, które ułatwiają pracę obsługi i strażaków, a nam umożliwiają stały wgląd do systemu poprzez korzystanie z komputera, smartfona lub tabletu.

Najważniejsze cechy wyróżniające system to niewątpliwie:

- stuprocentowa redundancja dla każdego z komponentów architektury programowej i sprzętowej centrali INTEGRAL IP MX,
- możliwość pracy w sieciach kratowych i połączenie w sieci LAN (TCP/IP),
- wykorzystanie nowoczesnej technologii pętli dozorowych X-LINE o długości do 3,5 tys. m i do 250 elementów,



- rozszerzona pamięć zdarzeń do 65 tys. pozycji (10 tys. dla centrali jednopętlowej INTEGRAL IP BXF),
- pełna kompatybilność z wcześniej produkowanymi systemami – funkcjonalność obniża koszty przyszłej rozbudowy systemu,
- praca w sieci do 62496 CSP.

Schrack Seconet ma wszelkie certyfikaty, deklaracje i świadectwa dopuszczenia na oferowane systemy. Systemy są kompatybilne wstecz, co oznacza, że po wielu latach eksploatacji można rozbudować je o nowsze elementy.

W celu usprawnienia procedur związanych z ewakuacją pensjonariuszy system sygnalizacji pożarowej może dodatkowo pokazywać szczegółowe informacje o zagrożeniu pożarowym na wyświetlaczach urządzeń przyzywowego i na telefonach mobilnych DECT/VoIP.

Nasze systemy są wykorzystywane w codziennej pracy personelu, jak również spełniają oczekiwania seniorów w domach opieki związane z rozszerzoną komunikacją. Od wielu lat współpracujemy z placówkami służby zdrowia, domami opieki – zarówno w kraju, jak i za granicą. Dzięki naszej szerokiej gamie rozwiązań możemy w pełni zaspokoić dzisiejsze, a także przyszłe wymagania inwestorów. □

#### Schrack Seconet Polska



ul. A. Branickiego 15  
02-972 Warszawa  
www.schrack-seconet.pl



**securex**<sup>®</sup>  
P O L A N D  
Międzynarodowe Targi Zabezpieczeń

ZAPRASZA  
**mtp**  
GRUPA

**21-23.04.2020**  
**POZNAŃ**

[www.securex.pl](http://www.securex.pl)



Międzynarodowe  
Targi Poznańskie

**ZABEZPIECZ SWÓJ SUKCES!**

W tym samym czasie





# Rozwiązania transmisji

## usprawniające działanie kolei

WRAZ Z POSTĘPUJĄCĄ URBANIZACJĄ SPOŁECZEŃSTW NA CAŁYM ŚWIECIE ROŚNIE LICZBA SYSTEMÓW TRANSPORTU KOLEJOWEGO (METRA). WEDŁUG RAPORTU TECHNAVIO W LATACH 2017-2022 WZROST W TYM SEKTORZE NA CAŁYM ŚWIECIE WYNIESIE ŚREDNIO OKOŁO 5 PROC. TOWARZYSZĄ TEMU ZWIĘKSZONE INWESTYCJE I ROZWÓJ RYNKU DOSTAWCÓW ROZWIĄZAŃ DLA KOLEI.

TEKST  
Prasanth Aby Thomas

Do najważniejszych trendów obserwowanych obecnie w branży kolejowej należą fuzje, postępująca cyfryzacja i wysiłki na rzecz walki z cyberprzestępczością. Wprawdzie plan połączenia niemieckiego Siemens i francuskiej firmy Alstom został zablokowany przez Komisję Europejską (jej zdaniem zagrażał konkurencji na rynkach kolei), to nie brak raportów sugerujących, że presja ze strony dostawców chińskich może zmusić znanych producentów do szukania sposobów na konsolidację.

Technologie cyfrowe wprowadzają kolejne innowacje ułatwiające przewoźnikom zwiększanie niezawodności, usprawnianie operacji i podniesienie poziomu obsługi klienta. Dysponujący potencjałem Internetu Rzeczy (IoT) producenci sondują nawet w obszarze zasobów krytycznych możliwości modeli cyfrowych bliźniaków (*digital twins*), aby symulować operacje i wyciągać wnioski.

Wraz z upowszechnieniem rozwiązań cyfrowych rosną także obawy związane z cyberbezpieczeństwem. Firmy kolejowe są zmuszone do zmiany wcześniejszego paradygmatu systemów „bezpiecznych od samego początku” (*safe by design*) na podejście „bezpieczne i chronione od samego początku” (*safe and secure by design*). Każdy węzeł sieci musi być poddany ocenie pod kątem podatności, które mogą być wykorzystane przez hakerów.

W związku z tym pojawia się pytanie, dlaczego technologie cyfrowe w systemach komunikacyjnych mają kluczowe znaczenie w usprawnianiu operacji, poprawie uwarunkowań i komponentów. A ponadto co decyduje o tym, że sieć komunikacyjna i pokładowe systemy dozoru wizyjnego stają się bardziej niezawodne.

### Znaczenie systemów łączności na kolei

**Cyfrowe systemy transmisji umożliwiają niezawodne działanie kolei. Osiąganie tego celu nie jest jednak łatwym procesem.**

Płynne i wydajne funkcjonowanie nowoczesnych systemów transportu wymaga niezawodnego systemu komunikacji. Jest to istotne ze względu na dużą liczbę podzespołów w systemach metra i kolei.

Zarządzanie systemami sygnalizacji kolejowej, systemami sprzedaży biletów, systemami dozoru wizyjnego oraz systemami zarządzania ruchem w środowisku, w którym liczba transmisji głosowych, wideo i danych (zarówno w obszarze operatorskim, jak i pasażerskim) szybko rośnie, staje się niemożliwe bez niezawodnych rozwiązań komunikacyjnych. Ze względu m.in. na szczególne wymagania dotyczące obsługi systemu metra jego funkcjonowanie bez niezawodnej sieci komunikacyjnej jest właściwie niemożliwe. Nie jest też możliwe korzystanie z sieci opartej na przestarzałych technologiach. Miałyby to poważny wpływ na wiele aspektów działania systemu, jego bezpieczeństwo i ochronę.

### Do czego może prowadzić brak prawidłowej komunikacji

Systemy łączności są niezbędne nie tylko do wykonywania codziennych operacji transportowych. Należy brać pod uwagę także nieoczekiwane zdarzenia, które będą utrudnieniem w typowych działaniach.

Poniżej podano przykłady sytuacji, w których system łączności odgrywa kluczową rolę.

1. Potrzeba uzyskania pomocy dla pasażera w przypadku nagłego, wymagającego interwencji medycznej wypadku, ustalenie planu działania i zapewnienie dostępu służbom ratunkowym.
2. Konieczność wymiany lub naprawy uszkodzonego sprzętu przez obsługę techniczną, aby pociąg odjechał o planowanej porze.
3. Koordynacja zmian w rozkładzie lub wymiana wadliwych składów.
4. Wezwanie do naprawy wadliwie działającego wyposażenia stacji, np. bramek dla pasażerów.
5. Zapewnienie pasażerom informacji o wszelkich zmianach w kursowaniu pociągów lub metra.
6. Koordynacja ewakuacji i/lub zamykanie stacji po zdarzeniach naruszających bezpieczeństwo.
7. Zapewnienie bezpiecznych operacji przełączania.

Niemożliwe jest działanie takiego systemu bez niezawodnej sieci komunikacyjnej lub przy wykorzystaniu sieci opartej na przestarzałych technologiach. Poważnie wpływa na wiele aspektów działania, bezpieczeństwa i ochrony. Wśród problemów, które mogą się pojawić, występują utrata świadomości sytuacyjnej, niedostępność podsystemu, niestabilne łącza danych, połączenia głosowe złej jakości czy kłopoty z artefaktami na zapisach z kamer. Trudno zliczyć problemy, których źródłem jest niewłaściwie funkcjonująca sieć. Przewoźnicy kolejowi muszą zmagać się z nimi podczas codziennych działań i w różnych scenariuszach operacyjnych.

### Zapewnienie trwałości

Okres eksploatacji pociągów jest od 10 do 20 razy dłuższy niż większości zaawansowanych technologicznie produktów elektronicznych. Z tego powodu koleje są modernizowane i wyposażane w nowoczesne rozwiązania sieciowe. Za sprawą postępu w technologii pojazdów nowe pociągi są w coraz większym stopniu uzależnione od danych. Dozór wizyjny, systemy informacji pasażerskiej, monitorowanie stanu taboru i inne aplikacje stawiają wysokie wymagania wobec sieci komunikacyjnej dla kolei. Oczekiwania dotyczące szybkiego i bezpiecznego zarządzania oraz przesyłania danych wyraźnie rosną. Obecnie operatorzy flot i producenci pojazdów szynowych potrzebują dostawców dogłębnie rozumiejących zagadnienia dotyczące sieci łączności kolejowej, którzy mogą zapewnić im skuteczną integrację i zwiększyć kompatybilność nowych rozwiązań ze starszym taborem.

### Najważniejsze aspekty niezawodnego systemu komunikacji dla kolei

**Kontrola i bezpieczeństwo to główne aspekty niezawodnego systemu komunikacji dla kolei. Wraz z przybywaniem połączeń nastąpiła zmiana podejścia.**

Solidne systemy łączności są gwarancją bezpiecznych, terminowych i w pełni skomunikowanych podróży. Do najważniejszych zadań systemu łączności należą sterowanie pociągiem i bezpieczeństwo.





➔ Oczywiście ostatecznym jego zadaniem jest szybka transmisja informacji do właściwego odbiorcy. Wdrożenia natomiast różnią się rodzajem przekazywanych informacji i ich celem.

#### Sterowanie pociągiem oparte na łączności

CBTC (*Communications-based Train Control*) to system sygnalizacji kolejowej wykorzystujący telekomunikację między pociągami a urządzeniami przytorowymi do zarządzania ruchem i infrastrukturą sterowania. Systemy CBTC dostarczają dokładniejsze informacje o lokalizacji pociągów w porównaniu z tradycyjnymi systemami sygnalizacji.

#### Systemy kamer dozorowych

Obecne systemy łączności metra w dużym stopniu wykorzystują również kamery w celu zapewnienia bezpieczeństwa infrastruktury kolejowej i pasażerów. System dozoru wizyjnego może np. wykryć osobę na torach, zaalarmować operatorów i ostrzec nadjeżdżający pociąg o niebezpiecznej sytuacji. Bez niezawodnej sieci nie można wdrożyć niezawodnego systemu bezpieczeństwa, który musi obsługiwać bardzo dużą liczbę kamer.

#### Komunikacja operacyjna

Do tego, by dyspozytor mógł bezproblemowo komunikować się z maszynistami, podejmując niezbędne działania, potrzebny jest również niezawodny system łączności głosowej. W godzinach szczytu każda sekunda decyduje o efektywności działań. Komunikacja głosowa potrzebna jest też personelowi wykonującemu prace konserwacyjne, odgrywa kluczową rolę w skutecznej pomocy pasażerom będącym w niebezpieczeństwie. Dzięki niezawodnej sieci łączności centrum operacyjne może ostrzegać pracowników ochrony o wystąpieniu sytuacji zagrożącej bezpieczeństwu publicznemu. System nagłośnienia PA ma kluczowe znaczenie w kontrolowaniu tłumu. Solidna sieć komunikacyjna jest niezbędna w codziennych operacjach, przekazując ważne wiadomości zainteresowanym stronom, a przede wszystkim zapewniając bezpieczeństwo. Strategia polega na tym, aby móc dotrzeć do zaangażowanego personelu, w dowolnym momencie i natychmiast. Dysponuje się wtedy możliwością informowania ludzi w razie potrzeby, poprawy ich świadomości sytuacyjnej, a także przyspieszenia

reakcji na sytuacje krytyczne wymagające natychmiastowej uwagi.

#### Integracja w ramach IoT

Można się spodziewać, że Internet Rzeczy (IoT), który w ostatnich latach objął niemal każdą branżę, będzie odgrywał istotną rolę również w systemach komunikacji kolejowej. Dzięki integracji systemów dozoru wizyjnego z intensywnie wykorzystywaną infrastrukturą sieci przewodowej i bezprzewodowej operatorzy uzyskują doskonalszy, kompleksowy i dostarczany w czasie rzeczywistym obraz pociągów, torów, składów i stacji. Monitoring tych zasobów może być objęty siecią kamer skomunikowanych w IoT. Umożliwi to operatorom wykorzystanie zaawansowanych funkcji, takich jak analityka dotycząca krytycznych aspektów i prowadząca do wykorzystania w praktyce inteligencji, by uzyskać poprawę wydajności systemu.

### Kluczowe elementy sieci telekomunikacyjnej dla metra

**Cała sieć telekomunikacyjna w metrze – rozwiązania zarówno przewodowe, jak i bezprzewodowe – wymaga standaryzacji. Powinna być w największym stopniu zabezpieczona przed włamaniami.**

Najogólniej mówiąc, systemy łączności w sieciach kolejowych można podzielić na bezprzewodowe i przewodowe. Oba te typy mają do odegrania ważną rolę i muszą być oparte na określonych standardach.

#### Rozwiązania przewodowe

Solidny i niezawodny system przewodowy cechują:

1. Niezawodność urządzeń. Przykładowo, przełącznik sieciowy klasy konsumenckiej (a nawet korporacyjnej) nie będzie oferował takiego poziomu niezawodności, jak urządzenie przeznaczone dla infrastruktury krytycznej, które ma wbudowaną redundancję.
2. Wysoka przepustowość sieci umożliwiająca transfer ogromnej ilości danych z różnych aplikacji.
3. Funkcje odporności utrzymujące ogólną funkcjonalność sieci komunikacyjnej, nawet w przypadku awarii łącza lub węzła.

4. Możliwość separowania ruchu i funkcje QoS (zarządzania jakością usług), co zapewnia, że każdy podsystem korzystający z sieci ma ustalone priorytety i poziom wydajności oraz nie wpływa na działanie innego podsystemu. Przykładowo, użytkownik pobierający plik z serwera sieciowego nie powinien przeciążać sieci i wpływać na wydajność systemu CCTV.

5. Możliwość rozbudowy. Ponieważ potrzeby w zakresie przepustowości rosną w szybkim tempie, system komunikacyjny powinien być w stanie sprostać takiemu wzrostowi bez poważniejszych modyfikacji lub wymiany kluczowych komponentów.

Ze względu na te wymagania w sieciach IP/MPLS powinno się używać rozwiązań dla infrastruktury krytycznej.

#### Rozwiązania bezprzewodowe

W przypadku sieci bezprzewodowej oprócz wcześniej wymienionych wymagań dla sieci przewodowej powinno się brać pod uwagę problemy z bezpieczeństwem i obsługą wielu użytkowników. Zabezpieczenie sieci bezprzewodowej nie jest zadaniem prostym. W ciągu ostatnich lat włamano się do wielu sieci bezprzewodowych, wykorzystując luki w zabezpieczeniach, a nawet socjotechnikę. Dlatego cyberbezpieczeństwo jest sprawą kluczową i bezwzględnie należy brać je pod uwagę.

Ważna jest także kwestia obsługi wielu użytkowników i aplikacji, ponieważ dostępne jest dla nich to samo współdzielone łącze bezprzewodowe. Kluczowe staje się więc zastosowanie takiego rozwiązania, które oferuje mechanizmy gwarantujące, że wszyscy użytkownicy i wszystkie aplikacje uzyskają dostęp do zasobów sieci bezprzewodowej, a w przypadku przeciążenia będą działać funkcje podtrzymujące komunikację sieciową.

Wszystkie te wymagania spełnia technologia LTE. Dzięki prywatnej sieci LTE kolej może wykorzystywać bezpieczną łączność bezprzewodową, która zapewnia użytkownikom najlepszą obsługę podczas wykonywania pracy.

#### Szeroko dostępna sieć i chronione urządzenia

Niezbędna jest niezawodna i dostępna sieć radiowa również w tak trudnych obszarach, jak tunele, zajezdnie, stacje i ich okolice. Sieć szkieletowa musi być redundantna, ponadto powinien być wdrożony system zarządzania siecią w celu jej monitorowania. Dwa kolejne kluczowe wymogi to posiadanie sprawdzonych, solidnych i zabezpieczonych urządzeń (terminali) oraz wyposażenie ich w najnowocześniejsze aplikacje. Umożliwi to użytkownikom końcowym korzystanie z transmisji danych, śledzenie lokalizacji oraz komunikację grupową i z centrum operacyjnym.

#### Zgodność ze standardami branżowymi

Przestrzeganie standardów ma kluczowe znaczenie w zapewnieniu bezpiecznego i wydajnego działania systemów łączności. Na standardach opierają się rozwiązania przewodowe i bezprzewodowe. Opracowane przez organizację IETF standardy IP/MPLS są szeroko stosowane przez dostawców usług komunikacyjnych na całym świecie, a także operatorów w branżach o znaczeniu krytycznym, w tym kolejowej. Technologia LTE natomiast jest znormalizowana przez forum 3GPP i ogólnodostępna. Zgodnie z LTE działają światowe sieci komórkowe, a prywatne wdrożenia LTE są obecnie wykorzystywane w różnych sektorach gospodarki.

W ostatnich latach wzrastają również obawy dotyczące cyberzagrożeń. Należy przestrzegać odpowiednich przepisów i stosować najlepsze praktyki z zakresu cyberbezpieczeństwa. To warunek niezbędny w zabezpieczaniu krytycznych sieci przed cyberatakami i wdrażaniu skutecznej strategii cyberochrony. Przewoźnicy kolejowi mogą w ten sposób uniknąć potencjalnych strat przychodów i zachować reputację jako dostawcy niezawodnych i terminowych usług.



WISENET

TAW-4000H16

**System dozoru wizyjnego dla Transportu (TMS)  
Efektywne zarządzanie flotą pojazdów**

- Szybkie wyszukiwanie nagrań, jednoczesne śledzenie lokalizacji i odtwarzanie wideo
- Automatyczne tworzenie kopii nagrań, zdarzeń oraz danych GPS
- Pełen raport dot. statusu systemu
- Detekcja ruchu, dźwięku, wstrząsów, zmian temperatury oraz sabotażu



## Zapewnienie niezawodnych rozwiązań dozoru wizyjnego dla systemów metra

**Pokładowy system monitoringu wizyjnego nie tylko podnosi poziom bezpieczeństwa, ale także dostarcza przydatne dane analityczne.**

Kamery dozоровe stały się integralną częścią systemów metra. Producenci systemów dozoru wizyjnego oferują rozwiązania pokładowe dostosowane do systemów metra i kolei. Kwestia bezpieczeństwa to niejedyny problem, który kamery mogą pomóc rozwiązać. Dozór wizyjny może być skutecznym wielofunkcyjnym narzędziem do poprawy wydajności przewoźnika i obniżenia kosztów, a także zwiększenia poziomu obsługi pasażerów, zmniejszenia opóźnień lub zakłóceń z powodu awarii mechanicznych, utrudnień na drodze lub zatorów komunikacyjnych.

### Zabezpieczony system dozoru wizyjnego

W przypadku monitoringu wizyjnego na kolei istotne jest, aby sieć mogła obsługiwać wiele kamer i skutecznie dystrybuować w trybie IP multicast wiele strumieni wizji do wielu centrów monitorowania i pamięci masowych. Sieć dobrze i kompleksowo zaprojektowana spełni krytyczne wymagania. Będzie niezawodna i elastyczna, obsługując zaawansowane mechanizmy QoS oraz zapewniając niewielkie rozszynchronizowanie i małe opóźnienia w celu dostarczania sygnału wizji wysokiej jakości. Zaspokoi bieżące potrzeby w zakresie ruchu sieciowego oraz będzie przygotowana na jego wzrost. Kluczowe znaczenie mają przepustowość, jakość usług (QoS) oraz zasięg. Gdy usługi tej samej sieci są współużytkowane przez różne aplikacje, np. transmisja strumieni wizji, głosu, danych o lokalizacji, danych itp., należy również ustalić priorytety ruchu zgodnie z tym, jak ważny jest dla funkcjonowania systemu.

### VMS

Można się spodziewać, że w najbliższych latach wdrożenia analityki wizji i innych złożonych funkcji będą coraz częstsze w transporcie publicznym. Jednak integracja wszystkich nowych technologii mnoży interfejsy, którymi operatorzy będą musieli zarządzać. W niestandardowych sieciach taka złożoność stanie się dla ich administratorów wyzwaniem. Rozwiązaniem tego problemu jest wdrożenie urządzeń i systemów VMS spełniających standardy ONVIF. Zapewnią one kompatybilność rozwiązań i umożliwią użytkownikom wykorzystanie ich interoperacyjności.

### Analityka wizji dla sieci kolejowych

W tej branży analiza obrazu wykonywana w różnych celach także zyskuje na popularności. Przykładem może być współpraca Siemens Mobility i Strukton Rail, której celem było wykorzystanie analityki wizji i sztucznej inteligencji (AI) do automatycznego wykrywania i oceny stanu izolowanych złączy szynowych. Analityka będzie również przydatna do określania przepływów i zachowania pasażerów, umożliwiając przewoźnikom wprowadzanie zmian zmniejszających zatory i podnoszących poziom jakości obsługi klienta. Wcześniej analiza obrazu ograniczała się do infrastruktury serwerów i pamięci masowych, obecnie coraz popularniejsze stają się rozwiązania typu edge (w urządzeniach brzegowych sieci). Dzięki nim można ją przeprowadzać wprost w kamerze, co przyspiesza przetwarzanie. □



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

Z naszych rozwiązań korzysta



**Największe centrum biznesowe  
w Polsce północnej - ponad 150 000 m<sup>2</sup>  
powierzchni biurowej klasy AA**

[www.alnetsystems.com](http://www.alnetsystems.com)



# Inteligentne pożegnanie z korkami

T E K S T  
Eifeh Strom

**Skutkiem szybko postępującej urbanizacji na całym świecie są m.in. zatłoczone drogi. Aby przeciwdziałać narastającym problemom, miasta wdrażają systemy zarządzania ruchem, które wchodzi w skład inteligentnych systemów transportowe (ITS).**



Zaawansowane systemy zarządzania ruchem (ATMS – *Advanced Traffic Management Systems*) w sposób ciągły monitorują drogi, przesyłając menedżerom ruchu mnóstwo cennych informacji. Na ich podstawie mogą oni podejmować właściwe decyzje zmierzające do rozładowania zatorów komunikacyjnych i upłynnienia ruchu.

