

CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 6(94)/2013

ZABEZPIECZENIA

WWW.ZABEZPIECZENIA.COM.PL • E-MAIL: ZABEZ@ZABEZPIECZENIA.COM.PL

ZBAR
www.zbar.com.pl



ochrona OBWODOWA OBIEKTÓW

W NUMERZE:

- Z kamerami wśród zwierząt
- Projektowanie instalacji z zasysającymi czujkami dymu
- System automatycznego rozpoznawania tablic rejestracyjnych
- Czujka PIR + kamera w systemie alarmowym – niezbędny gadżet?

to już **15** lat
Zabezpieczeń

SZYBKA, SKUTECZNA I KONKURENCYJNA.



KAMERA DZIEŃ/NOC

Z OŚWIETLACZEM LED

WIDZENIE DZIEŃ/NOC I TERMICZNE

ULISSE COMPACT SYSTEM ZAWIERAJĄCY NOWOCZESNĄ GŁOWICĘ UCHYLNO-OBROTOWĄ

Idealne rozwiązanie dla wymagających zewnętrznych instalacji bezpieczeństwa i monitoringu. ULISSE COMPACT gwarantuje płynne i stabilne pozycjonowanie, nawet przy pracy ciągłej. Zapewnia obraz doskonałej jakości, ogromną wytrzymałość oraz prostą obsługę i konfigurację.



PROTECTION



IP



THERMAL



WIPER



INFRARED

ONVIF

Driving network video through global standardization

SOLUTIONS FOR CCTV WWW.VIDEOTEC.COM



Kamery sieciowe PTZ

iPOLiS,
Your smart security solution



Nieźródlna
jakość obrazu

Efficient
Network
Transmission

Wydajna
transmisja
sieciowa



Komfort
użytkowania



Kompleksowe
rozwiązania
sieciowe



Mądry wybór profesjonalistów

IR Zoom – zintegrowany z obudową obiektywu oświetlacz automatycznie regulujący kąt i natężenie wiązki podczerwieni w zależności od aktualnej ogniskowej kamery i pozwalający na skuteczną obserwację obiektów w całkowitej ciemności na dystansie 100m.

Zoom x20 – zoom optyczny gwarantujący najwyższy poziom szczegółowości obrazu w rozdzielczości FullHD.

DIS – cyfrowa stabilizacja kompensująca drgania obrazu (np. w przypadku kamery zamontowanej na wysokim maszcie).

WDR – szeroki zakres dynamiki umożliwiający pracę kamer w bardzo wymagających warunkach oświetleniowych.

IVA – inteligentna analiza wideo dająca możliwość np. detekcji twarzy, czy przekroczenia wirtualnej bariery.

Edge storage – możliwość rejestracji nagrań bezpośrednio w kamerze na karcie pamięci SDHC.

Solidna obudowa – odporna na mgłę solną, umożliwiająca pracę w trudnych warunkach klimatycznych: IP66, IK10, zakres temp.: -50oC÷+55 oC.



SAMSUNG TECHWIN

SAMSUNG

SNP-6200RH

- Rozdzielczość max.: **1920 x 1080 @ 30kl/s**
- Czułość – 1.5lux (kol)/0lux (czb) przy włączonym oświetlaczu IR @1/30sec, F1.6, 50IRE
- Kompresja: 10 strumieni - H.264 / MJPEG
- Wejście /wyjście audio (full-dupleks) ; G711/G726
- Obiektyw: 4.45mm ÷ 89mm (**20X**); DC AI; F1.6, kąt widzenia: 62.9° ÷ 3.1°(w poz.)
- Zakres panoramowania w poziomie: 360°(nieograniczony), w pionie: 190° (-5° ÷ 185°)
- Szybkość panoramowania: 250°/s dla presetów, 0.024÷120°/s w trybie manualnym
- Mechaniczny filtr IR, S/N – 50dB; WDR – 60dB (@15kl/s), SSSR, SSNR III, BLC/HLC
- IVA: ruch, bariera, det. twarzy, sabotaż, det. audio; 12 stref prywatności, DIS
- Edge storage: SDHC do 32GB, ONVIF **Profile-S**, SNMP, SSL/TLS, UPnP
- **Oświetlacz IR zoom z regulacją optyczną - zasięg 100m**



SNP-6200RH

SNP-6201 / SNP-6201H

- Rozdzielczość max.: **1920 x 1080 @ 30kl/s**
- Czułość – 1.5lux (kol)/0.1lux (czb) @1/30sec, F1.6, 50IRE
- Kompresja: 10 strumieni - H.264 / MJPEG
- Wejście /wyjście audio (full-dupleks) ; G711/G726
- Obiektyw: 4.45mm ÷ 89mm (**20X**); DC AI; F1.6, kąt widzenia: 63° ÷ 3.49°(w poz.)
- Zakres panoramowania w poziomie: 360°(nieograniczony), w pionie: 210° (-15° ÷ 195°)
- Szybkość panoramowania: 500°/s dla presetów, 0.024÷120°/s w trybie manualnym
- Mechaniczny filtr IR, S/N – 50dB; WDR – 60dB (@15kl/s), SSSR, SSNR III, BLC/HLC
- IVA: ruch, bariera, det. twarzy, sabotaż, det. audio; 12 stref prywatności, DIS
- Edge storage: SDHC do 32GB, ONVIF **Profile-S**, SNMP, SSL/TLS, UPnP
- Odporność na uszkodzenia: IK10 (dla SNP-6201 w obudowie SHP-3701H)
- Szczelność IP66 (SNP-6201H / SNP-6201 w obudowie SHP-3701H), Zasilanie: 24VAC/ PoE+ (IEEE 802.3at)
- Temp.pracy: -50 ÷ +55°C przy zasilaniu 24VAC lub -30 ÷ +55°C dla POE+



SNP-6201

SNP-6201H

SNP-5300

SNP-5300H

SNP-5300 / SNP-5300H

- Rozdzielczość max.: **1280 x 1024 @ 30kl/s**
- Czułość – 0.5lux (kol)/0.03lux (czb) @1/30sec, F1.35, 50IRE
- Kompresja: 10 strumieni - H.264 / MJPEG
- Wejście /wyjście audio (full-dupleks) ; G711/G726
- Obiektyw: 3.5mm ÷ 105mm (**30X**); DC AI; F1.35, kąt widzenia: 54.85° ÷ 2°(w poz.)
- Zakres panoramowania w poziomie: 360°(nieograniczony), w pionie: 210° (-15° ÷ 195°)
- Szybkość panoramowania: 500°/s dla presetów, 0.024÷120°/s w trybie manualnym
- Mechaniczny filtr IR, **S/N – 50dB; WDR – 90dB (@15kl/s)**, SSSR, SSNR III, BLC/HLC
- IVA: ruch, bariera, det. twarzy, sabotaż, det. audio, 12 stref prywatności, DIS
- Edge storage: SDHC do 32GB, ONVIF **Profile-S**, SNMP, SSL/TLS, UPnP
- Odporność na uszkodzenia: IK10 (dla SNP-5300 w obudowie SHP-3701H)
- Szczelność IP66 (SNP-5300H / SNP-5300 w obudowie SHP-3701H), Zasilanie: 24VAC/ PoE+ (IEEE 802.3at)
- Temp.pracy: -50 ÷ +55°C przy zasilaniu 24VAC lub -30 ÷ +55°C dla POE+

SNP-3371 / SNP-3371TH

- Rozdzielczość max.: 704 x 576 @ 25kl/s
- Czułość – 0.7lux (kol)/0.07lux (czb) @1/30sec, F1.6, 50IRE
- Kompresja: 10 strumieni - H.264 / MJPEG
- Wejście /wyjście audio (full-dupleks) ; G711/G726
- Obiektyw: 3.5mm ÷ 129.5mm (37X); DC AI; F1.6, kąt widzenia: 55.5° ÷ 1.59°(w poz.)
- Zakres panoramowania w poziomie: 360°(nieograniczony), w pionie: 190° (-5° ÷ 185°)
- Szybkość panoramowania: 500°/s dla presetów, 0.024÷120°/s w trybie manualnym
- Mechaniczny filtr IR, S/N – 52dB; WDR – 52dB (@15kl/s), SSSR, SSNR III, BLC/HLC
- IVA: ruch, bariera, wejście/wyjście; 8 stref prywatności; autotracking - SNP-3371TH
- Edge storage: SDHC do 32GB, ONVIF Profile-S, SNMP, SSL/TLS, UPnP
- Odporność na uszkodzenia: IK10, Szczelność IP66 (tylko SNP-3371H)
- Zasilanie: 24VAC/ PoE+ (IEEE 802.3at)
- Temp.pracy: -50 ÷ +55°C przy zasilaniu 24VAC lub -10 ÷ +55°C dla POE+



SNP-3371

SNP-3371TH

SNP-3120 / SNP-3120VH

- Rozdzielczość max.: **704 x 576 @ 25kl/s**
- Czułość – 0.7lux (kol)/0.07lux (czb) @1/30sec, F1.65, 50IRE
- Kompresja: 10 strumieni - H.264 / MPEG-4 / MJPEG
- Wejście /wyjście audio (full-dupleks) ; G711
- Obiektyw: 3.69mm ÷ 44.32mm (**12X**); DC AI; F1.65, kąt widzenia: 54° ÷ 4.62°(w poz.)
- Zakres panoramowania w poziomie: 360°(nieograniczony), w pionie: 190° (-5° ÷ 185°)
- Szybkość panoramowania: 650°/s dla presetów, 0.05÷120°/s w trybie manualnym
- Mechaniczny filtr IR, S/N – 50dB; WDR – 52dB, SSSR, SSNR III, BLC
- IVA: ruch, bariera, wejście/wyjście; 12 stref prywatności
- Edge storage: SDHC do 32GB, ONVIF **Profile-S**, SNMP, SSL/TLS, UPnP
- Zasilanie: 24VAC/ PoE+ (IEEE 802.3at)
- Temp.pracy: -50 ÷ +55°C przy zasilaniu 24VAC (tylko SNP-3120VH)
- Odporność na uszkodzenia: IK10, Szczelność IP66 (tylko SNP-3120VH)



SNP-3120

SNP-3120VH

Spis treści

Wydarzenia, Informacje	4
Publicystyka	
Z kamerami wśród zwierząt – <i>Maciej Mroszczak</i>	30
SSWiN	
Nowoczesne manipulatory w ofercie firmy SATEL – <i>Michał Konarski, SATEL</i>	34
System REDWALL-IP z komunikacją IP i zasilaniem PoE – <i>Jacek Wójcik, OPTEX Security</i>	38
LightSYS2 w chmurze RISCO – <i>RISCO Group Poland</i>	42
Systemy zintegrowane	
MB-Secure – modułowa platforma SSWiN i kontroli dostępu – <i>Tomasz Szklarz, ADI</i>	46
Rozwiązania Bosch Security Systems dla kopalni odkrywkowych – <i>Michał Borzucki, Bosch Security Systems</i>	50
Telewizja dozorowa	
System automatycznego rozpoznawania tablic rejestracyjnych firmy GeoVision – <i>Grzegorz Żuk, POLVISION</i>	54
Kontrola dostępu	
Autonomiczne kontrolery KaDe – <i>Ryszard Sobierski, AAT Holding</i>	60
Ochrona przeciwpożarowa	
Projektowanie instalacji z zasysającymi czujkami dymu – <i>Andrzej Obłój, Xtralis, Mariusz Konik, Vision Polska</i>	64
Ochrona informacji	
Zadania i obowiązki pełnomocnika ds. ochrony informacji niejawnych związane z technicznym zabezpieczeniem obiektów wojskowych – <i>Czesław Cwiek, Ochrona Informacji Niejawnych i Danych Osobowych</i>	68
Strefa Inwestora	
Czujka PIR + kamera w systemie alarmowym – niezbędny gadżet? – <i>Daniel Kamiński, Ochrona Juwentus</i>	72
Strefa Biznesu	
Monitorowanie pracowników w kontroli operacyjnej firmy – <i>Tytus Andrzej Woźniak</i>	76
Case Study	
Lotnisko w Krakowie jest bezpieczne dzięki kamerom Axis Communications – <i>Axis Communications</i>	80
Karty katalogowe	82
Spis teleadresowy	92
Cennik i spis reklam	102



LightSYS2 w chmurze RISCO

42



Rozwiązania Bosch Security Systems dla kopalni odkrywkowych

50



Monitorowanie pracowników w kontroli operacyjnej firmy

76



Lotnisko w Krakowie jest bezpieczne dzięki kamerom Axis Communications

80



Międzynarodowe Targi Poznańskie



spotkaj przyszłość



securex[®]

P O L A N D

Międzynarodowe Targi Zabezpieczeń

**BEZPIECZEŃSTWO
SUKCESU**



8 – 11 kwietnia 2014

Poznań

www.securex.pl

ZGŁOŚ SIĘ JUŻ DZIŚ!

I wykorzystaj dodatkowe kanały
informacyjne dla Twojej firmy lub produktu

SIĘGNIJ PO UNIKATOWY
PAKIET KORZYŚCI
WWW.ZLOTYMEDAL.MTP.PL



SECUREX 2014

Hucznie, ale bezpiecznie



Zbliża się jubileuszowa 20. edycja największych i najbardziej prestiżowych targów branży zabezpieczeń w Polsce i Europie Środkowo-Wschodniej – **SECUREX 2014**. Targi odbędą się w dniach 8–11 kwietnia 2014 r. SECUREX odbywa się regularnie od 20 lat. Blisko 20 lat temu powstała też Polska Izba Systemów Alarmowych (PISA).

Już pierwszego dnia targów, **8 kwietnia 2014 r.**, organizatorzy SECUREX-u oraz PISA rozpoczną uroczyste obchody na specjalnej Gali Jubileuszowej, która odbędzie się w najbardziej prestiżowym miejscu, jakie mogą zaoferować Międzynarodowe Targi Poznańskie – w Sali Ziemi w Poznań Congress Center (pawilon 15).

Przyszłoroczna edycja, choć może wydawać się dość odległa, już w tej chwili aktywizuje zespół organizacyjny targów. – *Targi to przede wszystkim bezpośredni kontakt producentów, dystrybutorów, projektantów i konstruktorów z potencjalnymi klientami. SECUREX zdobył w środowisku opinię jednego z najlepszych i najskuteczniejszych narzędzi marketingu, stymulującego nawiązywanie interesujących kontaktów biznesowych. Dlatego właśnie priorytetem jest dla nas stworzenie jak najlepszej przestrzeni do prowadzenia spotkań i rozmów służących rozwojowi branży. Mając to na uwadze, już rozpoczęliśmy intensywne przygotowania* – mówi dyrektor projektu Joanna Jasińska.

Targi SECUREX z jednej strony pokazują najbardziej aktualną ofertę na

rynku, z drugiej zaś pozwalają wskazać kierunki jego rozwoju. Po dwóch latach przerwy będą one doskonałą okazją do tego, by spojrzeć na zmiany, które zaszły przez ten czas na rynku zabezpieczeń.

Choć do targów pozostało jeszcze kilka miesięcy, już w pierwszym terminie zgłoszeń ponad 50% oferowanej powierzchni wystawienniczej zostało zarezerwowane. Każdego dnia napływają nowe zgłoszenia. Już dzisiaj wiadomo, że wśród firm, które zgłosiły lub zapowiedziały swój udział, będą niekwestionowani liderzy rynku, polskie i zagraniczne firmy będące ważnymi partnerami biznesowymi, np. AAT Holding, ARPOL, Axis Communications, Bosch, C&C Partners, Gunnebo, Honeywell, Konsmetal, Metalkas, Nedap, SATEL, Schrack Seconet, Signal Group, UTC Fire & Security, TELENOT ELECTRONIC.

Renoma targów SECUREX wymaga, aby każda ich edycja inspirowała rynek, dlatego też w 2014 roku oprócz wydarzeń znanych z poprzednich edycji planowanych jest kilka zupełnie nowych. Jednym z nich będzie m.in. Dzień Integratora, w którym szczególnie uwy-

puklone zostaną tematy związane z synergią i przenikaniem się różnych gałęzi nauki i techniki w branży zabezpieczeń.

W ramach targów odbędą się IV Miistrzostwa Polski Instalatorów Systemów Alarmowych, jak również konkurs Polski Mistrz Techniki Alarmowej, którego organizatorem jest Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem POLALARM. Poruszone będą również zagadnienia dotyczące różnych aspektów bezpieczeństwa, o których będzie można podyskutować podczas III Konferencji Zarządzania Bezpieczeństwem przygotowanej wspólnie przez stowarzyszenie POLALARM i MTP. Konferencja ta odbędzie się drugiego dnia targów.

Warto już teraz zarezerwować sobie czas, by w dniach 8–11 kwietnia 2014 r. znaleźć się w Poznaniu, który stanie się europejską stolicą branży zabezpieczeń.

Bezpośr. inf. MTP



securex[®] 2014
P O L A N D
Międzynarodowe Targi Zabezpieczeń
International Security Fair

MTP i PISA zapraszają na Galę Jubileuszową

Uprzejmie informujemy, że w dniu 8 kwietnia 2014 r., w pierwszym dniu targów SECUREX, Międzynarodowe Targi Poznańskie i Polska Izba Systemów Alarmowych (PISA) organizują Galę Jubileuszową z okazji 20. edycji targów SECUREX i 20-lecia PISA.

Organizatorzy gali zaproszą do udziału w uroczystościach jubileuszowych przedstawicieli wszystkich wystawców SECUREX-u, firm członkowskich

PISA, współpracujących urzędów, instytucji i przedsiębiorstw.

Program gali, odbiegającej charakterem od podobnych jubileuszy, szczególnie miejsce (najnowocześniejsza w Europie „Sala Ziemi”) i oprawa techniczno-artystyczna pozwalają przypuszczać, że gala będzie wydarzeniem, które przejdzie do historii Międzynarodowych Targów SECUREX, PISA i całej branży zabezpieczeń.

Bezpośr. inf. PISA



Videotec powołał menadżera do spraw marketingu

Videotec, światowy lider w dziedzinie produkcji urządzeń wykorzystywanych w systemach CCTV, powołał **Alessandro Franchiniego** na stanowisko menadżera do spraw marketingu i komunikacji z klientami. Będzie on kierował zespołem marketingowym w celu dalszej poprawy relacji biznesowych z klientami i partnerami firmy Videotec na całym świecie. Alessandro ma ugruntowaną wiedzę na temat systemów bezpieczeństwa. Przez dziesięć lat koordynował współpracę firm działających w tej branży oraz organizował wystawy. Ostatnio zajmował stanowisko menadżera do spraw rozwoju kontaktów międzynarodowych w przodującej firmie działającej na rynku zabezpieczeń na terenie Rosji,



organizował doroczne międzynarodowe wystawy branżowe w Moskwie.

– To jest wyjątkowa i bardzo ekscytująca szansa na poprawę mojej sytuacji zawodowej i osobistej. W moim odczuciu firma Videotec zawsze stanowiła przykład przedsiębiorstwa wytwarzającego innowacyjne produkty najwyższej klasy. Utrzymanie tej szczytowej pozycji i sprostanie światowej konkurencji stanowi nie lada wyzwanie. Firma musi nieprzerwanie i dynamicznie nadążać za wymaganiami swoich klientów. Videotec bez wątplenia spełnia te warunki – powiedział Alessandro Franchini.

Bezpośr. inf. Martina Panighel
Videotec
Tłumaczenie: Redakcja

SNV-6012M firmy Samsung Techwin Kopułkowa kamera sieciowa 2 MP Full HD z WiseNetIII

SNV-6012M to niewielka kamera kopułkowa o rozdzielczości Full HD (1080p), która spełnia wymagania określone w normie EN50155, dzięki czemu może pracować w trudnych warunkach środowiskowych i jest odporna na drgania występujące w środkach transportu kołowego. Kamera spełnia również wymagania określone w normie EN50121, dotyczące odporności na emisje elektromagnetyczne spotykane w kolejnictwie. SNV-6012M ma obudowę o stopniu szczelności IP66 i jest wyposażona w złącze M12 zapewniające stabilne połączenie kabla komunikacyjnego przy ciągłych wibracjach i w trudnych warunkach środowiskowych.

Obraz wytwarzany przez kamerę SNV-6012M może być kompresowany wydajną metodą H.264. Możliwe jest także tworzenie obrazów kompresowanych metodą MJPEG. Kamera może wytwarzać wysokiej jakości obrazy kolorowe już

przy natężeniu oświetlenia zewnętrznego wynoszącym 0,03 lx, a także generować 60 obrazów na sekundę z zachowaniem rozdzielczości Full HD 1080p. Jest to szczególnie użyteczne podczas obserwacji szybko poruszających się obiektów, gdyż zapewnia wyrazisty obraz ich krawędzi. Technologia Samsung Motion Artefact Reduction pozwala na uniknięcie efektu rozmazywania się obrazów przedmiotów wywołanego ich szybkim ruchem w polu widzenia kamery.

Funkcja *Defog* może zostać wykorzystana do poprawy wyrazistości obrazu w trudnych warunkach pogodowych, takich jak deszcz lub mgła. Funkcja cyfrowej stabilizacji obrazu (DIS) zmniejsza wpływ wibracji kamery na jakość generowanego obrazu. Umożliwia to wyeliminowanie zjawisk związanych z pracą elektronicznej migawki kamery, takich jak chybotańcie i drżenie krawędzi przedmiotów na obrazie, które jest szczególnie widoczne na obrazach o wysokiej rozdzielczości.

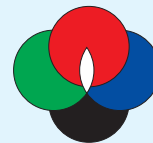
Ulepszony mechanizm rozszerzania zakresu dynamiki obrazu, jakim dysponuje procesor WiseNetIII, oferuje dynamikę na poziomie 120 dB, co pozwala na dokładne odwzorowanie scen zawierających jednocześnie elementy bardzo jasne i bardzo ciemne.

Kamera SNV-6012M jest zgodna ze standardem ONVIF, co umożliwia jej współpracę z wieloma systemami służącymi do rejestracji obrazu, dzięki czemu użytkownik może wybrać takie rozwiązanie, które najlepiej spełnia jego oczekiwania.



Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: Redakcja

Polski Mistrz Techniki Alarmowej 2014



Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem **POLALARM** zaprasza producentów oraz dystrybutorów elektronicznych i elektromechanicznych urządzeń oraz systemów przeznaczonych do ochrony osób i mienia do udziału w konkursie „Polski Mistrz Techniki Alarmowej 2014” im. Włodzimierza Kuczkowskiego. Będzie to XV edycja konkursu.

Zgłoszenia do udziału w konkursie będą przyjmowane do dnia 31 stycznia 2014 roku na drukach *Wniosku o udział w konkursie*. Wypełniony wniosek (wraz z załącznikami) należy przesłać na adres Biura Zarządu Sto-

warzyszenia POLALARM (ul. Nowogrodzka 18 lok. 8, 00-511 Warszawa, e-mail: polalarm@polalarm.com.pl).

Tytuły, nagrody i wyróżnienia zostaną przyznane do dnia 3 marca, a uroczystość wręczenia nagród laureatom odbędzie się w pierwszym dniu Międzynarodowej Wystawy Zabezpieczeń SECUREX 2014, tj. 8 kwietnia na terenie Międzynarodowych Targów Poznańskich.

Na stoisku Stowarzyszenia na targach SECUREX 2014 będziemy prezentować urządzenia i systemy, które zajęły pierwsze miejsce w grupie, oraz laureata głównej nagrody Złota Zbroja.

W miarę możliwości postaramy się zaprezentować wszystkie produkty zgło-

szone do konkursu. Wszyscy uczestnicy będą mogli umieścić na naszym stoisku ulotki i foldery reklamowe z informacją o zgłoszonych do konkursu wyrobach.

Regulamin Konkursu oraz *Wniosek o udział w Konkursie* są zamieszczone na stronie www.polalarm.org.

Informacji na temat konkursu udziela Biuro Zarządu Stowarzyszenia POLALARM (tel./faks: 22 626 90 31, 22 625 57 43).

Serdecznie zapraszamy do udziału w konkursie.

Bezpośr. inf. POLALARM

Bosch przedstawia nową wersję systemu BIS

Wersja 2.4 oprogramowania **BIS** (*Building Integration System*), modułowej platformy do centralnego zarządzania sygnalizacją alarmową i integracji podsystemów, jest już dostępna na rynku. Wersja BIS 2.4 działa w najnowszych systemach operacyjnych, m.in. w Windows Server 2008 R2 oraz Windows 7, co umożliwi zastosowanie jej w dowolnym istniejącym środowisku IT. Użytkownicy mogą skorzystać z rozszerzonych funkcji bezpieczeństwa tych systemów operacyjnych. System BIS 2.4 jest standardowo wyposażony w serwer Microsoft SQL Server 2008 Express Edition do mniejszych aplikacji. Współpracuje on również ze wszystkimi innymi wersjami oprogramowania SQL Server 2008 oraz SQL Server 2005 SP2.

Rozszerzone funkcje wizyjne

W systemie BIS 2.4 znacznie rozszerzono listę obsługiwanych urządzeń. Obecnie system obsługuje setki kamer CCTV różnych producentów, dzięki czemu stanowi odpowiednie rozwiązanie w przypadku heterogennych układów monitoringu wizyjnego składających się z różnych kamer. Usprawniony został mechanizm Video Engine, stanowiący jeden z głównych modułów BIS. Obecnie oferuje on mnóstwo nowych funkcji. Obsługa ekranów panoramicznych (16:9 i 16:10) oraz edytowalne schematy alarmów ułatwiają indywidualną konfigurację systemów. Nowy mechanizm rejestracji Video Recording Engine (VRE) jest kompatybilny z ok. 800 różnymi modelami kamer. Liczba ta obejmuje kamery Bosch MP. Współpracuje z najnowszymi rejestratorami Bosch, na przykład Divar 700, VRM, a także z popularnymi urządzeniami innych producentów.

Ulepszony interfejs użytkownika

Dzięki wizualnemu „odświeżeniu” produktu obsługa jest szybsza i bardziej intuicyjna. Ponadto użytkownik może teraz korzystać z trzech skrzynek odbiorczych służących

do odbioru komunikatów alarmowych. Komunikaty mogą być automatycznie przesyłane do jednej z tych skrzynek, w zależności od stopnia ważności, lub ręcznie przenoszone przez operatora metodą „przeciągnij i upuść”, co znacznie przyspiesza obsługę. Skrzynki odbiorcze są konfigurowalne. Można określać pojemność skrzynek. Pojawiają się one na ekranie jedynie w przypadku nadejścia komunikatu o zdarzeniu.

BIS to modułowy system zarządzania bezpieczeństwem, który można skonfigurować zgodnie z wymaganiami danego użytkownika. Poszczególne moduły integrują podsystemy, takie jak system monitoringu wizyjnego, system sygnalizacji włamaniania, system kontroli dostępu i system sygnalizacji pożarowej, umożliwiając użytkownikom zmniejszenie kosztów dzięki zakupieniu licencji na tylko te funkcje, które są im potrzebne, a jednocześnie gwarantując możliwość łatwej rozbudowy, jeśli w przyszłości wymagania ulegną zmianie.

Bezpośr. inf. Bosch Security Systems



Nowe kamery marki NOVUS – seria C

Asortyment oferowanych przez AAT Holding kamer analogowych marki NOVUS został powiększony o nową serię C. Do serii tej należy dziewięć modeli kamer – plastikowe kamery kopułkowe, wandaloodporne kamery kopułkowe oraz kamery w obudowach tulejowych.

Wszystkie kamery z serii C (oprócz modelu NVC-CC2111D) wyposażono w promienniki podczerwieni, w których wykorzystano od 24 do 76 diod świecących o rzeczywistym zasięgu dochodzącym do 25 metrów. Obserwowana scena jest oświetlana równomiernie w kącie 80 lub 120 stopni – w zależności od modelu.

Kamery zostały wyposażone w mechanicznie odsuwany filtr podczerwieni (oprócz NVC-CC2111D), dzięki czemu wiernie reprodukuje kolory i mają wyższą czułość w czarno-białym trybie pracy. Przełączanie trybów jest realizowane z wykorzystaniem wbudowanego czujnika światła widzialnego.

Kamery łączą wysoką czułość (0.05 lx/F1.2) z wysoką rozdzielczością, dlatego operator systemu ma możliwość rozpoznawania szczegółów na obserwowanym obrazie. W trybie



kolorowym rozdzielczość kamer wynosi 650 TVL, natomiast w trybie czarno-białym 700 TVL.

Kamery mogą być instalowane na zewnątrz budynków, mają stopień szczelności IP66 i pracują w zakresie temperatur od -30°C do +40°C. Kamery mają predefiniowane, zoptymalizowane ustawienia i podczas montażu nie wymagają żadnych zabiegów konfiguracyjnych.

Na stronie www.novuscctv.pl mogą Państwo znaleźć materiał filmowy, w którym pokazano pracę kamer.

Bezpośr. inf. Patryk Gańko

AAT Holding

SNV-6084 i SNV-5084 firmy Samsung Techwin

Nowe wandaloodporne kamery 2MP Full HD z WiseNetIII

Kamera **SNV-6084** ma stopień odporności na udary mechaniczne IK10 oraz stopień szczelności IP66. Pracuje w temperaturach z zakresu od -50°C do +55°C. Z powyższych względów może prawidłowo działać w bardzo trudnych warunkach środowiskowych. Kamera jest niedroga, dlatego doskonale nadaje się do wykorzystania w systemach nadzoru wizyjnego na lotniskach, w portach, na parkingach czy w centrach handlowych, gdzie wymagane jest zastosowanie wielu kamer wytwarzających obrazy o wysokiej rozdzielczości i wysokiej jakości.

Zarówno moduł kamery SNV-6084, jak i grzałka mogą być zasilane metodą PoE, dzięki czemu niepotrzebne są osobne kable do zasilania punktu kamerowego i do transmisji sygnału.