Zdaniem analityków z MarketsandMarkets w 2018 r. segment ATMS miał największy udział w całym rynku ITS. I ma się to nie zmienić do 2023 r. Ogólny wzrost rynku wynika z konieczności poprawy bezpieczeństwa publicznego, narastających problemów z tworzeniem korków w ruchu drogowym oraz inicjatyw rządowych na rzecz skutecznego zarządzania ruchem.

## Zatłoczone drogi wymagają zaawansowanych systemów zarządzania ruchem

Monitorując drogi w sposób ciągły, systemy ATMS oceniają natężenie ruchu, wspomagają jego uczestników w dotarciu do celu, wykrywają wypadki, a także gromadzą dane statystyczne pomocne w poprawie płynności ruchu.

W roku 2018 kierowcy w najbardziej zatłoczonych miastach tracili nawet 272 godziny, stojąc w korkach. Przekłada się to na straty finansowe o wartości miliardów dolarów. Brak płynności ruchu stwarza też problemy związane z zarządzaniem kryzysowym, m.in. reagowaniem na wypadki, przyczynia się także do wzrostu zanieczyszczeń i emisji dwutlenku węgla.

Dzięki postępowi w zakresie technologii sieciowych, usługom w chmurze, oprogramowaniu zdolnemu do autooptymalizacji

i ulepszonym interfejsom operatora w systemach zarządzania ruchem dostęp do informacji staje się łatwiejszy. Tym samym działania zmierzające do likwidowania zatorów drogowych mogą być szybsze i skuteczniejsze.

Zwiększanie płynności ruchu nie tylko skraca czas i poprawia jakość podróży, ale także zmniejsza ryzyko wypadków, usprawnia interwencje oraz ogranicza emisję CO<sub>2</sub>. Inwestując w technologie zarządzania ruchem, zarówno sprzętowe, jak i programowe, zdolne do generowania danych w czasie rzeczywistym oraz po ich przetworzeniu, miasta mają większe możliwości reagowania na sytuacje kryzysowe i angażowania się w planowanie optymalnej przepustowości dróg. Różne organizacje na całym świecie, na szczeblach zarówno regionalnym, jak i krajowym inicjują projekty mające na celu zmniejszenie zatłoczenia na drogach i poprawę bezpieczeństwa. Ze względu na wysokie koszty inwestycji i brak zaangażowania sektora prywatnego w niektórych regionach możliwości są jednak ograniczone.

## Preferencje i potrzeby użytkowników

W obliczu coraz większych korków na drogach i ulicach miast oraz problemów z zarządzaniem ruchem sięga się po inne formy transportu, np. MaaS (*Mobility-as-a-Service*), czyli mobilność w formie usługi.

Zanim miasta wdrożą rozwiązania do zarządzania ruchem na drogach, muszą skupić się nie tylko na bieżących potrzebach użytkowników, ale także brać pod uwagę przyszłe zmiany.

Tradycyjne systemy zarządzania ruchem wykorzystują zarówno urządzenia, jak i in-

teligentne oprogramowanie, m.in. do analizy wizyjnej. Takie rozwiązania zazwyczaj składają się z kilku modułów: gromadzących informacje (czujniki, kamery, stacje pogodowe, czytników tablic rejestracyjnych itp.), dostarczających informacje dla użytkowników dróg (panele informacyjne, telefoniczne centra obsługi) oraz przetwarzających informacje (np. w zakresie czasu podróży, poziomu usług itp.). Dochodzą do tego centra zarządzania, które zbierają, przetwarzają i rozpowszechniają informacje przydatne dla użytkowników dróg.

W miarę jak miasta się rozrastają, przybywa mieszkańców i pojazdów, a ulice coraz bardziej się korkują, zarządzanie ruchem staje się coraz bardziej złożone. Z tego powodu dochodzi do zmian w zachowaniu osób dojeżdżających do pracy czy przemieszczających się. Miasto musi poznać te nowe wzorce, by sprostać potrzebom użytkowników dróg. Ważnymi aspektami zarządzania ruchem stają się: kontrola dostępu, kontrola jakości powietrza, podatek od liczby przejechanych kilometrów czy systemy premiowania określonego zachowania.

Do osiągnięcia tego celu niezbędna jest szersza automatyzacja zadań i wykorzystanie dostępnych technologii ułatwiających pracę operatora. Umożliwia ją postęp w obszarach wspomagania decyzji i prognozowania oraz dostępność coraz doskonalszych pulpitu nawigacyjnych dających wgląd w ruch drogowy w czasie rzeczywistym i większą świadomość sytuacyjną, dzięki czemu można podejmować bardziej przemyślane decyzje. Ważne jest też zarządzanie przestrzenią publiczną, m.in. miejscami parkingowymi, ulicami i drogami – zapewnienie dostępności do tych zasobów staje się coraz bardziej istotne, szczególnie na wjazdach do centrów miast.

Aby sprostać wyzwaniom, miasta muszą postawić na cyfryzację swoich usług. Wtedy informacje będą mogły być gromadzone na bieżąco, a użytkownicy uzyskają do nich bezpośredni dostęp. Zarządzający infrastrukturą muszą także potrafić analizować wielkie zbiory danych gromadzonych w czasie rzeczywistym, by zasilać nimi „inteligencję” zdolną poprawić sytuację na drogach.

Najważniejsze obecnie aspekty transformacji dotyczą jednak pojawiających się alternatywnych środków transportu, w tym tzw. mikromobilności (rowery publiczne, hulajnogi itp.) oraz mobilności w formie usługi (MaaS). MaaS integruje w ramach jednej platformy i konta użytkownika (na aplikacji w smartfonie) dostęp do całej oferty transportu publicznego, mobilności współdzielonej i na żądanie. Przewiduje się, że ostatecznie nowe modele obejmą również połączone w sieci samochody i pojazdy autonomiczne.

Strategia zarządców dróg i autostrad będzie ewoluować w kierunku oferty MaaS dla użytkowników samochodów. Obejme ona inteligentne rozwiązania do pobierania opłat na drodze za dostęp do niektórych tras albo do wprowadzenia opłat modułowych i płatności w czasie rzeczywistym, których wysokość będzie zależała od warunków drogowych, dnia lub godziny, zajętości pojazdu itp. Radykalna zmiana doświadczeń z jazdy może nastąpić, gdy komunikacja stanie się bezpieczniejsza, a Internet Rzeczy (IoT) będzie stymulował rozwój połączonych i autonomicznych samochodów. Postęp technologiczny zapewni dostęp również użytkownikom do różnych informacji związanych z ruchem drogowym, pomagając w bezpieczniejszym prowadzeniu pojazdów.

Zmiany te po części wymuszają użytkownicy oczekujący wygodniejszych oraz łatwiejszych w zarządzaniu i kontroli środków transportu. Operatorzy autobusów, metra lub pociągów wkrótce będą dysponować zintegrowanym systemem zarządzania trasami, scentralizowanym oraz połączonym z informacjami dotyczącymi ruchu i podróżujących. Takim, w którym uczenie maszynowe i duże zbiory danych (*big data*) ułatwią redefiniowanie tras w czasie rzeczywistym lub wyznaczanie tras dostosowanych dla użytkowników różnych środków transportu.

## Co decyduje o tym, że system zarządzania ruchem jest zaawansowany

**Dodanie inteligentnych podsystemów do rozwiązań ATMS sprawia, że ich możliwości zarządzania zatorami komunikacyjnymi na drogach stają się jeszcze bardziej zaawansowane.**

Systemy ATMS są już same w sobie rozwiniętą formą rozwiązania do zarządzania ruchem. Dołączenie do nich inteligentnych podsystemów czyni je jeszcze bardziej skutecznymi. Podstawowym celem ATMS jest likwidowanie zatorów komunikacyjnych poprzez efektywniejsze wykorzystanie istniejącej infrastruktury dzięki stosowaniu technologii wykrywania, komunikacji i przetwarzania danych.

System staje się jeszcze wydajniejszy i bardziej efektywny, gdy dodatkowo wdroży się takie kluczowe podsystemy, jak systemy wykrywania incydentów, systemy opłat za przejazd i systemy zarządzania parkingami. Obecnie jest on uzupełniany także o zaawansowane funkcje gromadzenia informacji z różnych źródeł danych (np. Google Maps), a także z aplikacji mobilnych zbierających anonimowe dane GPS. Kolejnych danych dostarczają stacje po-



gody i systemy rozpoznawania tablic rejestracyjnych (LPR).

Kluczowa dla osiągnięcia najlepszej wydajności ATMS jest integracja informacji i współpraca z systemami gromadzenia danych o ruchu na poziomach krajowym, regionalnym i lokalnym. Pomocna w tym jest rosnąca dostępność czujników i technologii, które można wykorzystać do gromadzenia informacji o ruchu. Integracja danych z wielu źródeł ma na celu poszerzenie wiedzy nt. bieżącego stanu ruchu. Wymiana i zbieranie informacji może dotyczyć samych pojazdów – z pomocą przychodzi tu technologia połączonych samochodów, czyli inteligentnych aut skomunikowanych z Internetem.

ATMS nie jest już tylko systemem sterowania i kontroli ruchu, musi także zarządzać i przetwarzać ogromne zbiory danych dostarczanych z urządzeń Internetu Rzeczy (IoT) oraz rozwiązań V2X (*vehicle-to-everything*). System ATMS musi ewoluować, aby uwzględnić możliwości komunikacji pojazdów z pojazdami za pośrednictwem V2X, bez udziału tradycyjnej infrastruktury drogowej. V2X zmienia sposób zarządzania ruchem oraz interakcji z pojazdami i kierowcami.

Teraz, gdy rozwiązania V2I (*vehicle-to-infrastructure*) zyskały wyraźną ścieżkę rozwoju i wdrożeń, będą stanowić szkielet bezpośredniej interakcji z pojazdami i kierowcami uzupełniając zadania aplikacji bezpieczeństwa V2V (*vehicle-to-vehicle*).

**Uczenie maszynowe i uczenie głębokie jako miary inteligencji**  
Dzięki pogłębionej analizie danych dotyczących ruchu systemy zarządzania stają się bardziej inteligentne i efektywne.

Rozpoznawanie tablic rejestracyjnych (LPR) jest najbardziej znaną i szeroko wykorzystywaną w systemach zarządzania ruchem technologią analizy wizyjnej. Znajduje zastosowanie w systemach kontroli dostępu, billingu i rozwiązaniach security. W miarę rozwoju sztucznej inteligencji coraz powszechniej wykorzystuje się także uczenie maszynowe (*machine learning*) i głębokie (*deep learning*).

Dzięki temu w systemach zarządzania ruchem dostępna jest bardziej zaawansowana analityka wizji. Najczęściej dotyczy wykrywania w czasie rzeczywistym nietypowych sytuacji na drodze – nieoczekiwanego zatrzymania się pojazdu, tworzenia się kolejki samochodów, pojazdu jadącego pod prąd itp.

Ważne jest także gromadzenie statystycznych danych o ruchu, m.in. zliczanie i klasyfikacja pojazdów, określanie ich średniej prędkości, odległości między pojazdami itp. W warunkach miejskich przydatne bę-



## Kluczowa jest integracja informacji i współpraca z systemami gromadzenia danych o ruchu na poziomach krajowym, regionalnym i lokalnym

dą też dodatkowe funkcje analizy obrazu, np. zarządzanie oświetleniem czy określanie zajętości miejsc parkingowych.

Po dokonaniu modyfikacji i uzupełnień istniejącego ekosystemu sprzętowego zaawansowaną analitykę wizji można zastosować także w starszych systemach. W tym celu w centrum danych trzeba wdrożyć serwery zdolne do obsługi uczenia maszynowego. Zainstalowane na nich oprogramowanie przetwarza informacje z kanałów wizji i zgodnie z wymaganiami klienta stosuje reguły określone dla danego użytkownika.

Analityka wizji oparta na standardowym komputerowym rozpoznawaniu obrazu z użyciem kamer, których głównym celem jest monitoring wizyjny, nie może w pełni wykorzystać swojego potencjału. Umożliwia to dopiero integracja technologii *deep learning* z profesjonalnym systemem analizy obrazu.

Pozytywny wpływ na systemy zarządzania ruchem ma również zaawansowane przetwarzanie wizji na brzegu sieci bądź przetwarzanie scentralizowane. W celu ograniczenia wielkości strumieni wizyjnych w sieciach obciążonych lub o niskiej przepustowości obecnie w kamery wbudowuje się procesory o większej mocy obliczeniowej lub przetwarza dane w systemach lokalnych. Dotyczy to zwłaszcza obszarów miejskich o rozproszonej architekturze i niewystarczającym zasięgu sieci, gdzie wdraża się wbudowane rozwiązania analityczne. Wyniki analiz są przekazywane z terenu do systemów wyższego poziomu w centrach zarządzania ruchem. Obecnie modele uczenia maszynowego, wytrenowane przez programistów na komputerach z odpowiednimi zasobami GPU, mogą być przenoszone na maszyny lokalne o słabszej mocy.

Gdy analiza obrazu staje się coraz bardziej złożona, to właśnie uczenie maszynowe i głębokie umożliwiają skuteczne wykrywanie zdarzeń. Uczenie maszynowe optymalizuje algorytmy analizy, eliminując wady tradycyjnych technik. Identyfikuje wzorce, ciągle ucząc się systemu, i poprawia na bieżąco efektywność działania. Jest to szczególnie istotne w trudnych warunkach zewnętrznych, w jakich działają systemy zarządzania ruchem. Uczenie maszynowe wspomaga rozpoznawanie tablic rejestracyjnych nawet, gdy mają zakryte lub brudne fragmenty, usuwa fragmenty obrazu z zakłóceniami, eliminuje informacje spowodowane cieniami w ciągu dnia i poprawia wiarygodność danych dostarczanych w nocy. Ten ciągły cykl uczenia się i aktualizowania zwiększa możliwości predykcyjne systemu oraz zapewnia dokładniejsze wyniki.

Dostosowywanie głębokiego uczenia i uzyskiwanie bardziej zaawansowanych funkcji polega na przeprowadzaniu przez człowieka treningów w celu stworzenia modeli rozpoznawania, które

mogą znaleźć szersze zastosowanie. Inteligentne kamery można połączyć z tradycyjnymi czujnikami i uzupełniać informacje o atrybuty dodatkowe, dotyczące stref wejścia/wyjścia, oceny ryzyka wypadku, analizy zachowania i alertów. Wzbogaca to systemy zarządzania mobilnością o dane niestandardowe.

Co ważne, system analizy obrazu nie powinien być traktowany jako samodzielne rozwiązanie, ale jako część bardziej złożonej architektury zarządzania ruchem. Działa on w ścisłej integracji z innymi elementami (pamięcią masową, urządzeniami sieciowymi, systemem VMS, SCADA, platformą ITS itp.), które trzeba dostarczyć i wdrożyć.

### Zaawansowane technologie kamer usprawniają zarządzanie ruchem

Postęp w technologiach kamerowych, a jednocześnie bardziej przystępne ich ceny pozwalają włączyć je do rozwiązań zarządzania ruchem.

Jak wynika z raportu MarketsandMarkets, segment kamer dozoru wizyjnego na globalnym rynku zarządzania ruchem osiągnie największy potencjał do 2023 r. Analitycy zwracają uwagę na korzyści, jakie kamery oferują osobom dojeżdżającym do pracy. Dostarczają ważne dane o ruchu i pojazdach, monitorując ruch uliczny i rejestrując jego wzorce na potrzeby analiz, ale mogą też wystawić mandat za naruszenie przepisów ruchu drogowego.

Przetwarzanie obrazów i monitoring wizyjny wiążą się z wieloma możliwościami w rozwiązaniach zarządzania ruchem. Otwierają się teraz, gdy procesory stają się coraz wydajniejsze, pamięć masowa tanieje, a wbudowane funkcje analityczne upowszechniają się. Tradycyjne kamery monitorujące drogi mają jednak wiele wad, jeśli chodzi o całonocowe zarządzanie ruchem. Widoczność może być utrudniona w zależności od pory i warunków zewnętrznych – słabego oświetlenia w nocy albo gdy urządzenie jest skierowane bezpośrednio na słońce, a także przy niesprzyjających warunkach atmosferycznych, co wpływa na skuteczność wykrywania i dokładność pomiarów.

Kamery termowizyjne, w przeciwieństwie do kamer działających w świetle widzialnym, są mniej podatne na warunki zewnętrzne, takie jak pogoda i oświetlenie. Ich ceny znacznie spadły w ostatnich latach. W rezultacie te rozwiązania na rynku monitoringu miejskiego i monitorowania dróg stały się bardziej dostępne dla klientów. Niektórzy producenci w swoich kamerach integrują obie technologie.

Rośnie także popyt na radarowe systemy pomiaru ruchu. Taki radar to nic innego jak czujnik mikrofalowy (lub laserowy), który mierzy prędkość i wykonuje zdjęcia samochodów poruszających się powyżej określonej prędkości. Dodanie funkcji radaru i obrazowania termowizyjnego do tradycyjnej kamery poprawia skuteczność wykrywania pojazdu, zwłaszcza w warunkach słabego oświetlenia w nocy. Na popularności zyskują też kamery panoramiczne 360 stopni, z obiektywem typu „rybie oko” lub wieloprzetwornikowe. Takie urządzenia mogą zapewnić pełny widok skrzyżowania. Ich cena także przestaje być barierą.

Systemy sieciowe muszą obsługiwać cały transfer danych pochodzących ze wszystkich kamer. Przykładowo we wdrożeniu drogowym obejmującym 500 kamer sieć dla przekazu HD z jednej kamery będzie musiała zapewnić przepływność od 4 do 8 Mb/s. Do rejestrowania w czasie rzeczywistym obrazów ze wszystkich 500 kamer będzie więc potrzebne w centrum monitoringu pasmo 4 Gb/s. Wdrożenie sieci mogącej je zagwarantować nie jest już dzisiaj żadnym problemem. Nie można jednak zaniedbywać tego obszaru, bo przy braku odpowiednich systemów sieciowych trudno będzie uzyskać oczekiwaną wydajność i efektywność kamer oraz całego systemu zarządzania ruchem.

### Inteligentniejsze rozwiązania do pobierania opłat poprawiają przepływność na drogach

Systemy opłat drogowych diametralnie zmieniły się od czasów, gdy istniały tylko rozwiązania wymagające zatrzymania się kierowcy w punkcie poboru opłat i fizycznego zapłacenia należnej kwoty. Dzięki wykorzystaniu technologii rozpoznawania tablic rejestracyjnych oraz RFID elektroniczny pobór opłat (ETC) zyskuje na popularności na całym świecie.

Według analityków z MarketsandMarkets globalny rynek rozwiązań ETC ma do 2023 r. osiągnąć wartość 20,7 mld USD, przy średniej rocznej stopie wzrostu na poziomie 8,5 proc. Za rosnącą popularnością tych systemów stoją m.in. działania mające na celu ograniczenie zatorów komunikacyjnych i usprawnienie ruchu drogowego. Elektroniczne systemy opłat za przejazd są wdrażane również w celu sfinansowania nowej infrastruktury drogowej i utrzymania istniejącej. Te czynniki, obok wielu innych korzyści, będą w dalszym ciągu stymulować wzrost światowego rynku ETC. □



**ANALITYKA I SYSTEMY LPR/LPC**  
Wysokiej jakości inteligentny monitoring wideo

**PANORAMICZNE PROJEKTY**  
Wydajne systemy panoramiczne 180°/360°

**LICZENIE LUDZI I POJAZDÓW**  
Systemy liczenia dużej dokładności 3D i 2D

SOLUTIONS • CONSULTING • NINJA • EXPERT

Dystrybucja • Projekty • Integracja • Współpraca

Sumo  
30 lat

**POLSKA BRANŻA TRANSPORTU DROGOWEGO JEST OBECNIE W SZCZYCIE FAZY WZROSTU. SPRZYJA TEMU ROZWÓJ GOSPODARCZY KRAJU I ROSNĄCY HANDEL ZAGRANICZNY. OTWIERANE SĄ KOLEJNE CENTRA DYSTRYBUCYJNE. CIĄGLY WZROST ZAPOTRZEBOWANIA NA USŁUGI BRANŻY PRZY JEDNOCZESNYM NIEDOBORZE KIEROWCÓW, ZWIĘKSZAJĄCYCH SIĘ KOSZTACH PRACY I ZMIANACH W PRAWIE POWODUJĄ, ŻE JUŻ DZISIAJ BRANŻA TRANSPORTOWA STOI PRZED WYZWANIAM I, KTÓRE WYMUSZĄ WPROWADZENIE ROZWIĄZAŃ REWOLUCYJNYCH.**

# Transport przyszłości

## P

### Polska branża transportu drogowego jest obecnie w szczycie fazy wzrostu.

Do 2022r. szacowany całkowity wzrost wolumenów pod względem tonażu przewożonych towarów wyniesie 23%. Później oczekiwane jest spowolnienie dalszych wzrostów jest związane z prognozowanym wyhamowaniem wskaźników gospodarczych wpływających na branżę. Dotychczas segment przewozów międzynarodowych rozwijał się szybciej od przewozów krajowych. Po 2022 r. trend ten może ulec odwróceniu ze względu na zmiany przepisów prawa UE. W opinii przedstawicieli branży, planowane wprowadzenie Pakietu Mobilności, utrzymujący się na rynku pracy niedobór kierowców, wzrost kosztów w związku z regulacjami środowiskowymi i wzrost kosztów opłat drogowych doprowadzą do wzrostu kosztów w branży w przedziale 7-15% do końca 2020 r. w porównaniu z 2018 r.

Prognozowany rozwój gospodarczy Polski nie będzie mógł się obyć bez wzrostu w segmencie transportu. Obserwować można sygnały wskazujące na kontynuację trendów wspierających progres gospodarczy kraju, np. otwieranie na jego terenie centrów dystrybucyjnych europejskich operatorów. Na prognozę wzrostu w branży składają się dwa czynniki:

- przewidywane, pozytywne zmiany popytu na usługi transportowe na rynku wewnętrznym (w Polsce) z uwagi na wzrost PKB prognozowany na poziomie 3% w okresie 2018-2022,
- wzrost handlu zagranicznego Polski na poziomie 7% w okresie 2018-2020 oraz na dodatnim poziomie w latach 2021 i 2022.

W długim terminie (2023-2030) negatywne zmiany popytu na usługi polskich przewoźników na terytorium UE-28 (w konsekwencji przepisów Pakietu Mobilności) postrzegane są jako ogromne zagrożenie dla branży.

Niedobór kierowców o pożądanym umiejętnościach z wysokim prawdopodobieństwem będzie się pogłębiał do poziomu

### 5 SIŁ, KTÓRE KSZTAŁTUJĄ TRANSPORT DROGOWY W POLSCE W NAJBLIŻSZYCH LATACH



blisko 200 tys. kierowców (20% popytu na pracę) w roku 2022. Rewolucją dla branży będzie wdrożenie do użytku pojazdów autonomicznych, nie wypełni to jednak niedoboru w krótkiej perspektywie. Szacuje się, że rozwiązania w zakresie pełnej autonomii pojawią się na rynku dopiero po 2025 r. W początkowej fazie będzie wiązało się z nakładami inwestycyjnymi, jednak w długiej perspektywie umożliwi zwiększenie przewagi kosztowej. Autonomizacja pojazdów pozwoli na obniżenie kosztów działalności o 15% dzięki zmniejszeniu kosztów pracy. Równoległe rozwój napędów alternatywnych dostosuje branżę do rosnących

wymagań w zakresie emisji CO<sub>2</sub> i długookresowo również umożliwi ograniczenie kosztów transportu. Wdrożenie rozwiązań z zakresu digitalizacji będzie kluczowe dla obniżania kosztów działalności, dostosowania usług do zmieniających się potrzeb klienta oraz wdrażania rozwiązań o wysokiej wartości dodanej. W krótszej perspektywie czasowej będą one dostępne jednak dla dużych przewoźników, co może stworzyć dodatkową barierę dla mniejszych przedsiębiorców i przyczynić się do wzrostu koncentracji rynku. Obecny poziom digitalizacji branży transportu drogowego jest



niewielki, ponieważ w ostatnich latach przewoźnicy nie potrzebowali technologii do wzrostu. Globalni przewoźnicy postrzegają digitalizację jako nowe źródło przychodów, ale dla lokalnych będzie ona raczej źródłem poprawy efektywności. Inteligentne systemy transportowe oraz rozwiązania oparte na sztucznej inteligencji czy też *blockchain* są w fazie testów, dlatego prawdopodobnie w większej skali pojawią się na rynku dopiero w latach 2022-2023. W początkowej fazie (przed wprowadzeniem standardów) pozostaną one poza zasięgiem małych graczy z uwagi na wysokie nakłady inwestycyjne na ich wdrożenie.

### Rewolucja technologiczna jako czynnik zmian w branży transportu drogowego

- Zaawansowane technologie oparte na software i telematyce

Zaawansowane technologie oparte na software i telematyce będą naturalnym rozwinięciem rozwiązań wdrażanych w obszarze digitalizacji, ale mogą się one okazać niedostępne dla mniejszych przewoźników.

Choć wpływ nowych technologii nie jest jeszcze widoczny w pełni i trudno go skwantyfikować, można przyjąć, że zmiany te będą miały szczególne znaczenie dla kształtu rynku i działania przedsiębiorstw. Można oczekiwać, że do 2022 r. technologie takie jak sztuczna inteligencja, Internet Rzeczy, *big data* czy *blockchain* osiągną dojrzałość pozwalającą na szersze zastosowanie oparte na nich oprogramowania.

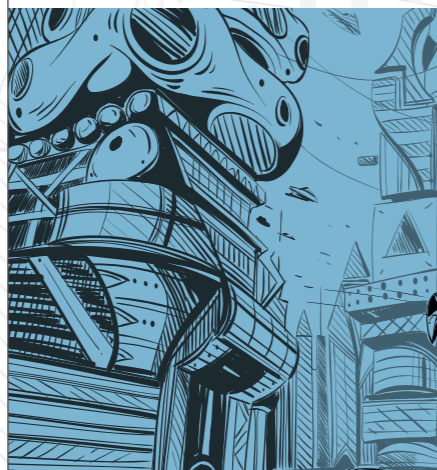
Na poparcie tej tezy można przytoczyć deklaracje globalnych spółek transportowych w zakresie realizowanych obecnie inwestycji w zaawansowane rozwiązania technologiczne w obszarze software i telematyki. Przedstawiony wynik wskazuje, że szczególną uwagę objęte są telematyka (tożsama z rozwiązaniami z obszaru Internetu Rzeczy) i sztuczna inteligencja. Na razie zainteresowanie technologiami opartymi na *blockchain* jest niewielkie. Może to być związane z postrzeganiem specyfiki tych rozwiązań – nie są one niezbędne i mają charakter wartości dodanej. Pośród różnych rozwiązań software'owych zidentyfikowano 5 najważniejszych, które będą miały największy wpływ na rynek:

- Zrobotyzowana automatyzacja procesów (RPA)

RPA to technologie automatyzacji procesów z wykorzystaniem botów software'owych, które zastępują operacje wykonywane przez ludzi na komputerach. W transporcie istnieje duża przestrzeń do automatyzacji procesów administracyjnych z wykorzystaniem botów. Wy-

nika to z tego, że wiele zadań takich np. przygotowanie dokumentacji transportowej jest powtarzalnych, a wzrost kosztów skłania przedsiębiorców do poszukiwania rozwiązań, które mogą je ograniczyć. O potencjale technologii świadczą prognozy – obroty spółek świadczących rozwiązania z zakresu RPA mają rosnąć z dynamiką przekraczającą 50% w latach 2016-2022.

- Inteligentne systemy transportowe (ITS) ITS to systemy zbudowane z użyciem telematyki/rozwiązań Internetu Rzeczy wspomagające zarządzanie ruchem miejskim, transportem publicznym, przepływem pasażerów i towarów, flotą i ładunkami oraz zbieranie i raportowanie informacji o ruchu drogowym pojazdów. Z perspektywy przedsiębiorców transportowych umożliwiają one lepsze zdalne zarządzanie pojazdami. Według prognoz oczekuje się, że do 2022 r. obroty spółek oferujących rozwiązania z zakresu inteligentnych systemów transportowych (ITS) w transporcie drogowym osiągną globalnie wartość ponad 72,3 mld USD, rosnąc w tempie 7,9% w latach 2016-2022.



- Utrzymanie predykcyjne (konserwacje) Utrzymanie predykcyjne polega na konserwacji sprzętu na podstawie bieżących i historycznych parametrów jego pracy mierzonych z użyciem czujników. Dostęp do zbiorów różnorodnych danych pochodzących z sensorów maszyn produkcyjnych czy transportowych daje możliwość nieustannej analizy stanu urządzeń. Pozwala także wykorzystywać dane w celu uniknięcia awarii czy uchybień.

W transporcie remonty predykcyjne mogą odegrać kluczową rolę w minimalizacji awarii, które mają ogromny wpływ na bezpieczeństwo użytkownika pojazdów. Podobnie jak w przypadku rozwiązań RPA szacuje się, że obroty spółek świadczących rozwiązania z zakresu utrzymania predykcyjnego będą rosły z dynamiką przekraczającą średniorocznie 37% w latach 2018-2022.

- Rozwiązania *blockchain*

Rozwiązania software oparte na *blockchain* wykorzystują zasadę działania rejestru rozproszonego, który dzięki zwielokrotnieniu zapisów w grupie różnych podmiotów pozwala na budowanie niezawodnych punktów odniesienia dla zbieranych danych. Uniemożliwia np. ukrywanie nielegalnego obrotu towarami w procesach rejestrowanych z użyciem tej technologii. Rozwiązania korzystające z łańcucha bloków umożliwiają branży transportu i logistyki osiągnięcie wielu korzyści, takich jak zwiększenie:

- **bezpieczeństwa** – identyfikacja produktu i możliwość audytu przy zachowaniu prywatności za pomocą kluczy skrótu,
  - **wydajności** – zmniejszone zapotrzebowanie na przetwarzanie dokumentów (dzięki automatyzacji),
  - **przejrzystości** – łatwiejsze i bardziej niezawodne śledzenie i sprawdzanie źródeł,
  - **niezawodności** – po wprowadzeniu informacji do sieci nie można jej łatwo zmienić.
- Można się spodziewać, że z czasem rozwiązania *blockchain* odnajdą swoją drogę na rynek transportu i logistyki, pozwalając na zwiększenie przejrzystości dokonywanych transakcji dla klientów.

- Rozwiązania sztucznej inteligencji Transport i logistyka oraz motoryzacja to dwie z czterech branż, które wg badań PwC wykazują najwyższe korzyści z wdrożenia rozwiązań z zakresu sztucznej inteligencji. Dla przedsiębiorcy świadczącego usługi transportu drogowego rozwiązania oparte na sztucznej inteligencji w obszarze zarządzania przepływem towarów w sieci, identyfikowania zależności i podejmowania decyzji pozwolą m.in. na lepsze zarządzanie flotą i przepływem pasażerów/towarów oraz lepsze planowanie działalności. Rozwiązania te, podobnie jak i wymienione wcześniej, wymagają jednak większej dojrzałości, zanim będą mogły być zastosowane na rynku w szerszej skali.

Szanse poprawy efektywności, jakie dają digitalizacja i zaawansowane technologie, są znaczące, jednak mali przedsiębiorcy będą mieli do nich ograniczony dostęp. Możliwość korzystania będzie uzależniona od posiadanych zasobów i w praktyce fakt, że takimi zasobami będą dysponowali więksi przewoźnicy, może spowodować wzrost barier dostępu do branży, a w konsekwencji – zwiększenie koncentracji rynku. □

Opracowano na podstawie raportu PWC przygotowanego na zlecenie Związku Pracodawców „Transport i Logistyka Polska”

Genway

Tiandy

# NOWA W RODZINIE 4 CALOWA KAMERA PTZ

TC-H324S SPEC: 25X/1/E



## KLUCZOWE CECHY:

- DO 1920x1080@30KL/S
- STARLIGHT
- 0.002LUX
- 25x, CYFROWY ZOOM 16x
- S+265/H.265/H.264/M-JPEG
- SMART IR, ZASIĘG PODCZERWIENI: 150M
- WBUDOWANA GRZAŁKA
- BEZWTYCZKOWA PRACA
- IP66
- WEJ/WYJ ALARMOWE 1/1, WEJ/WYJ AUDIO 1/1



Genway oficjalny Dystrybutor Tiandy

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

W PAŹDZIERNIKU UB. ROKU PODCZAS SZCZYTU GAPS W WARSZAWIE SZEF MIĘDZYNARODOWEGO ZRZESZENIA PRZEWOŹNIKÓW LOTNICZYCH IATA ALEXANDRE DE JUNIAC STWIERDZIŁ, ŻE W OBLICZU WYCZERPUJĄCEJ SIĘ PRZEPUSTOWOŚCI NAJWIĘKSZYCH LOTNISK NA STARYM KONTYNENCIE CENTRALNY PORT KOMUNIKACYJNY, CZYLI NOWY HUB, JEST JAK NAJBARDZIEJ POTRZEBNY. BIORĄC POD UWAGĘ ROSNĄCY POPYT NA LATANIE, POZOSTAWIENIE PRZEPUSTOWOŚCI EUROPEJSKICH LOTNISK NA OBECNYM POZIOMIE DOPROWADZIŁOBY W PRZYSZŁOŚCI DO NIEMAŁYCH PROBLEMÓW. WEDŁUG WYLICZEŃ IATA, BRAK NOWYCH INWESTYCJI LOTNISKOWYCH W EUROPIE SPRAWI, ŻE DO ROKU 2040 AŻ 160 MLN PASAŻERÓW NIE BĘDZIE MOGŁO SKORZYSTAĆ Z TRANSPORTU LOTNICZEGO ZE WZGLĘDU NA PRZEPEŁNIENIE INFRASTRUKTURY. O PRZYSZŁOŚCI PROJEKTU CENTRALNEGO PORTU KOMUNIKACYJNEGO ROZMAWIAMY Z KONRADEM MAJSZYKIEM, DYREKTOREM KOMUNIKACJI CPK.

# Centralny Port Komunikacyjny

Inwestycja na miarę przyszłości



Konrad Majszyk

## CZY CENTRALNY PORT KOMUNIKACYJNY BĘDZIE SIĘ WYRÓŻNIAŁ CZYMŚ NA TLE INNYCH LOTNISK?

Będzie, i to bardzo. Ten port lotniczy wraz z węzłem kolejowym zostaną zaprojektowane i wybudowane całkowicie od podstaw. Jesteśmy jedyną planowaną obecnie w Europie dużą inwestycją lotniskową typu *greenfield*. Jako inwestor nie jesteśmy więc skrupowani żadnymi ograniczeniami istniejącej infrastruktury, np. starego lotniska. To niepowtarzalna okazja i przewaga konkurencyjna. Możemy zaplanować, zaprojektować i wybudować port lotniczy „na miarę” – dokładnie pod potrzeby użytkowników. To właśnie z nimi konsultujemy obecnie koncepcję CPK: poprzez opiniowanie przez szeroko pojętą branżę briefu strategicznego CPK i konsultacje z liniami lotniczymi w ramach ACC (*Airport Consultative Committee*).

## CZY RYZYKO PRZEPEŁNIENIA ISTNIEJĄCEJ INFRASTRUKTURY W EUROPIE JEST GŁÓWNYM ARGUMENTEM STOJĄCYM ZA TĄ INWESTYCJĄ?

Prawda jest taka, że dla takiej inwestycji zlokalizowanej między Warszawą a Łodzią, tuż przy autostradzie A2, na skrzyżowaniu planowanych linii kolejowych dużych prędkości nigdy nie było lepszego czasu, miejsca i okoliczności rynkowych. Rynek lotniczy w Europie Środkowo-Wschodniej, a w Polsce w szczególności, rośnie w tempie rekordowym. Zbliżające się do granicy przepustowości Lotnisko Chopina, największy port lotniczy w kraju, coraz bardziej dotkliwie krepują bariery środowiskowe, np. strefa ograniczonego użytkowania i limity hałasowe, z których wynika tzw. *core night* (zakaz lotów nocnych). Do tego dochodzą ograniczenia infrastrukturalne, np. bliskość dużych dzielnic mieszkaniowych i tras szybkiego ruchu, zwłaszcza południowej obwodnicy Warszawy, które uniemożliwiają budowę trzeciego pasa. Lotnisko Chopina jest jak za ciasne ubranie, które kępuje ruchy i uniemożliwia dalszy rozwój. Ponadto w długim horyzoncie czasowym budowa CPK się po prostu dla gospodarki opłaca. Test Prywatnego Inwestora (TPI) wykonany na potrzeby CPK przez EY wykazał, że zakładana stopa zwrotu z lotniskowej części inwestycji wynosi ponad 10 proc. W drugiej połowie ub. roku doradcy techniczni AECOM i Arcadis sprawdzili dla CPK harmonogramy i CAPEX całej inwestycji, potwierdzając po raz kolejny, że ma ona swoje biznesowe podstawy. Taką tezę potwierdzają też m.in. raporty PWC oraz Baker McKenzie i Polityki Insight.

## JAKIE SĄ SZANSE, ABY NOWY PORT LOTNICZY STAŁ SIĘ GŁÓWNYM WĘZŁEM PRZESIADKOWYM W EUROPIE?

Nasz port lotniczy powstanie w samym sercu rynku o wielkim potencjale: obszarze 18 europejskich krajów, na których terenie mieszka łącznie ponad 180 mln ludzi. Dzisiaj największym portem w tym regionie jest Lotnisko Chopina, pod względem liczby pasażerów wyprzedzające Pragę, Budapeszt i Bukareszt. Co istotnie, na całym tym rozległym obszarze nie ma lotniska, które pretendowałoby do roli globalnego hubu. To oznacza wielką szansę dla nowego projektu CPK.

Fakty są takie, że CPK jest położony wręcz fenomenalnie. To niezwykle atrakcyjna lokalizacja dla obsługi ruchu między Europą a Dalekim Wschodem. Jeśli chodzi o połączenia do Ameryki Północnej, to CPK może być atrakcyjnym punktem przesiadkowym np. dla pasażerów z Europy Środkowo-Wschodniej. Z tego punktu widzenia dobrą wiadomością jest też zniesienie wiz do USA dla Polaków, co generuje dodatkowy ruch.

Z powodu zapóźnienia cywilizacyjnego, które jako kraj staramy się odrobić, liczba pasażerów w „nowych” krajach członkowskich UE rośnie dwukrotnie szybciej niż w krajach Europy Zachodniej. Spójrzmy na statystyki: w Polsce średnia liczba podróży przypadająca na mieszkańca wynosi w ciągu roku 1,4, podczas gdy w krajach Europy Zachodniej jest to z reguły od 3 do 7. To pokazuje, że z jak dużym potencjałem w regionie CEE mamy do czynienia. Wystarczy z tej szansy skorzystać.

Fot.: Terminal CPK. Koncepcja KPF

Fot.: Terminal CPK. Koncepcja Foster + Partners





## JAKIE ROZWIĄZANIA Z ZAKRESU SYSTEMÓW ZABEZPIECZEŃ – W KONTEKŚCIE ZAPEWNIENIA BEZPIECZEŃSTWA PRACY ZARÓWNO PORTU, JAK I PASAŻERÓW – SĄ PLANOWANE?

Kwestie bezpieczeństwa są absolutnie kluczowe dla funkcjonowania CPK w przyszłości. Dlatego bierzemy pod uwagę szeroki wachlarz zagadnień, takich jak bezpieczeństwo pasażerów, bezpieczeństwo statków powietrznych, zabezpieczenia cyfrowe itd. Na etapie master planu będziemy rozważać szczegółowe rozwiązania i tworzyć zręby polityki bezpieczeństwa. Zastosowanie technologii możemy rozważać po zrealizowaniu planu generalnego, kiedy przystąpimy do prac projektowych.

## NA JAKIM ETAPIE SĄ PRZYGOTOWANIA DO BUDOWY CPK? KIEDY TEMAT PROCEDUR BEZPIECZEŃSTWA WEJDZIE W FAZĘ UZGODNIENIA?

W tej chwili przygotowujemy postępowanie na master plan lotniska, czyli kompleksowe zestawienie najważniejszych założeń koncepcyjnych przyszłej infrastruktury. Mamy już gotowy brief strategiczny, czyli techniczny dokument opisujący funkcjonalności i elementy CPK. W jego konsultacjach wzięło udział ponad 130 firm i instytucji, które zgłosiły łącznie ponad 9,5 tys. uwag i propozycji. W master planie wszystkie zebrane dotychczas dane zostaną uszczegółowione w stopniu umożliwiającym uzyskanie odpowiednich zezwoleń administracyjnych. Znajdzie się tam m.in. dokładna lokalizacja lotniska, parametry poszczególnych elementów infrastruktury, założenia etapowania inwestycji oraz szczegółowe założenia modelu biznesowego.

W pierwszej fazie realizacji zamówimy studium specjalne (*Security Master Plan*), które obejmie m.in. ocenę potencjalnych zagrożeń, wytyczne planowania systemów bezpieczeństwa, definicję ogólnej strategii bezpieczeństwa lotniska. Po zrealizowaniu master planu, przystąpimy do konkretnych prac projektowych, które mogą przesądzić o granicach stref bezpieczeństwa, procedurach reagowania na incydenty, a nawet o wyborze konkretnych rozwiązań technologicznych.

**CZAS, JAKI MIJA OD ROZPOCZĘCIA PRAC PROJEKTOWYCH DO ICH REALIZACJI, NIEKIEDY OZNACZA**

Fot.: Terminal CPK. Koncepcja Zaha Hadid Architects



Fot.: Terminal CPK. Koncepcja Zaha Hadid Architects

## WYMIANĘ TECHNOLOGICZNĄ RÓWNIEŻ W BRANŻY SYSTEMÓW ZABEZPIECZEŃ. CO W PRZYPADKU GDY PRZED REALIZACJĄ POJAWIĄ SIĘ NOWE, SKUTECZNIEJSZE ROZWIĄZANIA?

Jesteśmy przekonani, że się pojawią, i czekamy na nie z otwartymi rękami. Podczas Airport Exchange w Abu Zabi w listopadzie ub. roku była omawiana koncepcja tak futurystycznych zabezpieczeń lotniskowych, że gdyby weszły w życie, to pasażer wchodziłby po prostu do terminalu, a następnie – gdyby zaawansowane, automatyczne systemy nie wykryły w jego zachowaniu, bagażu, statusie podróży czy historii rejsów niczego niepokojącego – to niemal bez zatrzymywania wsiadłby do samolotu. Dzisiaj trudno to sobie wyobrazić, ale większość kontroli i odpraw być może będzie możliwa bez fizycznego udziału pasażera. Pieśń przyszłości? Zobaczymy. Co do zasady, jesteśmy otwarci na nowe technologie, a koncepcja CPK zostanie opracowana w ten sposób, żebyśmy byli przygotowani do elastycznego dostosowania się do nowych rozwiązań.

Jedno jest pewne: CPK na pewno zastosuje się do międzynarodowych wytycznych i standardów bezpieczeństwa, które są ustalone m.in. przez EASA (European Union Aviation Safety Agency) i ICAO (International Civil Aviation Organization) oraz zgodnie z wytycznymi Urzędu Lotnictwa Cywilnego i IATA (International Air Transport Association). Te źródła norm i standardów tworzą najbardziej aktualną, podstawową, wspólną bazę wiedzy na temat potrzeb całej branży lotniczej w zakresie bezpieczeństwa.

## CZY PRZY USTALANIU STRATEGII DOTYCZĄCEJ BEZPIECZEŃSTWA BĘDZIECIE KORZYSTAĆ Z DOŚWIADCZEŃ INNYCH ŚWIATOWYCH PORTÓW?

Już dzisiaj prowadzimy dialog techniczny w sprawie wyboru doradcy strategicznego dla CPK. Rozmawiamy w tej sprawie z najlepszymi i najlepiej zorganizowanymi lotniskami przesiadkowymi na świecie, o dużym doświadczeniu w działalności doradczej. Negocjujemy m.in. z portami Narita w Tokio, Changi w Singapurze i Incheon w Seulu. Bierzymy pod uwagę też inne lotniska spoza tego regionu. Jesteśmy w stałym roboczym kontakcie z operatorami polskich i zagranicznych portów lotniczych.