Kamera SNV-6084 została wyposażona w obiektyw o ogniskowej regulowanej w zakresie od 3 mm do 8,5 mm, z silnikami sterującymi mechanizmem regulacji ogniskowej i ostrości, a także w mechanicznie odsuwany filtr promieniowania podczerwonego. Jest zgodna ze standardem ONVIF i została zaprojektowana tak, by wytwarzać kolorowe obrazy o rozdzielczości 1080p i wysokiej jakości z prędkością do 60 kl./s.



Kamera SNV-6084 ma funkcję rozszerzenia dynamiki obrazu WDR (120dB), co powoduje, że doskonale odwzorowuje na obrazie zarówno bardzo jasne, jak i bardzo ciemne obszary.

Kamera **SNV-5084** ma większość funkcji dostępnych w modelu SNV-6084, a wśród nich wydajny algorytm kompresji H.264, opcjonalną kompresję MJPEG oraz możliwość transmisji maksymalnie dziewięciu fragmentów obrazu w niezależnie konfigurowanych strumieniach wizyjnych, co umożliwia efektywne wykorzystanie dostępnego pasma sieciowego. Rozdzielczość kamery to 1,3 megapiksela.

Inną ważną zaletą kamery SNV-6084 jest funkcja cyfrowej stabilizacji obrazu (DIS) umożliwiająca znaczne złagodzenie skutków drgań kamery spowodowanych niestabilnością konstrukcji mocującej. Z kolei funkcja DeFog może być wykorzystywana do poprawy wyrazistości obrazu w przypadku zadymienia lub w trudnych warunkach pogodowych, takich jak deszcz czy mgła. Gniazdo służące do instalacji kart SD/SDHC/SDXC umożliwia rejestrację obrazów na karcie pa-

mięci umieszczonej wewnątrz kamery. Uprawnieni użytkownicy mogą przeglądać zarejestrowane w ten sposób obrazy.

Obie kamery, zarówno SNV-5084, jak i SNV-6084, mają zaimplementowane algorytmy inteligentnej analizy treści obrazu (IVA), które poprawiają skuteczność wykrywania określonych incydentów, takich jak przekroczenie wirtualnej linii przez intruza, wejście intruza na określony obszar, opuszczenie przez intruza określonego obszaru, zniknięcie lub pojawienie się obiektu. Kamery potrafią również wykrywać próby sabotażu, takie jak zamalowanie obiektywu czy nagła zmiana pola widzenia. Procesor WiseNetIII ma funkcję inteligentnej detekcji ruchu, która została opracowana w celu znacznego zredukowania liczby nieuzasadnionych alarmów. Kamery mają zdolność odróżnienia poruszających się obiektów od ruchomego tła, jakim mogą być na przykład liście drzew poruszane wiatrem.

Kamery SNV-6084 i SNV-5084 dołączają do 13 innych modeli z układem WiseNetIII. Kamery te powstały jako efekt badań rynkowych, które miały na celu określenie wymagań użytkowników i instalatorów wobec kamer IP o wysokiej rozdzielczości – zarówno w przypadku budowy nowego systemu nadzoru wizyjnego, jak i w przypadku modernizacji systemu istniejącego.

Bezpośr. inf. David Solomons

DRS Marketing

Nowe dekodery z serii VIDEOJET

Bosch Security Systems wprowadza na rynek dwa nowe dekodery z serii **VIDEOJET**. Urządzenia umożliwiają przesyłanie strumieni wizyjnych z kamer sieciowych i wyświetlanie obrazów na dużych, płaskich ekranach lub w systemach wielomonitorowych. Zachowana jest przy tym wysoka jakość obrazu i nie jest wymagane użycie dodatkowego sprzętu i oprogramowania.

Przejsie z technologii analogowej na cyfrową nie musi być kosztowne. Dzięki nowym dekoderym **VIDEOJET 3000** i **VIDEOJET 7000** firmy Bosch zakup dodatkowego sprzętu komputerowego i oprogramowania do przetwarzania sygnału wizyjnego nie jest już konieczne.

Obecnie jednym z najtrudniejszych zadań systemów wizyjnych jest przesyłanie obrazu o wysokiej jakości z nowoczesnych kamer sieciowych na ekrany analogowe. Dekoder **VIDEOJET 3000** potrafi temu sprostać. Pozwala na pełne dekodowanie obrazów HD przesyłanych za pośrednictwem sieci IP skompresowanych metodą H.264, a także wyświetlanie zdekodowanych obrazów z szybkością 60 klatek na sekundę, w standardzie PAL, NTSC lub HD. Urządzenie umożliwia dekodowanie jednego strumienia wizyjnego w trybie pełnoekranowym lub czterech strumieni o standardowej rozdzielczości na ekranie podzielonym na cztery części.

Dekoder VIDEOJET 3000 ma interfejs HDMI, co umożliwia bezpośrednie połączenie go z urządzeniem wyświetlającym, na przykład płaskim ekranem cyfrowym, i wyjście kompozytowe BNC, dzięki któremu można podłączyć go również do monitora analogowego. Urządzenie umożliwia nie tylko deko-



dowanie strumieni wizyjnych, ale także obsługę kanału dźwiękowego i klawiatury. Dzięki możliwości integracji dekodera z klientami wizyjnymi oraz systemami zarządzania sygnałem wizyjnym **VIDEOJET 3000** sprawdza się w różnej wielkości instalacjach – od małych systemów indywidualnych do dużych, rozproszonych instalacji z centralnym sterowaniem.

Dekoder VIDEOJET 7000 umożliwia wyświetlanie obrazów o wysokiej oraz standardowej rozdzielczości, pochodzących z kamer sieciowych lub urządzeń kodujących. Dekoder ma wszystkie funkcje modelu 3000, a ponadto umożliwia bezpośrednie sterowanie dwoma wyświetlaczami HD z niezależnie skonfigurowaną strukturą ekranu. Dzięki temu jest szczególnie polecany do obsługi systemów wielomonitorowych z płaskimi ekranami.

Model 7000 pozwala na dekodowanie strumieni wizyjnych o różnych rozdzielczościach, a także na skalowanie i pre-

zentowanie obrazów z zachowaniem najwyższej ostrości, niezależnie od żądanej struktury ekranu.

Nowe dekodery upraszczają proces transmisji obrazów. Dzięki temu osoby obsługujące system mogą skoncentrować się na prezentowanych treściach, a nie na nadzorowaniu jakości technicznej obrazu. To z kolei zwiększa szybkość ich reakcji na ewentualne zagrożenia.

Z dekoderymi **VIDEOJET** zintegrowane jest oprogramowanie operacyjne oraz oprogramowanie **VideoSDK5 Monitorwall** pracujące w standardzie HD. Oba programy zostały zoptymalizowane i przystosowane do dekodowania obrazu o wysokiej rozdzielczości. Można je pobrać zdalnie, dzięki czemu instalacja i aktualizacja systemu jest bardzo prosta. Dekodery **VIDEOJET 3000** i **VIDEOJET 7000** zastępują modele **VIP-XD** oraz **VIP-XDHD**.

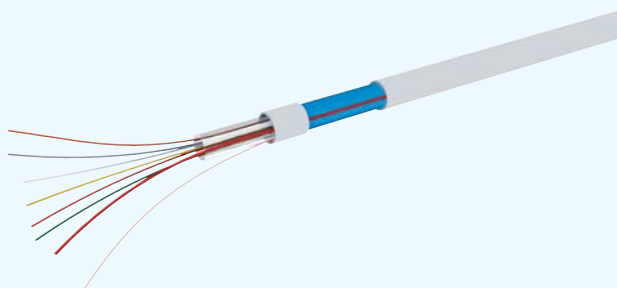
*Bezpośr. inf. Bosch Security Systems
Opracowanie: Redakcja*

Rynek oczekuje pełnej oferty kabli bezpośrednio od producenta

Firma **C&C Partners** wprowadza do swojej oferty nowe kable telefoniczne **SecurityNET**, a także kable do systemów zabezpieczeń jednego z czołowych producentów kabli, firmy **Twentsche Kabel Holding**, do której należy C&C.

Seria **SecurityNET** obejmuje kable skrętkowe, żelowane, koncentryczne do systemów telewizji dozorowej i telewizji satelitarnej, alarmowe i pożarowe.

Bezpośr. inf. C&C Partners



Rozpoznawanie tablic rejestracyjnych

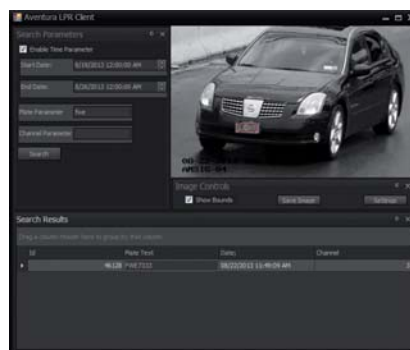
Amerykańska firma **Aventura Technologies** wprowadziła do swojej oferty oprogramowanie umożliwiające **rozpoznawanie tablic rejestracyjnych** samochodów.

Obraz może pochodzić z kamery analogowej albo cyfrowej i obejmować kilka pasów ruchu. Wszystkie zarejestrowane numery tablic są archiwizowane. Można w łatwy sposób ustalić, kiedy konkretny

samochód znajdował się w polu widzenia kamery.

Oprogramowanie rozpoznaje pojazdy poruszające się z prędkością do 240 km/h z dokładnością sięgającą 99%. Czas potrzebny na identyfikację tablicy rejestracyjnej wynosi 0,2 sekundy.

Oprogramowanie jest na tyle elastyczne, że rozpoznaje czcionki łacińskie, arabskie, chińskie oraz cyrylicę.



Więcej informacji na ten temat można uzyskać w firmie ZBAR oraz na stronie www.zbar.com.pl.

Krzysztof Witczak, Karolina Zasada
ZBAR



SND-6011R firmy Samsung Techwin Kopułkowa kamera sieciowa 2 MP Full HD z WiseNetIII i oświetlaczem IR

Ekonomiczna kamera **SND-6011R** doskonale sprawdzi się w systemach monitorowania instalowanych w szkołach, szpitalach, biurach oraz punktach sprzedaży detalicznej, których budżet jest znacznie ograniczony, lub gdy wymagane jest wykorzystanie dużej liczby punktów kamerowych dostarczających megapikselowe obrazy o wysokiej jakości.

SND-6011R dołącza do dziewięciu innych modeli kamer wykorzystujących układ DSP WiseNetIII. Został on opracowany przez firmę **Samsung** po przeprowadzeniu badań rynkowych, które pozwoliły określić, jakie funkcje, zdaniem użytkowników produktów Samsung Techwin, powinny mieć kamery sieciowe HD, aby stać się produktami preferowanymi zarówno w przypadku budowy nowego systemu nadzoru wizyjnego, jak i w przypadku modernizacji systemu istniejącego.

Kamera SND-6011R jest zgodna z ONVIF i została wyposażona w obiektyw o stałej ogniskowej równej 3,8 mm oraz mechanicznie odsuwany filtr promieniowania podczerwonego. Zaprojektowano ją tak, aby wytwarzała wysokiej jakości obrazy o rozdzielczości Full HD (1080p) z prędkością do 60 kl./s. w rozdzielczości Full HD (1080p). Dzięki wbudowanym diodom IR LED obiekty w odległości do dziesięciu metrów od kamery są widoczne nawet w całkowitej ciemności.

SND-6011R wykorzystuje wydajną metodę kompresji obrazu H.264 oraz standardową metodę MJPEG. Kamera ma funkcję transmisji wielu niezależnych strumieni wizyjnych, w których zakodowane

są jedynie fragmenty obrazu obserwowanej sceny, przy czym każdy z tych fragmentów może być transmitowany z inną rozdzielczością i inną liczbą klatek na sekundę. Umożliwia to efektywne wykorzystywanie dostępnego pasma sieciowego.

Jedną z kluczowych właściwości kamer SND-6011R jest szeroki zakres dynamiki obrazu (WDR) dochodzący nawet do 120 dB, który powoduje, że kamery te znakomicie nadają się do obserwacji obszarów ze sztucznym oświetleniem o dużym natężeniu oraz pomieszczeń o przeszkolonych ścianach. Kamery SND-6011R mają wbudowane gniazda na karty SD/SDHC/SDXC, co umożliwia rejestrację obrazu i dźwięku bezpośrednio w kamerach oraz zdalne pobieranie tak utworzonych nagrań.

Kamery SND-6011R mają funkcję inteligentnej analizy treści obrazów (IVA), która pomaga w wykrywaniu określonych incydentów, takich jak przekroczenie wirtualnej linii przez intruza, wejście intruza na określony obszar, opuszczenie przez intruza określonego obszaru, zniknięcie lub pojawienie się obiektu. Kamery potrafią również wykrywać próby sabotażu, takie jak zamalowanie

obiektywu czy nagła zmiana pola widzenia. Procesor WiseNetIII ma funkcję inteligentnej detekcji ruchu, która została opracowana w celu znacznego zredukowania liczby nieuzasadnionych alarmów. Kamery mają zdolność odróżnienia poruszających się obiektów od ruchomego tła, jakim mogą być na przykład liście drzew poruszane wiatrem.



Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: Redakcja

OPTEX oferuje kolumny z zamontowanymi barierami podczerwieni



Barierę podczerwieni zamontowaną w kolumnach wykorzystywane są w ochronie obwodowej obiektów wysokiego ryzyka. Wybór takiego sposobu montażu ma wpływ na podwyższenie poziomu bezpieczeństwa – trudno ustalić przebieg i oszacować liczbę wiązek podczerwieni, jeżeli nadajniki i odbiorniki są ukryte pod jednolitą pokrywą.

Zamontowanie standardowych barier w specjalnych kolumnach zajmuje sporo czasu, szczególnie w rozbudowanych instalacjach, dlatego OPTEX – japoński producent wysokiej jakości barier podczerwieni – przygotował gotowe rozwiązanie. W ofercie dystrybutorów są dostępne gotowe do instalacji kolumny o wysokości 150–300 cm, wyposażone w zestawy składające się z 2–4 barier o zasięgu do 200 m. Można także zamawiać kolumny z zamontowanymi 16-wiązkowymi barierami REDNET.

W zestawie znajduje się także zasilacz 230 V, do którego można przyłączyć akumulator, podgrzewacze z termostatem i wentylatorem wymuszającym obieg powietrza wewnątrz kolumny oraz panel zacisków służący do połączenia zespołu barier z centralą alarmową.



Kolumny można wyposażyć w dodatkowe czujniki wspinań, podstawy montowane w fundamencie betonowym oraz wsporniki i odcigi stabilizacyjne.

OPTEX Security zapewnia wsparcie techniczne przy konfiguracji kolumn oraz dopasowywaniu ich do wymagań obiektu.

*Bezpośr. inf. Jacek Wójcik
OPTEX Security*

Public Security Exhibition – podsumowanie



25 września w siedzibie Ambasady Brytyjskiej w Warszawie odbyła się **Public Security Exhibition (PSE Warsaw 2013)** – wystawa sprzętu wykorzystywanego przez służby bezpieczeństwa publicznego oraz służby biorące udział w akcjach ratowniczych w przypadkach klęsk żywiołowych i ataków terrorystycznych.

Zwiedzający mieli okazję obejrzeć miniaturowe kamery telewizyjne, które były ukryte w dość niecodzienny sposób, na przykład w butelce pełnej Coca-Coli, kamuflowane urządzenia radiokomunikacyjne wykorzystywane przez tajnych agentów, a także sprzęt diagnostyczny i dozymetryczny wykorzystywany do badań skażonych terenów. Osobną kategorię stanowiły maski ochronne i odzież robocza dla służb ratowniczych.

*Andrzej Walczyk
Redakcja*

Zapraszamy do obejrzenia fotorelacji na www.zabezpieczenia.com.pl.



Nowe kamery marki NOVUS – seria F



Na rynku pojawiły się **kamery analogowe serii F** marki **Novus**. Seria obejmuje 11 modeli kamer – plastikowe kamery kopułkowe, wandaloodporne kamery kopułkowe oraz kamery w obudowach. Kamery mogą pracować na zewnątrz budynków w zakresie temperatur od -30°C do $+40^{\circ}\text{C}$ lub od -30°C do $+50^{\circ}\text{C}$ (w zależności od modelu) i mają obudowy o stopniu szczelności IP65 lub IP66.

Kamera NVC-FDN3310H/IRH-2 ma dodatkowo wbudowaną grzałkę. Większość kamer została wyposażona w promienniki podczerwieni, a kamera NVC-FDN3310H/IRH-2 ma dwie diody LED dużej mocy, zasięgu 30 m i kącie świecenia 90 stopni. Intensywność świecenia diod można regulować za pomocą pokrętła.

Wszystkie kamery realizują przełączanie trybu pracy (kolorowy/czarno-biały) z wykorzystaniem czujnika światła widzialnego.

Do serii F należą modele z funkcją dzień/noc realizowaną elektronicznie (oznaczenie „FC” w nazwie), modele z mechanicznie odsuwanym filtrem podczerwieni (oznaczenie „FDN” w nazwie) oraz modele z obiektywami o stałej ogniskowej (równej 3,6 mm) i zmiennej ogniskowej (regulowanej w zakresie 2,8–11 mm lub 2,8–12 mm).

Kamery generują wysokiej jakości obraz o rozdzielczości 650 TVL w trybie kolorowym i 700 TVL w trybie czarno-białym. Wbudowany procesor DSP pozwala na zmianę ustawień w ekranowym menu. Kamery mają zaawansowane funkcje obróbki obrazu (m.in. poszerzanie zakresu dynamiki, kompensacja tylnego oświetlenia, redukcja szumów, redukcja skutków oślepienia kamery, definiowanie stref prywatności i detekcja ruchu w obrazie).

Na stronie www.novuscctv.pl mogą Państwo prześledzić pracę tych kamer.

Bezpośr. inf. Patryk Gańko
AAT Holding

Konferencja firm EBS i Orange – podsumowanie

Jak co roku firma **EBS**, znany na całym świecie producent i dystrybutor rozwiązań z dziedziny zabezpieczeń, we współpracy z firmą Orange, międzynarodowym operatorem sieci komórkowych, zorganizowała konferencję dla polskich przedstawicieli branży zabezpieczeń.

Cyklicznie organizowane przez EBS konferencje mają na celu nie tylko promocję własnych produktów, ale również merytoryczne dyskusje, poszerzenie wiedzy i wymianę doświadczeń. Co roku w konferencjach biorą udział firmy zewnętrzne. W tym roku odbyły się prezentacje firmy Motoguard z Poznania oraz firmy Gemalto, producenta modemów stosowanych w części urządzeń EBS.

Na konferencji zaprezentowano m.in. odbiornik GPS, który występuje już w trzech konfiguracjach z identyfikatorem

RFID oraz lokalizatorem GPS, a także aplikację ActiveView działającą w sieci WWW i obsługującą zarówno urządzenie ActiveGuard, jak i Active Track.

Bezpośr. inf. Agnieszka Bilaska-Gazda
EBS



Axis na Shopping Center Forum 2013 – podsumowanie

W dniach 18–19 września br. na warszawskich targach Shopping Center Forum firma **Axis Communications** zaprezentowała system wizyjny służący do optymalizacji procesów biznesowych w handlu detalicznym. Oferta jest adresowana do inwestorów budujących obiekty handlowe oraz do najemców dzierżawiących takie obiekty. Na stoisku był obecny **Johan Akesson** – dyrektor Działu Rozwoju Sektora Handlu Detalicznego w firmie Axis – oraz przedstawiciele firm partnerskich – **Top-Key** z Gdańska i **Axxon** z Moskwy.

Kluczową funkcją, która jest wykorzystywana do optymalizacji procesów handlowych, jest zliczanie klientów i dostarczanie danych dotyczących ich przemieszczania się po obiekcie. System firmy Axis wyznacza obszary, przez które przechodzi najwięcej osób, ustala miejsca, w których klienci zwalniają lub na chwilę się zatrzymują (tak zwane *dwell zones*), miejsca, w których się gromadzą, itp. System zbudowany z urządzeń Axis współpracuje ze specjalistycznym oprogramowaniem partnerów tej firmy służącym do obróbki strumieni wizyjnych wytwarzanych przez kamery. W efekcie system generuje szczegółowe raporty, które są wykorzystywane przez menedżerów handlowych do efektywnego zarządzania podległymi jednostkami.

Innowacyjność oferowanego rozwiązania polega na tym, że w systemie nie jest wykorzystywana żadna jednostka centralna. Moc obliczeniowa procesorów służących do obróbki obrazów w kamerach Axis jest na tyle duża, że mogą one obsługiwać wszystkie aplikacje niezbędne do działania systemu. Uzyskane w ten sposób dane liczbowe są przekazywane do serwera, który może być zainstalowany w dowolnym



miejscu, nawet z dala od obsługiwanego obiektu. Do tego samego serwera doprowadzane są dane z wielu urządzeń analitycznych oraz z kas i magazynów, dzięki czemu można dokładnie zbadać przebieg procesu sprzedaży. Dla kadry menadżerskiej dostępne są zarówno dane historyczne z dowolnych przedziałów czasowych, jak i aktualne, bieżące dane pochodzące wprost z obiektu.

Optymalizacja procesu handlowego polega między innymi na eliminacji kolejek przy poszczególnych stoiskach i przy kasach oraz na uzupełnianiu eksponowanych towarów w miarę ich ubywania. Analizowany może być wpływ sposobu rozkładania towarów na ruch klientów, a tym samym na ich zainteresowanie poszczególnymi ekspozycjami. Obrazy z tych samych kamer mogą być wykorzystywane do różnych celów. Przykładowo, mogą być wykrywane miejsca, w których rozlał się jakiś płyn, czy miejsca śliskie, omijane przez klientów, które powinny być możliwie szybko uporządkowane. Precyzyjne informacje dotyczące liczby osób przebywających w obiekcie mogą być wykorzystane w sytuacjach krytycznych, gdy konieczna jest szybka ewakuacja.

W efekcie działania systemu oferowanego przez firmę Axis możliwe jest uzyskanie danych niezbędnych do świadomego zarządzania obiektem handlowym, co przekłada się na wzrost obrotu i spadek kosztów związanych z działalnością obiektu. Możliwe jest także tworzenie analiz dotyczących ruchu klientów w różnych obiektach handlowych o podobnym charakterze. Tym samym możliwa jest ocena sprawności działania personelu zatrudnionych w tych obiektach. Jak widać, system oferowany przez firmę Axis jest uniwersalny i może znaleźć wiele zastosowań.

Andrzej Walczyk
Redakcja

Zapraszamy do obejrzenia fotorelacji na stronie www.zabezpieczenia.com.pl.



Ogólnopolskie Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy – podsumowanie

W dniach 10–11 października 2013 roku w Hotelu Windsor w Jachrance odbyła się druga edycja **Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy** będących kontynuacją ponad dwudziestoletnich Ogólnopolskich Szkoleń Projektowych **Schrack Seconet**.

Zgodnie z wcześniejszymi zapowiedziami spotkanie miało charakter wyłącznie szkoleniowy. W ciągu dwóch dni specjalistycznych, merytorycznych wykładów połączonych z praktycznymi warsztatami swoją wiedzę na temat zaawansowanych systemów zabezpieczeń poszerzyło ponad 400 uczestników!

Podczas merytorycznych spotkań z najlepszymi ekspertami w branży słuchacze mieli okazję zapoznać się z najnowszymi wytycznymi dotyczącymi projektowania takich systemów jak SSP, DSO, BMS, SMS, CCTV, SKD, SUG, systemów sterowania oddymianiem i wydzieleniami pożarowymi, a także systemów sieci strukturalnych. Swoje referaty wygłosili przedstawiciele najlepszych uczelni, niezależni eksperci zajmujący się problematyką systemów bezpieczeństwa oraz przedstawiciele firm partnerskich specjalizujący się w zagadnieniach dotyczących zabezpieczeń inteligentnych budynków.

Najważniejszym punktem imprezy była prezentacja działania wszystkich zintegrowanych systemów zabezpieczeń podczas pożaru. Scenariusz tej prezentacji został w tym roku rozszerzony o kilka modułów.

Uczestnicy szkolenia mogli nie tylko głębiej i pełniej zapoznać się ze specyfiką systemów zabezpieczeń w kontekście ochrony przeciwpożarowej, ale także zobaczyć, jak funkcjonują systemy zabezpieczeń budynków we wzajemnej interakcji.

Do współpracy przy organizacji szkolenia, które jest jednym z największych tego typu przedsięwzięć w branży, zostali zaproszeni producenci innych systemów: BELIMO Siłowniki –



czołowy producent napędów klap pożarowych oraz siłowników i zaworów przeznaczonych do instalacji HVAC; GAZEX – firma zajmująca się konstruowaniem, produkcją oraz propagowaniem stosowania elektronicznych urządzeń do wykrywania i pomiaru stężeń gazów toksycznych i wybuchowych; Johnson Controls International – czołowy dostawca produktów, usług oraz rozwiązań z dziedziny systemów HVAC, jak również systemów automatyki budynkowej i BMS; Schrack Technik Polska – dostawca produktów i rozwiązań z dziedziny rozdzielu energii elektrycznej oraz transmisji danych teletechnicznych; Sony Europe Limited – producent sprzętu audio, wideo, telekomunikacyjnego i informatycznego; Supo Cerber – dostawca systemów gaszenia mgłą wodną, które mogą być wykorzystywane zwłaszcza do gaszenia obiektów zabytkowych (drewnianych) oraz przemysłowych; TOA Electronics Europe – lider na rynku systemów nagłośnieniowych, komunikacyjnych i bezpieczeństwa (DSO); XTRALIS (UK) – dostawca systemów bardzo wczesnego wykrywania pożaru.

Udział w dwudniowych warsztatach został potwierdzony wspólnym certyfikatem, wystawionym przez

Schrack Seconet Polska oraz wszystkich Partnerów.

Na szczególną uwagę zasługuje fakt, że organizatorzy, podobnie jak w roku ubiegłym zadbali o stronę merytoryczną i edukacyjny charakter spotkania. W referatach przedstawicieli firm współorganizujących szkolenie nie były poruszane kwestie marketingowe.

Firma Schrack Seconet oraz wszyscy Partnerzy Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego 2013

dziękują wszystkim uczestnikom za udział w szkoleniu i już dziś zapraszają do udziału w kolejnej edycji w roku 2014.

*Bezpośr. inf. Marta Nowak
Schrack Seconet Polska*

Zapraszamy do obejrzenia fotorelacji na stronie www.zabezpieczenia.com.pl.



Systemy sygnalizacji pożarowej w ofercie firmy SATEL

18 września br. w hotelu Windsor Palace Hotel & Conference Center w Jachrance odbyła się prezentacja urządzeń firmy **SATEL** przeznaczonych do sygnalizacji pożarowej. Gości przywitali członkowie zarządu firmy – Ireneusz Kowaluk i Leszek Polakiewicz.

Dotychczas polska firma SATEL była znana jako producent systemów sygnalizacji i włamania. Jej produkty (między innymi centrale alarmowe z serii CA czy systemy MICRA, VERSA i INTEGRA) są znane na rynku polskim już od ponad dwudziestu lat. Firma SATEL od początku swego istnienia kładzie nacisk na rozwój techniczny swoich wyrobów poprzez realizowanie własnych opracowań oraz wdrażanie najnowszych technologii produkcji, w tym zautomatyzowanego montażu w technice SMD (montaż powierzchniowy elementów elektronicznych), automatycznego, wspomaganego komputerowo testowania wyrobów itp. W wyniku takich działań firma uzyskała certyfikat ISO-9001.

W ciągu ostatnich dziesięciu lat SATEL wzbogacił swoją ofertę o systemy kontroli dostępu i systemy monitorowania alarmów wykorzystujące unowocześnione i nowo opracowane centrale i moduły systemów sygnalizacji włamania. Opracowania te umożliwiają tworzenie jednorodnych instalacji ostrzegawczych od obiektu do stacji nadzorowania.

Najnowsza linia produktów firmy SATEL to elementy systemów sygnalizacji pożarowej: centrale, czujki, ręczne przyciski pożarowe, sygnalizatory oraz moduły współdziałające z systemami stanowiska nadzoru. Systemy są przewidziane dla obiektów małych i średnich. Prezentację prowadzili Maciej Domagalski (specjalista ds. szkoleń) i Adam Macholl (product manager ds. systemów sygnalizacji pożarowej).

W skład systemu sygnalizacji pożarowej firmy SATEL wchodzi obecnie dwie serie central – seria CSP-200, wyposażona w wyświetlacz ciekłokrystaliczny, i seria CSP-100, wyposażona w sygnalizację stanów i zdarzeń diodami LED znajdującymi się na panelu czołowym centrali. Obie serie central są dostarczane w wersji cztero- lub ośmioliniowej. Przyłączane są do nich konwencjonalne (czyli dwustanowe) ręczne lub automa-

tyczne detektory pożarowe. Identyfikacja miejsca powstania zagrożenia pożarem odbywa się poprzez identyfikację linii, do której przyłączono detektor sygnalizujący alarm. Każda z central ma dwa nadzorowane wyjścia prądowe, które mogą służyć na przykład do przyłączenia sygnalizatorów, cztery wejścia przeznaczone do przyłączenia urządzeń nadzorowanych oraz, w zależności od liczby linii dozorowych, cztery lub osiem nienadzorowanych wyjść przekaźnikowych o przeznaczeniu określonym przez projektanta lub instalatora systemu. Przewidziano możliwość dołączenia urządzeń do transmisji alarmu i uszkodzenia.

Urządzeniami uzupełniającymi centrale są panele wyniesione do zdalnej obsługi oraz moduł przewidziany do połączenia z komputerem, na którym zostanie zainstalowany wirtualny panel umożliwiający sygnalizowanie stanu systemu oraz jego obsługę przez sieć Ethernet.