## CZEGO OCZEKUJĄ PAŃSTWO OD BRANŻY SECURITY, ABY ZAPEWNIĆ WYSOKI POZIOM BEZPIECZEŃSTWA PASAŻEROM I ZAGWARANTOWAĆ SPRAWNE FUNKCJONOWANIE PORTU?

Dokładamy starań, żeby posiadać aktualną wiedzę na temat możliwych do zastosowania systemów zabezpieczeń i warunków, w jakich sprawdzają się one najlepiej. Przed wyborem zabezpieczeń potrzebne będą dokładne analizy zagrożeń i ich potencjalnych skutków. Technologie zabezpieczeń planujemy rozważać i oceniać w ramach prac projektowych CPK. Od branży niezmiennie oczekujemy na bardziej wydajne i niezawodne urządzenia. W przyszłości zapewne konieczne będzie też wsparcie przy implementacji technologii i integracji systemów.

## JAKIE SĄ NAJWAŻNIEJSZE PLANY CPK NA TEN ROK?

W tym roku ruszy dobrowolny wykup gruntów. Zamierzamy także wybrać spośród najlepszych światowych portów lotniczych doradcę strategicznego, który będzie naszym partnerem podczas planowania, projektowania i budowy CPK.

Jednocześnie trwają postępowania w celu wyboru doradcy do zarządzania zintegrowanym zespołem projektowym oraz konsultantów do spraw: master planu, ochrony środowiska i badań terenowych.

Nasz harmonogram zakłada, że w połowie roku wykonawca master planu będzie już wybrany i rozpocznie pracę. W pierwszej połowie roku chcemy ruszyć na szeroką skalę z badaniami środowiskowymi na terenie całej Polski. Na początku lutego rozpoczęliśmy konsultacje korytarzy i wariantów planowanych przez nas linii kolejowych.

## NAJWIĘKSZYM WYZWANIEM JEST HARMONOGRAM. W JAKI SPOSÓB TA INWESTYCJA MA SIĘ ZMIĘŚCIĆ W ZAKŁADANYM TERMINIE?

Biuro Pełnomocnika ds. CPK planuje do końca marca przedstawić zmiany w prawie, żeby skrócić procedury administracyjne, zmniejszyć liczbę wymaganych formalności i przyspieszyć proces inwestycyjny. Innymi słowy: w planach jest nowelizacja specustawy o CPK. Kolejnym planowanym na najbliższe tygodnie kamieniem milowym jest Program Wieloletni CPK, czyli rządowy plan finansowania inwestycji w kolejnych latach.

Prawda jest taka, że nie mamy czasu do stracenia. CPK jest potrzebny tu i teraz. Naszym obowiązkiem jest go mądrze zaplanować i zaprojektować, a potem sprawnie wybudować i uruchomić. Wszystko po, żeby wykorzystać wielką cywilizacyjną szansę i rynkową okazję, jaka pojawiła się przed polską gospodarką.

DZIĘKUJEMY ZA ROZMOWĘ

Fot.: Terminal CPK. Koncepcja Zaha Hadid Architects





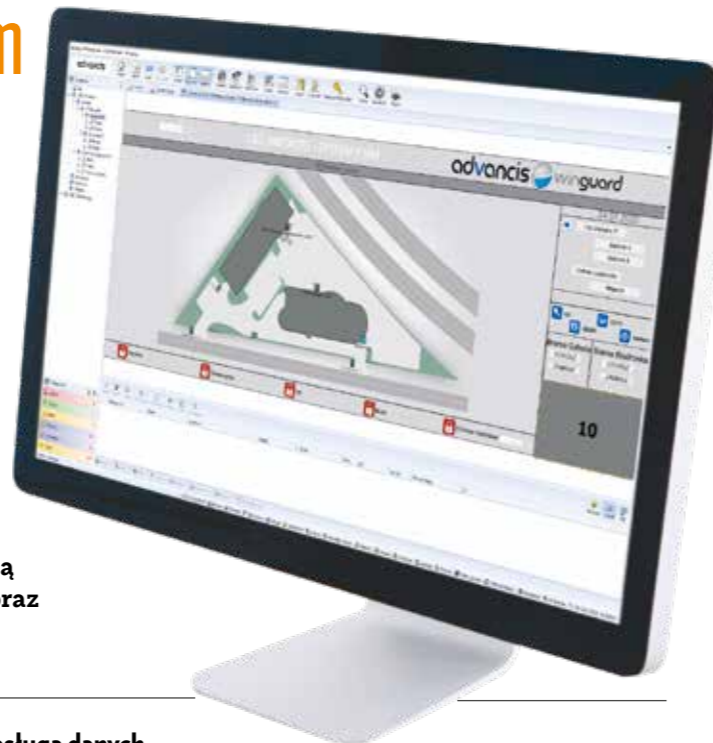


# WinGuard PSIM+ Transport publiczny

## Najwyższe standardy bezpieczeństwa w transporcie publicznym



Firma Advancis, bazując na zdobytym doświadczeniu i licznych referencjach, rozwija opracowane przez siebie rozwiązania wertykalne – WinGuard PSIM+ Transport publiczny, znajdujące się w ofercie C&C Partners. Zaawansowana wersja systemu oferuje predefiniowane funkcjonalności, które są wypadkową bieżących oczekiwań branżowych oraz śledzenia trendów rynkowych.



### Cyberbezpieczeństwo

Kluczowym obszarem rozwiniętym w ramach rozwiązania wertykalnego WinGuard PSIM+ Transport publiczny jest cyberbezpieczeństwo rozległych sieciowych instalacji, gdzie sprawa bezpiecznego, kontrolowanego dostępu do danych ma krytyczne znaczenie w obecnej rzeczywistości. WinGuard, zgodnie z najwyższymi standardami, zapewnia pełne szyfrowanie komunikacji sieciowej za pomocą protokołu AES-256. Umożliwia także pełne szyfrowanie bazy danych oraz integrację z usługą *Active Directory* (LDAP).

### Rozproszona architektura systemu

Sieciovanie i efektywne przesyłanie danych w rozległych rozproszonych strukturach, gdzie mogą występować różne typy połączeń sieciowych, to kolejne obszary, które zostały poddane gruntownej analizie. Odpowiedzią WinGuard jest możliwość zastosowania rozproszonej architektury systemu, gdzie poszczególne lokalizacje (stacje, tunele, budynki biurowe itd.) mogą być wyposażone w lokalne serwery bądź serwery interfejsów, w dalszej kolejności łączące się z nadrzędnymi lokalizacjami (np. centrami regionalnymi), a finalnie agregowane na poziomie centrum zarządzania. Jednocześnie system wspiera segmentację danych agregowanych na wyższych poziomach.

### Procesowa obsługa danych

Procesowa obsługa zdarzeń serwisowych ma na celu utrzymanie najwyższej sprawności i dostępności elementów infrastruktury bezpieczeństwa. Operator WinGuard, opierając się na informacjach otrzymywanych z poszczególnych systemów (np. o uszkodzeniu kamery), może inicjować automatyczne testy, zadysponować zespół serwisowy, śledzić postęp prac online, aż do momentu przywrócenia poprawnej pracy i formalnego zamknięcia zdarzenia. Pozwala to odpowiedzialnie i w pełni świadomie zarządzać podległą infrastrukturą.

### Zrealizowane projekty

Przykładem zastosowania rozwiązania wertykalnego WinGuard PSIM+ Transport publiczny jest projekt wykonany dla kolei austriackich, gdzie w ramach jednej instalacji systemu WinGuard PSIM dokonano integracji różnych systemów: telewizji dozorowej, SSP, systemu interkomowego, SSWiN, call center oraz dwóch wykorzystywanych systemów KD. Każdego dnia z dwóch centrów zarządzania bezpieczeństwem, zlokalizowanych w Wiedniu i Innsbrucku, operatorzy nadzorują blisko 11 tys. km tras, 300 tuneli i tysiące budynków infrastruktury kolejowej, co przekłada się na ponad 140 tys. punktów detekcyjnych w systemie WinGuard X4.

Jeden z realizowanych obecnie projektów w Polsce oparty na WinGuard PSIM+ Transport publiczny obejmuje integrację kilkunastu obiektów wchodzących w skład infrastruktury transportu publicznego w zakresie m.in. CCTV, SSP, KD, SSWiN, interkomów oraz systemów technicznych.

Podsumowując, WinGuard PSIM+ Transport publiczny to sprawdzone rozwiązanie do integracji i wizualizacji systemów, w pełni wspierające procesowe podejście do zarządzania bezpieczeństwem. Skalowalność, cyberbezpieczeństwo, neutralność oraz otwartość pozwalają na budowanie rozwiązań, które z jednej strony w ergonomiczny sposób wspierają codzienną pracę służb bezpieczeństwa, z drugiej – zapewniają interaktywne podnoszenie poziomu bezpieczeństwa w oparciu o korelację zdarzeń, umożliwiając śledzenie trendów czy wnioskowanie dedukcyjne. □

### C&C Partners

ul. 17 Stycznia 119, 121  
64-100 Leszno  
www.ccpartners.pl



# Kamery Hikvision w transporcie

Wdrożenia są różne, od autobusów, które mają maks. 10–12 kamer, po składy kolejowe, tzw. elektryczne zespoły trakcyjne wyposażone w ponad 40 kamer. Rozwiązania Hikvision sprawdzają się m.in. w takich realizacjach, jak SKM Warszawa, Koleje Mazowieckie, Koleje Wielkopolskie, MPK w Łodzi, MZK w Jeleniej Górze.

– Z firmą Hikvision zrealizowaliśmy już wiele projektów. Współpracujemy na trzech płaszczynach. Po pierwsze na rynku obiektów stacjonarnych, np. biurowce, urzędy, zajezdnie autobusowe – głównie na terenie Warszawy i Mazowsza. Po drugie na rynku komunikacji miejskiej, m.in. MZK w Jeleniej Górze, Tramwaje Śląskie, i kolejowym, np. SKM Warszawa, Koleje Mazowieckie. Po trzecie realizujemy projekty pośrednio do odbiorców końcowych poprzez producentów pojazdów, działając jako podwykonawca, np. PESA, Stadler, Solaris czy FPS – mówi Jakub Adamczyk, prezes Zarządu Polgard.

### Różnorodność oferty

Hikvision oferuje bogaty wybór modeli kamer dedykowanych do zastosowań transportowych. Wśród nich są modele pokładowe, które doskonale sprawdzają się zarówno wewnątrz pojazdu do monitoringu pasażerów, jak i do obserwacji szlaków oraz tego, co się dzieje na zewnątrz. Dostępne są również kamery zewnętrzne, tzw. lusterkowe, instalowane po prawej i lewej stronie kierowcy do obserwacji tego, co dzieje się po obu stronach autobusu lub pociągu. W przypadku autobusów dostępna jest również dedykowana kamera cofania.

### Niezawodność

Kolejnym argumentem przemawiającym za wyborem kamer Hikvision jest ich wy-

Firma Hikvision zbudowała mocną pozycję na rynku transportu. Z roku na rok przybywa wdrożeń w Polsce i na świecie. Dzięki współpracy z firmą Polgard kamery Hikvision zapewniają dziś bezpieczeństwo w kilkunastu polskich miastach, w różnych segmentach transportowych.

soka niezawodność. Jest to szczególnie ważne we wdrożeniach transportowych, dlatego że serwisowanie urządzeń w porzejeżdżającym się często na drugim końcu kraju jest kosztowne i czasochłonne, a także aby nie utracić zaufania klienta, który chce mieć sprawny tabor. – W związku z tym stawiamy na sprawdzonych dostawców, których urządzenia mają wskaźniki bezawaryjności na odpowiednim poziomie – podkreśla prezes firmy Polgard.

### Certyfikaty

Na rynku transportowym bardzo istotne są specjalistyczne certyfikaty. Kamery Hikvision mają wszelkie wymagane homologacje do zastosowań automotive, a na rynku kolejowym uzyskały certyfikaty na zgodność z normą PN-EN 50155 Zastosowania kolejowe. Wyposażenie elektroniczne stosowane w taborze i normą EN 45545 dotyczącą ochrony przeciwpożarowej, co ma zapewnić bezpieczeństwo osób i urządzeń wykorzystywanych w kolejnictwie.

– Współpraca w tym zakresie przebiega pozytywnie. Jeśli zgłaszamy Hikvision potrzebę uzyskania konkretnego certyfikatu, otrzymujemy taki. I to jest bardzo istotne zwłaszcza wtedy, gdy dostarcza się urządzenia bezpośrednio do producentów pojazdów – wyjaśnia Jakub Adamczyk. – Możemy też liczyć na profesjonalne wsparcie techniczne ze strony Hikvision. Bardzo szybko

otrzymujemy odpowiedzi na pytania związane z integracją. Stosujemy własne oprogramowanie do zarządzania materiałem wizyjnym w pojazdach i tutaj współpraca z producentem urządzeń musi być bardzo efektywna. Tak jest w tym przypadku, zgłaszane przez nas poprawki wprowadzane są bardzo sprawnie. Mamy też dobrą opiekę serwisową, urządzenia są dostarczane z magazynów w Europie, dlatego czas oczekiwania jest znacznie krótszy niż w przypadku dostaw z Azji.

W tym segmencie rynku bardzo istotne jest wsparcie partnerów na wszystkich etapach wdrożenia, od projektu, przez instalację, po obsługę posprzedażową. – Dbamy o ciągły rozwój oferowanych produktów, jesteśmy otwarci na współpracę z klientami, aby dostosować parametry kamer do ich wymagań. I właśnie to oraz elastyczność i niezawodność naszych rozwiązań uczyniło nas liderem rynku w sektorze zabezpieczeń w transporcie – mówi Piotr Świder, Business Development Manager w Hikvision Poland. □

### Hikvision Poland

ul. Zwirki i Wigury 16B,  
02-092 Warszawa  
tel. 22 460 01 50,  
faks 22 464 32 11  
e-mail: info.pl@hikvision.com





# smartGATE

## Innowacyjna usługa automatycznej kontroli procesów wjazdu i wyjazdu

Securitas wprowadził usługę smartGATE będącą odpowiedzią na rosnące zapotrzebowanie segmentu logistyki na usprawnienie procesu kontroli wjazdu i wyjazdu w centrach logistycznych, wytórczych i handlowych. Optymalizacja miała na celu usprawnienie awizacji i obniżenie kosztów, przy jednoczesnym utrzymaniu wysokiego poziomu bezpieczeństwa obiektu i zmniejszeniu udziału ochrony fizycznej stajęj.

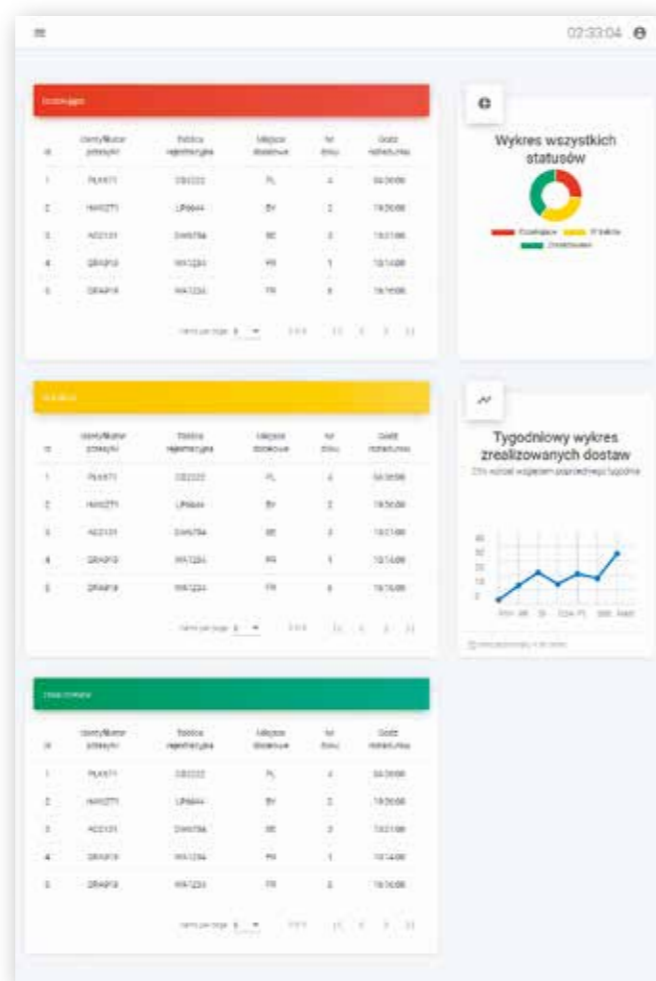
smartGATE pozwala na zarządzanie procesem załadunków oraz oszczędza czas kierowców i spedytora. Z punktu widzenia bezpieczeństwa zapewnia szyfrowany przepływ informacji oraz kilkustopniowy proces weryfikacji kierowcy i pojazdu dzięki zastosowaniu m.in.:

- systemu czytania tablic rejestracyjnych,
- przyznawania losowych kodów wjazdowych o ograniczonym terminie ważności, wysyłanych za pomocą SMS na numer telefonu kierowcy,
- czytnika dokumentów weryfikujących dane kierowcy lub transportowe,
- zestawu audio-wideo umożliwiającego połączenie się z pracownikiem Securitas.

smartGATE został oparty na najnowocześniejszych rozwiązaniach technicznych, łączących zalety chmury obliczeniowej i podejścia IoT. Dzięki temu ogranicza do minimum potrzebę inwestycji w rozwiązania sprzętowe pośredniczące w wymianie informacji. Algorytm systemu i modułowa konstrukcja smartGATE pozwala na dopasowanie do istniejących procesów biznesowych, zapewnia szybkie wdrożenie i zwrot z inwestycji. Dostęp do systemu z dowolnej sieci umożliwia świadczenie usługi przez pracowników ochrony będących w obiekcie, ale również w sposób zdalny przez operatorów Securitas Operation Center.

Bezpieczeństwo wymiany informacji jest zapewnione dzięki pełnemu szyfrowaniu między każdym elementem systemu, do którego dostęp jest w pełni kontrolowany i ograniczony do wybranych użytkowników. Responsywny interfejs pozwala na pracę na urządzeniach zarówno stacjonarnych, jak i mobilnych bez względu na wykorzystywaną platformę. Ponadto otwarte API zapewnia integrację z systemami logistycznymi i bezpieczeństwa.

Weryfikacja osób i pojazdów wjeżdżających i wyjeżdżających z obiektu jest jednym z kluczowych zadań pracowników ochrony. Decyzje podejmowane na tym etapie wpływają na działanie przedsiębiorstwa. Automatyzacja procesu kontroli ruchu kołowego pozwala utrzymać płynność operacyjną i zapewnia wysoki stopień dokumentacji. Jest to szczególnie istotne ze względu na rosnącą liczbę zadań zleczanych pracownikom ochrony, jak również zapotrzebowanie na optymalizację.



smartGATE został zaprojektowany w taki sposób, aby przyspieszyć prace administracyjne i odciążać użytkownika. Dane są wprowadzane do systemu w sposób intuicyjny za pomocą interfejsu webowego lub aplikacji w urządzeniach mobilnych z dostępem do Internetu. Możliwość korzystania z wielu języków sprawia, że smartGATE jest przyjazny również dla kierowców pochodzących z różnych krajów. System może być wyposażony w systemy skanowania podwozia, automatycznego ważenia lub odczytu numerów kontenerów. □

### Securitas Polska

Postępu 6, 02-676 Warszawa  
securitas@securitas.pl



**smartGATE**  
Innowacyjna usługa automatycznej kontroli i zdalnego zarządzania ruchem kołowym dla logistyki. Optymalizuje koszty i procesy, zapewnia kompletną dokumentację, łączy zalety chmury obliczeniowej i podejście IoT, ograniczając do minimum inwestycję w rozwiązania sprzętowe. Zapewnia szybkie wdrożenie i zwrot z inwestycji.





# Optymalizacja nie może oznaczać ograniczeń

Optymalizacja to w logistyce słowo klucz, które obejmuje wszystkie obszary działalności oraz procesy, zarówno operacyjne, jak i wspomagające, w tym również kwestie ochrony. Dla security managerów oznacza to konieczność ciągłego dostosowywania modelu ochrony do zmieniających się możliwości budżetowych i otoczenia.



T E K S T

Krzysztof Wilczyński

Dynamika zmian i często występujące w logistyce kontrakty krótkookresowe w większości przypadków ograniczają w ochronie wdrożenie rozwiązań długofalowych.

Zdarza się, że wiele z nich wprowadza się bez głębszej analizy tematu, co powoduje, iż cierpi na tym jakość usługi. Może to oznaczać, że ryzyko różnych zagrożeń, które wyeliminowano przez wcześniejsze rodzaje zabezpieczeń, czy możliwość ich wystąpienia zostało zminimalizowane, teraz powtórnie zaczyna rosnąć.

Dobrym przykładem jest chociażby ograniczanie liczby posterunków ochrony fizycznej (pracowników ochrony) i wykreślanie ich z instrukcji ochrony obiektu. Do jakiego minimum można tu dojść?

Jednocześnie człowieka może w wielu obszarach zastąpić technika.

Dzięki zaawansowanym technologiom, takim jak inteligentna analityka obrazu, bramka detekcyjna czy inne zabezpieczenia, istnieje możliwość ograniczenia liczby pracowników ochrony. Jednak nie należy zapominać o tym, iż na końcu zawsze jest człowiek, który musi posiadać odpowiednie kompetencje czy uprawnienia, aby obsłużyć konkretny sprzęt i systemy.

## Działania prewencyjne

Zdaję sobie z tego sprawę, iż obecnie nie jesteśmy w stanie powrócić do wielu działań prewencyjnych kiedyś stosowanych. Należy jednak poszukiwać takich rozwiązań, które wyeliminują dane zagrożenie lub co najmniej będą równoważne dokonanej zmianie. Nowatorskie działania prewencyjne są wykonywane na różne sposoby. Wideoobchód jest najlepszym przykładem rozwiązania, które zastąpiło patrole ochrony fizycznej. Pamiętajmy jednak, iż przy tego typu metodach kontroli ważny jest scenariusz, zgodnie z którym operator centrum monitoringowego dokonuje wideoobchodu. Scenariusz musi być jasno sprecyzowany, zamawiający usługę musi dokładnie wiedzieć, czego oczekuje.

Zdefiniowanie potrzeb stanowi podstawę dobrej współpracy z dostawcą usług ochroniarskich. Precyzyjne schematy postępowania pozwalają uniknąć wielu nieporozumień. Istotne jest przy tym, aby podejmowane działania prewencyjne zapewniły poczucie bezpieczeństwa osobom przebywającym w obiekcie i, co ważniejsze, nic nie umknęło działowi bezpieczeństwa.

Temat jest rozległy i trudno poruszyć wszystkie zagadnienia w krótkim artykule. Z osobami zainteresowanymi rozwinięciem tej problematyki chętnie spotkam się na najbliższym śniadaniu ekspertów. □

B I O

## Krzysztof Wilczyński

Specjalista ds. bezpieczeństwa. Zatrudniony w CEVA Logistics Poland, gdzie odpowiada za tworzenie i implementowanie procedur zwiększających poziom bezpieczeństwa. Dba o zapewnienie szczelności funkcjonujących procesów u klientów oraz rekomenduje nowoczesne rozwiązania optymalizujące.

# Głos branży



TRANSPORT I LOGISTYKA TO BRANŻA WYMAGAJĄCA SZCZEGÓLNYCH ROZWIĄZAŃ Z ZAKRESU SECURITY. O NAJWAŻNIEJSZYCH KWESTIACH OPOWIEDZIELI NAM UŻYTKOWNICY SYSTEMÓW I ICH OFERENCI.



Wojciech Andziak

DHL Parcel

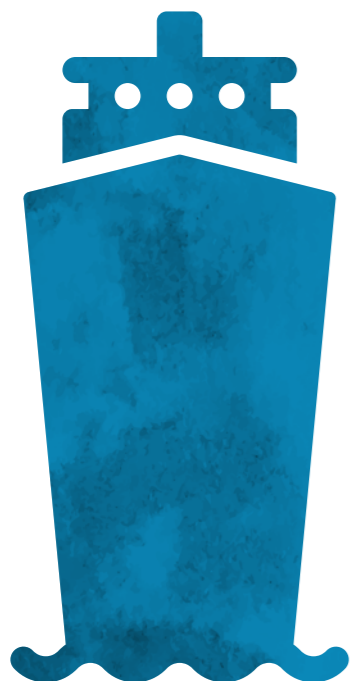
## Współpraca na rzecz poprawy bezpieczeństwa

Bezpieczeństwo transportu jest obecnie dużym wyzwaniem nie tylko dla branży security, ale także dla całego sektora logistyki. Mamy coraz lepszą infrastrukturę drogową, więcej parkingów i centrów logistycznych. Oprócz transportów krajowych Polska jest również krajem tranzytowym dla przewoźników z Europy i Azji. Po naszych drogach przemieszczają się pojazdy transportujące towary o bardzo dużej wartości, wzmożony ruch takich pojazdów wywołuje zainteresowanie grup przestępczych. Rozwiązaniem, które wg mnie może zapewnić bezpieczeństwo transpor-



tów, jest połączenie fizycznego zabezpieczenia pojazdu z zabezpieczeniem elektronicznym ładunku oraz kabiny kierowcy i naczepy. Jest jednak kilka warunków, żeby taki system był skuteczny, a jego obsługa nie była zbyt kosztowna, np. zasilanie systemu czy rotacja naczep (rzadko pojazd porusza się z tą samą naczepą). Nie chcę wymieniać szczegółów technicznych, bo jest ich sporo. Uważam, że najważniejszym aspektem skutecznego zabezpieczenia jest monitorowanie i natychmiastowe podjęcie interwencji w razie alarmu. W skutecznym zabezpieczeniu transportu mogą pomóc integracja systemów i tworzenie profesjonalnych centrów monitorowania pojazdów, o ustalonym standardzie zabezpieczenia mechanicznego i elektronicznego, do których dopuszczone są tylko pojazdy spełniające określone warunki.

Ważni są również sprawdzeni przewoźnicy, z których usług korzystają firmy logistyczne. Oprócz usług transportowych powinny mieć w ofercie nie tylko zabezpieczenie fizyczne, ale także monitorowanie alarmów przez profesjonalne centrum monitoringu agencji ochrony lub firmy, która specjalizuje się tylko w takich usługach. Idealnie byłoby, gdyby firma transportowa miała certyfikat bezpieczeństwa. Jedna firma monitorująca różne podmioty logistyczne, niezależnie od profilu ich działalności, może zapewnić bezpieczeństwo pojazdów różnych przewoźników. Wszyscy powinni korzystać ze skutecznych rozwiązań, które ze względu na skalę mogą znacznie obniżyć koszty. Bezpieczeństwa nie zapewni konkurowanie ze sobą, ale pomoc i wymiana doświadczeń. Konkurencja w biznesie tak, w bezpieczeństwie – nie.



Bogumił Szymanek

Axis Communications

## Najważniejsza jest stabilność i niezawodność rozwiązania

**Transport jest bardzo różnorodny, w ramach tego segmentu występuje kilka grup, które charakteryzują się zupełnie innymi potrzebami w zakresie systemów zabezpieczeń czy optymalizacji procesów. Wynika to z faktu, że również zagrożenia i cele przedstawiają się inaczej. Inne rozwiązania stosowane są w transporcie publicznym, inne w lotnictwie, logistyce, a zupełnie inne w portach morskich czy w systemach ruchu drogowego.**

W transporcie publicznym mogą zdarzać się różne incydenty: wypadki, kradzieże kieszonkowe, przemoc, kradzież infrastruktury, a nawet zagrożenie terrorystyczne. Różnorodna i rozproszona sieć transportowa sprawia, że konieczne jest szeroko zakrojone jej monitorowanie. Powoduje to również potrzebę scentralizowania operacji w jednym połączonym centrum zarządzania. Operatorzy przejawiają również zainteresowanie wykorzystaniem systemów dozoru wizyjnego do badania przepływu pasażerów i optymalizacji różnych usług pasażerskich oraz ofert. Również porty lotnicze są zainteresowane optymalizacją przepływu osób oraz analizą biznesową pasażerów handlowych dostarczających im znaczną część przychodów. Oczywiście jest również, że lotnictwo wymaga najwyższych standardów bezpieczeństwa i kontroli.

Z kolei w ruchu drogowym oprócz monitorowania zdarzeń systemy dozoru wizyjnego dostarczają danych do Inteligentnych Systemów Transportowych, pozwalają gromadzić i klasyfikować pobór opłat czy nawet dostarczać informacji pogodowych.

We wszystkich przypadkach najważniejsza jest stabilność i niezawodność rozwiązania, dlatego integratorzy wybierają produkty Axis jako pewny i niezawodny element całości. Otwartość integracyjna pozwala w efektywny sposób zbudować rozwiązanie dopasowane do potrzeb każdego klienta.



Marcin Walczuk

BCS

## Nowoczesna technologia daje poczucie bezpieczeństwa

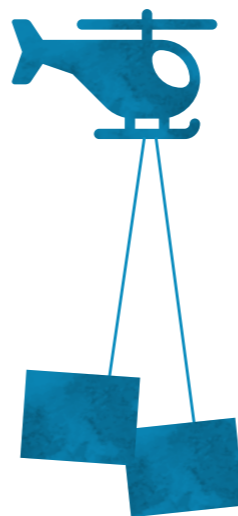
**Transport ludzi i towarów odgrywa dziś kluczową rolę w codziennym funkcjonowaniu całego świata. Codziennie miliony ludzi korzystają ze środków transportu publicznego. Jego zadaniem nie jest jedynie przewieźć pasażera z punktu A do B, ale również, a może przede wszystkim zrobić to w sposób bezpieczny.**

Pomijając wypadki komunikacyjne, za które w większości odpowiada czynnik ludzki, nad bezpieczeństwem podróżnych czuwają systemy monitoringu wizyjnego montowane w pojazdach transportu publicznego. Dzięki zastosowaniu monitoringu w wersji mobilnej zwiększa się poczucie bezpieczeństwa pasażerów. Również służby otrzymują sprawne narzędzie, by interweniować w sytuacjach zagrożenia lub po nim, by na zarejestrowanych nagraniach odszukać osoby, które za takie sytuacje są odpowiedzialne. Z pomocą mogą tutaj przyjść rejestratory mobilne projektowane z myślą o tak szczególnym środowisku pracy, jak różnego typu pojazdy. W parze z rejestratorem muszą oczywiście iść kamery, a te z racji mniejszej niż zwykle wysokości montażu muszą być odpowiednio zabezpieczone przed ewentualnymi aktami wandalizmu. W szczególnych przypadkach można się zdecydować

na kamery typu pinhole, które będą praktycznie niewidoczne wewnątrz pojazdu. Ale transport to nie tylko pojazdy, którymi przewożeni są podróżni i towary. To również stacje kolejowe, dworce autobusowe, lotniska, czyli miejsca, gdzie jednocześnie potrafi przebywać kilka czy nawet kilkadziesiąt tysięcy osób. Takie skupisko ludności to idealne miejsce do przeprowadzenia zamachu terrorystycznego. Aby zminimalizować ryzyko tego typu zdarzeń, z pomocą przychodzi technologia zaimplementowana w systemach telewizji dozorowej. Wszelkiego typu rozwiązania inteligentnej analizy obrazu pozwolą wyodrębnić potencjalnie niebezpieczne zdarzenia, jak nieuprawnione naruszenie strefy lub pozostawienie przedmiotu na dłuższy czas bez opieki.

Coraz częściej można spotkać się z systemami, które są wyposażone w algorytmy sztucznej inteligencji, dzięki czemu mogą się „uczyć” różnego typu podejrzanych zachowań. Chodzi tutaj np. o bezcelowe kręcenie się osobnika w wyznaczonej strefie, śledzenie jednej osoby przez drugą lub spontaniczne gromadzenie się tłumu. Wychwytywanie takich zdarzeń w połączeniu z umiejętnością kamer do określania nastroju, wieku, płci osoby lub po prostu porównania rysów twarzy ze zdjęciem z bazy danych pozwoli zawczasu wyeliminować zagrożenia.

Połączenie pracy systemów znajdujących się w obiektach stacjonarnych z tymi umieszczonymi w pojazdach gwarantuje pasażerowi poczucie bezpieczeństwa od momentu wejścia na stację, przez cały czas trwania podróży, aż do końca podróży. Ponadto niesie za sobą wymierne korzyści dla firm transportowych. Jeśli pasażer będzie czuł się bezpiecznie, chętniej skorzysta z usług danego przewoźnika w przyszłości.



Piotr Świder

Hikvision

## Nowe trendy w transporcie i logistyce

**W ostatnich latach na rynku transportu i logistyki nastąpił znaczny rozwój, w tym również systemów zabezpieczeń związanych z ochroną pasażerów i pracowników. Jeszcze kilka lat temu kamery instalowane w środkach komunikacji miejskiej czy kolejowej były rzadkością, a jeśli nawet były, to miały spełnić tylko jeden wymóg: „coś widzieć i nagrywać”. Obecnie obowiązują już ściśle określone prawem normy i wymagania względem systemów monitoringu wizyjnego montowanych w pojazdach. Hikvision, jako lider branży, planuje certyfikację swoich urządzeń, tak aby spełnić wszystkie wymogi, np. EN50155:2017 już na etapie projektowania urządzenia.**

Podobnie w logistyce zauważamy nowe trendy. Jest coraz więcej automatyzowanych i uruchamiane autonomicznie centra logistyczne. Często też dozorem wizyjnym obejmuje się całe procesy, np. sortowania czy wysyłki, aby mieć ścisłą kontrolę i uniknąć takich sytuacji, jak kradzieże lub zagubienie przesyłki. W mojej opinii w nadchodzących latach będziemy świadkami wprowadzania kolejnych nowinek technicznych takich jak autonomiczne pojazdy komunikacji publicznej czy robotyzacja w logistyce.



Jarosław Krasucki

Niezależny audytor

## Właściwe zabezpieczenie transportu

**Chciałbym poruszyć temat banalny w obszarze bezpieczeństwa terenu, budynków czy transportu.**

Często w swojej praktyce zawodowej dawałem pytania: czy zakładacie plomb, czy używacie plomb. Odpowiedź zawsze brzmiała: tak! Gorzej było, gdy prosiłem o pokazanie, jak to się robi. Gdy „przygotowałem” kilka plomb, aby sprawdzić znajomość tematyki i umiejętności pracowników ochrony, było źle, wręcz tragicznie. I to nawet w największych firmach ochrony. Mimo że dostawcy przeważnie dostarczają instrukcję korzystania z plomb, które oferują, mało kto je czyta i wdraża.

Nic to, że plomby mają przeważnie (te dobre mają zawsze) specjalne punkty, na które należy zwrócić uwagę przy ich zakładaniu, sprawdzaniu i zdejmowaniu. Pracownicy ochrony z reguły ich nie znają, tylko nieliczni potrafili na logikę, na zdrowy rozsądek (przeczuwając zły „podstęp”) zauważyć niektóre „chwyt”. Wiem, że to temat prozaiczny, nie wpływa ani na strategię, ani na poważne plany ochrony obiektu, ale wciąż mnie to martwiło.

A państwo? Jeśli wy lub wasi klienci macie plany bezpieczeństwa i plany ochrony, dobrą technikę i systemy sprawne, prawidłowo konserwowane – ekstra! Ale radzę sprawdzić, czy pracownicy zakładają (wieszają) plomby, czy PLOMBUJĄ powierzone im dozoru miejsca i transporty. Słyszysz się, że np. każdy kierowca i tak wie, jak uzyskać dostęp do przewożonego ładunku bez naruszenia plomb – ALE PO CO MU

**TO UŁATWIAC?**

Wiele razy słyszałem o zaginionych ładunkach lub ich części czy tzw. kontrabandzie. Ileż to razy próbowano mnie przekonać, że nie ma potrzeby stosowania plomb, bo magazynierzy i tak sprawdzają dostawy. To dobrze, tylko dlaczego nie stosować i tutaj zasad najlepszych praktyk?

**Jakub Sobek**

Linc Polska

**Niezawodność systemów dzięki innowacjom**

Coraz częściej słyszymy o nowych, autonomicznych pojazdach, które są w fazie testowania. Dynamika postępu technologicznego sprawia, że już niedługo pojazdy te mogą trafić na nasze drogi. Obecnie już w wielu miejscach i do różnych zastosowań testowane są zarówno samochody osobowe jak i ciężarowe. Są one wyposażone w odpowiednie, czujniki.

To przyszłościowe rozwiązanie zrewolucjonizuje nasze myślenie o podróżowaniu i transporcie towarów, jednocześnie efektywnie poprawiając nasze bezpieczeństwo. Wszystkie sensory zintegrowane z oprogramowaniem mogą nie tylko skutecznie zastąpić kierowcę, ale dodatkowo umożliwią bezpieczną podróż nawet w najtrudniejszych warunkach pogodowych i środowiskowych. Nie ma jednak jednego sensora, który sprawdzi się w każdym okolicznościach.

Dlatego tak istotne jest łączenie różnych technologii. Obecnie najczęściej stosowane i testowane są rozwiązania radarowe i termowizyjne. Postęp technologiczny w tym zakresie jest bardzo istotny także dla segmentu zabezpieczeń technicznych. Olbrzymia ilość kilometrów jakie pokonały do tej pory autonomiczne samochody pozwoliła na zebranie materiału, który przyspieszył dopraco-

wywanie wielu technologii, które mogą być wykorzystywane w wielu dziedzinach. Dzięki temu detekcja za pomocą radarów, nawet niewielkich obiektów, jest obecnie znacznie skuteczniejsza niż parę lat temu. Ta zmiana była możliwa w szczególności przez poprawienie algorytmów odpowiedzialnych za obróbkę sygnałów radarowych. Coraz częściej widać, że nawet radary krótkiego zasięgu, między 50 a 200 m, stosowane są w systemach zabezpieczenia perymetrycznego. To właśnie zwiększenie skuteczności oraz spadek cen przyczyniły się do wzrostu ich popularności.

Ponadto są proste w instalacji i kalibracji. Co więcej, mogą współpracować z kamerami obrotowymi, tworząc skuteczny system zabezpieczeń. Dzięki temu operator systemu nie tylko otrzymuje informację o alarmie, ale także widzi obraz z kamery, która przez cały czas śledzi wykryty obiekt.

W przyszłości samochody autonomiczne będą wyposażane w kolejne innowacyjne technologie. Dla branży zabezpieczeń technicznych może to oznaczać kolejne nowe rozwiązania, które podniosą niezawodność systemów. W nieodległej przyszłości kolejnym krokiem będzie dalsza integracja systemów zainstalowanych w pojazdach z systemami stacjonarnymi. To idealne połączenie dla koncepcji typu Smart City oraz dla firm logistycznych.

**Łukasz Lubera**

PKP CARGO SA

**Automatyzacja procesów i zabezpieczenie infrastruktury**

Dla zapewnienia bezpieczeństwa w transporcie kolejowym największym wyzwaniem pozostaje dalszy rozwój systemów i zabez-

pieczeń technicznych, mających na celu ograniczenie wpływu czynnika ludzkiego (i tym samym ograniczenie następstw ewentualnych błędów popełnianych w trakcie realizacji procesu przewozowego), jak również procesów wspomagających, np. czynności przeglądowo-naprawczych. Z punktu widzenia eksploatacyjnego niezbędna jest ewolucja systemów wspomagających przede wszystkim pracę maszynistów i dyżurnych ruchu, m.in. w zakresie urządzeń diagnostyki pokładowej pojazdów i urządzeń sterowania ruchem kolejowym. Ważnym elementem jest też zwiększanie automatyzacji procesu utrzymaniowego pojazdów, zwłaszcza w odniesieniu do części biegowych (diagnostyka zestawów kołowych wraz z oceną stanu węzła łożyskowego) oraz procesu utrzymania infrastruktury kolejowej (stanu torów i urządzeń przytorowych).

Dla zapewnienia najwyższych standardów bezpieczeństwa pasażerów niezwykle istotną jest dalsza intensyfikacja działań w obszarze security – wdrażanie nowych rozwiązań ograniczających potencjalne ryzyko i ewentualne skutki działań o charakterze terrorystycznym, a także cyberataków na systemy odpowiedzialne za bezpieczne planowanie i prowadzenie ruchu kolejowego. Od branży security oczekujemy rozwoju systemów biometrycznych oraz zabezpieczeń infrastruktury IT.

Rok 2020 jest przełomowy, w czerwcu upływa bowiem termin implementacji przepisów filaru technicznego IV pakietu kolejowego. Wiąże się to m.in. z koniecznością wdrożenia w bliskiej perspektywie Europejskiego Systemu Zarządzania Ruchem Kolejowym (ERTMS), a co za tym idzie z inwestycjami podmiotów rynku kolejowego – przewoźników kolejowych i zarządców infrastruktury – w Europejski System Sterowania Pociągami (ETCS) oraz Globalny System Kolejowej Radiokomunikacji Ruchomej (GSM-R). Jest to strategiczne przedsięwzięcie, od którego w znacznej mierze zależy podniesienie poziomu bezpieczeństwa i zwiększenie konkurencyjności kolei.

**Adam Sawicki**

DSV Panalpina

**Najważniejsza jest stała edukacja**

Szeroko rozumiane bezpieczeństwo jest jednym z najważniejszych aspektów sprawnego funkcjonowania firm branży logistycznej na każdym etapie operacji, począwszy od załadunku, poprzez przyjęcie towaru, transport, przesunięcia magazynowe, skończywszy na inwentaryzacji oraz wydaniu produktu. Niewątpliwie największym wyzwaniem jest możliwie pełna integracja systemów zabezpieczeń z dowolnymi bazami danych i systemami zewnętrznymi. Chodzi głównie o analizę obrazu w systemach VSS, która w połączeniu z big data daje ogromną przewagę w postaci oszczędności czasu, a w efekcie optymalizację procesów logistycznych. Zmieniająca się branża security stała się jeszcze ważniejsza z punktu widzenia zarządzania systemami zabezpieczeń przy jednoczesnym minimalizowaniu fałszywych alarmów. Wykorzystanie nowoczesnych technologii w elektronicznych systemach zabezpieczeń, dronach, aplikacjach mobilnych pozwala na osiągnięcie najwyższego możliwego poziomu bezpieczeństwa przy zachowaniu minimalnej liczby pracowników.

Bardzo ważną z punktu widzenia użytkowników, operatorów systemów VSS (CCTV), SWiN oraz KD jest ich stała edukacja pozwalająca na maksymalne wykorzystanie dostępnych funkcji tych systemów oraz reagowanie zgodne z polityką bezpieczeństwa i procedurami obowiązującymi w firmie. Automatyzacja procesów logistycznych oraz integracja systemów zabezpieczeń pozwala na utrzymanie najwyższych światowych standardów.

Jednym z największych wyzwań w transporcie i logistyce staje się obecnie możliwość bezpiecznego przemieszczania się pojazdów autonomicznych. W połączeniu z bezpiecznym przechowywaniem dóbr w magazynach typu self storage wydaje się kolejnym dużym krokiem w przyszłość, kiedy to bezpieczeństwo wejdzie na zupełnie nowy poziom.

**Krzysztof Wilczyński**

CEVA Logistics

**Główne wyzwanie – dotrzymanie warunków umowy**

Firmy ochrony powinny patrzeć na produkt całościowo, aby do swojej oferty skutecznie wprowadzać różnego rodzaju systemy zabezpieczeń technicznych. Największym wyzwaniem jest zorganizowanie odpowiedniej liczby załóg interwencyjnych, które będą szybko i skutecznie reagować na dane zdarzenie alarmowe.

W obecnej sytuacji rynkowej, przy braku wykwalifikowanych pracowników ochrony, czasy kiedy obsada grupy liczyła dwie uzbrojone osoby odeszły już dawno w zapomnienie. Dzisiaj nawet największe firmy ochroniarskie muszą korzystać z podwykonawców, przede wszystkim w mniejszych aglomeracjach.