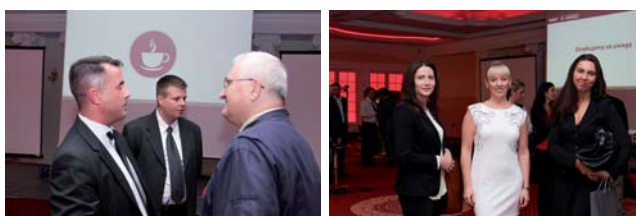
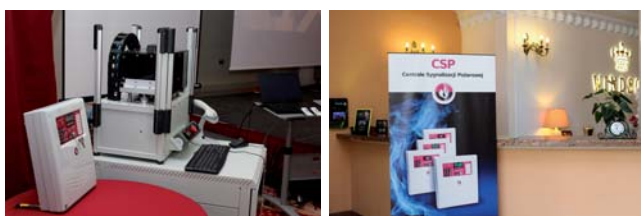
Ofertę urządzeń przeznaczonych do budowy systemów sygnalizacji alarmów pożarowych uzupełniają czujki optyczne dymu i optyczno-termiczne czujki dymu i ciepła, termiczne czujki ciepła, ręczne przyciski pożarowe (zewnętrzne i wewnętrzne). Do czujek pożarowych dostępne są podstawy zwykłe lub przemysłowe, chroniące czujki przed zalewaniem z sufitu.

Czujki dymu, aczkolwiek dwustanowe, mają ciekawą, niespotykaną w systemach konwencjonalnych właściwość polegającą na automatycznym dopasowaniu progu zadziałania do wzrastającego w miarę upływu czasu zabrudzenia komory czujki. Pozwala to na odpowiednio wczesne zasygnalizowanie konieczności wyczyszczenia czujki i uniknięcie wynikających z zabrudzenia fałszywych alarmów. Takie rozwiązanie pozwoli na przejście do następnego etapu, którym będzie zaoferowanie adresowalnych analogowych systemów sygnalizacji pożarowej.

Bezpośr. inf. Stanisław Banaszewski

Redakcja

Zapraszamy do obejrzenia fotorelacji na stronie www.zabezpieczenia.com.pl.



Spotkanie Projektantów Instalacji Niskoprądowych –



W dniach 25–26 września w Wiedniu odbyła się kolejna edycja SPIN – imprezy, w której biorą udział producenci, dystrybutorzy, projektanci i instalatorzy z branży instalacji niskoprądowych. **11. SPIN** zgromadził ponad 270 uczestników, w tym 170 projektantów, partnerów, ekspertów oraz przedstawicieli mediów.

Tegoroczną, jesienną edycję SPIN merytorycznie wspierało 25 partnerów, a wśród nich firmy: Nedap, BKT Elektronik, Drahtel, Konsorcjum FEN, OPTEX, Miwi-Urmet, Ela-compil, Salto Systems, BOSCH Robert Bosch, Unicard, Legrand, Honeywell Life Safety, European Security Trading, Software Mind, ZDANIA, HP, NEC Display Solution i Veracomp, Romi, Linc, AVAYA, C&C Partners Telecom, Elmat, Verint, Polon-Alfa, ELTCRAC.

Partnerzy podzielili się z uczestnikami swoimi doświadczeniami nabytymi podczas integracji oferowanych przez nich systemów. Przedstawienie systemów funkcjonujących wzbogaciło teoretyczną stronę prezentacji.

– *Dla nas jako organizatora spotkań bardzo istotne są zarówno sugestie partnerów, jak i uczestników. To na ich podstawie budujemy program kolejnych edycji. Dlatego koncepcja tegorocznego 11. SPIN uwzględniała m.in. case study. Odpowiedzią na sugestie uczestników była również możliwość konsultacji z ekspertami z branży niskich prądów reprezentującymi różnorodne dziedziny: od multimediów, przez teleinformatykę, po systemy sygnalizacji pożarowej i systemy automatyki – podsumowała prezes firmy LOCKUS Magdalena Kniszner.*

Panele eksperckie stały się już nieodłączną częścią SPIN. W trakcie tej edycji uczestnicy mieli okazję wziąć udział w czterech zróżnicowanych tematycznie sesjach.

Wygłoszono następujące referaty:

- *Pojęcie równoważności w przetargach publicznych na budowę systemów teleinformatycznych (Piotr Zychowicz),*
- *Gdzie kończy się wysoka rozdzielczość? Czyli przyszłość projektowania systemów multimedialnych (dr inż. Grzegorz Augustyn),*
- *Współpraca instalacji użytkowych z instalacją sygnalizacji pożarowej – zasady sterowań i zasilania, przykłady praktyczne (mł. bryg. mgr inż. Edward Skiepmo),*
- *Ocena wpływu systemów automatyki na efektywność energetyczną budynków w świetle normy PN-EN 15232 (mgr inż. Paweł Kwasnowski).*



podsumowanie



Panelom merytorycznym towarzyszyły prezentacje systemów na stoiskach wystawienniczych. Partnerzy 11. SPIN mieli okazję wykazać się inwencją i pomysłowością podczas planowania stoisk. Po raz pierwszy w historii SPIN odbył się konkurs na najbardziej funkcjonalne i oryginalne stoisko wystawiennicze – „SPIN-owisko”. Stoiska firm Unicaard, C&C Partners, BKT Elektronik oraz Miwi Urmet zostały ocenione przez uczestników najwyżej.

*Bezpośr. inf. Magdalena Skórkiewicz-Foltyn
Lockus*

Nowa metalowa obudowa ME-5 do urządzeń systemu kontroli dostępu



Fot. Kontrolery, zasilacz oraz akumulator widoczne na fotografii nie wchodzą w skład ME-5

Firma **ROGER** wprowadziła do swojej oferty **obudowę ME-5**. Obudowa ta jest wyposażona w cztery szyny montażowe T 35 mm i czujnik antysabotażowy drzwiczek. Jest w niej miejsce na zasilacz buforowy oraz akumulator 12 V/17 Ah. Może pomieścić dziewięć kontrolerów typu PR402DR-12VDC lub osiemnaście kontrolerów typu PR102DR. Obudowa jest dostępna również w zestawie ME-5-S z dozorowanym zasilaczem buforowym 13,8 V/11 A oraz modułem dystrybucji napięcia.

Bezp. Inf. ROGER



Intelligent Building Technologies & Multimedia Management 2013

– podsumowanie

Redakcja *Zabezpieczeń* została zaproszona do udziału w odbywającej się w Krakowie, w dniach 16–18 października, pierwszej międzynarodowej konferencji *Intelligent Building Technologies & Multimedia Management (IBTMM)*, jako jeden z jej patronów medialnych. Organizacja konferencji wynikała z połączenia pod wspólnym zarządkiem, w jednym miejscu i w tym samym czasie trzech konferencji:

- 7th Congress on Intelligent Building Systems InBuS 2013,
- 10th International Conference New Building Technologies & Architectural Design NBTAD 2013,
- 1st Integrated Multimedia Systems Conference IMSC 2013.

Organizatorami IBTMM 2013 byli: AGH w Krakowie, Politechnika Krakowska, Emmerson Lumico, Lockus, Fundacja dla AGH, WFO-ŚiGW, Województwo Małopolskie.

Przedsięwzięcie to, ze wszech miar trudne pod względem organizacyjnym, naukowym i technicznym, podjęto pod wspólnym hasłem: „zapewnić zrównoważony rozwój budynków i przestrzeni, w tym oddziaływań technicznych, środowiskowych i multimedialnych”.

Czy osiągnięto ten cel? W tej chwili trudno to jednoznacznie stwierdzić. Naukowe referaty, materiały oraz praktyka inżynierska, zarządcza i architektoniczna potwierdzają potrzebę takiego zrównoważonego rozwoju. Rozwój inteligentnego budownictwa w połączeniu z dbałością o estetykę zagospodarowania przestrzeni i środowisko naturalne jest korzystna dla wszystkich. Sygnalizowana oraz wdrażana innowacyjność w nauce i praktyce to nowoczesne rozwiązania techniczne połączone z efektywnym finansowaniem oraz transferem

poszczególnych technologii między współpracującymi stronami.

- Na obradach poruszano następujące zagadnienia:
- planowanie inteligentnych budynków wraz z ich nowoczesną architekturą, wkomponowanych medialnie w otoczenie, przyjaznych ludziom i ziemi;
 - zarządzanie i sterowanie prowadzące do uzyskania bezpieczeństwa technicznego, technologicznego, architektonicznego, zrównoważonego z potrzebami i oczekiwaniami użytkowników inteligentnych budynków;
 - projektowanie budynków z wykorzystaniem nowych technologii, a zarazem z rozsądnym podejściem do ograniczeń prawno-normatywnych, czyli z uwzględnieniem bezpieczeństwa nie tylko w jego technicznym aspekcie;
 - wykorzystanie nowoczesnych środków i sposobów oddziaływań multimedialnych na rzecz użytkowników budynków, ich bezpieczeństwa wewnątrz i na zewnątrz obiektów.



W ramach poszczególnych paneli (sesja główna i sesje programowe), w ponad stu referatach i prezentacjach sponsorskich, przedstawiono nie tylko wizje rozwoju nowoczesnych technik zarządzania, ale także już funkcjonujące systemy oraz pozytywne skutki dostosowywania starych obiektów do wymagań współczesnych w ramach działań rewitalizacyjnych. Omawiano różnorodne rozwiązania rodem z Hiszpanii (Technical University of Madrid), Stanów Zjednoczonych (University of Kansas), Niemiec (Universität Osnabrück) i Kazachstanu (Eurasian National University-Astana). Omawiano problemy i dzielono się doświadczeniami zdobytymi przez projektantów i wykonawców na różnych rynkach budowlanych: polskim, brytyjskim, niemieckim, ukraińskim. Przedstawiano aktualne problemy związane z ekologią („zielone budynki”) i bezpieczeństwem energetycznym obiektów (unijna dyrek-

tywa EPBD oraz norma EN 15232:2012) w warunkach projektowania nowych systemów budynkowych i budynków użyteczności publicznej (w celu osiągnięcia maksymalnej efektywności energetycznej przy zachowaniu wszystkich opcji zarządzania bezpieczeństwem obiektu w świetle zalecanych i obowiązujących norm).

Na konferencji omówiono także wykorzystanie sztucznej inteligencji w zarządzaniu budynkami (INBUS 2013), uzyskiwanie trwałości i niezawodności obiektów dzięki nowym systemom budowlanym (NBTAD 2013) oraz wiarygodność komunikacji wizyjnej w środowiskach sieciowych (IMSC 2013), wskazując zarazem na dotychczasowe osiągnięcia z tego zakresu.

Ewenementem był nowoczesny pokaz „Universum” zrealizowany w komorze Staszica w kopalni soli w Wieliczce (komora ma wysokość 36 m) z wykorzystaniem możliwości współczesnych technik i technologii multimedialnych. Uczestników zaproszono do „podróży w czasie” – pokazano historyczne techniki wydobycia oraz warunki pracy w żupie solnej. Ostatniego dnia konferencji (18 paź-

dziernika) wszyscy zgłoszeni chętni mogli zapoznać się z systemem BMS zastosowanym w Kampusie 600-lecia Odnowienia Uniwersytetu Jagiellońskiego oraz uczestniczyć w sesji panelowej.

Warto wspomnieć o ciekawych wystąpieniach i prelekcjach sponsorów, a także o stoiskach firmowych i prezentacjach plakatowo-multimedialnych na parterze, antresoli i pierwszym piętrze hotelu, w którym odbywała się konferencja. Wszystkie stoiska były bogato wyposażone w udostępniane zainteresowanym materiały informacyjne i obsadzone przez nad wyraz kompetentnych, znających omawiane zagadnienia przedstawicieli firm.

Multikonferencja była udana, jak twierdziła większość zapytanych uczestników (choć byli i niezadowoleni), ale „jeszcze się taki nie urodził, co by wszystkim dogodził”, zatem czekamy na jej kolejną edycję.

Opracował: dr inż. Marek Blim
Redakcja

Zapraszamy do obejrzenia fotorelacji na stronie www.zabezpieczenia.com.pl.



Inteligentny Klucz – nagrody rozdane

18 października br. (na zakończenie pierwszej międzynarodowej konferencji *Intelligent Building Technologies & Multimedia Management*) w Krakowie odbyło się rozstrzygnięcie pierwszej edycji konkursu **Inteligentny Klucz**, w którym wzięli udział wykonawcy oraz integratorzy systemów automatyki budynkowej w obiektach budowlanych.

Organizatorem konkursu **Inteligentny Klucz** była krakowska firma **Lockus** specjalizująca się w organizacji konferencji i szkoleń.

Spśród projektów zgłoszonych do konkursu wybrano pięć wyróżniających się wysokim poziomem integracji systemów bezpieczeństwa, zarządzania i multimedialnych w obrębie budynku.

Statuetki **Inteligentnego Klucza 2013** otrzymały następujące firmy:

– **Fadom** (Wschodnioeuropejskie Centrum Kongresowo-Sportowe ARŁAMÓW);



- **DYSKRET POLSKA** (Centrum Biurowe VINCI w Krakowie);
- **Zdania** (Instytut Zoologii w Kampusie 600-lecia Odnowienia Uniwersytetu Jagiellońskiego w Krakowie);

W gronie finalistów wyróżnione zostały również następujące firmy:

- **bt electronics** (Hotel Galaxy w Krakowie);
- **Unima 2000 Systemy Teleinformatyczne** (Centrum Urazowe Medycyny Ratunkowej i Katastrof Szpitala Uniwersyteckiego w Krakowie);

Konkurs **Inteligentny Klucz** był podzielony na dwa etapy. Pierwszy etap obejmował przyjęcie wniosków firm realizujących projekty, weryfikację wniosków pod względem merytorycznej zgodności z założeniami regulaminu konkursu oraz kwalifikację firm do grona finalistów. W drugim etapie wybrano projekty wyróżniające się zaawansowaniem integracji systemów i przyznano statuetki **Inteligentnego Klucza**.

Bezpośr. inf.
Magdalena Skórkiewicz-Foltyn
Lockus

EBS Open Days 2013 – podsumowanie

Już po raz drugi firma **EBS** zaprosiła swoich klientów i dystrybutorów do Polski na międzynarodową konferencję. W tym roku przybyło kilkudziesięciu gości zachęconych ciekawą tematyką i polską gościnnością. 28 osób z 18 firm, z Kanady, Kolumbii, Brazylii, RPA, Francji i Litwy, aktywnie uczestniczyło w przygotowanym przez **EBS** programie konferencji.

Pierwszego dnia goście zwiedzili Warszawę, a następnie uczestniczyli w uroczystej kolacji w polskiej karczmie. Drugiego dnia odbyła się całodzienna konferencja, na której prelegentami byli przedstawiciele firm **Motoguard** i **Gemalto**.

Dni otwarte miały na celu przede wszystkim wymianę doświadczeń. Ogromne zainteresowanie imprezą, wysoki poziom

merytoryczny, liczne pytania i dyskusje na konferencji świadczą o tym, jak bardzo potrzebne są takie spotkania. Żywym zainteresowaniem cieszyły się prezentacje naszych partnerów z Kolumbii, Niemiec oraz Francji, które dotyczyły tamtejszych rynków oraz współpracy z **EBS**.

Przedstawiciele firmy **EBS** zaprezentowali m.in. nowe produkty, takie jak czytnik linii papilarnych **FPX** oraz całą gamę urządzeń **GPS**, w tym **Active Track** z **RFID** oraz **GPS** do śledzenia naczep samochodowych.

Bezpośr. inf. Agnieszka Bilka-Gazda
EBS



Forum Monitoringu Polskiego – podsumowanie

W dniach 3–4 października 2013 roku na terenie Domu Polonii w Pułtusku odbyła się dwudniowa sesja piętnastego **Forum Monitoringu Polskiego** zorganizowana przez stowarzyszenie **POLALARM**. Patronat honorowy nad imprezą objął Generalny Inspektor Ochrony Danych Osobowych dr Wojciech Rafał Wiewiórowski. Program forum obejmował trzy podstawowe zagadnienia, to jest podstawy prawne, aspekty normatywne i kierunki rozwoju technicznych systemów zabezpieczających. Uczestnikami byli przedstawiciele krajowych firm zajmujących się projektowaniem i instalacją elektronicznych systemów zabezpieczających, a także przedstawiciele przodujących producentów i dystrybutorów

sprzętu służącego do budowy takich systemów. Podczas trwania sesji wygłoszonych zostało kilkanaście referatów. Głos zabrali znani eksperci i doświadczeni praktycy z branży zabezpieczeń. Wśród zagadnień technicznych dominowała technika telewizyjna, jednak nie zabrakło referatów na temat łączności radiowej, nowoczesnych czujek ruchu, a także ochrony danych osobowych. Swoimi doświadczeniami podzielili się także przedstawiciele władz lokalnych, którzy do dziś analizują przyczyny i przebieg tragicznej powodzi, jaka miała miejsce w Pułtusku w 1979 roku. Imprezę uświetniła uroczysta kolacja w sali zamkowej.

Redakcja

Zapraszamy do obejrzenia fotorelacji na stronie www.zabezpieczenia.com.pl.



SAP 2013 – XXI Ogólnopolskie Warsztaty „Sygnalizacja i automatyka pożarowa” – podsumowanie

W dniach 19–21 września br., w gościnnych progach Centrum Kongresowo-Szkoleniowego Magellan, już po raz dwudziesty pierwszy firma **Polon-Alfa** zorganizowała **Warsztaty SAP 2013** – jedną z największych tego typu imprez w Polsce. Rosnące z roku na rok zainteresowanie Warsztatami dowodzi, że specjaliści z szeroko rozumianej branży zabezpieczeń nieustająco spragnieni są wiedzy przekazywanej przez najlepszych fachowców.

Niezwykle ciekawy temat wiodący, przygotowany przez organizatorów *Instalacje sygnalizacji pożarowej – metody ochrony specyficznych obiektów*, zgromadził 220 uczestników, którzy z ogromną uwagą wysłuchali wygłaszanych referatów i z takim samym zainteresowaniem przyglądali się prezentacjom.

Wiele obiektów, zwłaszcza przemysłowych, ze względu na specyfikę produkcji czy stosowane procesy technologiczne, narażonych jest na wpływ niekorzystnych warunków środowiska.

Jak pracują, w niekiedy bardzo specyficznych warunkach, systemy wykrywania i sygnalizowania pożaru? Jakie metody ochrony zastosować? Jakie rozwiązania wybrać? Jaki wpływ na istniejący w obiekcie system sygnalizacji pożarowej ma jego przebudowa lub modyfikacja? Jakie warunki należy spełnić, by system dalej działał niezawodnie?

Wszystkie te pytania, które sygnalizują trudności napotymane nawet przez bardzo doświadczonych projektantów i instalatorów, znalazły odpowiedzi podczas wykładów i kuluarowych rozmów prelegentów i uczestników spotkania.

Omówione zostały również istotne zagadnienia projektowe związane z wykorzystaniem w instalacjach sygnalizatorów akustycznych i optycznych oraz nowe zalecenia dotyczące systemów monitoringu pożarowego. Duże zainteresowanie wzbudziło przedstawienie konsekwencji wejścia

w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 305/2011, regulującego zasady wprowadzania na rynek wyrobów budowlanych. Przedstawiono także możliwości stosowania niecertyfikowanych urządzeń w instalacjach sygnalizacji pożarowej.

Uczestnicy Warsztatów wysłuchali następujących referatów:

- *Czy istnieje możliwość instalowania sygnalizatorów optycznych/akustycznych na liniach dozorowych central sygnalizacji pożarowej?* (Jerzy Ciszewski – ITB, Warszawa);
- *Koncepcje ochrony wybranych obiektów w trudnych warunkach środowiskowych – oddziaływanie środowiska pracy na instalację* (Janusz Sawicki – ITB, Warszawa);
- *Aspekty praktyczne oceny i weryfikacji stałości właściwości użytkowych wyrobów służących do ochrony przeciwpożarowej wg CPR* (Tomasz Kielbasa – CNBOP PIB, Józefów);
- *Zasady stosowania w instalacjach sygnalizacji pożarowej urządzeń niecertyfikowanych* (Paweł Stępień – CNBOP PIB, Józefów);
- *Wymagania techniczne dla systemów sygnalizacji pożarowej i transmisji alarmów* (Piotr Wojtaszewski – KG PSP, Warszawa).

Inżynierowie wsparcia technicznego Polon-Alfa wygłosili referaty, które wzbudziły ogromne zainteresowanie:

- *System sygnalizacji pożarowej POLON 6000 – centrale o architekturze rozproszonej* (Mariusz Radoszewski);
- *Projektowanie instalacji w oparciu o system POLON 6000 – współpraca z innymi systemami* (Krzysztof Marchlewski).

Tradycyjnie zaprezentowane zostały nowości wprowadzane na rynek, a wśród nich m.in.:

- 1) System POLON 6000, wykorzystujący centrale o architekturze rozproszonej, który został specjalnie zaprojektowany





do ochrony dużych obiektów, złożonych lub rozproszonych na rozległym terenie, z dużą liczbą współdziałających urządzeń automatyki pożarowej (czyli ze złożonymi scenariuszami zdarzeń), tzw. inteligentnych budynków, dużych zakładów przemysłowych itp. Centrala POLON 6000 może pracować z nowymi elementami liniowymi szeregu 6000, jak i z elementami szeregu 4000.

- 2) Wielosensorowa czujka DTC-6046. Jest to czujka pożarowa z detektorami dymu, ciepła i tlenku węgla, która jest najbardziej zaawansowanym urządzeniem spośród nowych czujek wprowadzanych do oferty firmy Polon-Alfa. Czujka jest przeznaczona do stosowania w ramach systemów POLON 4000 i POLON 6000.
- 3) Czujka ciepła TUN-6046, pracująca w systemie POLON 6000, z nowymi funkcjami, które umożliwiają m.in. określenie jej lokalizacji na pętli dozorowej.
- 4) Elementy kontrolno-sterujące serii EKS-6000, które umożliwiają synchronizowane i grupowane przełączanie wyjść, impulsowe działanie i ustawianie bezpiecznej pozycji przekaźników i trzystanową kontrolę wejść. Dodatkowo elementy te są programowane w całkowicie zmieniony sposób, który umożliwia elastyczne powiązania scenariuszy pożarowych.
- 5) Rodzina sygnalizatorów akustycznych SAW-6000 – adresowalnych i konwencjonalnych, tonowych i z możliwością rozgłaszania zaprogramowanych komunikatów głosowych.
- 6) Trójpasmowa czujka płomienia PPW-40REx – w obudowie przeciwybuchowej, przeznaczona do zastosowania w obiektach przemysłowych, w miejscach zagrożonych wybuchem.
- 7) Konwerter CM-180-29, dzięki któremu można włączyć system POLON do wszystkich systemów zarządzających, w których stosuje się protokół ModBUS.
- 8) Przyciski przewietrzania PP-61/62, włączane do central sterujących UCS 6000, które stanowią rozszerzenie oferty Polon-Alfa.

Przedstawiono także platformę integrującą VENO firmy AAT Holding, łączącą w ramach zintegrowanego systemu nadzoru obiektu instalacje sygnalizacji pożarowej, sygnalizacji włamaniowej, telewizji i kontroli dostępu.

Dla wszystkich uczestników przygotowano ponad stustronicowe wydawnictwo zawierające wszystkie referaty wygłoszone podczas warsztatów.

Dużą dawkę wiedzy, czyli coś dla ducha, trzeba było jakoś zrównoważyć, więc było też i coś dla ciała. Pierwszego wieczoru, podczas uroczystej kolacji, goście mogli wsłuchać się w przyjemne dźwięki jazzu tradycyjnego w wykonaniu zespołu The Warsaw Dixielanders. Popołudnie drugiego dnia upłynęło na rywalizacji polegającej na... budowaniu pieca, wypiekaniu w nim własnoręcznie przygotowanej pizzy i przygotowaniu lodowej rzeźby. Kreatywność uczestników konkursu przerosła najśmielsze oczekiwania organizatorów. Pyszna pizza, która w mgnieniu oka znikała w ustach reszty uczestników, fantazyjne figury lodowe przygotowane z pełną ofiarnością – to wszystko stanowiło ciekawą formę odreagowania po przedpołudniowych wykładach. W międzyczasie uczestnicy zabawy mogli podziwiać mistrza świata w rzeźbieniu w lodzie, który

wyczarował dla wszystkich podziwiających jego umiejętności i fantazję bajkową postać.

Chociaż w całej Polsce było pochmurno, a w niedalekiej okolicy padał deszcz, nad Magellanem świeciło piękne słońce, sprzyjające zarówno pogłębianiu wiedzy, jak i integracji uczestników.

Firma Polon-Alfa serdecznie dziękuje za przybycie na XXI Ogólnopolskie Warsztaty SAP 2013 wszystkim zaproszonym gościom, wykładowcom oraz uczestnikom.

Poniżej rozmowy z kilkoma z uczestników warsztatów.

Jak podoba się Panu na naszych warsztatach?

Gość 1: *Jestem na Państwa warsztatach już kolejny rok z rzędu. Cenię sobie wykłady specjalistów. Nie bez znaczenia są oczywiście również konsultacje i rozmowy w kuliurach.*

Który z wykładów najbardziej Pana zainteresował?

Bardzo zaciekały mnie informacje na temat nowego systemu, jego zastosowań w obiekcie. Czekam z niecierpliwością, aż będzie można go kupić i zainstalować.

POLON 6000 jest już w certyfikacji. Przewidujemy, że w drugim kwartale przyszłego roku centrale będą dostępne.

Bardzo podoba mi się, że system POLON 6000 będzie kompatybilny z POLON 4000. Jest to moim zdaniem problem przy wielu inwestycjach, gdy obiekt jest zabezpieczony przez konkurencję, a co kilka lat wprowadzany jest nowy system i stare elementy już po prostu nie pasują. Zresztą z przykrością muszę stwierdzić, że w przypadku starszych central Polon-Alfa jest podobnie, np. linii dozorowych ALFA 3800 nie można przepiąć bezpośrednio do nowszych central POLON 4000.

W systemie ALFA 3800 adresowalne były gniazda czujek, do tego z przelącznikami. W przypadku central POLON 4000 komunikacja z czujkami jest cyfrowa. Zresztą nie tylko czujki mogą komunikować się z centralą – centrala może komunikować się z czujkami, zmieniać ich konfigurację czy odpytywać je w celu sprawdzenia stanu układu pomiarowego.

Racja, jednak nie raz spotkałem się z tym, że przy rozbudowie obiektu trzeba było wymienić centralę POLON 4200 na POLON 4900, więc trzeba było wymienić również czujki, bo zainstalowane były czujki szeregu 4043.

Czujki szeregu 4043 nie są przewidziane do pracy z centralą POLON 4900, ze względu na ich prostszą konstrukcję i uboższy zestaw funkcji.

Już od wielu lat wykorzystuję Państwa centrale w projektach systemów sygnalizacji pożarowej. Po pierwsze dlatego, że są wysokiej jakości, po drugie – konstrukcja i łączenie elementów jest dobrze przemyślane, po trzecie – jestem dumny z tego, że centrale polskiej firmy mogą konkurować jak równy z równym z centralami zachodnich producentów. Niemniej jest parę mankamentów, które można by było poprawić w centralach następnych generacji. Na przykład warto byłoby zadbać o więcej miejsca między łączówkami, bo w takich centralach jak IGNIS 1520M jest go zdecydowanie za mało, by wygodnie przyłączać do centrali elementy systemu. Daje się to we znaki zwłaszcza wtedy, gdy trzeba wymienić jakieś elementy lub odłączyć pojedyncze przewody w obiekcie, w którym system działa już od pewnego czasu i wszystkie elementy są już przyłączone.

Przekaż te informacje konstruktorom. Na pewno uwzględnią je przy projektowaniu kolejnych urządzeń.

Wracając do warsztatów, bardzo podoba mi się występ zespołu jazzowego. To świetny pomysł. Kupiłem nawet płytę.

Jak ocenia Pan merytoryczną stronę warsztatów?

Gość 2 (instalator z Wielkopolski): *Będąc uczestnikiem spotkania już po raz kolejny, mogę z całym przekonaniem stwierdzić, że poziom merytoryczny zawsze był i jest bardzo wysoki. Myślę, że zasługą jest poruszanie innej, specyficznej tematyki w każdej kolejnej edycji. Obecność odpowiednio dobranych ekspertów umożliwia omówienie wielu problemów pojawiających się zarówno podczas instalacji, jak i w procesie projektowania systemów sygnalizacji pożarowej.*

Co mógłby Pan powiedzieć o zapowiadanych nowościach firmy Polon-Alfa?

Prezentacja zupełnie nowego systemu sygnalizacji pożarowej wywarła duże wrażenie. Nowy system stanowi bardzo duży krok do przodu. Ma duże możliwości, a jego konfiguracja jest elastyczna. Wprowadzenie go można uznać za działanie podobne do wymiany generacji TELSAP na POLON 4000 kilka lat temu.

A sama organizacja imprezy?

Organizacja warsztatów, obsługa, wsparcie organizatorów, branie przez nich pod uwagę sugestii – to wszystko jest bez zarzutu.

Co powoduje, że co roku przyjeżdża Pan na warsztaty SAP organizowane przez firmę Polon-Alfa?

Gość 3: *Regularnie, od kilkunastu lat przyjeżdżam na warsztaty w celu wysłuchania wykładów prowadzonych przez ekspertów z różnych dziedzin związanych z wykrywaniem i sygnalizacją pożaru. Na warsztaty przyciąga mnie także możliwość zawarcia nowych znajomości i poznania najznamienitszych osobistości z branży systemów sygnalizacji pożarowej.*

Jak ocenia Pan część wykładową warsztatów SAP 2013?

Część merytoryczną, jak co roku, oceniam bardzo wysoko. Eksperti poruszyli interesujące i aktualne tematy związane z systemami sygnalizacji pożarowej.

Który wykład był dla Pana najciekawszy?

Bardzo zainteresował mnie wykład pana Janusza Sawickiego na temat specjalistycznych zabezpieczeń stosowanych w przemyśle. Szczególnie przydatne dla mnie były przykłady zastosowania liniowych czujek ciepła i systemów zasysających w instalacjach przemysłowych.

Jak ocenia Pan wystawę urządzeń?