Problemem, z którym może borykać się branża ochrony w 2020 roku, będzie dotrzymanie czasu dojazdów załóg interwencyjnych na wezwanie, nie wspominając już o realizacji ambitniejszych usług, których katalog jest bardzo szeroki.

**Andrzej Żochowski**

TNT

**Integracja systemów poprawi bezpieczeństwo**

W mojej ocenie największym wyzwaniem i oczekiwaniem od dostawców systemów zabezpieczeń technicznych jest rozwój technologii, która będzie coraz efektywniej podnosiła poziom bezpieczeństwa obiektów logistycznych (magazynów) charakteryzujących się dużymi powierzchniami wewnętrznymi i zewnętrznymi. Mam na myśli przede wszystkim systemy monitoringu wizyjnego i kontroli dostępu. Bardzo ważną jest przy tym możliwość maksymalnego zintegrowania tych systemów, aby osoby odpowiedzialne za bezpieczeństwo mogły zdalnie nimi zarządzać, a także monitorować ich techniczną poprawność, sprawność działania i ewentualne usterek i oraz szybko na nie reagować.

Równie istotne jest zapewnienie bezpieczeństwa technicznego w toku operacji transportowych (szczególnie transportu drogowego) ze względu na potrzebę stałego monitorowania zarówno ruchu pojazdów, jak i przewożonych ładunków oraz prawidłowości wykonywanych czynności, np. przez kierowcę. Ważną rolę odgrywa też stały rozwój systemów zabezpieczeń technicznych w aspekcie sukcesywnego zastępowania nimi (redukcji kosztów) usług ochrony fizycznej ze względu na jej stale rosnące koszty. □





# Norma NFPA 601 w kontekście bezpieczeństwa centrum logistycznego

**NFPA 601 TO STANDARD POSTĘPOWANIA DLA SŁUŻB OCHRONY W PRZECIWDZIAŁANIU STRATOM ZWIĄZANYM Z POŻARAMI. [1] MIMO ŻE JEST ROZWIJANY OD PONAD 90 LAT, W POLSCE WCIAŻ JEST MAŁO ZNANY. A SZKODA, BO ZAWIERA KONKRETNE WYMAGANIA MOGĄCE POPRAWIĆ BEZPIECZEŃSTWO ORGANIZACJI.**



T E K S T

Lukasz Stępień

**Krajowe (amerykańskie – przyp. red.) Stowarzyszenie Przeciwdziałania Pożarom (NFPA) jest najstarszą na świecie organizacją zajmującą się badaniami oraz opracowywaniem norm z zakresu bezpieczeństwa pożarowego.** W Europie najbardziej popularne są normy dotyczące montażu (NFPA 13) oraz przeglądów (NFPA 25) instalacji tryskaczowych. Jednak w swoim katalogu NFPA ma ponad 100 różnych norm i wytycznych dotyczących ochrony przeciwpożarowej. NFPA 601 stanowi zbiór minimalnych wymogów, które pozwalają na efektywne zaangażowanie zespołu ochrony w działania związane z przeciwdziałaniem pożarom oraz minimalizacją ich skutków.

Wielkopowierzchniowe obiekty magazynowe, takie jak centra logistyczne, są szczególnie podatne na wystąpienie straty całkowitej w przypadku pożaru. Rozporządzenie Ministra Infrastruktury z 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie, określa maksymalne powierzchnie, jakie mogą obejmować strefy pożarowe w budynkach produkcyjno-magazynowych. Ograni-

czenia zależą od założonego obciążenia ogniowego (energia w MJ na m<sup>2</sup>, jaka może się wytworzyć w trakcie pożaru) oraz wysokości obiektu. W przypadku zastosowania samoczynnych urządzeń oddymiających powierzchnia strefy pożarowej może być powiększona o 50%, a w przypadku zastosowania stałych urządzeń gaśniczych (np. tryskaczy) o 100%. Przy zastosowaniu obu rozwiązań rozmiar strefy pożarowej może być zwiększony o 150%. Powierzchnia strefy pożarowej nie jest w żaden sposób ograniczona, jeżeli stosuje się jednocześnie automatycznie działające klapy oddymiające oraz stałe urządzenia gaśnicze, a sama strefa obejmuje tylko jedną kondygnację.

Inwestorzy często korzystają z możliwości, jakie dają im regulacje prawne, i tworzą ogromne hale bez oddzielenia pożarowych. Fakt spełnienia wymogów prawnych może skutkować fałszywym poczuciem bezpieczeństwa. Regulacje prawne określają minimum, jakie musi spełnić budynek, aby umożliwić bezpieczną ewakuację osób będących wewnątrz, ale nie mają nic wspólnego z zapobieganiem stratom mienia. Budynki spełniające funkcje magazynów charakteryzują się nagromadzeniem w jednym miejscu materiałów palnych o dużej „kaloryczności”. Szacuje się, że średnia moc pożaru w miejscu, gdzie składowane są np. stopy palet drewnianych do wysokości 0,5 m, wynosi 1250 kW/m<sup>2</sup>. W przypadku zwiększenia wysokości składowanych palet do 3 m obciążenie wzrasta do 6000 kW/m<sup>2</sup>. Dla porównania, średnia

wartość mocy pożaru w galerii sztuki to 250 kW/m<sup>2</sup>. Jeżeli powierzchnie magazynowe są podnajmowane podmiotom zewnętrznym, ryzyko wzrasta ze względu na możliwość łamania przez najemcę standardów bezpieczeństwa pożarowego (np. składowanie wewnątrz obiektu butli z gazem bądź beczek z cieczami łatwopalnymi).

Dla obiektów wyposażonych w klapy oddymiające jedyną szansą na uratowanie budynku jest szybkie wykrycie pożaru i natychmiastowe wezwanie straży pożarnej. Niestety często w momencie dotarcia jednostek ratowniczo-gaśniczych pożar jest już na takim etapie rozwoju, że jedynym działaniem, jakie może podjąć straż pożarna, jest zabezpieczenie okolicznych obiektów i czekanie, aż pożar dopali się w kontrolowanych warunkach. Znacznie efektywniejszym zabezpieczeniem są stałe urządzenia gaśnicze. Zgodnie z wytycznymi normy NFPA 13 instalacje tryskaczowe w magazynach powinny zmienić budynek w obiekt „samobroniący się”. O ile w obszarach biurowych i produkcyjnych tryskacze mają za zadanie wstrzymać rozwój pożaru aż do czasu przybycia straży pożarnej, o tyle w obszarach magazynowych muszą samodzielnie ugasić pożar. Mimo że efektywność tryskaczy, rozumianą jako ograniczenie skutków pożaru, szacuje się na 96%, są to zabezpieczenia bardzo wrażliwe na działanie człowieka. NFPA podaje, że aż 93% zdarzeń,

Najwłaściwszym momentem na podjęcie prac związanych z wdrożeniem normy NFPA 601 jest etap przygotowywania do podpisania kontraktu z firmą ochrony

w których zadziałanie tryskaczy nie było efektywne, wynikało z błędu człowieka. Wystarczy brak zachowania wymaganego odstępu pomiędzy paletami na regałach magazynowych, składowanie materiałów w alejkach pomiędzy regałami albo zmiana materiałów składowanych w magazynie. W efekcie tempo rozwoju pożaru oraz jego rozmiar może znacznie wykraczać poza przyjęte założenia projektowe i zadziałanie stałych urządzeń gaśniczych nie przyniesie oczekiwanego efektu. Jednak nawet uruchomienie tryskaczy może prowadzić do ogromnych strat. Przepływ wody na tryskaczach przeznaczonych do magazynu może wynosić 480 l/min. Odpowiada to mniej więcej wylewaniu dwóch pełnych wanien wody na minutę, aż do momentu zakręcenia dopływu wody do instalacji. Dlatego nawet gdy dojdzie do ugaszenia pożaru, wciąż trzeba się liczyć z ogromnymi stratami materialnymi związanymi z zalaniem.

Są to powody, dla których warto rozważyć wykorzystanie dodatkowej „warstwy” ochrony w postaci zespołu ochrony fizycznej. Jasne wytyczne w tym zakresie daje NFPA 601 i pozwala przejść od zabezpieczenia teoretycznego – „tak, mamy ochronę”, do faktycznego, w którym są sprecyzowane wymagania względem zespołu ochrony, a ich realizacja jest nadzorowana.

Najwłaściwszym momentem na podjęcie prac związanych z wdrożeniem normy NFPA 601 jest etap przygotowywania do podpisania kontraktu z firmą ochrony. Niemniej jednak większość rozwiązań można też wdrożyć, gdy taka współpraca została już nawiązana. Na wszystkich etapach opracowywania standardów powinny być zaangażowane osoby posiadające kompetencje z zakresu ochrony fizycznej oraz przeciwdziałania stratom związanym z pożarami. Najlepszym rozwiązaniem jest zaangażowanie specjalistów pracujących w organizacji lub konsultantów zewnętrznych. Dużym ryzykiem może być zlecenie



→ tego zadania firmie, która realizuje lub będzie realizowała w obiekcie usługi z zakresu ochrony fizycznej. Taka dokumentacja może skupiać się na ułatwieniu realizacji kontraktu niż na zapewnieniu poziomu bezpieczeństwa oczekiwanego przez zarządcę obiektu.

Każde centrum logistyczne powinno mieć opracowaną koncepcję zabezpieczenia obiektu, zgodnie z którą na podstawie analizy ryzyka wskazuje się obszary ważne z punktu widzenia realizacji celów organizacji, i na tej podstawie określa zastosowane środki bezpieczeństwa.

NFPA 601 nakładają wymóg, aby koncepcja zabezpieczenia obiektu uwzględniała również zagrożenia pożarowe. Bardzo przydatnym dokumentem na tym etapie będzie rzetelnie opracowana i aktualna instrukcja bezpieczeństwa pożarowego (IBP). To dokument wymagany dla wszystkich stref pożarowych, gdy występuje strefa zagrożenia wybuchem lub ich kubatura brutto przekracza 1000 m<sup>3</sup>. IBP zawiera komplet informacji o obiekcie, takich jak warunki ochrony przeciwpożarowej, systemy ppoż., miejsca, w których mogą występować strefy zagrożenia wybuchem, oraz informacje o obecności cieczy łatwopalnych.

**Co ciekawe, norma dotycząca przeciwdziałania stratom związanym z pożarami nakłada obowiązek zorganizowania ochrony w sposób zapobiegający dostaniu się na teren obiektu osób i pojazdów nieuprawnionych.** Może to wynikać nie tylko z faktu, że mogą one podjąć celowe działania prowadzące do powstania szkód, ale także ze względu na nieznaną zasad bezpieczeństwa mogą doprowadzić do powstania zagrożenia pożarowego.

Funkcje ochrony powinny być również uwzględnione w ogólnych procedurach postępowania w sytuacjach awaryjnych, takich jak zanik prądu czy awaria zasilania. Bazą do opracowania procedur może być po raz kolejny instrukcja bezpieczeństwa pożarowego, ponieważ zawiera informacje na temat postępowania w przypadku wystąpienia pożaru i innych sytuacji niebezpiecznych oraz zasady ewakuacji ludzi. Jeżeli w obiekcie jest zainstalowany system sygnalizacji pożarowej, to najczęściej panel sterujący jest nadzorowany całodobowo przez pracowników ochrony.

Każdy pracownik ochrony musi wiedzieć, jak taki panel obsługiwać. Co ważne, nie może bazować na „wiedzy plemiennej” przekazywanej przez starszych kole-

## W normie są zawarte konkretne wymagania, jakie powinny zostać spełnione, aby zwiększyć poziom bezpieczeństwa pożarowego w obiekcie

gów, ale na instrukcjach wynikających z procedur zaakceptowanych przez zarządcę obiektu. Co zrobić w momencie pojawienia się alarmu pierwszego i drugiego stopnia? W jaki sposób i kto ma być informowany o tym zdarzeniu? Czy zdarzenie wymaga natychmiastowej komunikacji, czy tylko notatki w raporcie? Wszystkie te procedury muszą być uwzględnione we właściwej dokumentacji. Każdy związany z branżą bezpieczeństwa wie, że nie ma czegoś takiego jak „rzeczy oczywiste”. Zgodnie z normą wydarzeniami wymagającymi natychmiastowej reakcji są:

- brak sprawności elementów systemu ppoż. (uszkodzenie elementu detekcji/pozostawienie zakręconych zaworów mimo zakończenia testów na instalacji tryskaczowej);
- prowadzenie prac pożarowo niebezpiecznych bez wymaganych pozwoleń;
- inne działania, które mogą mieć negatywny wpływ na funkcjonowanie obiektu.

W niektórych obiektach przyjęto schemat działania, zgodnie z którym zespół ochrony informuje najpierw swojego przełożonego (opiekuna kontraktu), a dopiero ten wykonuje telefon do osób odpowiedzialnych za zarządzanie obiektem. To bardzo niebezpieczne podejście, mogące skutkować nie tylko opóźnieniem reakcji, ale także efektem „głuchego telefonu” i chaosem komunikacyjnym. Pracownicy ochrony muszą również znać obiekt i potrafić przekazać komunikaty przybyłym na miejsce zdarzenia zastępom straży pożarnej. Jest to o tyle ważne, że w momencie wystąpienia pożaru w obiekcie zespół ochrony może być pierwszym kontaktem dla straży pożarnej.

Byłoby dobrze, gdyby z chwilą przybycia jednostek na teren centrum logistycznego informacja nie ograniczała się tylko do „tam się pali”, ale także obejmowała przekazanie właściwych kluczy, informacji na temat dróg dojazdowych, pożarowych wyłączników prądu oraz najbliższych hydrantów. Proste informacje pozwolą znacznie zwiększyć efektywność działań



PROJEKTUJEMY *zgodnie ze sztuką*

### SYSTEMY SYGNALIZACJI POŻAROWEJ

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

### UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

### SYSTEM DETEKЦИИ GAZÓW SDG 6000

POLON-ALFA S.A.

85-861 Bydgoszcz, ul. Glinki 155 | [www.polon-alfa.pl](http://www.polon-alfa.pl)



ratowniczo-gaśniczych prowadzonych przez jednostki straży pożarnej. Tak jak żołnierz poznaje najlepiej broń podczas czyszczenia, tak pracownik ochrony najlepiej poznaje obiekt podczas patrolu.

Trasy patroli pracowników ochrony powinny zostać wytyczone na podstawie koncepcji zabezpieczenia obiektu oraz zaakceptowane przez osobę odpowiedzialną za bezpieczeństwo pożarowe. Dobrą praktyką jest wykorzystanie rzutów graficznych dołączonych do instrukcji bezpieczeństwa pożarowego. W normie znajduje się wymóg opracowania nie tylko trasy patrolu, ale także listy informacji, na co osoba realizująca patrol powinna zwrócić uwagę. Bardzo pomocne jest uzupełnienie listy kontrolnej o instrukcje fotograficzne. Pozwoli to w przyszłości uniknąć nieporozumień na linii zarządcy obiektu – dostawca usług ochrony.

Norma rekomenduje częstotliwość patroli nie mniejszą niż raz na godzinę. W przypadku zdarzeń zwiększających zagrożenie pożarowe, takich jak niesprawność elementów systemów przeciwpożarowych czy pozostanie wieczorem w obiekcie kierowcy, który zatrzymał się na „pauzę” (obowiązkowy odpoczynek), liczba patroli powinna zostać odpowiednio zwiększona. Ochrona powinna być poinformowana o planowanych w obiekcie pracach niebezpiecznych pod względem pożarowym lub działaniach na instalacji tryskaczowej, aby odpowiednio zmodyfikować trasy patrolowe.

Zgodnie z wytycznymi normy szczególną uwagę należy zwracać na obszary, gdzie są realizowane prace remontowo-budowlane. Coraz więcej organizacji w ramach umów na wykonanie takich prac zastrzega możliwość dodatkowych kontroli BHP realizowanych przez inwestora i wydelegowane przez niego osoby, np. pracowników ochrony fizycznej. Pożar z obszaru budowy może swobodnie przenieść się na pozostałą część budynku. Obiekt jest najbardziej narażony na zagrożenie pożarowe w momencie nieobecności pracowników w obiekcie. Z tego powodu w planie patrolu kluczowa jest realizacja pierwszego patrolu w ciągu 30 minut od zakończenia zmiany roboczej. Powinien to być bardzo dokładny patrol otwarcia, którego zadaniem jest potwierdzenie, że po zakończeniu zmiany nie ma zagrożeń pożarowych. Patrol otwarcia powinien obejmować m.in. kontrolę:

- pomieszczeń biurowych, z uwzględnieniem zamknięcia drzwi i okien,
- drożności dróg i drzwi ewakuacyjnych oraz dróg pożarowych,
- koszy zawierających odpady nasączone smarami,
- zaworowni, jeżeli obiekty są wyposażone w instalację tryskaczową.

W ramach procedur musi być również określone wyposażenie, jakim dysponuje zespół ochrony, żeby wykonywać swoje obowiązki. W przypadku patroli na obszarach magazynowych mogą być wymagane środki ochrony osobistej, np. buty bezpieczne, hełmy ochronne i kamizelki odbłaskowe. Norma nakłada wymóg, by pracownicy ochrony byli łatwo przez wszystkich identyfikowalni. Dlatego oprócz specyficznego umundurowania powinni dysponować kamizelkami z odpowiednim nadrukiem, umożliwiającym szybką identyfikację funkcji, jaką dana osoba pełni.

Zgodnie z wytycznymi NFPA 601 z każdego incydentu i zauważonej nieprawidłowości powinna powstać notatka zawierająca podstawowe informacje dotyczące gdzie i kiedy miało miejsce zdarzenie, co się zdarzyło oraz kto w nim brał udział. Ponadto po każdej zmianie powinny być opracowywane i przesyłane raporty dziennie. Norma rekomenduje zastosowanie formy listy kontrolnej z rodzajami incydentów, jakie mogą mieć miejsce w obiekcie, oraz



metryczkę z datą i informacją o osobach pełniących służbę. Każdy taki raport powinien być wysyłany zgodnie z ustaloną i zaakceptowaną przez zarządcę obiektu listą dystrybucyjną. Zgodnie z dobrą praktyką na takiej liście powinny być uwzględnione osoby reprezentujące chroniony obiekt, aby w przypadku wykrycia niezgodności można było przeprowadzić niezależną weryfikację dokumentacji. W ramach wyboru dostawcy usług ochrony norma rekomenduje również weryfikację polisy ubezpieczeniowej posiadanej przez firmę świadczącą te usługi – szczególną uwagę należy zwrócić na zakres ubezpieczenia oraz wyłączenia polisy.

Najsłabszym elementem systemu bezpieczeństwa jest zawsze człowiek. Gdy jest opracowana koncepcja zabezpieczenia obiektu wraz z procedurami, są określone oczekiwania względem zespołu ochrony, można przystąpić do realizacji kolejnego wymogu z normy NFPA 601 – określenia minimalnych kompetencji oraz cech psychofizycznych, jakie musi mieć pracownik ochrony pełniący daną funkcję. Konieczne jest również określenie odpowiednich wymogów zdrowotnych. Często wykluczającymi mogą być brak możliwości pracy samodzielnej lub pracy w godzinach nocnych.

Jako anegdotę opowiada się sytuację z pewnego obiektu na Dolnym Śląsku, gdy pracownik ochrony, słysząc alarm ewakuacyjny z centrali pożarowej, ściszył swój aparat słuchowy, bo „hałas przeszkadzał mu w pracy”. Na szczęście, mimo że nie było takiego wymogu prawnego, obiekt ten był podłączony bezpośrednio transmisją alarmów do straży pożarnej, która przyjechała na miejsce zdarzenia i podjęła akcję gaśniczą. Choć brzmi to komicznie, a w przypadku strat zawsze można podjąć próbę dochodzenia roszczeń od firm świadczących usługi ochrony, to pełne koszty przywrócenia obiektu do sprawności oraz utratę zaufania klientów trudno wycenić.

W normie są zawarte konkretne wymagania, jakie powinny zostać spełnione, aby zwiększyć poziom bezpieczeństwa pożarowego w obiekcie. Jednak żadne wymagania jeszcze nigdy nikomu nie pomogły, dopóki nie zmieniły się w faktyczne działania. □

B I O

**Łukasz Stępień**

Specjalista z zakresu bezpieczeństwa pożarowego i zarządzania kryzysowego. Członek Krajowego Stowarzyszenia Ochrony Przeciwpożarowej w USA.

## PROFILE FLEXIBLE – system sygnalizacji pożarowej firmy ZETTLER

W dzisiejszych czasach potrzeby związane z ochroną przeciwpożarową cechują się dużą złożonością. Każdy budynek ma niepowtarzalną konstrukcję, która wymaga innej konfiguracji systemu. Dlatego oferowany przez firmę ZETTLER system sygnalizacji pożarowej PROFILE Flexible został zaprojektowany tak, aby w praktycznie każdej sytuacji zapewnić wydajne i wszechstronne rozwiązanie z zakresu ochrony przeciwpożarowej.

**Elastyczna konstrukcja systemu i zaawansowane oprogramowanie konfiguracyjne**

PROFILE Flexible jest zaawansowaną centralą opartą na technologii MZX. Dzięki rozbudowanemu oprogramowaniu konfiguracyjnemu, modułowej konstrukcji oraz integracji ze standardowymi systemami oprogramowania do zarządzania budynkiem (BMS) system PROFILE Flexible jest w stanie spełnić nawet najbardziej wyśrubowane wymagania. Jego modularność oraz możliwość dzielenia pętli przekładają się na niemal nieograniczoną liczbę konfiguracji sprzętowych. Duże możliwości i elastyczność oprogramowania pozwalają na sprawne wdrażanie różnych konfiguracji – od bardzo prostych po wyjątkowo złożone. Dzięki standardowym protokołom system można w pełni zintegrować z oprogramowaniem BMS innych firm, zyskując sprawniejsze scentralizowane zarządzanie. To połączenie elastycznej konstrukcji i zaawansowanego oprogramowania sprawia, że ZETTLER PROFILE Flexible znakomicie sprawdzi się w niemal każdym środowisku ochrony przeciwpożarowej.

**Gotowość na przyszłe wyzwania i niższe całkowite koszty eksploatacji**

Każdy obiekt podlega zmianom – czasem stosunkowo dużym. Nowe potrzeby i wyzwania związane z budynkiem wymagają wprowadzania odpowiednich modyfikacji w obszarze ochrony przeciwpożarowej. System PROFILE Flexible to przyszłościowe rozwiązanie, które pomaga w obniżeniu długookresowych kosztów eksploatacji budynku. System zawiera wysokiej jakości centrale modułowe, których rozszerzal-

ność i sieciowy charakter pozwalają ściśle dostosować całe rozwiązanie do specyfiki chronionego obiektu. Ponadto centrale są zgodne ze wszystkimi starszymi i przyszłymi urządzeniami pętlowymi, takimi jak czujki, moduły wejścia i wyjścia, sygnalizatory akustyczne i optyczne itp. System PROFILE Flexible spełnia też wymogi normy EN54-13, co zapewnia pełną zgodność między centralami i urządzeniami peryferyjnymi. Jego elastyczność pod kątem przyszłych wyzwań i niższe całkowite koszty eksploatacji sprawiają, że PROFILE Flexible to rozsądna, długofalowa inwestycja dla każdego budynku.

**Niższy koszt instalacji i prostsze okablowanie**

Optyczne sygnalizatory alarmowe zużywają dużo prądu, co ogranicza maksymalną liczbę urządzeń zasilanych z pętli dozorowej. System PROFILE Flexible firmy ZETTLER zapewnia prąd pętli na poziomie 1 ampera, co jest wartością dwukrotnie wyższą niż w większości konkurencyjnych systemów. Oznacza to, że do każdej pętli można podłączyć więcej urządzeń, co zmniejsza liczbę wymaganych pętli oraz central. A mniejsza liczba pętli i central usprawnia prace projektowe oraz obniża koszty okablowania i instalacji.

**Najwyższa niezawodność i dokładna detekcja**

Dla właściciela budynku jeden fałszywy alarm może być przyczyną poważnych problemów. Tylko firma ZETTLER łączy centrale systemu PROFILE Flexible z czujkami trójsensorowymi 850PC 30Tec, umożliwiając jednocześnie monitorowanie dymu, temperatury i tlenu węgla. Ta zaawansowana technologia potrójnej detekcji znacznie ogranicza liczbę fałszywych alarmów i umożliwia wcześniejsze wykrywanie zagrożeń. Dzięki dopuszczeniom wydanym w wielu krajach Europy ZETTLER jest liderem w dziedzinie szybszej i dokładniejszej detekcji pożarów. □

Więcej informacji na temat firmy ZETTLER i linii produktów PROFILE Flexible można znaleźć na stronie zettlerfire.com.

**Johnson Controls International**

ul. Krakowiaków 50, 02-255 Warszawa  
www.johnsoncontrols.com  
www.zettlerfire.com







# Komunikacja za pomocą systemów przyzywowych

## a ochrona prywatności i godności pacjenta



Współczesne standardy ochrony zdrowia wymagają zastosowania w placówkach medycznych nowoczesnych urządzeń, infrastruktury i systemów informatycznych. Dotyczy to m.in. obszaru komunikacji personelu medycznego z pacjentem, który obecnie jest coraz częściej wspierany przez tzw. systemy przyzywowe. Ze względu na szczególne przeznaczenie systemy takie powinny być dobierane, projektowane i wykorzystywane z odpowiednim uwzględnieniem aspektu ochrony prywatności i intymności pacjenta oraz w sposób, który zapewnia dostęp do informacji dotyczących pacjenta tylko osobom do tego upoważnionym, czyli zasadniczo tylko personelowi udzielającemu świadczenia medycznego.



TEKST  
Agata Marcinkowska



TEKST  
Adrianna Żyrek

### Gdzie leży problem?

Komunikacja personelu medycznego z pacjentem jest nieodzownym elementem świadczeń zdrowotnych, wpływającym wprost na poprawność diagnozy, a także na jakość oraz efektywność terapii i leczenia pacjenta. Personel medyczny jest w tym obecnie wspierany przez nowoczesną infrastrukturę komunikacji z pacjentem, w tym systemy przyzywowe<sup>1)</sup>. Kryteriami wyboru, a następnie wdrożeń takich rozwiązań powinny być nie tylko ich cechy funkcjonalne czy ekonomiczne, ale również aspekt ochrony godności, prywatności i intymności pacjenta. Ponadto – co wydaje się szczególnie istotne z punktu widzenia podmiotów zarządzających placówkami medycznymi – nie chodzi w tym przypadku tylko o podniesienie jakości świadczeń

medycznych i komfortu pacjenta (choć to oczywiście jest kluczowe), ale także o spełnienie wymagań stawianych przez obowiązujące prawo.

Oceniając stan obecny, warto wskazać, że zgodnie z raportem Najwyższej Izby Kontroli z 2018 r. placówki zdrowia w wielu przypadkach niewystarczająco dbają o zapewnienie w praktycznym wymiarze prywatności i intymności w szpitalach, m.in. ze względu na nieodpowiednią infrastrukturę i organizację sposobu udzielania świadczeń medycznych. Na mocy przepisów ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta każdemu pacjentowi przysługuje prawo do poszanowania jego intymności i godności, w szczególności w czasie udzielania mu świadczeń zdrowotnych, stąd może on domagać się realizacji tego prawa w praktyce leczniczej. Niedostateczne uwzględnienie takich prawnie uzasadnionych oczekiwań pacjenta może skutkować ich roszczeniami w stosunku do podmiotów prowadzących odpowiednie placówki (np. roszczeniami dot. wypłaty zadośćuczynienia za naruszenie prywatności).

Warto także wskazać, że przetwarzanie danych dotyczących stanu zdrowia będzie podlegać dodatkowym wymogom wynikającym z Rozporządzenia o Ochronie Danych Osobowych (RODO), przewidującego m.in. obowiązek uwzględnienia ochrony danych osobowych w trakcie projektowania przyszłych rozwiązań technicznych służących komunikacji pacjentów z personelem opieki. Ze względu na charakter przekazywanych informacji, stanowiących w zdecydowanej większości tzw. dane osobowe szczególnej kategorii (np. dane o stanie zdrowia), wymogi ochrony stawiane przez RODO są w tym przypadku wyższe, a interpretacja adekwatności sposobu ochrony takich danych osobowych powinna być dokonywana według podwyższonych kryteriów i standardów. Należy bowiem zwrócić uwagę, że przewidziane w RODO podejście – oparte na ryzyku – przetrzuca na administratora danych ocenę, czy zastosowane przez niego środki (w tym techniczne, organizacyjne) na etapie projektowania i wdrażania odpowiednich rozwiązań zostały dobrane adekwatnie do ryzyka.

<sup>1)</sup> Systemy przyzywowe to zbiorcze określenie dla zestawów urządzeń komunikacyjnych umożliwiających pośredni – głosowy kontakt pacjenta placówki medycznej z jej personelem, w tym np. wezwanie przez pacjenta pomocy lub zgłoszenie indywidualnego zapotrzebowania. W skład takich zestawów wchodzi standardowo urządzenia komunikacyjne dla pacjenta (umieszczone np. przy łóżku pacjenta lub w sali chorych) oraz połączone z nimi urządzenia komunikacyjne dla personelu medycznego (umieszczone np. w pokoju służbowym lub dedykowane dla konkretnego pracownika w postaci osobistego urządzenia, takiego jak słuchawka/telefon)

### Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta

Prawo do godności, prywatności i intymności pacjenta w obszarze ochrony zdrowia jest zagwarantowane zarówno w Konstytucji<sup>2)</sup>, jak i w ustawie z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, poprzez nakaz poszanowania prawa do intymności i godności pacjenta, w szczególności w czasie udzielania mu świadczeń zdrowotnych<sup>3)</sup>. Jednym z warunków poszanowania prywatności pacjenta jest obecność w trakcie realizacji świadczeń jedynie osób wykonujących zawód medyczny, niezbędnych ze względu na rodzaj udzielanego świadczenia zdrowotnego – uczestnictwo innych osób co do zasady wymaga zgody pacjenta.

Prawo pacjenta do prywatności oznacza również, że wszystkie informacje o stanie zdrowia, diagnozach, rokowaniu, przeprowadzonych czynnościach leczniczych, rehabilitacyjnych muszą być traktowane jako poufne i nie mogą być ujawnione przez osoby wykonujące zawód medyczny osobom nieupoważnionym<sup>4)</sup>. W tym kontekście wątpliwość budzi m.in. takie zaprojektowanie systemów komunikacji z pacjentem, w tym systemów przyzywowych, które nie zapewnia poufności rozmowy pacjenta z konkretną osobą udzielającą mu świadczenia medycznego lub z osobą pomocniczo uczestniczącą w realizacji takiego świadczenia. Mowa tu o stosowaniu przyłóżkowych urządzeń przyzywowych - interkomowych, za których pomocą pacjent (często niemający innej możliwości skomunikowania się z personelem medycznym) może być zmuszony do prowadzenia rozmów o stanie swojego zdrowia za pomocą urządzeń głośnomówiących, co powoduje ryzyko ujawnienia informacji na temat stanu zdrowia innym pacjentom lub osobom nieupoważnionym (np. przebywającym w sali wieloosobowej lub podczas wizyty gości odwiedzających pacjentów).

W przypadku naruszenia prawa pacjenta do intymności i poszanowania godności osobistej sąd może przyznać na rzecz poszkodowanego pacjenta odpowiednią kwotę tytułem zadośćuczynienia pieniężnego za doznaną krzywdę. Realizacja roszczenia pacjenta odbywa się na podstawie art. 448 kodeksu cywilnego.

### Systemy przyzywowe a RODO

Informacje dotyczące stanu zdrowia stanowią dane osobowe i niezależnie od wskazanych powyżej regulacji podlegają wymogom Rozporządzenia o Ochronie Danych Osobowych (RODO). Zgodnie z nim dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

Z kolei *privacy by design* to obowiązek zaplanowania zgodnego z RODO procesu przetwarzania danych osobowych – z wyprzedzeniem, w sposób przemyślany, świadomy i odpowiedzialny. Dobór rozwiązań, w tym technicznych i organizacyjnych, powinien uwzględniać stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wynikających z przetwarzania. Pojawiają się zatem w tym wypadku pytania o odpowiedzialność w tym zakresie projektanta systemów przyzywowych i dokonany przez niego dobór urządzeń mających spełniać określone zadania w obszarze komunikacji pacjenta z personelem medycznym.

<sup>2)</sup> Art. 30 i art. 47 Konstytucji RP

<sup>3)</sup> Art. 20 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta

<sup>4)</sup> Art. 13 i art. 14 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta



Administrator (najczęściej podmiot prowadzący placówkę zdrowia), zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania ma obowiązek wdrażać odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, w tym zasady minimalizacji danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą. Zgodnie z motywem 78 RODO, jeżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, należy zachęcać wytwórców tych produktów, usług i aplikacji, by podczas ich opracowywania i projektowania wzięli pod uwagę prawo do ochrony danych osobowych i z należytym uwzględnieniem stanu wiedzy technicznej zapewnili administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych.

Jak podkreślono w ww. motywie, zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę w przetargach publicznych.

Co istotne, dobór odpowiednich rozwiązań służących do przetwarzania danych osobowych, spełniających wymogi RODO, to przede wszystkim obowiązek administratora danych osobowych (zamawiającego), który w tym zakresie może jednak posiłkować się wsparciem profesjonalnego podmiotu zewnętrznego (dostawcy rozwiązania lub projektanta).

Konsekwencją naruszenia przepisów o ochronie danych osobowych jest możliwość pociągnięcia właściwego podmiotu do odpowiedzialności, w tym odpowiedzialności cywilnej realizowanej w oparciu o przepisy kodeksu cywilnego, a także – co w praktyce może się okazać bardzo dotkliwe – odpowiedzialności administracyjnej w postaci administracyjnej kary pieniężnej nakładanej w drodze decyzji Prezesa Urzędu Ochrony Danych Osobowych<sup>5)</sup>.

### Problemy z realizacją – raport NIK

Realizacja prawa do prywatności i intymności pacjenta, a tym samym także ochrona jego danych osobowych, wciąż pozostaje dużym wyzwaniem dla placówek medycznych, w wymiarze zarówno organizacyjnym, osobowym, finansowym, jak i infrastrukturalnym. W praktyce realizacja powyższych wymogów dotyczy wielu aspektów funkcjonowania placówek medycznych – od stworzenia określonych procedur po zachowanie personelu szpitala (np. stosowanie parawanów między szpitalnymi łózkami, unikanie omawiania stanu zdrowia w miejscach, gdzie przebywają osoby nieuprawnione) czy po dobór i projektowanie określonych rozwiązań technicznych, w tym infrastruktury komunikacyjnej i nadzoru wizyjnego. Jak wskazano w raporcie NIK dot. ochrony intymności i godności pacjenta w szpitalach z 2018 r.<sup>6)</sup>:

*W skontrolowanych szpitalach warunki udzielania świadczeń zdrowotnych nie zapewniają pacjentom pełnej ochrony ich intymności i godności. Przyczynami tego była przestarzała infrastruktura szpitali, nieprawidłowe zachowanie personelu medycznego wobec pacjentów oraz niewłaściwa organizacja systemu monitoringu wizyjnego. [...] Bez radykalnej poprawy infrastruktury szpitali i uwrażliwienia personelu medycznego na potrzeby i uczucia hospitalizowanych osób intymność i godność pacjenta pozostanie tylko formalną deklaracją.*

<sup>5)</sup> W przypadku placówek medycznych wysokość kary pieniężnej będzie zależeć nie tylko od rodzaju i wagi naruszenia (oraz innych czynników wpływających na wysokość administracyjnej kary pieniężnej, o których mowa w art. 83 RODO), lecz również od statusu jednostki – zasadniczo wysokość kary administracyjnej może wynosić nawet 2%-4% całkowitego obrotu, przy czym w przypadku jednostek sektora finansów publicznych, o których mowa w art. 9 pkt 1–12 i 14 ustawy z 27 sierpnia 2009 r. o finansach publicznych – 100 tys. zł, a w przypadku jednostek sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z 27 sierpnia 2009 r. o finansach publicznych – 10 tys. zł

<sup>6)</sup> Treść raportu dostępna jest pod linkiem: <https://www.nik.gov.pl/plik/id,20223,wp,22913.pdf>; cytowany fragment – zob. s. 105-106

<sup>7)</sup> Por. projekt Kodeksu Branżowego w Ochronie Zdrowia – dostępny na stronie internetowej: <http://www.rowozdrowiu.pl/>

### Kluczowe wnioski

Decydując się na wdrożenie w ramach placówki ochrony zdrowia systemu wspierającego działanie personelu medycznego lub pomocniczego, w tym systemów komunikacji z pacjentem służących lub mogących służyć do przekazywania i przetwarzania informacji o często „wrażliwym” charakterze, a przez to realizacji działań podlegających szczególnym „obstrzeżeniom” prawnym, konieczne jest dokonanie każdorazowej oceny, czy oferowane rozwiązania, ich możliwości funkcjonalne, projekt implementacji, przy przewidywanym sposobie ich przyszłej eksploatacji, będą wystarczające dla spełnienia wymagań prawnych, a późniejsze korzystanie z wdrożonego systemu nie będzie stanowiło nieuprawnionej ingerencji w sferę praw i wolności pacjenta.

W obecnym stanie prawnym ocena standardów postępowania i dobrych praktyk (choć pierwsze projekty tego rodzaju kodeksów w branży medycznej nie odnoszą się do tak szczegółowych kwestii<sup>7)</sup>) nie będzie jednak łatwa ze względu na generalny charakter prawnych regulacji mających zapewnić taką ochronę co najmniej do czasu wypracowania ich przez rynek, przy współpracy z właściwymi organami nadzoru. Regulacje te (np. RODO) przerzucają konieczność dokonania oceny ryzyka oraz doboru odpowiednich rozwiązań na podmiot zamierzający wdrożyć odpowiednie rozwiązania. Ryzyko ewentualnego błędu nieadekwatności i konsekwencji wiążących się ze stosowaniem rozwiązań ostatecznie niezgodnych z prawem lub nienadających się do pewnych zastosowań (np. przekazywania informacji o „wrażliwym” charakterze) alokowane jest zasadniczo w większości po stronie nabywcy i przyszłego użytkownika systemu. Nie zmienia to jednak faktu, że chroniona prawem sfera praw i wolności pacjenta, nawet w słusznym celu, jakim bez wątpienia jest usprawnienie komunikacji pacjenta z personelem medycznym, nie powinna zostać naruszona, zwłaszcza w sytuacji, gdy może ona zostać właściwie zabezpieczona przez odpowiedni dobór i zaprojektowanie tego typu rozwiązań. Istotne jest zatem, aby już na etapie wyboru danego systemu przyzywowego, a następnie na etapie jego wdrożenia brać pod uwagę realizację podstawowego prawa pacjentów – prawa do poszanowania godności i intymności oraz zasadę poufności danych pacjenta i ograniczenia dostępu do jego danych osobowych, które nie realizują świadczeń medycznych. □

### B I O

#### Agata Marcinkowska

Radca prawny w Kancelarii Radców Prawnych Barta&Kaliński (<https://bartakalinski.pl>) – specjalizuje się w prawie nowych technologii oraz ochrony danych osobowych.

#### Adrianna Żyrek

Aplikantka radcowska w Kancelarii Radców Prawnych Barta&Kaliński (<https://bartakalinski.pl>) – specjalizuje się w prawie nowych technologii oraz ochrony danych osobowych.



# New Security Concept

nowe podejście  
do bezpieczeństwa  
z poziomu zarządzania  
organizacją



T E K S T

Rafał Łupkowski

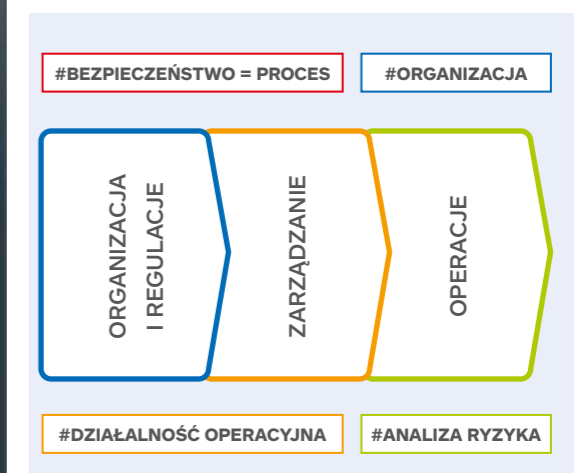
Ostatnie lata naszych doświadczeń na rynku komercyjnym sprowadzają się do jednego kluczowego wniosku, który jak mantra przewija się w tekstach i opracowaniach, a nawet prezentacjach produktowych: „Bezpieczeństwo to proces”. Warto nim zarządzać, ponieważ ma bezpośredni wpływ na podstawową działalność operacyjną organizacji i bezwzględnie powinien ją wspierać. Teza ta jest genialna w swojej prostocie, a do tego poparta solidną metodologią: badanie, rekomendacje i w rezultacie wdrożenie procesu bezpieczeństwa w trzech najważniejszych dla organizacji płaszczyznach:

- Formalnej
- Zarządczej
- Operacyjnej

Takie podejście zawsze daje oczekiwany rezultat. Uzupełnione o solidną analizę zagrożeń i oszacowanie ryzyka pozwala na prawidłowe określenie:

- Stanu bezpieczeństwa danej organizacji
- Miejsc, w których bezpieczeństwo jako proces jest zaburzone
- Rekomendacji pozwalających wdrażać skuteczne rozwiązania

Jeśli każdą organizację zbadamy na trzech przedstawionych na rysunku poziomach, wnioski powinny nasunąć się same.



Rys. 1. Trzy płaszczyzny organizacji



Nasi zleceniodawcy bardzo często stoją przed trudnymi decyzjami wiążącymi się z kosztami i zmianami organizacyjnymi. Właściwa analiza oparta na proponowanej przez nas metodzie pomaga określić kierunek działań do osiągnięcia celu, przy zastosowaniu adekwatnych środków i rozwiązań organizacyjnych. W efekcie przekłada się to na odpowiedni poziom bezpieczeństwa.

Co to oznacza w praktyce? Przejdźmy przez szybkie case study:

### KLIENT 1 ma poważny problem

– dokonano u niego kradzieży mienia ruchomego. Strata wyniosła 1 milion złotych. Na stole leży oferta na kilkaset tysięcy złotych na wyposażenie kilometra ogrodzenia w kamery, aby cyt. „mysz się nie prześlizgnęła”. Kupować czy nie?

Analiza wykonana przez naszą firmę doradczą szybko wykazuje, że zaproponowany w ofercie sposób nadawania praw dostępu do mienia jest nieskuteczny, kompletnie dziurawy. W jej efekcie klient wprowadza najpierw odpowiednie regulaminy, a następnie, wg określonych założeń funkcjonalnych, wdraża system. Zaczyna od systemu klucza master (tzw. Master Key) za ułamek pierwotnej kwoty wyceny.

### KLIENT 2 buduje obiekt o znaczeniu strategicznym

Uruchomienie produkcji w tej części Europy ma dla niego znaczenie kluczowe, dotychczas bowiem była prowadzona tylko w Azji. Klient chce poznać lokalny rynek, jego specyfikę, a także uniknąć nadmiernych kosztów. Otrzymywanych ofert na ochronę obiektu i systemy zabezpieczeń nie poprzedzały żadne pytania o działalność operacyjną ani żadna analiza zagrożeń. A przecież oczywiste jest, że bez tej podstawowej wiedzy

trudno skutecznie zarządzać bezpieczeństwem prowadzonego biznesu. Mało tego, klient, którego obiekt jeszcze nie powstał, otrzymał skopiowaną instrukcję ochrony opracowaną dla innego obiektu oraz ofertę opiewającą na miliony złotych za nieokreślony funkcjonalnie system.

Brzmi znajomo? W ramach naszego podejścia New Security Concept – klient otrzymał dokładny opis celu, wymagania operacyjne i analizę zagrożeń od poziomu zarządu do poziomu organizacji zadań i konkretnych funkcji w systemach zabezpieczeń.