Ciekawie zapowiada się nowy system POLON 6000. Rozwiązanie, które Polon-Alfa proponuje, jest bardzo innowacyjne i jako projektant mogę powiedzieć, że nie mogę doczekać się wprowadzenia systemu do sprzedaży. Bardzo cieszy mnie fakt, że polski producent jest w stanie skutecznie konkurować z potężnymi europejskimi koncernami. Zawsze staram się uwzględniać w projektach polskie produkty i promować polski przemysł, zwłaszcza wówczas, gdy te polskie produkty przewyższają jakością urządzenia zagraniczne.

Czy zwrócił Pan uwagę na coś jeszcze podczas wystawy urządzeń?

Podobał mi się nowy program wizualizacji VENO współpracujący z naszą centralą. Program ten jest ciekawy, bo może zintegrować ze sobą na jednym panelu system sygnalizacji pożarowej, system sygnalizacji włamaniowej, telewizję dozorową i systemy kontroli dostępu. Bardzo podobała mi się funkcja automatycznego kierowania kamery w stronę wystąpienia alarmu pożarowego.



Co sądzi Pan o nowych sygnalizatorach tonowo-głosowych zaprezentowanych przez Polon-Alfa?

Sądzę, że sygnalizatory z możliwością transmisji komunikatów głosowych bez wątpienia znajdą swoje zastosowanie. Szczególnie w obiektach, w których nie jest wymagany system DSO, a ewakuacja ludzi musi być szybka. Głosowa informacja potwierdzająca, że to nie jakiś alarm włamaniowy, tylko prawdziwy alarm pożarowy, z całą pewnością usprawni ewakuację. Jeżeli zastosowane są klasyczne rozwiązania z sygnalizatorami tonowymi bez DSO, ludzie mogą nie wiedzieć, jak się zachować w przypadku alarmu pożarowego.

Jak ocenia Pan obecną ofertę firmy Polon-Alfa?

Jeśli ograniczone są możliwości instalowania okablowania w obiekcie, wówczas, pomimo możliwości wykorzystania czujek radiowych, pojawia się ograniczenie związane z ręcznymi ostrzegaczami. Właściwym posunięciem byłoby wprowadzenie przez Polon-Alfa właśnie radiowych ręcznych ostrzegaczy pożarowych w celu uzupełnienia istniejącego rozwiązania bezprzewodowego. Ponadto warto wprowadzić urządzenie, dzięki któremu dowolna czujka stanie się radiowa, a nie wyłącznie jeden typ.

Jesteśmy świeżo po prezentacji nowego systemu POLON 6000 i jego funkcji. Jak ocenia Pan jego możliwości?

Cieszy mnie rozszerzenie funkcjonalności w stosunku do systemów dotychczasowych i to, że producent wziął pod uwagę sugestie uczestników szkoleń. Chciałbym jednak dowiedzieć się, jak szybko będą realizowane te wysterowania grupowe.

Opóźnienia w przypadku wysterowań jednej grupy nie będą przekraczać pojedynczych milisekund, to jest też związane z nowym podejściem do systemu, co Pan o nim sądzi?

Bardzo ciekawie przedstawia się architektura nowego systemu. Na pewno sprawdzi się w rozległych instalacjach. Jak system będzie zachowywać się w przypadku uszkodzenia toru transmisji lub utraty łączności z węzłem master?

Połączenia będą realizowane w sposób redundantny, co jest szczególnie istotne w przypadku dużych obiektów.

Zatem może przy okazji prac nad nowym systemem można by uzupełnić jego możliwości o funkcję testowania całego systemu? Mam na myśli proste włączenie jednym przyciskiem bądź wybranie funkcji dostępnej tylko dla upoważnionego operatora po to, by centrala i elementy detekcyjne pracowały w trybie testowym i nie istniało ryzyko przypadkowego uruchomienia zabezpieczeń pożarowych.

Czy ma Pan jeszcze jakieś przemyślenia po wykładzie? Jak ocenia Pan nowy wygląd urządzeń?

Powinniście rozważyć zmianę wzornictwa w przypadku wskaźnika zadziałania. Architekci mają swoje wyobrażenia dotyczące wyglądu wnętrza i nie zawsze łatwo dopasować do tych wnętrz zabezpieczenia przeciwpożarowe.

Może Pan powiedzieć coś jeszcze na temat funkcji? Może jest jakaś opcja, na którą warto zwrócić uwagę?

Jeśli zestaw funkcji czujek będzie rozszerzany, może udało by się wprowadzić pewne elementy związane z automatyką, na przykład moduły umożliwiające kontrolę wartości analogowych i przedstawianie tych wartości w centrali wraz z odpowiednią reakcją wyjść systemu, zależną od założonych poziomów wartości z kontrolowanych wejść. Tego typu właściwości umożliwiłyby rozszerzenie współpracy z automatyką budynku.



Zapraszamy do obejrzenia fotorelacji na stronie
www.zabezpieczenia.com.pl

Axis Partner Conference Polska 2013

– podsumowanie

We wrześniu, tym razem na wyspie Ven w Szwecji, odbyła się kolejna konferencja połączona z bogatym programem rekreacyjnym, organizowana przez firmę Axis Communications – Axis Partner Conference Polska.

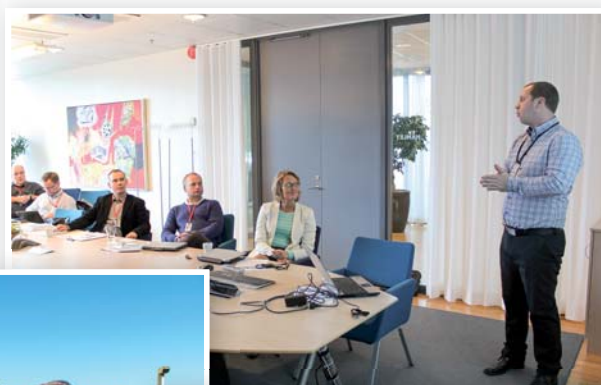
Cykliczne wyjazdy partnerów, wybranych na podstawie osiągniętych wyników, to już stały punkt działalności firmy Axis. Firma traktuje go jako atrakcyjną formę szkolenia dotyczącego produktów Axis i ich zastosowań, a także nagrody za dobre wyniki sprzedaży i motywacji do dalszych efektywnych działań w tym zakresie.

Jak co roku kilkusobowa grupa przedstawicieli firm, do których dołączyło dwoje redaktorów prasy branżowej, udała się do Lund, uroczego uniwersyteckiego miasteczka i głównej siedziby Axis Communications, w celu bliższego zapoznania się z działalnością firmy, planami dotyczącymi jej dalszego rozwoju, nowymi technologiami i produktami. Powitała nas **Anna Forsberg** – Regional Director na Wschodnią Europę, która podała zebranim aktualne informacje o korporacji oraz lokalnym rynku, za który jest odpowiedzialna. Opisała polski rynek i porównała go do innych w danym regionie.

Daniel Ferm – Produkt Manager Axis'a – zapoznał nas z nowościami, które ukażą się w najbliższej przyszłości, a także z produktami przeznaczonymi do ochrony obwodowej na przykładzie kamer termowizyjnych. Oprowadził partnerów po Axis Experience Center (co roku eksponowane są w nim nowe produkty). Następnie, co zawsze bardzo podoba się zwiedzającym, pokazał poszczególne pracownie oraz dział badań i rozwoju.



Mieliśmy okazję poznać **Stanislava Guchię**, który jest odpowiedzialny za rozwój kanałów sprzedaży i za tworzenie dobrych warunków do współpracy klientów końcowych, integratorów dostawców rozwiązań IT i firmy Axis. Tęgo typu współdziałanie zostało zainicjowane w Rosji i przynosi wymierne korzyści wszystkim współpracującym. Prelekcję na temat systemów usprawniających organizację handlu detalicznego z wykorzystaniem kamer Axis poprowadził **Aleksey Mayorov**, który od pewnego czasu kieruje zespołem przygotowującym rozwiązania systemowe przeznaczone dla sektora handlu detalicznego. Jedną z podstawowych korzyści uzyskiwanych dzięki zastosowaniu kamer Axis jest możliwość implementacji systemów analitycznych, dzięki którym obrazy z kamer dostarczają wielu dodatkowych informacji dotyczących liczby, wieku, płci klientów oraz umożliwiają tworzenie tak zwanych map cieplnych, które odzwierciedlają intensywność ruchu klientów na obserwowanych obszarach. Firma Axis oferuje oprogramowanie Axis Camera Companion, zdobywające ostatnio dużą popularność nie tylko na rynku handlu detalicznego, które idealnie nadaje się do obsługi niedużych instalacji zawierających maksymalnie 16 kamer. Oprogramowanie pozwala na sterowanie pracą kamer oraz na zarządzanie zarejestrowanym materiałem wizyjnym.





Wieczorem, po intensywnym programie dydaktycznym, udaliśmy się na spacer po Västra Hamnen, nowej mieszkaniowej dzielnicy Malmö, która powstała na dawnych terenach przemysłowych i portowych, blisko centrum, i która stała się wizytówką nowoczesnego Malmö. Jej największą atrakcją architektoniczną jest 190-metrowy wieżowiec mieszkalny Turning Torso mający 54 kondygnacje. Jest to drugi najwyższy budynek mieszkalny w Europie (po Triumph Palace w Moskwie). Zaprojektował go światowej sławy hiszpański architekt Santiago Calatrava. Gmach jest skrzycony od podstawy aż do wierzchołka (najwyższe kondygnacje są obrócone względem najniższych o 90 stopni). Jest znakiem rozpoznawczym miasta. W pogodny dzień widać z niego piękną panoramę Malmö i jego okolic, Øresund Bridge, cieśninę, a nawet Kopenhagę. Znajdują się w nim czynszowe mieszkania z całodobową recepcją obsługującą mieszkańców (ewenement w Szwecji). Kolacja w Turning Torso, w towarzystwie przedstawicieli Axisa, była okazją do podziwiania zapierających dech w piersi widoków.

Ven (duń. Hven) to należąca do Szwecji wyspa, a może raczej wysepka, położona w cieśninie Sund między Danią a Szwecją (powierzchnia: 7,48 km²; długość: 4,5 km; szerokość: 2,4 km; 354 stałych mieszkańców), na której słynny duński astronom Tycho Brache spędził dwadzieścia jeden lat swojego życia, poświęcając się bez reszty nauce. Prowadził obserwacje nieba, dokonał istotnych odkryć dotyczących ruchu księżyca oraz komet. Obserwatorium astronoma to miejsce o niesamowitej atmosferze, spotęgowanej odpowiednio dobraną muzyką i oświetleniem.

Na Ven popłynęliśmy promem. Na wyspie najpopularniejszym środkiem transportu – zarówno dla mieszkańców, jak i turystów – jest rower. Nie można zabrać tam auta. Prom przewozi jedynie zarejestrowane na Ven pojazdy, a jest ich tam zaledwie kilka. Życie na wyspie toczy się spokojnie, można tam całkowicie się zrelaksować. Mimo to niektórzy uczestnicy wyprawy nawet tam nie potrafili zapomnieć o biznesie i prowadzili przez swoje smartfony i telefony komórkowe rozmowy handlowo-biznesowe, a pierwsze pytanie, jakie padało w recepcji hotelu, dotyczyło możliwości podłączenia laptopów do Internetu.





Na wyspie nie ma policji. Widocznie nie jest potrzebna. Jest natomiast klub golfowy – pięknie zlokalizowany, z widokiem na cieśninę Sund. Przyjeżdżają do niego również emeryci. Koszty nie są wysokie. My również – po raz pierwszy – mieliśmy okazję pograć w tę ciekawą i nietatwą grę. Niektórzy złapali bakcyła i stwierdzili, że będą nadal ćwiczyć po powrocie.

Wycieczka rowerowa z przewodnikiem wokół wyspy też bardzo się wszystkim podobała, bo widoki są tam bajkowe, a powietrze kryształowo czyste. Niektórzy korzystali z każdej wolnej chwili, aby wsiąść na rower i pojechać w nowo poznane, najpiękniejsze miejsca na wyspie, a pomimo jej niewielkich rozmiarów było ich całkiem sporo. Mieliśmy również okazję zwiedzić małą miejscową gorzelnię whisky, a następnie degustować jej produkty. Przedostatnim punktem programu była wyprawa kutrem rybackim na połów ryb w okolicznych wodach Bałtyku. Trudno opisać, jak dużą mieliśmy frajdę, wyciągając wędkę z kilkoma rybami na haczykach na raz. Zapewne z upływem czasu piękne okazy będą w naszych wspomnieniach i opowieściach coraz większe. Przed odlotem do Polski zwiedziliśmy mały kopenhaski browar, zlokalizowany w drugim najstarszym parku rozrywki świata – Tivoli.

Agata Majkucińska – menadżer ds. kluczowych klientów – podczas pobytu na wyspie Ven zorganizowała dla grupy spotkanie podsumowujące wspólne działania. O zaletach uczestnictwa w Programie Partnerskim Axis opowiedział jeden z jego uczestników – **Marcin Guziński**. Nową, uproszczoną procedurę gwarancyjną Return Material Authorization (RMA) omówiła Agata Majkucińska. Jak co roku była też ankieta (stały punkt programu) zawierająca istotne dla menadżera ds. kluczowych klientów pytania. Szczere odpowiedzi uczestników corocznych Axis Partner Conferences umożliwiają lepsze zrozumienie potrzeb i oczekiwań partnerów firmy. Bogata, ciągle uzupełniana oferta firmy Axis jest powiązana z silnym wsparciem technicznym, edukacją i otwarciem się na potrzeby instalatorów, inwestorów i końcowych klientów. To wszystko składa się na sukces firmy.

Teresa Karczmarzyk

Zapraszamy do obejrzenia fotorelacji na stronie www.zabezpieczenia.com.pl.



20th MOSCOW INTERNATIONAL PROTECTION & SECURITY EXHIBITION & CONFERENCE

ufi
Approved
Event

Mips OSCOW

14–17 APRIL 2014
PAVILION 75, VVC, MOSCOW



01010100101111110101010010101010
00101111111010101001010101010100101001011111101010010101010
0011101010100101010100101010010101001000001011111010101010101010010100101111101010011001010101010
000010111111010101001010101010101010010101001011111101010100101010
0011101010100100010101010101010100100000101111110101001010101010010100101111101010010101010



CCTV
& Surveillance



Security
Technologies
& Solutions



Perimeter
protection
systems.
Fencing.



Fire safety.
Rescue
equipment.
Safety at work



Smart Cards



Organiser:



Martyna Michalska

T: +48 61 6627244

F: +48 61 6627246

E: michalska@ite-poland.com

Supported by:



Ministry
of the Interior
of the Russian Federation

www.mips.ru



Z kamerami wśród zwierząt

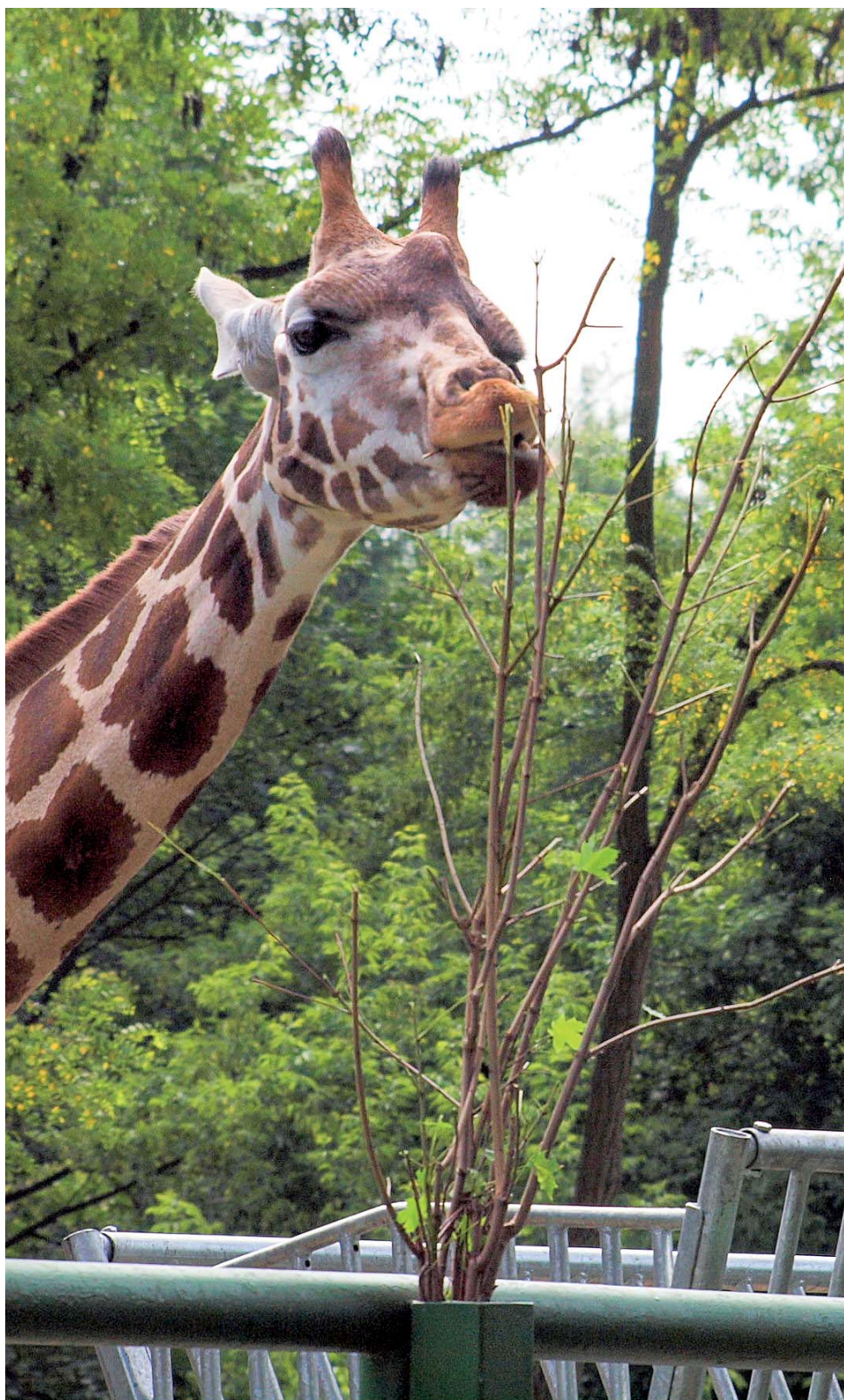
Maciej Mroszczak

Pod koniec października 2012 roku firma Sprint zawarła umowę z Zarządem Zieleni Miejskiej w Łodzi na budowę systemu zabezpieczeń w Miejskim Ogrodzie Zoologicznym. Prace związane z przygotowaniem projektu, instalacją okablowania, zakupem oraz instalacją urządzeń niezbędnych do uruchomienia systemu trwały dziewięć miesięcy i zakończyły się w lipcu tego roku.

W ramach realizacji kontraktu zainstalowano nowoczesny system dozoru wizyjnego wraz z systemem powiadamiania głosowego.

Ponadto na terenie ogrodu zainstalowane zostały czujki ruchu dalekiego zasięgu i oświetlacze.

Wszystkie te elementy są nadzorowane i sterowane z centralnego punktu, za pomocą dedykowanego oprogramowania



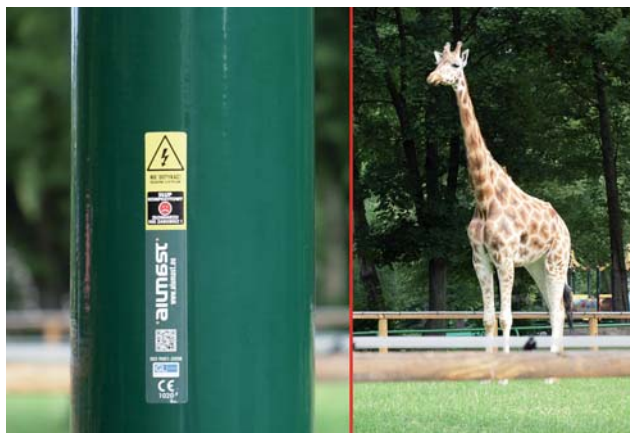
W ramach realizacji projektu wybudowano światłowodową sieć transmisyjną. Sieć ma topologię pierścienia, a do jej instalacji użyto urządzeń aktywnych – sieciowych przełączników przemysłowych Moxa serii EDS-510A. Punkty kamerowe zostały wyposażone w wysokiej rozdzielczości kamery obrotowe Axis Q6035-E oraz stacjonarne Axis P1346, generujące obraz o wyjątkowej ostrości, kolorystyce i rozdzielczości Full HD. Dodatkowo w ogrodzie zainstalowano zestawy do powiadamiania głosowego składające się z głośników tubowych i mikrofonów pojemnościowych Monacore. System

uzupełniono o czujki ruchu dalekiego zasięgu Redwall SIP (do alarmowania oraz do pozycjonowania kamer obrotowych) oraz zdalnie sterowane oświetlacze emitujące białe światło.

Całość jest zarządzana w centralnym punkcie dozorowym, który znajduje się w budynku ochrony. Operatorom udostępniono oprogramowanie służące do sterowania systemem nadzoru wizyjnego oraz do zarządzania innymi elementami systemu. W punkcie dozorowym można korzystać ze wszystkich funkcji systemu – przeglądać obrazy z kamer, sterować kamerami, nadawać komunikaty głosowe, które są odbierane w wybranych punktach, weryfikować sygnały z czujek ruchu i mikrofonów oraz sterować oświetleniem.

System ma kilka funkcji dodatkowych. Należą do nich podgląd i rejestracja obrazów z kamer przenośnych, ustawianych na statywach, służących do monitorowania życia zwierząt (na wybiegach oraz w szpitalu dla zwierząt), oraz automatyczna analiza obrazu z dedykowanych kamer dla celów statystycznych. Analizowane jest natężenie ruchu osób zwiedzających zoo.





Punkty kamerowe zostały rozmieszczone w głównych ciągach komunikacyjnych, między innymi w pobliżu wybiegów dla zwierząt niebezpiecznych (tygrysów, gepardów i niedźwiedzi) i wrażliwych (żyraf). Urządzenia zlokalizowano w taki sposób, aby każde wtargnięcie intruza na teren ogrodu zoologicznego zostało wykryte przez czujki ruchu i skutkowało zarejestrowaniem obrazu z kamer obserwujących miejsce zajścia. Kamery zostały umieszczone także w zabudowaniach, w których nocują zwierzęta. Wybór lokalizacji kamer był podyktowany koniecznością prowadzenia całodobowej kontroli terenu pod kątem detekcji osób postronnych oraz monitorowania zachowania zwierząt w nocy.

Przetarg na budowę systemu został ogłoszony kilka miesięcy po incydencie, jakim było wtargnięcie wandalów na teren ogrodu zoologicznego. Zdarzenie miało miejsce w nocy. Chuligani zdemolowali wybieg dla tygrysów, zniszczyli infrastrukturę ogrodu i przestraszyli dwie żyrafy, które zdechły wskutek stresu wywołanego tym zdarzeniem. Wkrótce po tym zajściu zdecydowano, że konieczne jest zainstalowanie systemu wykrywającego intruzów i służącego do nadzoru wizyjnego nad terenem zoo. Nowoczesny system dozoru wizyjnego odstraszy potencjalnych chuliganów i tym samym zapobiegnie podobnym sytuacjom w przyszłości.

Po godzinach, w których ogród jest dostępny dla zwiedzających, system gwarantuje wykrycie osób przebywających na jego terenie, a także umożliwia dokumentację zdarzeń i identyfikację sprawców wykroczeń. W ciągu dnia, gdy zwierzęta są narażone na przykład na dokarmianie, operatorzy systemu korzystając z kamer i głośników zapobiegają tego typu zdarzeniom. Zainstalowane urządzenia umożliwiają całodobową obserwację życia podopiecznych łódzkiego zoo i podejmowanie natychmiastowych działań w razie wypadku. Już w pierwszym tygodniu działania systemu, dzięki stałemu podglądowi obrazów z kamer, udało się uratować dwie mary patagońskie, których matka padła podczas porodu.

Dzięki zaprojektowaniu i uruchomieniu nadmiarowej sieci transmisyjnej można zainstalować nowe punkty kamerowe i punkty dozоровe, a także zwiększyć liczbę kamer przenośnych i dowolnie je ustawiać. Sieć transmisyjna może zostać wykorzystana do wdrożenia innych systemów teleinformatycznych, które planuje się uruchomić. Zastosowane oprogramowanie umożliwia wykorzystanie dodatkowych czujników, czujek i modułów wejść/wyjść alarmowych.

W przyszłości planuje się podłączenie systemu dozoru wizyjnego łódzkiego zoo do miejskiej sieci światłowodowej, a tym samym do miejskiego systemu dozoru wizyjnego, i udostępnienie zarówno bieżących obrazów, jak i materiałów archiwalnych operatorom systemów bezpieczeństwa w policji i Straży Miejskiej. Planuje się też udostępnienie wysokiej jakości strumieni wizyjnych z kamer szerokiej publiczności – użytkownikom Internetu.

Łódzkie zoo jest pierwszym ogrodem zoologicznym w kraju, w którym wybudowano tak nowoczesny system zabezpieczeń. Dzięki wdrożeniu nowoczesnych rozwiązań i zainstalowaniu wysokiej klasy urządzeń znanych i sprawdzonych producentów system zainstalowany w łódzkim zoo przez wiele lat będzie służyć jego pracownikom i gościom, a przede wszystkim zapewni bezpieczeństwo zwierzętom.

Maciej Mroszczak



Axis Communications' Academy Budowanie kompetencji w dziedzinie sieciowych systemów wizyjnych

Liczba klientów i sukces Twojej firmy zależą od tego, czy dysponujesz najbardziej aktualną i wszechstronną wiedzą w branży. Dzięki szkoleniom w ramach Axis Communications' Academy łatwiej być o krok przed konkurencją – wiedza z dziedziny sieciowych systemów wizyjnych jest w zasięgu ręki.

Akademia oferuje bogactwo informacji, które umożliwiają budowanie kompetencji w zakresie zaawansowanych rozwiązań Axis – od interaktywnych narzędzi do projektowania systemów, praktycznych instrukcji „krok po kroku” i specjalistycznych seminariów internetowych po szko-

lenia stacjonarne i programy certyfikacyjne. Tę wiedzę przekazują przeszkoleni specjaliści Axis. Jest ona dostępna w każdej chwili, w każdym miejscu i po polsku.

Gdy źródłem Twojej wiedzy jest firma, która opracowała pierwsze sieciowe systemy wizyjne i nadal ustanawia branżowe standardy w zakresie innowacji, świadomi klienci doceniają Twoje doświadczenie, co przynosi w konsekwencji wymierne korzyści.

**Przyjmij punkt widzenia Axis.
Bądź zawsze o krok do przodu.**
Odwiedź www.axis.com/academy

Axis Communications' Academy - globalne centrum wiedzy z dziedziny sieciowych systemów wizyjnych

AXIS[®]
COMMUNICATIONS

Nowoczesne manipulatory w ofercie firmy SATEL

Michał Konarski

Nowoczesne systemy alarmowe oferują swoim użytkownikom coraz większe możliwości. Niektóre inteligentne systemy umożliwiają zarazem wykrywanie włamań i innych zagrożeń oraz sterowanie urządzeniami domowymi. Wykorzystanie takiego potencjału wymaga jednak zmiany sposobu obsługi i sterowania



Fot. 1. INT-TSI – manipulatory graficzne z ekranem dotykowym 7"



Urządzenia mobilne są dobrym przykładem na to, że ekran dotykowy umożliwia wygodną i łatwą obsługę technicznie zaawansowanych urządzeń. Dlatego właśnie firma SATEL zdecydowała się wykorzystać najnowsze rozwiązania techniczne w manipulatorze, który stał się prawdziwym centrum dowodzenia, zaawansowanym, inteligentnym systemem alarmowym wykorzystującym centrale INTEGRA.

Manipulator INT-TSI jest niezwykle urządzeniem ze względu na zastosowany osprzęt i oprogramowanie. Już na pierwszy rzut oka wyróżnia się bardzo dużym panoramicznym ekranem TFT LED o przekątnej 7". Prosty i minimalistyczny wygląd ekranu podkreśla podstawową funkcję urządzenia. Konstrukcja manipulatora jest pozbawiona jakichkolwiek dodatkowych elementów – nie ma dodatkowych przycisków czy diod sygnalizujących stan systemu. Doskonale wpisuje się to we współczesne trendy wzornicze, wyznaczone przez urządzenie powszechnego użytku.

Sercem manipulatora jest wydajny procesor ARM Cortex A8 gwarantujący płynną obsługę nawet rozbudowanego interfejsu graficznego. Centrala umożliwia podłączenie ośmiu manipulatorów. Czytnik kart MicroSD (złącze SDHC) oraz złącze USB umożliwiają instalatorowi łatwe przenoszenie danych do pamięci manipulatora. Warto podkreślić, że w konstrukcji ekranu wykorzystano technologię pojemnościową, dlatego doskonale reaguje on nawet na najłżejsze dotknięcie palcem – nie ma konieczności dociskania ekranu jak w przypadku prostszych urządzeń z ekranami rezystancyjnymi.

Manipulator INT-TSI pozwala dopasować wygląd i sposób działania panelu obsługi niezależnie dla każdego użytkownika. Personalizacja interfejsu jest zadaniem dla instalatora systemu, które może być wykonane za pomocą narzędzia TSI Builder. Dzięki takiej personalizacji użytkownicy wykorzystujący jedynie podstawowe funkcje systemu mogą mieć do nich uproszczony dostęp i mogą korzystać ze specjalnych przycisków przypisanych do określonych akcji.

Użytkownicy wykorzystujący dodatkowe funkcje systemu będą mogli skorzystać z rozbudowanego panelu obsługi.