### KLIENT 3 jest właścicielem i zarządcą budynku,

w którym dwukrotnie okradziono jego największego najemcę. Szuka wsparcia w firmie z sektora ochrony. Ta, nie wnikając w potrzeby zarządcy, ogranicza się do zwolnienia swoich ludzi, którzy w dniu kradzieży pełnili tam służbę. Tymczasem okradziony światowy koncern oczekuje konkretnych działań i zwraca się z roszczeniem. Firma ochrony twierdzi, że zareagowała poprawnie. Nasze podejście do sprawy zgodnie z metodyką New Security Concept przynosi zaskakujące efekty. Światowy koncern zmienia swoje procedury i podejmuje ścisłą współpracę z zarządcą – firma ochrony pokrywa straty, ponieważ metodyczna i konsekwentna analiza wskazują konkretne ryzyka (po stronie zwolnionych pracowników ochrony było ich relatywnie niewiele, ponieważ jak to w życiu bywa „ryba psuje się od głowy”).

To zdumiewające, jak często zdarzają się przypadki i próby desperackiego ratowania sytuacji bez jakiegokolwiek analizy i zasadności:

- Ukradli? – „Kamerujemy”,
- Inwestujemy? – Kupmy tanio,
- Co ma robić system? – Jak powstanie to później pomyślimy,
- Usługa nie działa? – Zróbmy audyt,
- Wdrożyć rekomendacje? – Po co wdrażać, przecież mamy raport – to wystarczy.

Brzmi znajomo? Jeśli tak, to oznacza, że organizacja potrzebuje metodyki New Security Concept. Nie jest to na pewno złoty środek na wszystkie problemy związane z bezpieczeństwem biznesu, ale przyznam, że przyjemnie pracuje się przy projektach wymagających kompleksowego, metodycznego podejścia, z którego efektów nasi klienci mogą czerpać korzyści. ▣

B I O

**Rafał Łupkowski**

Business Security Advisor, Chief Operating Officer w firmie doradczej Trustman

Nasi zleceniodawcy  
bardzo często stoją  
przed trudnymi  
decyzjami wiążącymi  
się z kosztami  
i zmianami  
organizacyjnymi

# TRUSTMAN

NOWE PODEJŚCIE DO BEZPIECZEŃSTWA

## Security Concept<sup>©</sup>



### KOMPLETNY RAPORT Z REKOMENDACJAMI DOT. BEZPIECZEŃSTWA FIZYCZNEGO:

- organizacja bezpieczeństwa
- warunki formalno-prawne
- strefy bezpieczeństwa
- analiza ryzyka
- wymogi dla technicznych systemów zabezpieczeń
- opis funkcjonalny rozwiązań
- rekomendacje

### ZAPEWNIENIE BEZPIECZEŃSTWA LUDZIOM I DANYM (W TYM OSOBYM I HANDLOWYM), INFRASTRUKTURZE, URZĄDZENIOM I WYPOSAŻENIU W ZAKRESIE:

- zagrożeń zewnętrznych
- zagrożeń środowiskowych
- nieuprawnionego dostępu do pomieszczeń
- ochrony danych osobowych





# Bezpieczeństwo w handlu

**Jak zapewnić bezpieczeństwo w obiektach handlowych, zastanawiali się uczestnicy kolejnego śniadania ekspertów a&s Polska.**

**Spotkanie odbyło się w grudniu ub.r. w hotelu Novotel Centrum Warszawa.**

**Dyskusję przy wspólnym stole prowadzili przedstawiciele producentów i dystrybutorów firm z rynku security oraz specjaliści i security managerowie firm i instytucji związanych z sektorem retail.**



**Jacek Bechta**

Euronet

→ **Śniadanie było bardzo ciekawe.** Uważam, że powinno być częściej organizowane, dlatego że jest tu możliwość wymiany doświadczeń nie tylko pomiędzy szefami bezpieczeństwa sieci handlowych, ale również firmami z nami współpracującymi, dostarczającymi nam różne rozwiązania.



**Roman Bielecki**

TK Maxx

→ **Tego typu spotkania w naszej polskiej rzeczywistości są bardzo rzadko spotykane.** Jest to więc bardzo duża wartość dla grona osób, które są zainteresowane tematyką bezpieczeństwa, w tym przypadku bezpieczeństwa w handlu. To fantastyczna rzecz posłuchać różnego rodzaju opinii z różnych stron, opinii osób, które są w to zaangażowane, a z drugiej strony dostarczają rozwiązań dla zapewnienia bezpieczeństwa biznesu w handlu. Było tutaj kilka bardzo ciekawych wypowiedzi.



**Adam Brzezicki**

Axis Communications

→ **Poruszyliśmy oczywiście wiele aktualnych tematów,** takich jak automatyzacja procesów, jak wpływa ona na życie firmy, z jakimi zagrożeniami się wiąże i jakie benefity potrafi przynieść. Rozmowa cały czas toczyła się na profesjonalnym poziomie, widać było zaangażowanie ekspertów, którzy mieli bardzo szeroką wiedzę zarówno praktyczną, jak i teoretyczną dotyczącą wszystkich poruszanych kwestii.



**Michał Czuma**

MC Consulting

→ **Bardzo ciekawym tematem,** który pojawił się podczas tego śniadania, była świadomość ludzi, iż obecne zmiany klimatyczne, niestety idące w złym kierunku, mogą generować nowe ryzyka i to nie w dalekiej, ale bardzo bliskiej perspektywie. Przypomniałem sobie sytuację, w której mi wyłączono prąd. Nie wiem, czy Państwo zastanawialiście się kiedyś, co się zacznie dzieć, kiedy zabraknie prądu. Czy będziecie mogli naładować swoją komórkę, czy będziecie w stanie włączyć komputer i jak długo będzie pracował bez doładowania. Czy jesteście zabezpieczeni na sytuację, kiedy wszystkie nasze pieniądze są na karcie i nie mamy gotówki. To są wszystkie elementy, o których warto pomyśleć, kiedy mówimy o bezpieczeństwie nas wszystkich, naszych firm, naszych klientów. I o tym dzisiaj rozmawialiśmy.



**Mirosław Lukowski**

Niezależny ekspert

→ **Na kolejnym śniadaniu ekspertów kolejny raz Grupa a&s sprostała wyzwaniu.** Znowu tematy, które były ważne, nie tylko działanie post factum, ale i prewencyjne. Takie spotkania ekspertów zawsze przynoszą chwile zastanowienia się nad tym, co robimy, jak robimy i jak możemy robić. Jak zawsze, mam pozytywne odczucia.



**Adam Nowakowski**

Linc Polska

→ **Usłyszeliśmy dużo opinii na temat wyzwań,** jakie czekają branżę retail, jeśli chodzi o zapewnienie bezpieczeństwa, przy jednoczesnej optymalizacji kosztów. Przeniesienie części usług na stronę techniczną czy zastępowanie ochrony fizycznej lub w ogóle różnych usług systemami elektronicznymi, systemami autonomicznymi to jest na pewno krok, który musimy wykonać w przyszłości.



**Michał Sidor**

Schrack Seconet

→ **Jak zwykle na śniadaniu ekspertów usłyszeliśmy wiele interesujących informacji,** zarówno od klientów końcowych, jak i dostawców urządzeń i integratorów. W tym miesiącu mieliśmy przyjemność prowadzić ożywioną dyskusję o bezpieczeństwie obiektów handlowych. Spotkanie zakończyło się sukcesem, zachęcam wszystkich do udziału w kolejnym.



**Marek Szafran**

CNS Outsourcing IT

→ **Najbardziej odpowiada mi forma tego spotkania,** bo nie jest ona sztuczna. Nie jest to prezentacja, gdzie ktoś zabiera głos, a ktoś odpowiada. Tu można dyskutować, spierać się. Nie trzeba być w krawacie, nie trzeba być w marynarce. Będzie to swego rodzaju luz i człowiek bardziej sam się otwiera, wchłania więcej informacji od innych. Według mnie w aspekcie bezpieczeństwa cały czas pokutuje podstawowy błąd, który niestety odbija się na całości zagadnienia. Mianowicie bezpieczeństwo jest postrzegane jako coś na zasadzie zakupu produktu „sztuk raz”. Nikt nie patrzy na to jako na proces. A jest to permanentny proces, tak samo jak uczenie się. Dziecko najpierw uczy się chodzić, potem idzie do szkoły podstawowej, średniej, na studia itd. Tak samo bezpieczeństwo, to też jest proces. To jest proces produktowy, to jest proces szkolenia ludzi, powstają nowe przypadki, nowe zdarzenia i nigdy się to nie kończy.



**Marcin Walczuk**

BCS

→ **Spotkanie jak zwykle bardzo owocne.** Mieliśmy możliwość wymiany poglądów pomiędzy dwiema czy nawet trzema stronami barykady, łącznie z potrzebami klientów i tym, co dostawcy mogą im zaoferować. Wszystko to zebrane w pigułce, na jednym spotkaniu. Jak zwykle to dobry prognostyk na kolejne takie spotkania.



## Wisenet X-Lite – kamera kompaktowa z motozoomem



**Wisenet X-Lite XNZ-L6320 – najnowsza pozycja w ofercie kamer marki Wisenet produkcji Hanwha Techwin – to atrakcyjna cenowo 2-Mpix kamera kompaktowa wyposażona w obiektyw zmiennoogniskowy z optycznym 32-krotnym motozoomem i automatyczną regulacją ostrości.**

Zastępuje cieszący się dużą popularnością model Wisenet SNZ-6320, ale jest znacznie mniejsza i bardziej atrakcyjna cenowo.

Wisenet XNZ-L6320 to kamera z prawdziwą funkcją dzień/noc, uswanym mechanicznie filtrem podczerwieni (ICR) i udoskonalonym szerokim zakresem dynamiki (WDR) 120

dB, umożliwiającym uzyskiwanie wyraźnych obrazów, gdy w kadrze występują jednocześnie jasne i ciemne obszary. W przeciwieństwie do standardowego WDR, gdy rejestrowane obrazy składają się z 2 klatek zapisanych przy różnych wartościach ekspozycji, Wisenet XNZ-L6320 wykorzystuje do tego 4 klatki. □

### NAJWAŻNIEJSZE FUNKCJE:

- Obsługa kompresji H.265, H.264 i MJPEG oraz Wise-Stream II (technika kompresji dostępna tylko w kamerach Wisenet).
- Wbudowana inteligentna analiza obrazu (IVA), m.in. algorytmy wykrywania sabotażu, podejrzanego zachowania, kierunku przemieszczania się, utraty ostrości, zamglenia, wejścia/wyjścia do/ze strefy, pojawienia się/zniknięcia obiektu, dźwięku, twarzy, ruchu, a także wirtualna linia.
- Klasyfikacja dźwięku: funkcja analizy audio rozpoznająca dźwięki o krytycznym znaczeniu (np. podniesiony głos, krzyk, dźwięk rozbijanego szkła, wystrzał z broni palnej i wybuch) – kamera generuje powiadomienia umożliwiające szybkie reagowanie na incydenty.
- Cyfrowa stabilizacja obrazu (DIS) ogranicza rozmycie obrazu wynikające z ruchu kamery (silny wiatr lub wibracje).
- Gniazdo karty pamięci SD/SDHC/SDXC umożliwiające przechowywanie zapisu wideo lub danych bezpośrednio w kamerze w razie zakłóceń połączenia z siecią.
- Dwukierunkowa transmisja dźwięku umożliwia operatorom komunikowanie się z ludźmi w pobliżu kamer (udzielenie pomocy lub pouczenie intruzów).
- Technologia PoE eliminuje potrzebę instalacji osobnego zasilania i okablowania kamery.

## PTZ FLIR Quasar™4K obserwuje, wykrywa i klasyfikuje

PTZ FLIR Quasar™4K to połączenie kamery tradycyjnej z termowizyjną, gwarantujące doskonałą jakość obrazu zarówno w dzień, jak i w nocy, bez względu na warunki atmosferyczne. Ta głowica obrotowa wykorzystuje najnowszą technologię PTZ, optykę i mechanikę, umożliwiając integrację z systemami zarządzania sygnałem wizyjnym (VMS).



Kamera została zaprojektowana z myślą o bezpieczeństwie sieciowym. Jej system cyberbezpieczeństwa został wzmocniony przed nowymi zagrożeniami. Ulepszony interfejs sieciowy ułatwia konfigurację wszystkich kamer marki FLIR, a nowa aktualizacja pozwala na bezpieczny dostęp do urządzeń. Rozdzielczość 4K i wysoka czułość gwarantują wyraźny obraz

przy słabym oświetleniu również przy 22x zoomie optycznym. Kamera ma ulepszony szeroki zakres dynamiki i wbudowane oświetlacze podczerwieni. PTZ FLIR Quasar™4K IR PTZ to idealne, kompleksowe rozwiązanie do monitoringu wizyjnego miast, infrastruktury krytycznej czy lotnisk. □

Więcej na: [www.linc.pl](http://www.linc.pl)



## Hochiki & NSC systemy sygnalizacji pożarowej w ofercie MIWI URMET

Z początkiem br. firma MIWI URMET wprowadziła do swojej oferty dwa modele central sygnalizacji pożarowej niemieckiej firmy NSC – Solution F1 oraz Solution F2.

Solution F1 to nowa generacja modułowych i innowacyjnych central ppoż. Zawierają wiele nowych funkcji, niektóre z nich są rzadko spotykane w branży zabezpieczeń i m.in. dzięki takiemu wyposażeniu zdobywają coraz większą rzeszę klientów. Centrala Solution F1 może być rozbudowana do 18 pętli, w sieci może również pracować do 64 central. Solution F2 jest centralą nowej

generacji przeznaczoną głównie do mniejszych systemów, ale jednocześnie stwarzającą możliwości rozbudowy. Maksymalna konfiguracja tej centrali to dwie pętle. Obie centrale współpracują z urządzeniami pętlowymi firmy Hochiki (czujniki, ROP-y, moduły, sygnalizatory). Na jednej pętli można zainstalować do 127 urządzeń Hochiki oraz 127 sygnalizatorów w podstawach czujek. □

## Aplikacja Traffic CaMMRa i kamery Axis

Dzięki nowej aplikacji Traffic CaMMRa kamery Axis Communications można przekształcić w czujniki rozpoznające tablicę rejestracyjną, kierunek jazdy, kolor, markę, typ, a w niektórych przypadkach określony model pojazdu. Aplikacja działająca bezpośrednio w kamerze została opracowana przez FF Group.



Możliwości zastosowania Traffic CaMMRa są naprawdę szerokie: od monitorowania ruchu, liczenia i gromadzenia danych, aż po automatyczne pobieranie opłat. Aplikacja może identyfikować ciężarówki, wychwytywać naruszenia, np. niedozwolone wyprzedzanie czy jazda po złym pasie, a nawet wyszukiwać skradzione samochody. W kolejnym etapie chcemy poszerzyć jej możliwości o pomiar prędkości pojazdu, otwierając kolejne szerokie pole do działania – mówi Jan Hazlbauer, menedżer projektu w FF Group. Oprogramowanie działa bezpośrednio w kamerach sieciowych Axis, wykorzystując ich

moce obliczeniowe, i nie wymaga dodatkowego sprzętu ani serwera. Jednocześnie Axis Communications wprowadził nową kamerę AXIS Q1700-LE przeznaczoną do rozpoznawania tablic rejestracyjnych i w pełni dostosowaną do dalszej integracji z zewnętrznym oprogramowaniem, niezależnie od tego, czy są to systemy serwerowe, czy aplikacje ACAP, takie jak Traffic CaMMRa. Połączenie specjalistycznej kamery AXIS Q1700-LE i aplikacji Traffic CaMMRa daje wiele możliwości. Dzięki dużej mocy obliczeniowej wszystkie dane, w tym ich analiza, są błyskawicznie przetwarzane w kamerze.

System jest bardzo szybki, aplikacja może wykryć pojazd jadący z prędkością do 160 km/h w 120-250 ms. Zasięg analizy wynosi do 240 m w ciągu dnia i około 40 m w nocy. Kamery Axis są otwarte na aplikacje innych firm, co pozwala nam współpracować z ekspertami branżowymi. W rezultacie wspólnie powstają rozwiązania dopasowane do konkretnych potrzeb klientów. Traffic CaMMRa jest tego świetnym przykładem. Ponadto kamerę wraz z aplikacją można łatwo zintegrować z systemami VMS – podsumowuje Dalibor Smažinka, Business Development Manager w Axis Communications. □  
Więcej na [www.ff-group.org/axis](http://www.ff-group.org/axis).

R E K L A M A

VdS

klasa  
B i C

EN

grade  
2 i 3według normy  
EN 50131-2-6:2008

ALARMTECH

www.alarmtech.pl

## CZUJKI MAGNETYCZNE DO BRAM, OKIEN I DRZWI

Seria MC

**ALARMTECH**  
20 lat doświadczenia

Projektant, producent, dostawca  
Detektorów i czujników do SSWiN  
w klasie bezpieczeństwa 2 & 3




## HIKVISION INNOVATION SUMMIT 2020

DISCOVER. COLLABORATE. EXPAND.

Hikvision Innovation Summit to niezwykle wydarzenie, które firma Hikvision organizuje wraz z najważniejszymi Partnerami Technologicznymi. Uczestnikom zaprezentujemy korzyści wynikające z połączenia rozwiązań, a wspólnej dyskusji zostaną podane najnowsze trendy rynkowe.

Dzięki ogromnym możliwościom w zakresie badań i rozwoju – 16 tys. inżynierów pracuje w ośmiu centrach R&D – Hikvision przoduje w opracowywaniu technologii do szerokiej gamy rozwiązań. Razem z Partnerami Technologicznymi łączy wiedzę, doświadczenie i wyjątkowe umiejętności, dostarczając optymalne rozwiązania, rozszerzając zakres działalności i zwiększając rentowność. Podczas wydarzenia będzie można wysłuchać merytorycznych prezentacji Partnerów Technologicznych, a ich rozwiązania przetestować na specjalnie przygotowanych stoiskach.

Hikvision Innovation Summit odbędzie się 12-13.03.2020 w Taets Art and Event Park w Amsterdamie. Wśród platynowych Partnerów wydarzenia znalazły się takie firmy, jak Western Digital, Vemco Group i Telescopic Mast. Będą też obecni reprezentanci firm Eagle Eye Networks, IQ Messenger, Acoba. Udział w wydarzeniu jest bezpłatny.  Więcej informacji oraz rejestracja na stronie: <https://hikvision-innovation-summit.eventmaker.io/>

## Zabezpiecz swój sukces


Przed nami 23. edycja Międzynarodowych Targów Zabezpieczeń SECUREX, które odbędą się 21-23 kwietnia 2020 r. Producenci oraz dystrybutorzy zaprezentują w Poznaniu najnowsze rozwiązania i premiery produktowe w segmentach monitoringu, kontroli dostępu, systemów alarmowych, ochrony informacji, mienia, rozwiązań smart building, jak również wszelkich zabezpieczeń – od mechanicznych po systemy IT.

W tym samym czasie odbędą się także: targi INSTALACJE, Poznań Drone Expo, targi SAWO, targi GreenPOWER oraz targi EXPOPOWER.

Targi Securex są największym w Europie Środkowo-Wschodniej wydarzeniem branży zabezpieczeń. To miejsce bezpośredniego kontaktu dostawców i firm oferujących wdrożenia i usługi z zakresu zabezpieczeń, klientów biznesowych, inwestorów prywatnych i instytucjonalnych, przedstawicieli służb i ekspertów. Będzie można poznać z bliska i przetestować innowacje technologiczne, porozmawiać o ich możliwościach, skorzystać z doradztwa specjalistów i ekspertów. Bogaty program wydarzeń towarzyszących – konferencji, otwartych prelekcji i debat, atrakcyjnych pokazów

specjalnych – poszerzy wiedzę i zainspiruje do implementacji i integracji najnowocześniejszych rozwiązań.

Fachowe umiejętności i doświadczenie instalatorów i służb ochrony będzie można podziwiać podczas VII Mistrzostw Polski Instalatorów Systemów Alarmowych organizowanych wspólnie z Polską Izbą Systemów Alarmowych oraz Mistrzostw Polskiej Izby Ochrony w Strzelectwie, na które zaprasza Polska Izba Ochrony. PIO przygotuje też pokazy skutecznej interwencji służb ochrony oraz debatę nt. bezpieczeństwa imprez masowych. Wielkopolska policja udostępni autentyczną dyspozytornię systemu powiadamiania ratunkowego 112, w której będzie można sprawdzić się w roli dyspozytora. Funkcjonariusze zapre-

zentują także interwencje z wykorzystaniem wyszkolonych psów, które odegrają kluczową rolę w zatrzymaniu groźnego przestępcy oraz wykrywaniu substancji niedozwolonych. Krajowe Stowarzyszenie Ochrony Informacji Niejawnych oraz Stowarzyszenie Wspierania Bezpieczeństwa Narodowego zorganizują punkty konsultacyjne w zakresie ochrony informacji niejawnych, biznesowych, danych osobowych oraz zarządzania kryzysowego i ochrony infrastruktury krytycznej. Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem POLALARM zaproszą do konsultacji z rzeczoznawcami w zakresie technicznej ochrony osób i mienia oraz zarządzania bezpieczeństwem. 

4.06.2020 r.

4. MIĘDZYNARODOWA KONFERENCJA

# Warsaw Security Summit

4th INTERNATIONAL CONFERENCE

ZAPRASZA



Więcej informacji:  
[www.WarsawSecuritySummit.eu](http://www.WarsawSecuritySummit.eu)



# HIKVISION INNOVATION SUMMIT 2020

DISCOVER. COLLABORATE. EXPAND.

Marzec 12-13, 2020 | Taets Art - Amsterdam

## DOŁĄCZ DO NAJWIĘKSZEGO WYDARZENIA HIKVISION!

- Weźmiesz udział w 2 dniach prezentacji i paneli największych Partnerów Technologicznych Hikvision
- Przekonasz się jak połączone technologie Hikvision i Partnerów Technologicznych wspierają rozwój takich rynków jak Miasto, Handel, Logistyka czy Opieka Zdrowotna
- Spotkasz ponad 30 wystawców z którymi będziesz miał okazję porozmawiać na stoiskach
- Dołączysz do 1000 klientów z całej Europy, którzy przyjadą do wyjątkowego Taets Art and Event Park

Bilety: Udział bezpłatny  
Zarejestruj się!