Do obsługi systemu za pomocą manipulatora INT-TSI służą ekranowe obiekty – widżety, które mogą być umiesz-



Fot. 2. Wygląd i sposób działania manipulatora INT-TSI może zostać dostosowany do indywidualnych potrzeb konkretnego użytkownika. Personalizacja interfejsu jest zadaniem dla instalatora systemu. Za pomocą specjalnego programu TSI Builder można stworzyć szablony obsługi systemu dla każdego użytkownika z osobna



Fot. 3. Manipulator INT-TSI udostępnia tzw. terminal ekranowy symulujący tradycyjny manipulator LCD na ekranie INT-TSI. Klawiatura ekranowa w takim terminalu umożliwia pełną obsługę systemu INTEGRA, włącznie z korzystaniem z przeznaczonych do weryfikacji poprawności pracy systemu funkcji serwisowych i testowych

zone na wielu zakładkach ekranu. Z zakładek korzysta się łatwo i szybko. Widżety, które można umieszczać na zakładkach, mogą mieć różne funkcje. Niektóre z nich są przeznaczone do podawania informacji: stanu czuwania, temperatury czy bieżącego czasu. Inne służą do sterowania – mogą one mieć formę przycisku, także w połączeniu z graficzną prezentacją aktualnego stanu sterowanego urządzenia. Bardziej szczegółowe informacje oraz dodatkowe sterowanie jest możliwe po wyświetleniu listy, np. listy stref pokazującej ich stan i umożliwiającej włączenie czuwania czy listy zdarzeń w systemie.

Jednym z priorytetów przy projektowaniu INT-TSI była wygoda sterowania urządzeniami automatyki. Właśnie dlatego zastosowanie tego manipulatora jest tak dobrym rozwiązaniem w przypadku systemów, w których skład wchodzi takie urządzenia. Umożliwia on przypisanie do dowolnego widżetu całej sekwencji akcji, co ułatwia wykonywanie złożonych czynności pojedynczym dotknięciem. W taki sposób można np. łatwo wybierać sceny świetlne, sterować bramą garażową, roletami czy ogrzewaniem i klimatyzacją.

W przypadku konieczności skorzystania z rzadziej używanych funkcji na dotykowym ekranie manipulatora INT-TSI można wywołać terminal ekranowy udostępniający tradycyjne funkcje manipulatora LCD. Umożliwia on m.in. programowanie funkcji



Fot. 4. Oprócz obsługi systemu alarmowego oraz automatyki INT-TSI umożliwia obsługę monitoringu wizyjnego wykorzystującego cyfrowe kamery IP



Fot. 5. Manipulator INT-TSG jest gotowy do pracy zaraz po wyjęciu z pudełka i podłączeniu do systemu. Codzienna obsługa systemu za jego pomocą jest bardzo prosta i przyjemna.

centrali w trybie serwisowym oraz wykonywanie testów funkcjonowania systemu.

Dużą zaletą manipulatora INT-TSI jest możliwość podglądu bezpośrednio na ekranie aktualizowanego na żywo obrazu z wybranych kamer dozorowych IP. W ten sposób manipulator staje się prawdziwym centrum sterowania systemami bezpieczeństwa.

Dla tych użytkowników, którzy cenią interfejsy dotykowe, ale INTEGRA to dla nich przede wszystkim rozbudowany i zaawansowany system alarmowy, dobrym wyborem może być manipulator INT-TSG. Jest on wyposażony w dotykowy ekran pojemnościowy (tak jak INT-TSI) o przekątnej 4.3". W przypadku manipulatora INT-TSG obszar ekranu jest uzupełniony wskaźnikami LED sygnalizującymi najważniejsze informacje o stanie systemu alarmowego.

Manipulator INT-TSG jest fabrycznie skonfigurowany do wykonywania standardowych zadań w systemie alarmowym.

Ikony na głównym ekranie umożliwiają korzystanie z najbardziej potrzebnych funkcji systemu – takich jak włączanie i wyłączanie czuwania, przeglądanie komunikatów o zdarzeniach czy wzywanie pomocy. Dostęp do rzadziej używanych funkcji, podobnie jak w INT-TSI, jest możliwy w trybie terminalu ekranowego symulującego działanie standardowego manipulatora LCD.

Manipulator INT-TSG umożliwia sterowanie urządzeniami automatyki przyłączonymi do centrali INTEGRA. Ułatwieniem tego zadania są makropolecenia wywołujące określoną sekwencję czynności. Takie makropolecenia mogą być przypisane do czterech grup, co ułatwia ich logiczny podział według funkcji realizowanych przez system i w konsekwencji ułatwia codzienną obsługę. Manipulator INT-TSG jest wszechstronnym urządzeniem pozwalającym na wygodną obsługę systemu alarmowego INTEGRA poprzez ekran dotykowy.

Użytkownicy preferujący standardowy sposób obsługi systemu, ale oczekujący niebanalnego wzornictwa, mogą zainteresować się nowym manipulatorem INT-KLF. Wyróżnia się on ciekawym i modnym wyglądem. Przypomina sensoryczny manipulator INT-KSG, ale jest wyposażony w standardowy wyświetlacz LCD oraz klawiaturę z przyciskami ukrytymi pod kłapką. Taki manipulator bardzo dobrze sprawdzi się w podstawowej obsłudze systemu, w której głównie wykorzystywane funkcje to włączanie i wyłączanie czuwania.

Wszystkie nowe manipulatory z oferty firmy SATEL zostały opracowane z myślą o tym, aby użytkowanie systemów alarmowych było łatwe i wygodne. Ponadto wyszukane wzornictwo z pewnością przypadnie do gustu tym użytkownikom, którzy lubią otaczać się niebanalnymi przedmiotami.

Michał Konarski
kierownik działu badań w firmie SATEL



Fot. 6. Manipulator INT-KLF łączy nowy design ze standardową obsługą centrali INTEGRA za pomocą dwuwierszowego, tekstowego wyświetlacza LCD oraz standardowej klawiatury z fizycznymi przyciskami. INT-KLF jest wyposażony w kłapkę zakrywającą obszar klawiatury, która po zamknięciu tworzy wraz z szybą okalającą wyświetlacz gładką, błyszczącą powierzchnię. Pod względem funkcjonalności nowy manipulator jest podobny do dotychczasowego manipulatora INT-KLCD



NOWOŚĆ

INT-TSI

centrum dowodzenia inteligentnym systemem alarmowym

Dzięki swojej unikalnej funkcjonalności, dotykowy manipulator INT-TSI to dużo więcej niż tylko atrakcyjny i nowoczesny sterownik systemu alarmowego. Możliwość swobodnego personalizowania interfejsu dla każdego użytkownika, łatwy dostęp do zaawansowanych funkcji sterowania oraz obsługa strumienia wideo z kamer IP powodują, że staje się on niezastąpionym elementem inteligentnego systemu alarmowego łączącego funkcje bezpieczeństwa i automatyki.

Więcej informacji na
www.satel.pl

Wyjątkowe cechy urządzenia:

- pojemnościowy panel dotykowy
- wyświetlacz TFT LCD z podświetleniem LED o rozdzielczości WVGA
- jednorodzeniowy procesor Cortex A8
- złącze Ethernet do podłączenia INT-TSI do sieci lokalnej
- dedykowany program do konfigurowania interfejsu (TSI Builder)
- funkcja wygaszacza ekranu (fotoramka), umożliwiająca wyświetlanie zdjęć z umieszczonej w urządzeniu karty SD (złącze SDHC)

Satel

Satel Sp. z o.o.
ul. Franciszka Schuberta 79, 80-172 Gdańsk, tel.: (58) 320 94 00, fax: (58) 320 94 01, e-mail: satel@satel.pl
www.satel.pl

System REDWALL-IP z komunikacją IP i zasilaniem PoE

Jacek Wójcik

OPTEX wprowadził na rynek serię urządzeń REDWALL-IP. Jednym z jej elementów są zewnętrzne czujki ruchu dalekiego zasięgu REDWALL-V, które w połączeniu z koderem PIE-1 mogą się komunikować z systemem przez sieć IP i mogą być zasilane metodą PoE



Quality detection system for video surveillance

REDWALL®

Unrivalled performance

Założenia systemu REDWALL-IP

Systemy nadzoru wizyjnego z kamerami IP są coraz częściej podstawą zabezpieczeń zewnętrznych obiektów. Kamery z funkcjami wykrywania ruchu wydają się urządzeniami wszechstronnymi. Praktyka pokazuje jednak, że systemy wizyjne warto rozszerzyć o detekcję intruzów bazującą na innych technologiach. Możliwość łatwego podłączenia czujek ruchu do sieci IP, w której stosowane jest zasilanie wybranych urządzeń metodą Power over Ethernet, ułatwia podjęcie decyzji o wykorzystaniu ich w planowanym lub istniejącym systemie CCTV IP.

System REDWALL-IP ma umożliwiać:

- zarządzanie systemem kamer CCTV i czujkami ochrony zewnętrznej za pośrednictwem oprogramowania systemu nadzoru wizyjnego;
- uproszczenie instalacji i współpracy systemu kamer i czujek (zasilanie metodą Power over Ethernet);
- poprawę detekcji ruchu w warunkach ograniczonej widoczności oraz w przypadku występowania zakłóceń powodowanych przez insekty, opady itp.;
- wizyjną weryfikację zdarzeń sygnalizowanych przez czujki ruchu.

W tym celu wykorzystano cztery typy detektorów ruchu połączonych z dedykowanymi koderami zamieniającymi sygnały z wyjść przekaźnikowych na dane cyfrowe w kodzie ASCII. Kodery mogą być zasilane bezpośrednio z sieci IP, metodą

Power over Ethernet, i wytwarzają odpowiednie napięcie, niezbędne do zasilania czujek.

Koder PIE-1

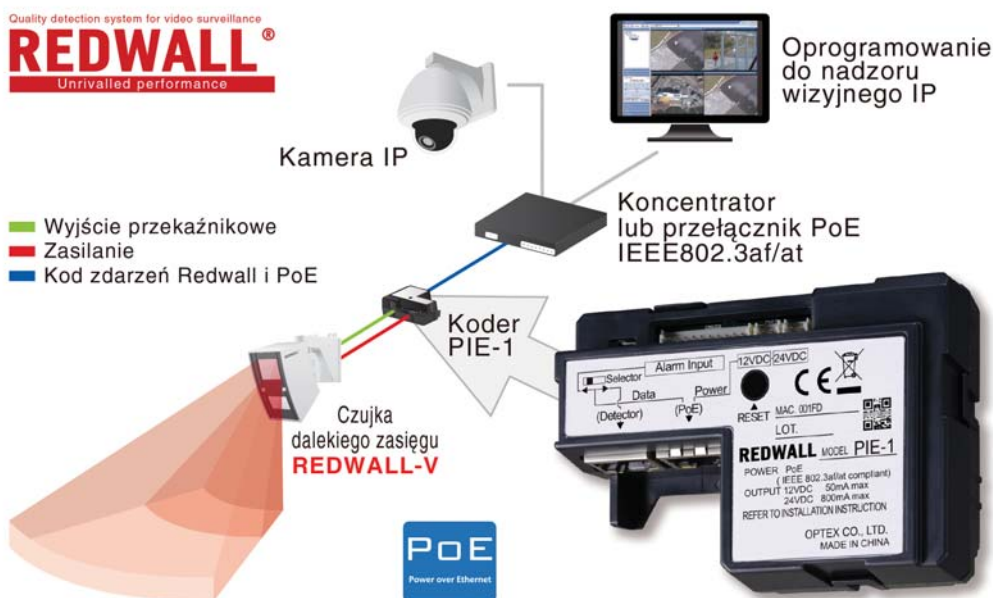
Elementem odpowiedzialnym za integrację urządzeń zewnętrznych z systemem zarządzania obrazem jest koder PIE-1. Do komunikacji z systemem wykorzystywany jest protokół REDWALL Event Code (UDP/TCP). Składnia pojedynczego komunikatu (w kodzie ASCII) nie jest skomplikowana i dane mogą być wprowadzane do oprogramowania jako ciąg tekstowy. Najłatwiejszym sposobem prowadzącym do tego celu jest użycie gotowego sterownika, jak ma to miejsce w pakiecie XProtect firmy Milestone – najpopularniejszym na świecie oprogramowaniu VMS.

Koder PIE-1 zasilają urządzenia peryferyjne metodą Power over Ethernet (IEEE802.3 af/at). Można stosować zarówno PoE, jak i PoE Plus (w przypadku urządzeń o mocy do 25,5 W). Koder jest urządzeniem niezależnym – przewody dostarczone wraz z nim są wyposażone w szybkozłącza i służą do połączenia kodera z wyjściami przekaźnikowymi detektorów. Niewielkie wymiary kodera ułatwiają zamontowanie go w standardowej puszcze montażowej. Koder wraz z pozostałymi elementami infrastruktury sieciowej można też umieścić w skrzynce instalacyjnej.

PIE-1 jest konfigurowany w przeglądarce internetowej, gdzie można łatwo sprawdzić jego działanie, przyporządkowanie wejść fizycznych oraz przypisać adres sieciowy.

Zewnętrzne czujki ruchu dalekiego zasięgu REDWALL-V

Czujki REDWALL-V japońskiej firmy OPTEX zaprojektowano jako elementy współpracujące z systemami monitoringu wizyjnego. Zastosowane rozwiązania, zasięg działania i rodzaj obiektów, w których są instalowane, wskazują na to, że sygnał alarmowy powinien być weryfikowany za pomocą obrazów z kamer, których pole widzenia odpowiada obszarowi detekcji czujki. Takie połączenie gwarantuje szybką



Rys. 1. Koder PIE-1 jest wykorzystywany do zasilania czujki metodą PoE i zamiany sygnałów z wyjść przekaźnikowych na dane cyfrowe w kodzie ASCII (Redwall Event Code). Koder jest konfigurowany za pomocą przeglądarki internetowej



Rys. 2. Czujkę REDWALL-V można zamontować na szczelnej puszcze montażowej, w której umieszczony jest koder PIE-1. Wejście sabotażowe kodera można wykorzystać także do wykrywania otwarcia szafki montażowej

identyfikację źródła alarmu przez centrum nadzoru. Typowe zastosowania tego typu czujek to ochrona rozległych obiektów, np. elektrowni słonecznych, ujęć wody, magazynów, zakładów przemysłowych, jednostek wojskowych itp.

Zasięg działania

Czujki z serii SIP to urządzenia o charakterystyce powierzchniowej i kurtynowej oraz zasięgach od 30 do 100 m. Konfigurację systemu ułatwia to, że charakterystyka przestrzenna czujek jest dopasowana do kątów widzenia obiektywów kamer pracujących w systemie monitoringu wizyjnego. Informacja o obszarze detekcji jest zawarta w oznaczeniu typu, np. SIP-5030 oznacza obszar detekcji o długości 50 m i szerokości 30 m, a oznaczenie SIP-3020/5 informuje o tym, że czujka jest wyposażona w dodatkowy detektor strefy podejścia o zasięgu 5 m.

Charakterystyka detekcji

Seria REDWALL-V to pasywne czujki podczerwieni wyposażone w oddzielne zestawy detektorów dla strefy bliższej i dal-

szej oraz detektor strefy podejścia (w modelach SIP-xxx/5). Za kształtowanie obszaru detekcji odpowiedzialne są lustra skupiające. Elementy aktywne są pokryte filtrem eliminującym zakłócenia elektromagnetyczne oraz światło widzialne.

Analiza sygnałów przebiega w dedykowanych mikroprocesorach z zaawansowanym algorytmem detekcji. Rozdzielenie torów obróbki sygnału dla poszczególnych kanałów daje możliwość niezależnego dla każdej strefy ustawiania czułości detekcji, wyboru trybu pracy (*AND* lub *OR*) lub wyłączenia strefy dalekiej.

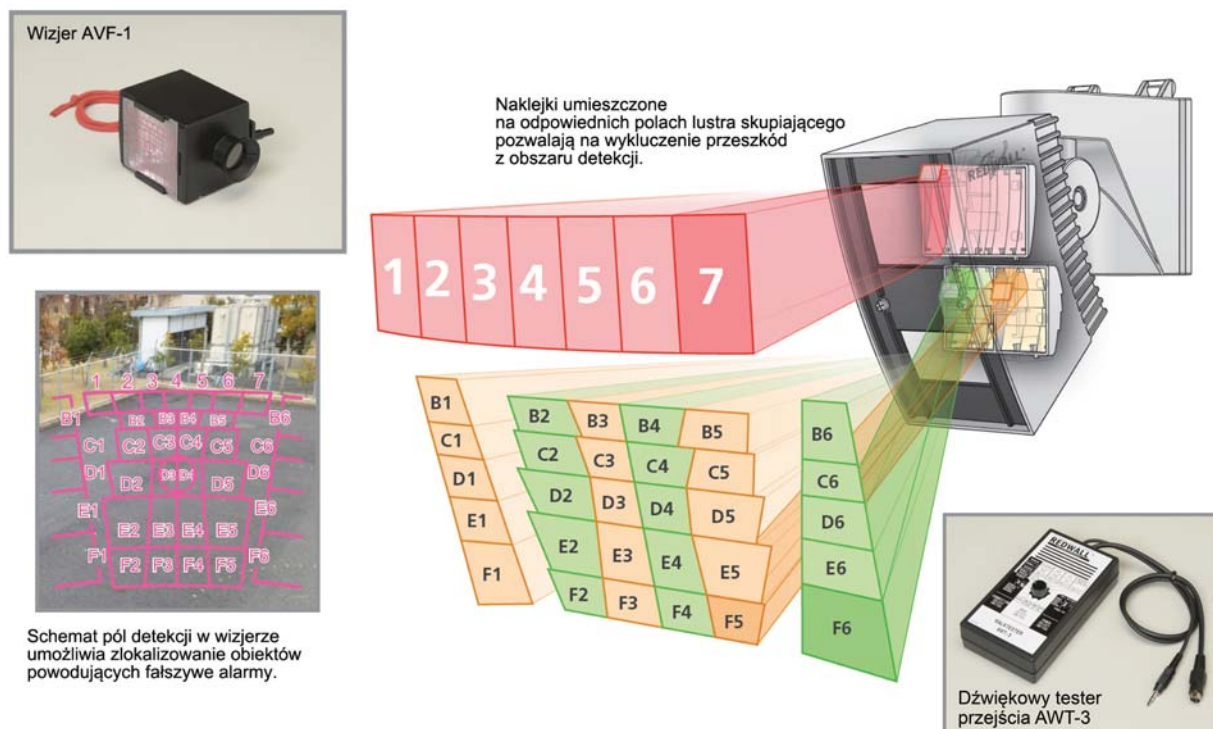
Możliwe jest zablokowanie wyjścia alarmowego na określony czas po pierwszym wykryciu intruza. Zapobiega to kolejnym aktywacjom czujki przez ten sam obiekt i daje operatorowi czas na weryfikację zdarzenia. Zasadą detekcji na dużym obszarze jest dwukrotne wykrycie intruza przez ten sam detektor przed wysłaniem sygnału alarmowego (tryb *AND*). Wpływa to na zmniejszenie liczby nieuzasadnionych aktywacji.

Urządzenia zewnętrzne powinny aktywnie reagować na zmiany temperatury otoczenia. Zasada działania pasywnej czujki podczerwieni polega na reakcji na zmianę rozkładu temperatur w obszarze detekcji. Klasyczne rozwiązanie może dawać niepełne informacje przy znacznej różnicy temperatur tła i otaczającego powietrza. Po słonecznym, gorącym dniu podłoże – chodnik, trawnik, asfalt – pozostaje nagrzane pomimo spadku temperatury powietrza. Z tego powodu czujki o prostej konstrukcji mogą mieć trudności w odróżnieniu intruza od termicznego obrazu tła. Czujki SIP są wyposażone w czujniki oświetlenia i temperatury, których zadaniem jest określanie stopnia nagrzania podłoża w ciągu dnia i czasu jego stygnięcia wieczorem. Ma to znaczny wpływ na algorytm detekcji intruzów w krytycznych warunkach środowiskowych.

Niezależne wyjścia alarmowe są podłączane do kodera PIE-1.

Ochrona przed wandalizmem

Czujki zewnętrzne są narażone na działania zakłócające lub zniszczenie, zaś promieniowanie ultrafioletowe stanowiące jeden



Rys. 3. Prawidłowe strojenie czujek REDWALL-V jest ułatwione dzięki wizjerowi AVF-1 i testerowi przejścia AWT-3

ze składników światła słonecznego niszczy tworzywo obudowy. Korpusy czujek REDWALL-V są wykonane ze wzmocnionego poliwęglanu. Gwarantuje to niezawodną i długoletnią pracę czujek oraz ich odporność na akty wandalizmu.

Zamaskowanie czujki – świadome lub nieświadome, np. przez przyklejony liść czy kawałek folii niesionej przez wiatr – powoduje zakłócenie jej działania. Układ sygnalizujący maskowanie nie zapobiegnie zakłóceniom, ale pozwoli je zauważyć w momencie ich powstania. Podobnie jak we wszystkich czujkach OPTEX, układ wykrywający maskowanie wykorzystuje aktywną czujkę podczerwieni i automatycznie dopasowuje się do naturalnego zanieczyszczenia okna czujki. Ważne jest to, że po odsłonięciu czujki wyjście sygnalizujące usterkę przechodzi w stan czuwania bez udziału operatora systemu.

Czujka jest wyposażona w aktywny uchwyt służący do jej zamocowania i skierowania jej w odpowiednią stronę, a także do ochrony samego urządzenia. Zmiana położenia czujki na uchwycie (zerwanie, odwrócenie) jest rejestrowana przez czujnik przemieszczenia i traktowana jako sabotaż.

Wysokość montażu czujki stanowi jej dodatkowe zabezpieczenie. Dosięgnięcie niewielkiego urządzenia zawieszzonego cztery metry nad ziemią wymaga sprawności, umiejętności, narzędzi i czasu. Dodatkowym utrudnieniem jest detektor strefy podejścia.

Łatwość instalacji

Konstrukcja czujek serii SIP umożliwia instalatorom precyzyjne dopasowanie zasięgu detekcji do ochranianego obszaru. Do każdej czujki dołączona jest przezroczysta płytką ze schematem

rozkładu pól detekcji, którą zakłada się na opcjonalny wizjer. Dzięki temu monter widzi dokładnie to samo, co czujka. Jeżeli w poszczególnych polach detekcji znajdują się obiekty powodujące fałszywe alarmy, można precyzyjnie zamaskować te fragmenty lustra, które przekazują niepożądane sygnały.

Wstępne określenie źródeł zakłóceń, sprawdzenie poprawności zamaskowania pewnych obszarów w polu detekcji oraz ostateczne potwierdzenie poprawności ukształtowania obszaru detekcji jest dokonywane za pomocą dźwiękowego testera przejścia podłączanego bezpośrednio do układu detekcji. Dzięki temu sygnalizowane są wszystkie reakcje układu pomiarowego, a nie tylko te krytyczne, wywołujące alarm. W ten sposób można precyzyjnie wykluczyć źródła zakłóceń, takie jak poruszające się na wietrze krzewy i gałęzie drzew czy ruch na drodze za ogrodzeniem.

Stopień ochrony obudowy (IP65) i uchwytu (IP55) zapewnia odporność na czynniki środowiskowe. Do ochrony przed oślepieniem przez słońce czy zasłonięciem przez śnieg służy metalowy daszek.

Mamy nadzieję, że przedstawione informacje przybliżyły Czytelnikom zalety technologii wpływających na skuteczność detekcji, możliwość integracji czujek REDWALL-V z sieciowym systemem nadzoru wizyjnego oraz łatwość ich instalacji i strojenia.

Szczegółowe parametry techniczne, instrukcje montażu oraz wskazówki dotyczące instalacji są zamieszczone pod adresem www.optex.com.pl/redwall.

Jacek Wójcik
OPTEX Security



**CZUJKA WEWNĘTRZNA
STOPIEŃ 3 EN50131
CDXseria**

PORUSZENIE W DETEKCJI WEWNĘTRZNEJ

OPTICAL



DIGITAL



MICRO
WAVE



CDX-DAM czujka dualna PIR & MW
15 x 15m z antymaskingiem

CDX-NAM kurtyna PIR
24 x 2m z antymaskingiem

CDX-AM czujka PIR
15 x 15m z antymaskingiem

od 177 PLN*

*sugerowana cena detaliczna netto CDX-AM

NOWOŚĆ



OPTEX Security Sp. z o.o.
ul. Bitwy Warszawskiej 1920r. 7b, 02-366 Warszawa
e-mail: optex@optex.com.pl tel. (22) 598 06 60

www.optex.com.pl

LightSYS2 w chmurze RISCO

RISCO Group Poland

W połowie bieżącego roku rozpoczęła się sprzedaż drugiej generacji systemu alarmowego LightSYS. Zgodnie z zapowiedziami wprowadzone zostały nowe funkcje: współpraca z chmurą RISCO Cloud, obsługa systemu alarmowego za pomocą aplikacji smartfonowej i internetowej oraz możliwość stosowania dwukierunkowych urządzeń bezprzewodowych



Z technologią chmury spotykamy się w życiu codziennym coraz częściej. Technologią tą od dawna posługują się centra obliczeniowe, projektanci i informatycy. Usługę przechowywania plików na wirtualnym dysku w chmurze oferują dostawcy Internetu oraz sprzedawcy smartfonów i tabletów. Chmura daje możliwość przechowywania dowolnych danych poza naszymi domami lub firmami i dostępu do nich, po autoryzacji, upoważnionym osobom w dowolnym miejscu.

W chmurze stworzonej przez RISCO przechowywane są wybrane informacje o systemie alarmowym, takie jak przy-

dział linii dozorowych do partycji, lista użytkowników, nazwy własne zaprogramowane przez instalatora, historia zdarzeń, ostatnie alarmy oraz zdjęcia z czujek PIR z kamerą (tylko dla systemu Agility3). Informacje te są w sposób czytelny pokazane w aplikacji internetowej na serwerze www.riscocloud.com oraz w aplikacji iRISCO dla telefonów z systemem Android lub iOS.

Użytkownik może przeglądać informacje o aktualnym stanie systemu, partycji i linii, a także wykonywać czynności związane z obsługą systemu alarmowego, takie jak włączenie w dozór (zwykle i domowe) i wyłączenie z dozoru partycji oraz zablokowanie i odblokowanie linii. Dzięki temu, będąc na urlopie lub w delegacji, można sprawdzić stan swojego systemu alarmowego lub zostać powiadomionym o tym, że w domu lub firmie wystąpiło zdarzenie alarmowe, np. włamanie, pożar, zalanie wodą, awaria sieci energetycznej lub ogrzewania. Technologia chmury umożliwia jednoczesny dostęp wielu osób do systemu.

Warunkiem koniecznym do współpracy systemu LightSYS2 z chmurą jest wyposażenie centrali w moduł GSM/GPRS (RP432GSM) z kartą SIM z włączoną transmisją danych lub w moduł karty IP (RW132IP) przyłączony do sieci TCP/IP, np. do routera internetowego w domu. Dzięki jednej z wymienionych metod komunikacji centrala regularnie łączy się z chmurą, przekazuje w formie zaszyfrowanej informacje o swoim aktualnym stanie oraz odbiera polecenia od użytkowników.

Sam proces instalacji systemu alarmowego pozostaje bez zmian. Instalator uruchamia system alarmowy, wykonuje wszystkie czynności związane z programowaniem wynikające z realizowanego projektu i na samym końcu uruchamia łączność z chmurą. Po sprawdzeniu w historii zdarzeń, że centrala jest połączona z serwerem chmury, użytkownik może przystąpić do rejestracji swojego systemu na serwerze www.riscocloud.com, gdzie podaje swój adres e-mail i hasło dostępu do serwera, a także wprowadza 15-cyfrowy numer identyfikacyjny, jaki znajduje się na opakowaniu lub płycie centrali LightSYS2.

Po odebraniu e-maila z potwierdzeniem rejestracji użytkownik może rozpocząć korzystanie z aplikacji internetowej i smartfonowej. W tym celu wprowadza login (e-mail podany podczas rejestracji), hasło do chmury oraz swój kod dostępu do systemu alarmowego.

Często pada pytanie, czy moduł GSM lub IP użyty do współpracy z chmurą może jednocześnie wysyłać raporty do stacji monitorowania. Otóż w przypadku chmury zarządzanej przez RISCO nie jest to możliwe, ponieważ nie ma interfejsu do systemu odbiorczego żadnej polskiej stacji monitorowania. Należy spodziewać się, że – podobnie jak w innych krajach – niektóre polskie agencje ochrony lub stacje monitorowania kupią licencje od RISCO i stworzą swoje prywatne chmury wraz interfejsami do systemów odbiorczych swoich stacji.

Kolejną nowością związaną z wprowadzeniem systemu LightSYS2 jest dwukierunkowy system bezprzewodowy. Zaletą stosowania czujek z transmisją dwukierunkową jest szybsza instalacja i konserwacja, ponieważ do programowania i diagnostyki używa się klawiatury systemu lub programu konfiguracyjnego. Użytkownicy mają do dyspozycji nowego pilota (RW132KF) i bezprzewodowe klawiatury (RW132K2P i RW132KL1P) wyposażone we wskaźniki LED informujące





Fot. 1. Aplikacja internetowa RISCO

o aktualnym stanie systemu, co ułatwia obsługę i umożliwia weryfikację wykonanych operacji. Trzeba pamiętać, że klawiatury LED nie umożliwiają instalatorskiego programowania systemu, zatem w systemie LightSYS2 przynajmniej jedna klawiatura powinna być przewodowa. RISCO Group ma w swojej ofercie wewnętrzne i zewnętrzne sygnalizatory bezprzewodowe. Mimo iż instalowanie ich jest w Polsce raczej rzadkością, teraz, w razie potrzeby, mogą być zastosowane.

LightSYS2 to system alarmowy przeznaczony do instalacji w małych i średniej wielkości obiektach: biurach, obiektach handlowych, magazynach, domach jednorodzinnych i mieszkaniach.

Płyta centrali jest wyposażona w osiem linii dozorowych. System może zostać rozbudowany do maksimum 32 linii, które mogą być dowolnie przydzielone do czterech niezależnie włączanych w dozór i wyłączanych z dozoru partycji. Aby go rozbudować, trzeba zainstalować ośmioliniowe moduły rozszerzenia, czujki magistralowe lub moduł odbiornika radiowego z czujkami bezprzewodowymi. Instalator ma do wyboru 35 typów linii dozorowych i różne warianty sygnalizacji akustycznej. Linie mogą pracować w konfiguracjach: NC, NO, z jednym rezystorem (EOL) lub z dwoma rezystorami parametrycznymi (DEOL). Dla każdej przewodowej linii dozorowej ta konfiguracja jest ustawiana indywidualnie. Wartość rezystorów parametrycznych jest ustawiana grupowo dla linii

dozorowych na płycie (Z1-Z8) oraz niezależnie dla każdego modułu ośmiu linii przewodowych. Wszystkie dostępne w ofercie firmy RISCO czujki magistralowe mogą zostać przyłączone do centrali.

Maksymalna obciążalność wyjść płyty centrali zasilających magistralę komunikacyjną i czujki to 800 mA. Oprócz dedykowanego wyjścia sygnalizacji BELL o wydajności 500 mA na płycie centrali dostępne są cztery programowalne wyjścia przekaźnikowe: trzy o wydajności 100 mA i jedno o wydajności 1 A. W systemie LightSYS2 można zaprogramować maksymalnie 14 wyjść. Instalator ma do dyspozycji wiele opcji programowania wyjść związanych z wystąpieniem różnych zdarzeń dotyczących systemu, partycji, linii oraz użycia wybranych kodów dostępu.

System alarmowy może być obsługiwany za pomocą maksymalnie czterech klawiatur. Ponieważ w menu programowania i obsługi są nazwy zawierające polskie znaki specjalne, należy stosować klawiatury LCD serii RP432 oraz dotykowe serii RP128KP. Bezprzewodowe klawiatury LED mają funkcjonalność ograniczoną do podstawowych operacji.

Program centrali umożliwia zdefiniowanie szesnastu kodów dla użytkowników mających różne uprawnienia i niejednakowy dostęp do wybranych partycji. Każdy posiadacz kodu może posługiwać się również brelokiem zbliżeniowym, dlatego identyfikacja jest możliwa także na skutek zbliżenia breloka do klawiatury z wbudowanym czytnikiem.

Można wysłać raporty do stacji monitorowania, wybierając jeden z trzech dostępnych numerów telefonów. Raporty mogą być przesyłane w formacie SIA lub Contact ID. Oba te formaty komunikacji są bardzo popularne. Oprócz typowej komunikacji w sieci telefonicznej (PTSN, kanał głosowy GSM) dostępne są też opcje przesyłania informacji o zdarzeniach w formie wiadomości SMS lub pakietów sieciowych (GPRS, TCP/IP). Standardowy dialer telefoniczny znajduje się na płycie centrali. Opcjonalne moduły GSM/GPRS oraz IP mogą zostać zainstalowane na specjalnych złączach. Aby odbierać raporty w postaci pakietów sieciowych, konieczne jest zainstalowanie w stacji monitorowania programu odbiorczego IP/GSM Receiver, który dokonuje transkodowania przesyłanych danych. System LightSYS2 charakteryzuje się rozbudowanymi funkcjami powiadomiania osobistego *Follow Me*. Umożliwia wybranie szesnastu odbiorców powiadomienia w formie komunikatów głosowych pochodzących z modułu głosowego, SMS-a lub e-maila, w zależności od wyposażenia centrali w odpowiednie moduły.

RISCO Group umożliwia aktualizację oprogramowania centrali bez jej demontażu. Warunkiem jest obecność w systemie modułu GSM z dostępem do usługi GPRS lub modułu IP. Proces aktualizacji nie powoduje skasowania ustawień zaprogramowanych przez instalatora.

Aktualnie RISCO Group pracuje nad wdrożeniem weryfikacji wizyjnej. Zgodnie z planem w systemie LightSYS2 będzie można zainstalować kilka bezprzewodowych czujek PIR z kamerą serii eyeWave. Po wystąpieniu alarmu użytkownik korzystający ze smartfonu będzie mógł otrzymać stosowną informację wraz ze zdjęciem. Funkcja ta jest już dostępna w przypadku central Agility3 pracujących w chmurze RISCO.



Fot. 2. Aplikacja internetowa RISCO



Kamery z serii Eco-Savvy

Megapikselowe kamery sieciowe

3 korzyści

- Mały pobór mocy przez kamery — oszczędność 50%
- Wydajna kompresja — oszczędność na paśmie sieciowym i na objętości pamięci
- Praca przy bardzo słabym oświetleniu — wysoka jakość obrazów w porze nocnej

Rekomendowane kamery →



Kamera sieciowa w wodoodpornej obudowie tulejowej z oświetlaczem IR, praca w trybie 1,3 / 2 Mpix i Full HD



Kamera sieciowa w wodoodpornej i wandaloodpornej obudowie kopułkowej z oświetlaczem IR, praca w trybie 1,3 / 2 Mpix i Full HD



Niewielkich rozmiarów kamera sieciowa z oświetlaczem IR, praca w trybie 1,3 / 2 / 3 Mpix i Full HD



Obrotowa kamera sieciowa z oświetlaczem IR, praca w trybie 1,3 / 2 Mpix i Full HD

CE FC CCC UL RoHS ISO 9001:2000



DAHUA TECHNOLOGY CO., LTD.

No.1199 Bin'an Road, Binjiang District, Hangzhou, China. 310053

Tel: +86-571-87688883 Fax: +86-571-87688815

Email: overseas@dahuatech.com

www.dahuasecurity.com

MB-Secure

modułowa platforma SSWiN i kontroli dostępu

Tomasz Szklarz

Inwestorzy poszukujący systemów zabezpieczających dla swych obiektów znajdują na rynku wiele różnych rozwiązań, jednak nie wszystkie te rozwiązania umożliwiają stworzenie systemu o dowolnej wielkości i bez zbędnych funkcji. Przyjrzyjmy się proponowanej przez firmę Honeywell platformie MB-Secure, która spełnia najwyższe wymagania klientów



Honeywell Security Group to globalna grupa technologiczna oferująca systemy sygnalizacji włamania i napadu, systemy kontroli dostępu, systemy zarządzania czasem i bezpieczeństwem pracy oraz wizyjne systemy dozоровe. Firma oferuje nowoczesne urządzenia o wysokiej jakości i zintegrowane rozwiązania systemowe, które spełniają wszystkie potrzeby klientów – od domowych systemów bezpieczeństwa po kompleksowe, zintegrowane rozwiązania dla obiektów biznesowych czy przemysłowych.

MB-Secure firmy Honeywell jest modułową platformą SSWiN i kontroli dostępu. Można wykorzystać tylko te modu-

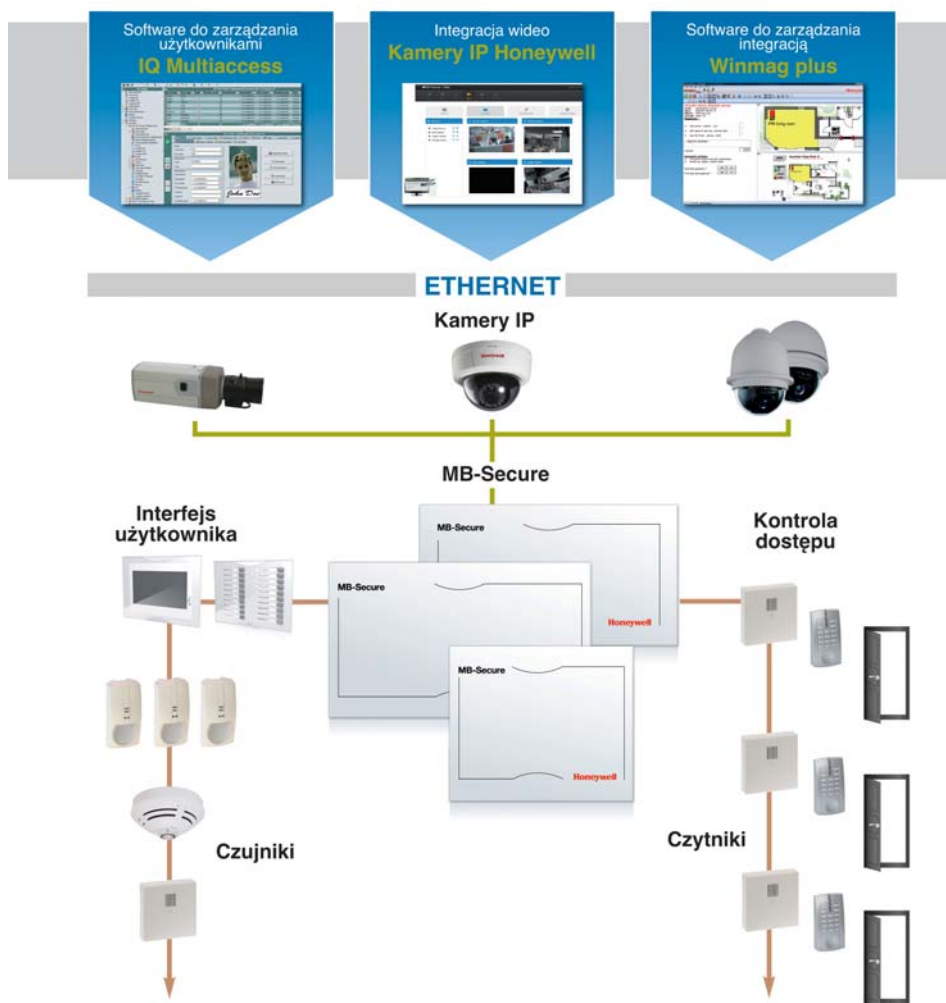


ły, które są w danym przypadku potrzebne, i stworzyć z nich system zabezpieczeń odpowiadający faktycznym potrzebom użytkownika. Stosując dodatkowe moduły BUS lub moduły wejścia/wyjścia i dodatkowe urządzenia peryferyjne można go łatwo rozbudować, a także zintegrować z innymi systemami, na przykład z wizyjnym systemem dozоровym. Do obsługi tak zintegrowanych systemów służy zaawansowane oprogramowanie WINMAG Plus. Dzięki modułowości sprzętu i oprogramowania można więc stworzyć prosty system zabezpieczający, a w razie potrzeby zwiększyć jego możliwości, modyfikując oprogramowanie.

Niezbędne funkcje mogą być łatwo aktywowane poprzez wymianę kluczy licencyjnych. Centrale systemowe mogą być instalowane w różnych obudowach, więc system może zostać skonfigurowany w dowolny sposób, w zależności od tego, czy potrzebne są ekonomiczne rozwiązania dla małych budynków czy wielosystemowe platformy bezpieczeństwa dla rozległych obiektów. Architektura systemu umożliwia użycie czterech magistral komunikacyjnych BUS-2 lub – opcjonalnie – RS485. W pierwszym przypadku możliwe jest dołączenie maksymalnie 64 modułów na jednej magistrali i – co istotne – tworzenie odgałęzień na tej magistrali. Dzięki temu można tworzyć bardzo duże systemy, dostosowane do konkretnych wymagań wynikających ze specyfiki zabezpieczanych obiektów. Należy dodać, że elastyczność systemów MB-Secure można zwiększyć, stosując technologię bezprzewodową. System radiowy umożliwia łatwe, równoległe podłączenie urządzeń bezprzewodowych (pasywnych czujek podczerwieni, kontaktronów alarmowych, sygnalizatorów, czujek pożarowych) i standardowych urządzeń przewodowych w celu stworzenia hybrydowego systemu służącego do sygnalizacji włamań. Działanie w trybie Dual Band w pasmach 433 MHz lub 868 MHz i możliwość wyboru jednej z tych częstotliwości gwarantuje stabilną transmisję sygnałów.

Funkcje kontroli dostępu mogą być realizowane przez adresowalne moduły podłączane do magistrali BUS-2, a także przez moduły DCM, które pozwalają na użycie typowych czytników Wiegand. Dzięki temu można używać różnego rodzaju kart identyfikacyjnych. Do modułów zainstalowanych na magistrali BUS-2 można podłączyć maksymalnie cztery czytniki zbliżeniowe z interfejsem RS485. Specjalny interfejs zapewniający komunikację z czytnikami IdentKey oferuje unikatowe funkcje dla użytkownika końcowego, np. łatwe załączanie w dozór/wyłączenie z dozoru partycji systemu poprzez użycie przycisków on/off i przyłożenie karty. Akcesoriami podwyższającymi poziom bezpieczeństwa i ułatwiającymi wprowadzanie nowych użytkowników do systemu kontroli dostępu są podkładka służąca do czytania podpisów i skaner do paszportów.

Inną kluczową cechą systemów MB-Secure jest proste i komfortowe zarządzanie za pomocą programowalnych przycisków umieszczonych w manipulatorach LCD lub LED. Aby uzbroić poszczególne partycje, wystarczy przyłożyć kartę do czytnika zainstalowanego w oznaczonym miejscu i nacisnąć odpowiedni przycisk. Trójkolorowa dioda umieszczona obok przycisku informuje o aktualnym stanie systemu i efekcie wykonanej czynności. Jest to bardzo wygodny sposób obsługi systemów MB-Secure. Dla wymagających użytkowników lub



Rys. 1. Architektura MB-Secure

administratorów dostępny jest duży wyświetlacz dotykowy. Dzięki nowoczesnym aplikacjom mobilnym, przeznaczonym do zdalnej obsługi systemów MB-Secure, można łatwo ustalić aktualny stan systemu alarmowego i obsługiwać go za pomocą smartfonu.

Pisząc o systemie MB-Secure, nie można pominąć wątku jego współpracy z systemem zarządzania budynkiem o nazwie WINMAG Plus. W ramach jednolitego interfejsu użytkownika oprogramowanie WINMAG integruje i wizualizuje działanie systemu ochrony antywłamaniowej i systemu kontroli dostępu (MB-Secure), a także systemu ochrony przeciwpożarowej, systemu dozoru wizyjnego, dźwiękowego systemu ostrzegawczego wykorzystywanego podczas ewakuacji, systemu automatyki budynku oraz systemów innych producentów, takich jak systemy ogrzewania i wentylacji oraz systemy HVAC (sterowane przez interfejs OPC). Interesującą wersją tego oprogramowania jest WINMAG touch. Ta wersja, dostarczana razem z komputerem wyposażonym w duży ekran dotykowy, tworzy zupełnie nowy, innowacyjny system sterowania z graficzną prezentacją map. Aktualne stany czujek są symbolizowane przez ikony o odpowiednim kolorze. Klikając ikonę odpowiadającą czujnikowi, wywołujemy okno informacyjne z metadanymi dotyczącymi stanu tego czujnika, przedstawionymi w postaci graficznej z użyciem dynamicznych symboli, tabel lub informacji w formie tekstu. Okna informacyjne są w pełni programowalne, dzięki czemu można je dostosować

do indywidualnych potrzeb każdego z klientów. Opcja Engine 3D programu WINMAG Plus pozwala używać modeli 3D, aby wyświetlić wszystkie połączone moduły nie tylko trójwymiarowo, ale także z użyciem preprogramowalnych scenariuszy wizualizacji zdarzeń.

Na koniec warto wspomnieć, iż system MB-Secure został zainstalowany w wielu nowoczesnych i prestiżowych obiektach w Europie i skutecznie je zabezpiecza, dowodząc swojej elastyczności i zdolności do sprostanania najwyższym oczekiwaniom klientów. Z braku miejsca na pełną listę obiektów wymienię tylko Terminal 5 lotniska Heathrow w Londynie, hotel Hilton w Wiedniu, budynek Dexia Bank Internationale w Luxemburgu i ultranowoczesny biurowiec Main Point Karlin w czeskiej Pradze. Z pewnością nie bez znaczenia dla wielu inwestorów będzie pełna zgodność systemu MB-Secure z restrykcyjnymi normami EN50131 oraz VDS.

Tomasz Szklarz



Ultrak Security Systems Sp. z o.o.

Lubieszyn 8, 72-002 Dołuje
tel.: +48 91 485 40 60-69
e-mail: info.pl@adiglobal.com
www.adiglobal.com/pl

Nowa generacja central MB-Secure



Honeywell

Modułowa platforma dla rozwiązań security - integracja bez kompromisów

Z MB-Secure, firma Honeywell daje użytkownikowi modułową platformę detekcji alarmowej i kontroli dostępu, jednocześnie zapewniając niezwykłą łatwość integracji z innymi systemami bezpieczeństwa.



Rozwiązania Bosch Security Systems dla kopalni odkrywkowych

Michał Borzucki

Rozległość terenu, występowanie
stref zagrożenia wybuchem
i oczywiście wszechobecne
zapylenie w kopalni odkrywkowej
utrudnia zabezpieczenie obiektu,
ochronę ludzi i ewakuację



Wymagania, jakim muszą odpowiadać kopalnie odkrywkowe będące obiektami infrastruktury krytycznej, są szczególne ze względu na potencjalne zagrożenia, które mogą mieć następstwa niekorzystne także dla mieszkańców i całej gospodarki danego regionu. Bosch Security Systems oferuje odpowiednie rozwiązania dla sektora przemysłowego – najwyższej klasy urządzenia i systemy, które można zintegrować, wsparcie techniczne i serwis.

Televizja dozorowa – dozór nad terenem oraz ułatwienie pracy

Systemy dozoru wizyjnego są najbardziej efektywnym elementem ochrony zakładu przemysłowego. W ostatnich dziesięciu latach zaszły ogromne zmiany technologiczne w dziedzinie telewizji dozorowej. Systemy bazujące na sieciach TCP/IP, kamery megapikselowe i termowizyjne są coraz tańsze i coraz częściej stosowane.

Firma Bosch jest producentem systemów telewizji dozorowej. Oferuje między innymi urządzenia przeznaczone do pracy w trudnych warunkach przemysłowych, w tym kamery obrotowe z serii MIC. Urządzenia tej serii to kamery szybkoobrotowe z silnikami bezszczotkowymi, przystosowane do pracy w trudnych warunkach środowiskowych. MIC-550 to kamera w obudowie o stopniu szczelności IP68, wyposażona w moduły optyczne PAL z obiektywami zmienneogniskowymi o krotności 28× lub 36×. Kamera ma wbudowane oświetlacze o zasięgu do 60 m, pracujące w podczerwieni. Model MIC-612 jest obrotową kamerą termowizyjną, w którą dodatkowo wbudowany jest moduł PAL z obiektywem zmienneogniskowym o krotności 36×, przeznaczony do pracy w świetle widzialnym, w ciągu dnia. W strefach zagrożonych wybuchem stosuje się urządzenia MIC-440 z certyfikatem ATEX. Kamery MIC-400 mają obudowy ze stali nierdzewnej i doskonale sprawdzają się w środowiskach żrących i zapyłonych. Modele Bosch MIC od wielu lat wyznaczają standard w dziedzinie wyspecjalizowanych kamer obrotowych przeznaczonych do instalacji w miejscach odznaczających się ekstremalnie trudnymi warunkami środowiskowymi. Asortyment kamer stałopozycyjnych marki Bosch jest równie szeroki. Modele EX65 mają obudowy z certyfikatem ATEX, w których znajdują się kamery z serii Dinion 2X odznaczające się dużą dynamiką oraz zaawansowanymi metodami przetwarzania obrazu. W środowiskach, w których występują skrajne temperatury oraz ekstremalne warunki atmosferyczne, stosowane są kamery EX14 w obudowach z tworzywa ABS.



Fot. 1. Maszyny stosowane w górnictwie odkrywkowym mają duże rozmiary. Koparka wielonaczyniowa jest jedną z największych wybudowanych dotychczas maszyn służących do robót ziemnych. Manewrowanie takim kolosem jest ekstremalnie trudne. Bosch Security Systems oferuje kamery, które pomagają operatorom w manewrowaniu maszynami. Kamery te są instalowane w miejscach niewidocznych z kabiny operatora, ten zaś ma możliwość podglądu obrazu i sterowania kamerami. Od wielu lat wśród kamer obrotowych wyróżnia się seria kamer Bosch MIC – mają one zwarte obudowy i odznaczają się ekstremalnie dużą odpornością na wstrząsy

Nie mniej istotnymi elementami systemów dozoru wizyjnego są systemy rejestracji obrazów. Firma Bosch jest twórcą producentem technologii rejestracji obrazów dla dużych systemów monitorowania. Video Recording Manager z opcją bezpośredniego zapisu nagrań na jednostkach iSCSI jest najbardziej zaawansowanym rozwiązaniem przeznaczonym do rejestracji obrazów w systemach TCP/IP – gwarantującym wysoką niezawodność oraz możliwość wykorzystania lokalnego zapisu w kamerach w pełnym zakresie funkcjonalnym. Programowanie zarządzające Bosch Video Management System (BVMS) jest jednym z najbardziej popularnych programów zarządzających systemami wizyjnymi klasy Enterprise.

Systemy sygnalizacji pożarowej – najważniejsza jest szybka detekcja zagrożeń

Każdy pożar – zarówno ten powstały z przyczyn technologicznych, jak i ten, który został wywołany czynnikiem zewnętrznym – stanowi największe zagrożenie dla zdrowia i życia ludzi przebywających na terenie kopalni odkrywkowej. Nie ulega żadnej wątpliwości, że szybka detekcja, weryfikacja i zlokalizowanie ognia na terenie zakładu jest zadaniem priorytetowym. System sygnalizacji pożarowej musi obejmować najważniejsze obiekty w zakładzie, zarówno te *stricto* przemysłowe, jak i zaplecze. Poszczególne obiekty muszą być objęte działaniem jednego systemu gwarantującego szybkie powiadomienie służb ratunkowych i podjęcie akcji gaśniczej.

Bosch Security Systems oferuje rozmaite czujki pożarowe przystosowane do pracy w każdych warunkach (także w strefach Ex), przeznaczone do wykrywania pożarów wszystkich

GUNNEBO®

For a safer world

Bramki szybkie SpeedStile FL



- Najwyższy poziom bezpieczeństwa
- Najbardziej zaawansowana technologia
- Eleganckie wzornictwo
- Idealne rozwiązanie dla nowoczesnych biurowców



www.bramkigunnebo.pl

Gunnebo Polska Sp. z o.o
62-800 Kalisz
ul. Piwonicka 4,
tel. + 48 62 768 55 70
fax + 48 62 768 55 71
www.gunnebo.pl



Fot. 2. Wpływ czasu spędzonego przed monitorem na efektywność pracy operatora systemu monitorującego był opisywany już wielokrotnie w różnych opracowaniach. Operator jest kluczowym elementem systemu bezpieczeństwa, ale technologia musi maksymalnie ułatwiać mu pracę. Taką pomocą jest na przykład zaawansowana analiza obrazu Bosch IVA, dzięki której operator zwraca uwagę tylko na istotne zdarzenia. Podstawowe funkcje wykorzystywane w systemach ochrony obiektów przemysłowych to wykrywanie przerzucania przedmiotów przez ogrodzenie, wykrywanie naruszenia strefy ogrodzenia, wykrywanie gromadzenia się osób w nieodpowiednich miejscach czy też monitorowanie ruchu pojazdów na terenie zakładu. System Bosch IVA umożliwia analizę materiału archiwalnego z zastosowaniem algorytmów inteligentnej analizy obrazów. Przykładowo – można sprawdzić, czy na zarejestrowanych obrazach są osoby w ubraniach mających określony kolor

możliwych rodzajów. Oferuje także system wykrywania dymu z czujkami zasysającymi, liniowe czujki dymu czy też przewody sensoryczne. Od strony zarządzania kluczowe funkcje związane z zarządzaniem realizuje centrala modułowa serii FPA-5000. Możliwe jest sieciowe łączenie wielu takich central w jeden system. Elastyczne moduły funkcyjne ułatwiają wymianę danych i sterowanie elementami wykonawczymi, takimi jak kłapy dymowe czy systemy tryskaczy.

Kontrola dostępu – trzymaj intruzów z daleka

Potencjalne ataki terrorystyczne, akty sabotażu czy wtargnięcia intruzów spędzają sen z powiek osobom odpowiedzialnym za bezpieczeństwo w zakładach infrastruktury krytycznej – tym bardziej że jednocześnie trzeba zapewnić dostęp osobom uprawnionym i odpowiednim służbom. Systemy kontroli dostępu służą do zarządzania dostępem do poszczególnych stref czy pomieszczeń. Typowe systemy kontroli dostępu mają jednak ograniczoną funkcjonalność, co wynika z metod transmisji danych między elementami systemu. Zmniejsza to możliwości aplikacyjne w tak dużych obiektach jak kopalnie odkrywkowe. Takich ograniczeń nie ma system kontroli dostępu firmy Bosch. Komunikacja w systemie odbywa się za pośrednictwem sieci TCP/IP, a więc standardowa infrastruktura sieciowa umożliwia stworzenie systemu zabezpieczającego przejścia i drzwi na terenie bardzo rozległego zakładu. Kontrolery KD marki Bosch współpracują z różnymi czytnikami kart i czytnikami biometrycznymi. Platforma TCP/IP ułatwia integrację systemu kontroli dostępu z innymi systemami. Możliwe jest zintegrowanie go z wizyjnym systemem dozoru umożliwiającym ustalanie przyczyn zdarzeń, a także jego pełne



Fot. 3. Wizyjna weryfikacja przyczyn zdarzeń zachodzących w systemie kontroli dostępu ma zastosowanie w ochronie najważniejszych stref i pomieszczeń w zakładzie. Scenariusz weryfikacji jest elastyczny i może być konfigurowany indywidualnie. Operator systemu KD potwierdza tożsamość osoby przykładającej kartę do czytnika dzięki obrazom z kamer i zdjęciom przechowywanym w rejestrze. Z jednym czytnikiem można powiązać maksymalnie pięć kamer. Operator może sprawdzić, czy za pracownikiem, którego tożsamość jest weryfikowana, nie stoi kolejna osoba i czy do chronionego pomieszczenia nie dostał się ktoś niepowołany

współdziałanie z systemem zarządzania bezpieczeństwem obiektu (Security Management System).

Integracja systemów – sposób na sprawne zarządzanie bezpieczeństwem

Liczba zachodzących zdarzeń i operacji dokonywanych w kilku systemach bezpieczeństwa w dużym i złożonym obiekcie z założenia jest ogromna. Niezależna analiza i obróbka danych jest czasochłonna i kosztowna. Integracja znacznie zwiększa efektywność systemów bezpieczeństwa w zakładach infrastruktury krytycznej. Umożliwia ona korelację zdarzeń zachodzących w różnych systemach, dzięki czemu operator uzyskuje możliwie najpełniejszy obraz sytuacji. Jednocześnie reakcje na zdarzenia mogą być szybsze i bardziej skoordynowane.

Firma Bosch ma w swojej ofercie wszechstronne narzędzie do integracji systemów bezpieczeństwa w postaci oprogramowania Building Integration System (BIS). BIS zawiera składniki automatyzacji i integracji zapewniające pełną kontrolę nad wszystkimi systemami bezpieczeństwa i pozwalające na spójną wizualizację i zarządzanie wszystkimi systemami zainstalowanymi w obiekcie.

Podstawowym nośnikiem danych jest sieć TCP/IP, więc integracja jest łatwa i nie pociąga za sobą dodatkowych kosztów związanych z transmisją danych. BIS może służyć nie tylko do integracji systemów bezpieczeństwa z oferty Bosch. Dzięki standardom OPC można zarządzać dowolnymi systemami innych producentów – nie tylko systemami bezpieczeństwa.

Na koniec warto wspomnieć, że klientom z branży infrastruktury krytycznej firma Bosch proponuje nie tylko rozwiązania z dziedziny zabezpieczeń. W ofercie firmy Bosch znajdują się także systemy napędu i sterowania Rexroth, systemy grzewcze i urządzenia solarne grupy Bosch Termotechnika, a także profesjonalne narzędzia Power Tools.

Firma Bosch, istniejąca od 125 lat, chce być aktywnym i długofalowym partnerem dla firm zarządzających kopalniami odkrywkowymi. Rozwijając produkty ze wszystkich branż, a także dzieląc się zdobytymi doświadczeniami i wiedzą, chcemy wspierać gałąź przemysłu wydobywczego w podwyższaniu poziomu ochrony i zwiększaniu efektywności procesów produkcyjnych.

Michał Borzucki
Bosch Security Systems

Cyfrowy system nagłośnieniowy **PLENA matrix**

Zaskakująca wszechstronność.
Intuicyjna obsługa.



PLENA matrix to system wyznaczający nowe standardy w dziedzinie wydajności i wszechstronności. Technologia zaawansowanego przetwarzania dźwięku DSP, funkcje oszczędzania energii oraz możliwość bezprzewodowej obsługi sprawiają, że PLENA matrix to synonim doskonałej jakości dźwięku z możliwością kierowania go zdalnie do wielu stref. Przy pomocy urządzeń pracujących pod kontrolą systemu operacyjnego iOS zarządzanie nagłośnieniem jest intuicyjne i bardzo wygodne. Więcej informacji u najbliższego przedstawiciela Bosch lub na naszej stronie www.boschsecurity.pl







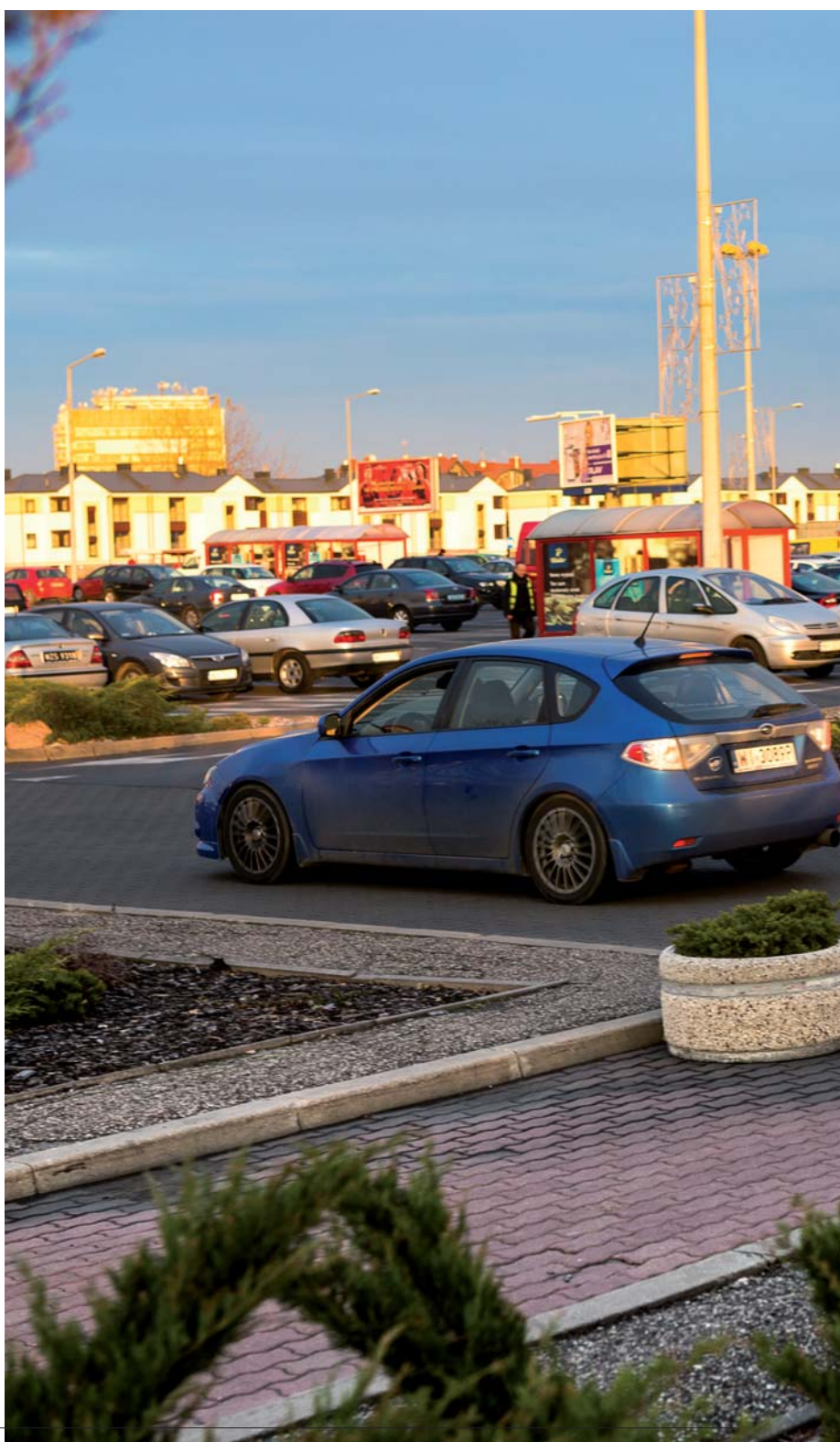
BOSCH

Technologia bliżej nas

System automatycznego rozpoznawania tablic rejestracyjnych firmy GeoVision

Grzegorz Żuk

Od pewnego czasu obserwujemy na polskim rynku znaczny wzrost zainteresowania systemami rozpoznawania tablic rejestracyjnych. Inwestorzy, projektanci oraz integratorzy dostrzegli znaczny potencjał tkwiący w systemach wykorzystujących zaawansowaną analizę obrazu do automatycznego odczytu numerów z tablic rejestracyjnych pojazdów. Artykuł ma na celu prezentację produktów firmy GeoVision oferowanych przez wrocławskiego dystrybutora – firmę POLVISION



W literaturze przedmiotu istnieje kilka skrótów oznaczających systemy automatycznego rozpoznawania tablic rejestracyjnych. W niniejszym artykule używany będzie skrót ARTR (Automatyczne Rozpoznawanie Tablic Rejestracyjnych). Poza tym można spotkać oznaczenia angielskojęzyczne: LPR – *Licence Plate Recognition*, ANPR – *Automated Number Plate Recognition*.

System ARTR analizuje treść obrazu telewizyjnego w celu:

- wykrycia tablicy rejestracyjnej,
- określenia odpowiedniego obszaru rozpoznania,
- korekcji obszaru rozpoznania poprzez zastosowanie kompensacji zniekształceń geometrycznych,
- rozpoznania pojedynczych znaków,

- odczytu ciągu znaków,
- zapisu odczytanych znaków,
- reakcji w zależności od wyniku porównania rozpoznanego ciągu znaków z danymi zapisanymi w bazie danych zgodnie z zaprogramowanym algorytmem.

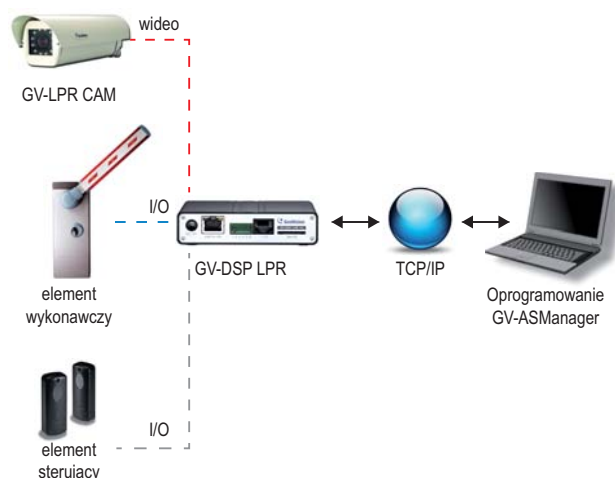
Źródłem obrazu telewizyjnego są specyficznie skonfigurowane kamery analogowe lub megapikselowe kamery IP.

Wykorzystujący rozwiązania firmy GeoVision system służący do rozpoznawania i odczytu tablic rejestracyjnych może mieć wiele zastosowań – od prostych systemów sterowania szlabanami lub bramami wjazdowymi (specyficzna odmiana systemu kontroli dostępu, w którym weryfikacja uprawnień do wjazdu jest dokonywana przez sprawdzenie numeru odczytanego z tablicy rejestracyjnej), poprzez systemy usprawniające proces profilowania/lokalizacji klientów odwiedzających centra handlowe czy systemy zarządzania ruchem na parkingach, po rozległe systemy śledzenia oraz nadzorowania ruchu w obszarach miejskich.

Typowe obszary zastosowań systemów ARTR to:

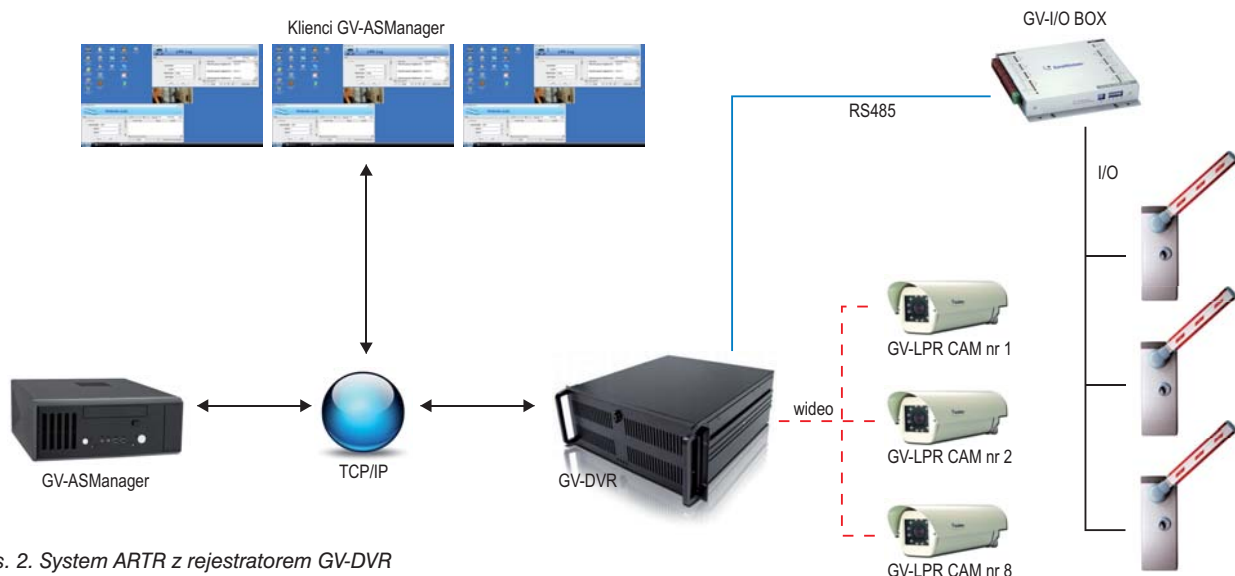
- zarządzanie ruchem na wjazdach/wyjazdach (firmy transportowe, hotele, motele, biurowce, apartamentowce, szpitale, wspólnoty mieszkaniowe),
- sterowanie ruchem pojazdów (systemy szlabanowe, systemy kontroli dostępu),
- kontrola graniczna,
- wyszukiwanie (lokalizowanie) pojazdów,
- wypożyczalnie samochodów,
- systemy parkingowe (centra handlowe, lotniska, parkingi wielopoziomowe),
- systemy automatycznego poboru opłat,
- kontrola transportu towarów (m.in. wagi, systemy wag drogowych),
- kontrola czasu pobytu, czasu podróży oraz wyznaczanie średniej prędkości przejazdu,
- zapobieganie kradzieży paliwa (stacje paliw),
- sterowanie ruchem aut w centrach logistycznych,
- tworzenie statystyki ruchu (zliczanie pojazdów, badanie miejsca zamieszkania kierowców, sprawdzanie częstotliwości przejazdów lub parkowania).

Systemy ARTR pozwalają wyeliminować niezbyt wygodne w użyciu systemy kontroli dostępu bazujące na kartach



Rys. 1. Przykład zastosowania systemu ARTR do sterowania pracą szlabanu





Rys. 2. System ARTR z rejestratorem GV-DVR

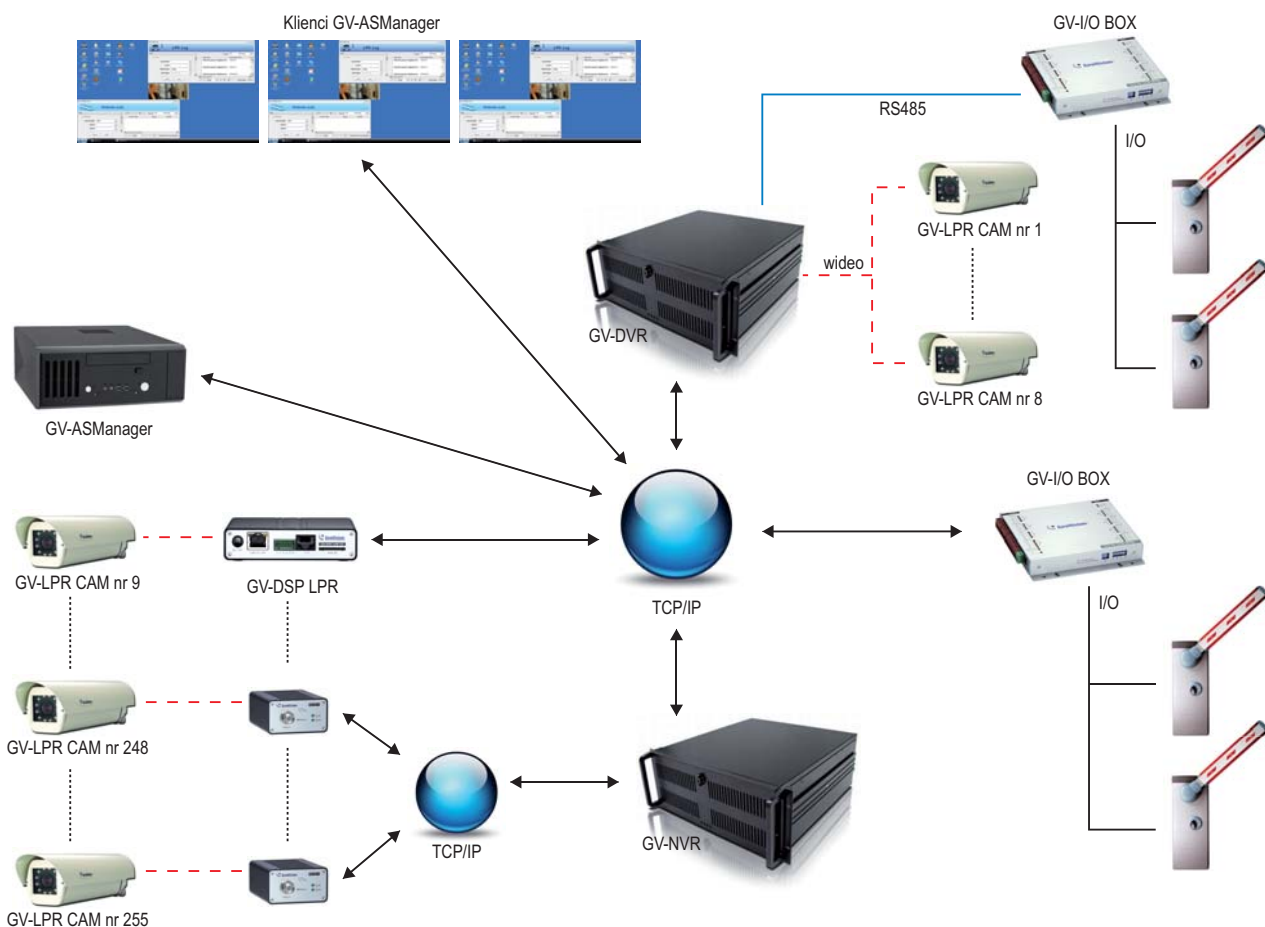
stykowych, kartach zbliżeniowych, pilotach i innych aplikacjach bazujących na rozwiązaniach RFID. Oprócz wyeliminowania identyfikatorów do dodatkowych zalet systemów ARTR należy skrócenie czasu identyfikacji. Proces rozpoznawania i odczytu tablic rejestracyjnych może być inicjowany przez mechanizm detekcji ruchu zaszyty w kontrolerach (GV-DSP LPR, GV-DVR, GV-NVR) jak i przez elementy zewnętrzne, takie jak czujniki ruchu, fotokomórki, pętle indukcyjne itp.

ARTR firmy GeoVision, którego centralnym punktem jest serwer z oprogramowaniem GV-ASManager, jest rozwiązaniem niezwykle przyjaznym zarówno dla instalatora, jak i dla użytkownika

końcowego. Duża skalowalność umożliwia budowę zarówno prostych systemów, złożonych z jednej lub kilku kamer, jak i rozległych, rozproszonych, składających się z kilkudziesięciu kamer, rejestratorów i serwerów wizyjnych GV-DSP LPR.

Przykładem najprostszego zastosowania ARTR jest system złożony z analogowej kamery GV-LPR CAM 10A/20A i serwera wizyjnego GV-DSP LPR, sterujący np. szlabanem/bramą wjazdową lub współpracujący z wagą samochodową (rys. 1.).

Rozwiązania bazujące na serwerach wizyjnych GV-DSP LPR są szczególnie polecane w sytuacjach, w których trudno o zapewnienie ciągłości komunikacji pomiędzy rozproszonymi punktami



Rys. 3. System ARTR – rozwiązanie hybrydowe z zastosowaniem GV-NVR lub GV-DVR oraz GV-DSP LPR

rejestracji a serwerem centralnym. W przypadku wystąpienia problemów z połączeniem serwer wizyjny GV-DSP LPR pracuje jako autonomiczny kontroler realizujący wcześniej skonfigurowany algorytm i zapisujący wyniki rozpoznania na karcie microSD. Po przywróceniu połączenia sieciowego następuje synchronizacja danych, a wyniki rozpoznania są przesyłane do serwera centralnego.

W przypadku obiektów takich jak zakład przemysłowy, osiedle z wieloma wjazdami czy kompleks magazynowy możliwe jest zastosowanie rejestratora GV-DVR lub GV-NVR jako kontrolera systemu ARTR.

W zależności od konfiguracji i wydajności rejestrator jest w stanie obsłużyć do 32 kamer CCTV, w tym osiem kamer służących do rozpoznawania i odczytu numerów z tablic rejestracyjnych. Do rejestratora można podłączyć moduły wejścia/wyjścia i stworzyć rozległy, uniwersalny system dozoru CCTV z funkcją ARTR. Przykład konfiguracji z zastosowaniem rejestratora GV-DVR przedstawiono na rysunku 2.

Aplikacja GV-ASManager umożliwia tworzenie rozbudowanych systemów hybrydowych, łączących rejestratory serii GV-NVR, GV-DVR oraz GV-DSP. Ta uniwersalność pozwala na optymalne wykorzystanie wszystkich możliwości urządzeń i oprogramowania oferowanych przez GeoVision. Hybrydowy system ARTR, współpracujący z serwerami wizyjnymi GV-DSP LPR i rejestratorami GV-NVR i GV-DVR, przedstawiono na rysunku 3.

Zarządzanie funkcjami ARTR odbywa się przy użyciu aplikacji GV-ASManager. Ta prosta w obsłudze aplikacja wykorzystuje funkcje typowe dla systemów kontroli dostępu do zarządzania wszystkimi elementami systemu ARTR. Użytkownik, który zetknął się z systemami kontroli dostępu, jest w stanie bez trudu przyswoić sobie podstawowe zasady obsługi aplikacji GV-ASManager i w pełni korzystać z wielu funkcji służących do konfiguracji, zarządzania uprawnieniami i harmonogramami czasowymi itp.

Na szczególną uwagę zasługuje bardzo użyteczne narzędzie GV-ASManagera, dzięki któremu można obsługiwać system z wykorzystaniem przeglądarki WWW – użytkownik ma możliwość konfigurowania systemu, przeglądania informacji o zdarzeniach, tworzenia raportów i wykonywania innych czynności, korzystając z dowolnego komputera mającego dostęp do sieci. Nie trzeba instalować w tym celu jakiegokolwiek dodatkowej aplikacji.

Wbudowany w system moduł obsługi gości może znaleźć zastosowanie np. w hotelach. Osoba, która chce wjechać do obiektu, loguje się na stronie udostępnionej przez system – podaje na niej swoje dane, np. imię, nazwisko, numer telefonu, adres e-mailowy, cel i termin wizyty, numer tablicy rejestracyjnej. Wprowadzone przez gościa dane trafiają do administratora systemu bądź do pracowników recepcji lub ochrony. Obsługa decyduje, czy wprowadzić dane gościa do systemu i czy nadać mu uprawnienia do wjazdu.

Obecnie firma POLVISION intensywnie testuje systemy ARTR, w których wykorzystywane są kamery megapikselowe. Wyniki dotychczasowych testów są bardzo obiecujące. Poinformujemy o nich wkrótce, w kolejnym artykule.

Grzegorz Żuk
POLVISION
www.polvision.com.pl



ZABEZPIECZENIE PRZECIWPRIĘCIOWE ANALOGOWYCH SYSTEMÓW VIDEOMONITORINGU

AXON Video Protector 16



Ochrona 16 linii analogowych 1Vpp/BNC 750m

Nominalny prąd wyładowczy linia-uziem.	$i_N=5kA - 8/20\mu s [C2]$
Poziom protekcji dla i_N , zgodnie z PN EN 61643-21	$U_{ps} \leq 1000V [C2]$
Pasma przenoszenia	0 – 100MHz
Tłumienie	0,05dB dla 5MHz
Obudowa: metalowa do szafy 19" 1U	444(490)/60/44mm/1,3 kg

AXON Video Protector



Ochrona 1 linii analogowej 1Vpp/BNC 750m

Nominalny prąd wyładowczy linia-uziemienie	$i_N=5kA - 8/20\mu s [C2]$
Poziom protekcji dla i_N , zgodnie z PN EN 61643-21	$U_{ps} \leq 1000V [C2]$
Pasma przenoszenia	0 – 100MHz
Tłumienie	0,05dB dla 5MHz
Obudowa metalowa	63x30x20mm/0,1kg

AXON RS485 Protector



Ochrona 1 linii sterującej RS485 i biphaso do kamer PTZ

Napięcie nominalne	$U_N=6V$
Nominalny prąd wyładowczy linia-uziemienie	$i_N=5kA - 8/20\mu s [C2]$
Poziom protekcji dla i_N , zgodnie z PN EN 61643-21	$U_{ps} \leq 1000V [C2]$
Pasma przenoszenia	0 – 1MHz
Obudowa metalowa	68x30x20mm/0,1kg

Karty katalogowe tych oraz pozostałych wyrobów wraz z raportami z badań w Instytucie Łączności są dostępne na:

www.hsk.com.pl



HSK Data Ltd. Sp. z o.o., 30-198 Kraków, ul. E. Godlewskiego 22
tel. +48 12 638 75 57, fax +48 12 637 09 84, e-mail: info@hsk.com.pl



Firma stosuje system zarządzania jakością spełniający wymagania normy ISO 9001:2008 i potwierdzony certyfikatem wydany przez TÜV SÜD Management Service GmbH

Dane techniczne zgodne z normą: PN-EN 61643-21



Kontrolery autonomiczne przeznaczone do pracy w małych systemach kontroli dostępu



Zintegrowane z czytnikiem kart UNIQUE i HID Prox (125 kHz)

Kontrola 1 przejścia jedno- lub dwustronnie

Instalacja wewnątrz i na zewnątrz, dostępne modele wandaloodporne

Łatwe programowanie

Przystępna cena



C-30-U/H



KZ-400-U/H



KZ-500-U/H



KZ-600-U



KZ-700-U/H



AAT Holding sp. z o.o.

ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01

e-mail: aat.warszawa@aat.pl, www.aat.pl

Kontrolery autonomiczne dedykowane są do najprostszych zastosowań. Ich główną zaletą jest łatwa i szybka instalacja. Sprawdzą się wszędzie tam, gdzie potrzebna jest podstawowa kontrola dostępu w przystępnej cenie.

Kontrolery autonomiczne są doskonałym rozwiązaniem do domów prywatnych i małych firm, a także urzędów czy szpitali, które zwykle dysponują skromnymi funduszami.

Dwuformatowe czytniki kart zaimplementowane w kontrolerach odczytują karty w technologii 125 kHz UNIQUE i HID (za wyjątkiem modelu KZ-600-U).

Obie technologie są bardzo popularne na rynku, dlatego kontrolery mogą stanowić proste uzupełnienie istniejącego systemu zbudowanego na kontrolerach standardowych.

Kontrolery autonomiczne

KZ-400-U/H

Kontroler autonomiczny zintegrowany z czytnikiem kart UNIQUE i HID Prox (125 kHz). Kontrola 1 przejścia jednostronnie. Na wyposażeniu pilot i 2 karty do programowania. Pamięć 2000 kart. Identyfikacja użytkownika za pomocą karty. Do instalacji wewnątrz i na zewnątrz.

KZ-500-U/H

Kontroler zintegrowany z czytnikiem kart UNIQUE i HID Prox (125 kHz). Kontrola 1 przejścia jedno- lub dwustronnie. Na wyposażeniu pilot i 2 karty do programowania. Port drugiego czytnika. Pamięć 10 000 kart. Identyfikacja użytkownika za pomocą karty. Do instalacji wewnątrz i na zewnątrz.

KZ-600-U

Kontroler zintegrowany z czytnikiem kart UNIQUE oraz klawiaturą. Kontrola 1 przejścia jednostronnie (2 przełączniki). Programowanie za pomocą wbudowanej klawiatury. Pamięć 1200 kart. Identyfikacja użytkownika za pomocą karty, kodu lub karty + kodu. Do instalacji wewnątrz i na zewnątrz (wandaloodporny, IP 68).

KZ-700-U/H

Kontroler zintegrowany z czytnikiem kart UNIQUE i HID Prox (125 kHz) oraz klawiaturą. Kontrola 1 przejścia jedno- lub dwustronnie (2 przełączniki). Na wyposażeniu 2 karty programujące. Port drugiego czytnika. Pamięć 2100 kart. Identyfikacja użytkownika za pomocą karty, kodu lub karty + kodu. Do instalacji wewnątrz i na zewnątrz (wandaloodporny, IP 68).

Czytnik kart zbliżeniowych

C-30-U/H

Czytnik kart zbliżeniowych UNIQUE i HID Prox (125 kHz). Interfejs Wieganda 26/37 bitów. Zasięg odczytu karty 3 - 10 cm. Do instalacji wewnątrz i na zewnątrz. Współpracuje z kontrolerami autonomicznymi oraz standardowymi KaDe i Kantech.

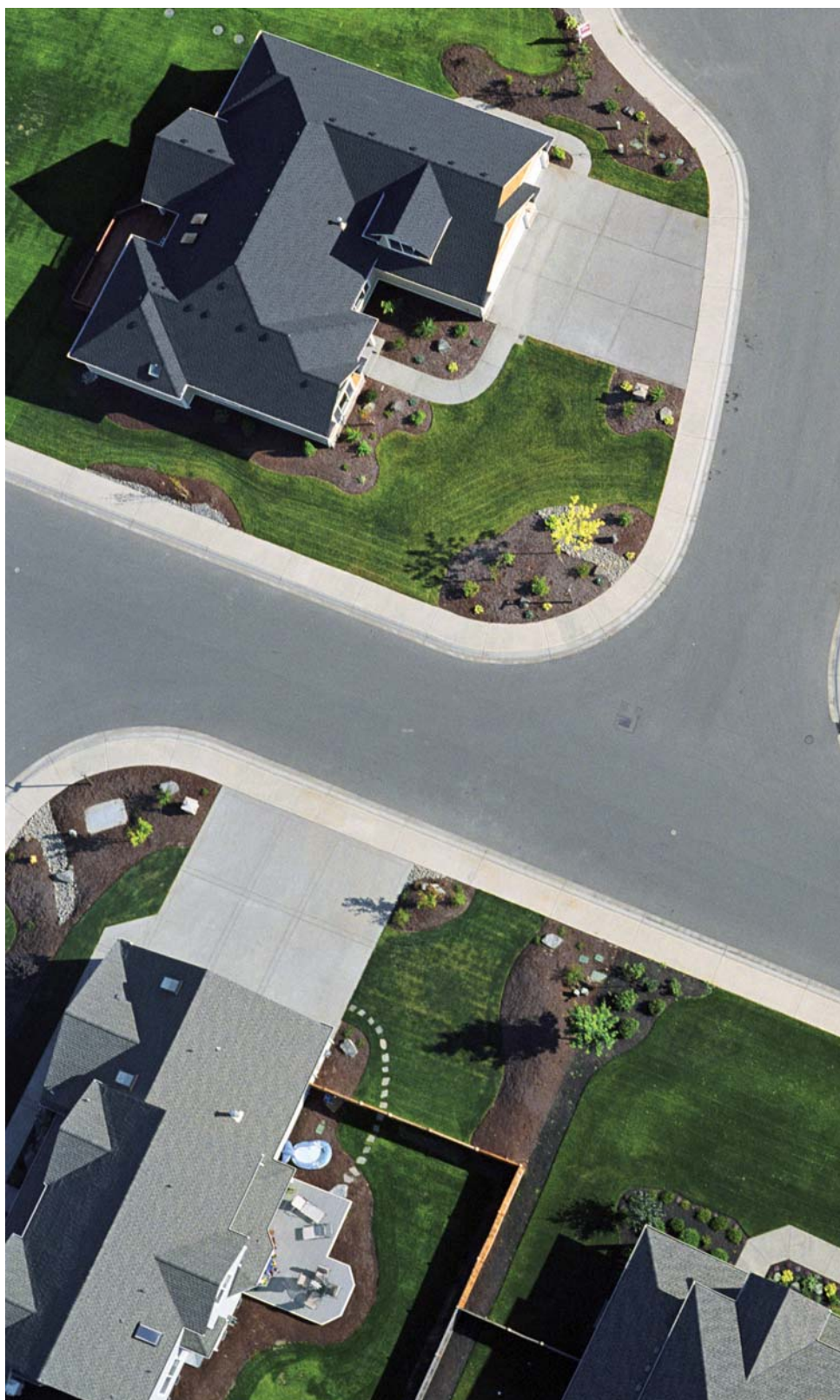
Autonomiczne kontrolery KaDe

Ryszard Sobierski

W systemach kontroli dostępu najczęściej stosowane są systemy zarządzane przez program nadzorczy umieszczony na serwerze.

W przypadku dużych i średnich systemów jest to w zasadzie jedyne sensowne rozwiązanie, które umożliwia administratorowi łatwe i szybkie przesyłanie bazy danych do kontrolerów. Wymaga to połączenia wszystkich kontrolerów w jedną sieć. W wielu przypadkach nie jest to jednak potrzebne i uzasadnione ekonomicznie – wystarczą urządzenia pracujące autonomicznie.

Takim produktom poświęcony jest niniejszy artykuł



System KaDe opisywałem w poprzednich artykułach zamieszczonych w czasopiśmie *Zabezpieczenia*. Dotyczyły one wersji KaDe Lite i Premium, które pracują pod kontrolą programów nadzorczych o tych samych nazwach. Kontrolery pracujące w tych systemach posiadają porty komunikacyjne, które umożliwiają komunikację z programem nadzorczym na komputerze. Są to porty RS485 i Ethernetowe z protokołem TCP. Standardowe kontrolery mają postać modułów elektronicznych umieszczonych w obudowach specjalnych zasilaczy buforowych. Dołączone są do nich

czynniki i pozostałe akcesoria, które są instalowane na kontrolowanym przejściu.

Kontrolery autonomiczne, które chciałbym Państwu zaprezentować, charakteryzują się tym, że nie posiadają portów komunikacyjnych umożliwiających wymianę danych z programem nadzorczym, dlatego ich programowanie odbywa się w inny sposób, który przedstawię w opisie każdego z urządzeń. Drugą, najczęściej spotykaną cechą tego typu urządzeń jest integracja kilku podzespołów w jednej fizycznej obudowie. Obudowa taka zawiera:

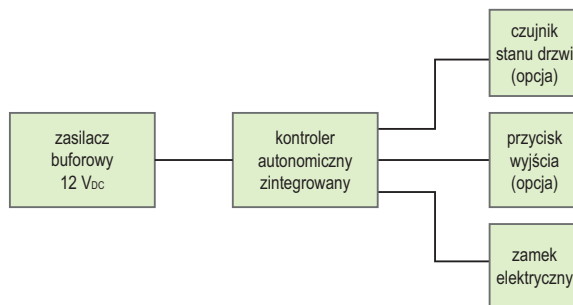
- miniaturowy moduł kontrolera,
- czytnik kart określonego typu,
- klawiaturę kodową (opcjonalnie),
- sygnalizatory: optyczny (dwukolorowa dioda LED) i akustyczny,
- złącze lub kabel do przyłączenia: zasilania, zamka elektrycznego, przycisku wyjścia, czujnika stanu drzwi, portu drugiego czytnika (opcjonalnie) do realizacji kontroli dwustronnej.

Podstawową zaletą tego typu urządzeń jest łatwa i szybka instalacja, możliwa do wykonania nawet przez osoby niemające specjalistycznej wiedzy niezbędnej do zainstalowania i uruchomienia systemu z programem nadzorczym. Te cechy w połączeniu z relatywnie niską ceną takich rozwiązań poszerzają krąg potencjalnych użytkowników. Tego typu produkty znajdują nabywców wśród osób, które do tej pory nie rozważały zainstalowania systemu kontroli dostępu na karty zbliżeniowe lub kody w swoich małych, liczących często kilku lub kilkunastu pracowników firmach, dla których główną barierą jest cena, a często również skomplikowana obsługa. Zwracam uwagę również na fakt, że takie systemy składające się z kilku kontrolerów nie wymagają połączenia magistralą komunikacyjną, co znacznie obniża koszt instalacji i skraca jej czas.

Wprowadzone w bieżącym roku do oferty naszej firmy urządzenia charakteryzują się powyższymi cechami. Są to kontrolery autonomiczne, zintegrowane. Gabaryty tych urządzeń są porównywalne z rozmiarami zwykłych czytników. Niektóre modele wykorzystują wręcz istniejące, gotowe obudowy czytników znanych producentów.

Nowa gama produktów wprowadzonych do oferty obejmuje następujące modele autonomicznych, zintegrowanych kontrolerów: KZ-400-U/H, KZ-500-U/H, KZ-600-U i KZ-700-U/H.

Kontrolery te są przeznaczone do najprostszych zastosowań – wszędzie tam, gdzie potrzebna jest prosta kontrola dostępu w bardzo przystępnej cenie. Mogą one znaleźć zastosowanie nawet w miejscach, w których dotychczas ich nie



Rys. 1. Kontroler autonomiczny z akcesoriami



instalowano, np. przy furtce czy bramie prywatnej posesji, garażu itp. Są idealnym rozwiązaniem dla małych firm oraz urzędów czy szpitali, które zwykle dysponują skromnymi funduszami na takie cele. Jak prosta jest instalacja elektryczna, pokazuje rys. 1.

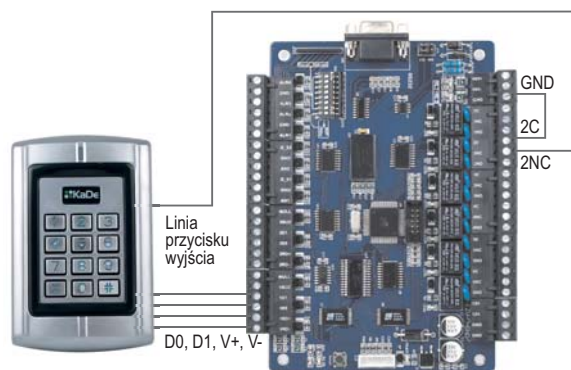
Bardzo ważnymi elementami tych kontrolerów są dwuformatowe czytniki kart. Czytniki te odczytują karty UNIQUE i HID pracujące w polu sygnału 125 kHz (za wyjątkiem modelu KZ-600-U, który odczytuje tylko karty UNIQUE). Oba rodzaje kart są bardzo popularne na naszym rynku, dlatego takie kontrolery mogą stanowić proste uzupełnienie istniejącego systemu, w którym wykorzystywane są standardowe kontrolery. Wystarczy zainstalować jeden z wyżej wymienionych modeli w miejscu, w którym potrzebna jest dodatkowa kontrola dostępu, a nie ma możliwości zainstalowania i przyłączenia do magistrali kontrolera standardowego, i nadać uprawnienia wybranym użytkownikom.

Każdy z modeli wymaga standardowego zasilacza +12 V_{DC}. Zalecany jest zasilacz buforowy z akumulatorem. Taki zasilacz jest wykorzystywany równocześnie do zasilania zamka elektrycznego. Gwarantuje to prawidłową pracę kontrolowanego przejścia po zaniku napięcia zasilającego 230 V_{AC}.

W zależności od modelu programowanie tych urządzeń może odbywać się za pomocą znajdujących się w wyposażeniu kart administratora (*Dodaj kartę*, *Usuń kartę*), za pomocą pilotów na podczerwień (modele KZ-400 i KZ-500) lub za pomocą wbudowanych klawiatur (modele KZ-600 i KZ-700).

Godny uwagi jest miniaturowy pilot dodawany do kontrolerów KZ-400 i KZ-500. Jest to rodzaj przenośnej klawiatury, którą po zakończeniu procesu programowania można schować w bezpiecznym miejscu. W przypadku każdego modelu uruchomienie trybu programowania wymaga podania hasła.

Modele KZ-400 i KZ-500 posiadają obudowy z tworzywa ABS w kolorze czarnym, a modele KZ-600 i KZ-700 – obudowy wandaloodporne wykonane z metalu. Wszystkie są przeznaczone do pracy na zewnątrz i wewnątrz obiektu. Liczba możliwych użytkowników jest zróżnicowana w zależności od modelu – od 2000 użytkowników w przypadku modelu KZ-400 do 10000 użytkowników w przypadku modelu KZ-500. W przypadku modeli KZ-600 i KZ-700 użytkowników można podzielić na dwie grupy z różnymi prawami dostępu.



Rys. 3. Kontroler KZ-700 w trybie czytnika

Modele KZ-600 i KZ-700 mają wbudowane po dwa przełączniki. Dzięki temu każde z tych urządzeń może kontrolować dwa zlokalizowane obok siebie przejścia, co zmniejsza o połowę koszty w przeliczeniu na jedno drzwi. Model KZ-700 umożliwia również wykorzystanie przycisku # na klawiaturze do sterowania dzwonkiem.

Modele KZ-400, KZ-600 i KZ-700 mogą włączyć bistabilny tryb pracy przełączników (zmiana stanu na skutek kolejnych odczytów karty). Umożliwia to np. wykorzystanie ich do włączania w dozór i wyłączania z dozoru systemu alarmowego za pomocą karty.

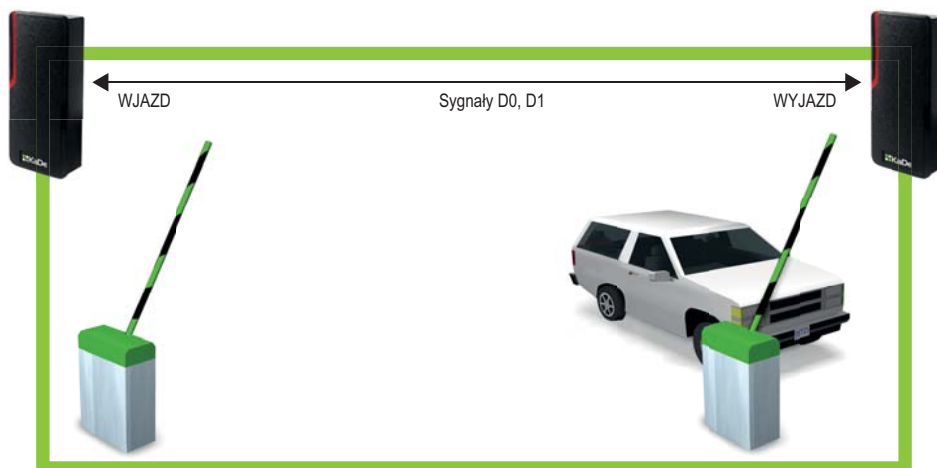
W przypadku modelu KZ-500 możliwa jest aktywacja funkcji *anti-passback* dla jednego lub dwóch przejść (np. oddzielnego wjazdu i wyjazdu z parkingu).

Wszystkie modele mają zabezpieczenia antysabotażowe typu LDR, a modele KZ-500, KZ-600 i KZ-700 specjalne wyjście do sygnalizatora alarmu.

Na koniec podam dwa przykłady zastosowania modeli KZ-500 i KZ-700 w niestandardowy sposób.

KZ-500 jako kontroler parkingowy

Model KZ-500 może pracować również jako kontroler parkingowy. W szczególności chodzi tu o parkingi, które mają dwa niezależne szlabany – jeden na wjeździe, a drugi na wyjeździe. Jeżeli oba szlabany są zainstalowane na przeciwległych obrzeżach parkingu, wymagane są dwa takie kontrolery – każdy do innego szlabanu. Dodatkowym warunkiem jest aktywacja funkcji *anti-passback* w obu kontrolerach obejmującej jeden obszar pomiędzy szlabanami. Dla



Rys. 2. KZ-500 jako kontroler parkingowy

Projektowanie instalacji z zasysającymi czujkami dymu

Andrzej Obłój, Mariusz Konik



Nie wszystkie rzeczy i zjawiska są oczywiste

Zasysające czujki dymu nie są najprostszymi urządzeniami w instalacjach sygnalizacji pożaru. Zdarza się, że projektanci i instalatorzy zapominają o niektórych ich właściwościach, co skutkuje narzekaniami, że czujki zasysające są za czułe i wywołują fałszywe alarmy... Równie dobrze możemy narzekać na samochody – są za szybkie i stąd biorą się mandaty. Z drugiej strony wyjątkowe zalety tych czujek często nie są doceniane i wykorzystywane, – bo nie pamiętamy o nich...

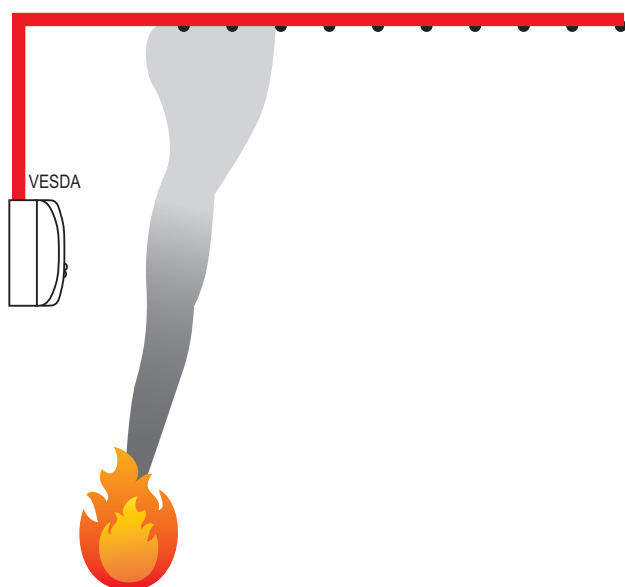
Otwory, nie rury!

Najistotniejszymi elementami systemów zasysających są... otwory. Otwory powinny być rozmieszczone w miejscach, w których chcemy wykryć dym. Miejsca te są często sugerowane przez odpowiednie wytyczne. Rury są złem koniecznym – trzeba w jakiś sposób dostarczyć dym do czujki. Można jednak zrobić to na wiele różnych sposobów. Są na przykład na rynku czujki VESDA FIRE TRACER - 15, które nie pracują z typowymi rurami 25 mm. Każdy otwór zasysający jest połączony z czujką za pomocą długiej, cienkiej, giętkiej kapilary, którą można układać jak kable elektryczne.

Istotne jest rozpoczęcie realizacji projektu od właściwego rozmieszczenia otworów zasysających, a nie rur. Od rozmieszczenia tych otworów będzie zależeć skuteczność wykrywania. Długość, układ i przebieg rur wyznaczmy w programach narzędziowych dostawców czujek zasysających. Minęły już czasy, kiedy konieczne było dopasowywanie sztywnego i zadanego układu orurowania (I, U, H itd.) do pomieszczenia.

Tło

Każdy chroniony obiekt jest w jakimś stopniu zapyłony. Punktowe czujki dymu mają czułość na tyle małą, że pył na ogół tylko je brudzi, ale czułość czujek zasysających może być znacznie większa i niepamiętanie o zapyleniu w tle może skutkować fałszywymi alarmami – z winy człowieka, a nie czujki.



Rys. 1. Wykrywanie dymu przez jeden otwór. Rozcieńczenie dymu w rurze czystym powietrzem

Typowe zapylenie tła latem w biurach to około 0,01% zaciemnienia na metr. Zimą jest dwukrotnie większe, bo działa ogrzewanie. W hali przemysłowej zapylenie wyniesie od 0,08% do nawet 0,5% i więcej. Żeby było trudniej, – tło silnie fluktuuje.

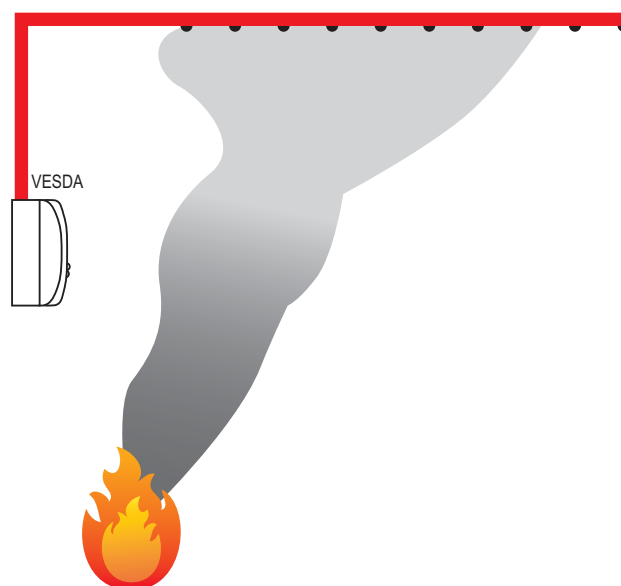
Czułość otworu a nastawa czujki

Wyobraźmy sobie sytuację taką jak na rysunku 1. Czujka zasysa powietrze wieloma (tu dziesięcioma) otworami. Jeśli w czasie pożaru do jednego z tych otworów dotrze dym, to zostanie on w rurze rozcieńczony przez czyste powietrze zasysane pozostałymi otworami, a więc do czujki dotrze dym o gęstości dziesięć razy mniejszej. To oznacza, że aby wykryć dym o określonej gęstości przy jednym otworze, trzeba nastawić czujkę na wykrywanie dymu o gęstości dziesięć razy mniejszej, czyli zwiększyć jej czułość tak, aby była dziesięciokrotnie większa.

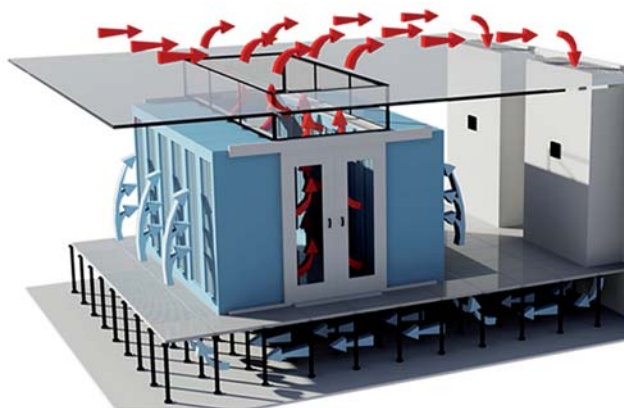
Wyobraźmy sobie największy system zasysający, jaki możemy zbudować, wykorzystując jedną czujkę. To VESDA LASER PLUS i 100 otworów zasysających. Przyjmijmy, że chcemy wykrywać dym o gęstości 5%, czyli chcemy, aby czułość otworu wynosiła 5%. Ile wynosi nastawa czujki? 0,05%. A więc w hali fabrycznej będziemy mieć stale fałszywy alarm. Zapomnieliśmy o tle...

Efekt kumulacyjny

Efekt kumulacyjny to „gratis”, który dostajemy od czujek zasysających. Dzięki niemu wykrycie zagrożenia w dużej przestrzeni następuje znacznie wcześniej, niż można by się tego spodziewać, biorąc pod uwagę czułości otworów. Wyobraźmy sobie sytuację, którą ilustruje rysunek 2. Dym rozchodzi się po pomieszczeniu i dociera do wszystkich otworów. W rurze nie następuje rozcieńczanie dymu, bo nie dochodzi do niej czyste powietrze. Przy jakiej gęstości dymu przy otworach zasysających czujka ustawiona na 0,5% zaalarmuje? Przy 0,5%, a nie dopiero przy 5%, jak obliczyliśmy dla najgorszego przypadku zilustrowanego rysunkiem 1. W praktyce oznacza to, że im bardziej dym rozprzestrzeni się w chronionej przestrzeni, tym szybciej zareaguje czujka zasysająca. To duża przewaga czujek zasysających nad punktowymi.



Rys. 2. Wykrywanie dymu przez wszystkie otwory. Efekt kumulacyjny



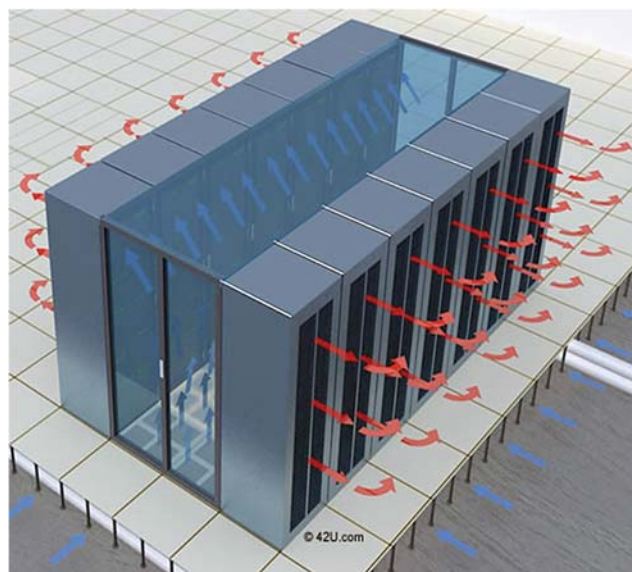
Rys. 3. Wykrywanie dymu w nowoczesnych serwerowniach stało się skomplikowanym zadaniem. Wentylacja wyrzuca powietrze do góry

Równowaga

Intuicja podpowiada, że zasysanie dymu przez otwory położone blisko czujki jest skuteczniejsze niż przez otwory położone daleko. Chcielibyśmy jednak, żeby każdy otwór miał podobne parametry wykrywcze. Jaki jest dopuszczalny rozrzut czułości otworów? Wytyczne różnych krajów sugerują, że nie powinien być większy niż 50% lub 70%. Przyjmijmy 50% dla orurowań rozległych i 70% dla skupionych. Jak jest obliczany ten parametr? Szukamy otworu o największej czułości – odpowiada jej najmniejsza gęstość dymu, która wywołuje alarm w sytuacji pokazanej na rysunku 1. Powiedzmy, że czułość ta wynosi 2%. Teraz szukamy otworu o najmniejszej czułości. Powiedzmy, że czułość ta wynosi 5%. Dzielimy pierwszą czułość przez drugą i dostajemy parametr zrównoważenia wynoszący 40%. To za mało. Musimy poprawić równowagę.

Trudne aspekty podstawowego zastosowania

Serwerownie i inne tego typu obiekty to miejsca, w których rutynowo stosuje się czujki zasysające. Mogłoby wydawać się, że po trzydziestu latach ich wykorzystywanie powinno być opanowane, jednak rozwój i różnorodność metod chłodzenia urządzeń IT sprawia, że wybierając rozwiązanie dla serwerowni,



Rys. 4. Wykrywanie dymu w nowoczesnych serwerowniach. Wentylacja wyrzuca powietrze na boki

trzeba bardzo uważać i mieć pełny obraz sposobu jej chłodzenia. Popatrzmy na rysunki 3 i 4. Na rysunku 3 ciepłe powietrze (a więc i dym!) zostają wyrzucone nad kiosk. Tam łatwo jest wykryć zagrożenie pożarem. Zastosowanie tego samego rozwiązania w przypadku kiosku z rysunku 4 to duży błąd... Tutaj trzeba wykrywać zagrożenie z boków kiosku i tam powinny znaleźć się otwory zasysające.

Co po wykryciu zagrożenia?

Wyobraźmy sobie typową sytuację w serwerowni – system zasysający wykrył dym o tak małej gęstości, że obsługa nie jest w stanie go zobaczyć. Co zrobi obsługa? Uzna, że to fałszywy alarm, a jeśli nie będzie mogła go skasować, stwierdzi, że pewnie czujka jest uszkodzona. Dlatego alarm pożarowy powinien być poprzedzony ostrzeżeniami sygnalizowanymi po przekroczeniu progów odpowiadających niższym poziomom zadymienia. Jeden próg alarmowania nie wystarcza!

Zasilanie czujek zasysających

Każda czujka zasysająca ma wentylator, który pobiera sporo prądu – typowo od około 200 mA do 1,3 A. Taki pobór prądu może przyprawić projektanta o ból głowy, gdy wyliczy pojemność akumulatorów potrzebną do 72-godzinnego podtrzymywania.

Zauważmy, że czujki zasysające są najczęściej stosowane w obiektach ważnych (z różnych względów), a wiele z tych obiektów jest wyposażonych w układy zasilania awaryjnego, które pozwalają na zastosowanie krótszych czasów podtrzymania zasilania systemu, niekiedy nawet tylko przez cztery godziny.

Podsumowanie

Pierwotnie systemy zasysające stworzono w celu bardzo wczesnego wykrywania zagrożenia pożarem w takich obiektach jak serwerownie, centra przetwarzania i przechowywania danych, obiekty telekomunikacyjne, czyste pomieszczenia technologiczne. Stąd wzięła się nazwa VESDA (*Very Early Smoke Detection Apparatus*). Obecnie zdecydowana większość zastosowań jest inna. Czujki zasysające są stosowane w takich obiektach, jak chłodnie, magazyny wysokiego składowania, szyby windowe, przestrzenie bez dostępu serwisowego, hale fabryczne itp., w których wykrywanie pożaru jest trudne i nie może być rozwiązane przy użyciu innych technik. Aby wybrać odpowiednie dla trudnego obiektu rozwiązanie, potrzebna jest specjalistyczna, aktualna wiedza i determinacja, ponieważ w trudnych warunkach żadne rozwiązanie nie będzie bezproblemowe.

Autoryzowanym dystrybutorem produktów VESDA, OSID i XCC firmy Xtralis w Polsce jest Vision Polska (ul. Unii Lubelskiej 1, 61-249 Poznań, www.visionpolska.pl, e-mail: biuro@visionpolska.pl).

Andrzej Obłój
dyrektor techniczny na Europę Centralną i Wschodnią
w firmie Xtralis
Mariusz Konik
Technology and Expert Practices Manager, Vision Polska

IGNIS 2040

OCHRONA
PRZECIWPÓŻAROWA
MAŁYCH
OBIEKTÓW



WEJŚCIA ▼	IGNIS 2040	WYJŚCIA ▲
<p>do 32 czujek punktowych</p>		<p>➔ przekaźniki alarmu i uszkodzenia</p>
<p>do 10 ręcznych ostrzegaczy pożarowych</p>		<p>➔ zasilanie urządzeń zewnętrznych (24 V)</p>
<p>czujka liniowa</p>		<p>➔ linie sterujące sygnalizatorami</p>
<p>czujki iskrobezpieczne</p>		<p>➔ odczyt pamięci zdarzeń</p>
	<ul style="list-style-type: none"> • od 4 do 6 linii dozorowych • 2 linie sterujące sygnalizatorami (zamiennie z liniami dozorowymi) • 5 lat gwarancji 	

Zadania i obowiązki

pełnomocnika ds. ochrony informacji niejawnych związane
z technicznym zabezpieczeniem obiektów wojskowych

Czesław Ćwiek

Zgodnie z art. 14 ust. 1 ustawy
z dnia z dnia 5 sierpnia 2010 r.
o ochronie informacji niejawnych
(Dz. U. Nr 182, poz. 1228), zwanej
dalej ustawą, na kierowniku
jednostki organizacyjnej, w której
przetwarzane są informacje
niejawne, spoczywa obowiązek
zorganizowania i zapewnienia
funkcjonowania ochrony



Zadania pełnomocnika ds. ochrony informacji niejawnych określa w tym zakresie art. 15 ust. 1 ustawy, który nakłada na pełnomocnika obowiązek opracowania planu ochrony informacji niejawnych w jednostce organizacyjnej, w którym musi on z należytą dbałością opisać zastosowane zabezpieczenia fizyczne wspomagające ochronę posiadanych/przetwarzanych zasobów niejawnych podlegających ochronie. Właściwa realizacja zadań związanych z zabezpieczeniem wiąże się między innymi z realizacją inwestycji związanej z instalacją technicznych zabezpieczeń ochraniających obiektów. Głównym celem tego procesu jest stworzenie systemu zabezpieczającego, który będzie niejawny i zabezpieczony przed sabotażem



zarówno na etapie projektowania, jak i podczas jego budowy oraz eksploatacji.

- Działania poprzedzające inwestycję obejmują nw. czynności:
- inwentaryzację posiadanych zasobów niejawnych (informacji, dokumentów, materiałów);
 - analizę zagrożeń i ocenę ryzyka;
 - opracowanie „Koncepcji organizacji zabezpieczenia posiadanych zasobów niejawnych”.

Na ich podstawie zostaną następnie przygotowane pozostałe wymagane prawem dokumenty inwestycyjne:

- minimalne wojskowe wymagania organizacyjno-użytkowe – MWWO-U (opracowuje je użytkownik, a weryfikuje i zatwierdza beneficjent);
- program organizacyjno-użytkowy/program inwestycji
 - POU lub PI (inwestor opracowuje go na podstawie zatwierdzonych MWWO-U lub zleca to zadanie uprawnionemu podmiotowi – w zależności od wielkości, zasięgu i rodzaju inwestycji);
- dokumentację kosztorysowo-projektową (która powstaje na podstawie POU lub PI oraz podlega ocenie i zatwierdzeniu przez komisję oceny projektu inwestycji – KOPI);

Na koniec wydawana jest prawomocna decyzja i zlecenie wykonania zadania.

Przygotowanie planu realizacji inwestycji musi obejmować organizację pracy i opracowanie harmonogramów wykonywania poszczególnych prac – z podziałem na branże (budowlana, instalacje elektryczne i elektrotechniczne niskoprądowe, sieci strukturalne przeznaczone do przetwarzania informacji niejawnych oraz elektroniczne systemy zabezpieczeń).

Ważnym elementem realizacji zadania inwestycyjnego jest ciągły nadzór pełnomocnika ds. ochrony lub wyznaczonej przez niego osoby z pionu ochrony nad pracami budowlanymi i instalowaniem elementów wchodzących w skład zabezpieczenia obiektu, a w późniejszym okresie także odbiór, eksploatacja i serwisowanie.

Stworzenie systemu zabezpieczeń musi być poprzedzone analizą zagrożeń i oszacowaniem prawdopodobieństwa ich wystąpienia. Analiza jest potrzebna ze względów technicznych i organizacyjnych. Należy wybrać urządzenia odpowiedniej klasy – adekwatnie do zagrożeń. Wysoki poziom ryzyka wystąpienia zagrożeń, na przykład w jednostce wojskowej, wymusza zastosowanie urządzeń, które muszą być zgodne z normami obronnymi. Odpowiedni projekt i dobór rozwiązań jest w tym przypadku podstawą kosztorysu inwestorskiego. Następnym etapem jest przygotowanie minimalnych wojskowych wymagań organizacyjno-użytkowych, w których należy określić zakres prac, ich obszar, branże, których dotyczą, oraz wymagania użytkownika dotyczące ochrony informacji niejawnych. W związku z ochroną informacji niejawnych powinno się wskazać odpowiednie rozwiązania techniczne oraz określić zasady organizacji i wymagania odnoszące się do wykonawców prac, dotyczące zwłaszcza przestrzegania zasad ochrony informacji niejawnych.

Wymagania MWWO-U są punktem wyjścia do przygotowania pozostałej dokumentacji dotyczącej zabezpieczenia realizowanej inwestycji (projektu inwestorskiego – POU/PI, specyfikacji indywidualnych warunków zamówienia – SIWZ, dokumentacji przetargowej, zlecenia wykonania, dokumentacji

powykonawczej) oraz, w efekcie końcowym, decyzji PINB – zezwalającej na użytkowanie obiektu.

Przygotowany na zlecenie inwestora projekt musi być uzgodniony z pełnomocnikiem ds. ochrony w zakresie zastosowanych rozwiązań technicznych, planowanych urządzeń technicznych, budowlanych i elektronicznych systemów zabezpieczeń. Pełnomocnik wraz z osobami z branży budowlanej oraz osobami będącymi administratorami elektronicznych systemów zabezpieczeń ocenia, czy projekt spełnia kryteria wskazane w Minimalnych Wojskowych Wymaganiach Organizacyjno-Użytkowych, czy wybrane rozwiązania są adekwatne do zagrożeń, zgodne z normami obronnymi i czy informacje niejawne będą właściwie chronione. Niejednokrotnie projekt dotyczy tylko przebudowy, rozbudowy lub budowy samego systemu zabezpieczeń.

W efekcie końcowym powstaje projekt konfiguracji systemu odpowiedniego pod względem technicznym i ekonomicznym, a zatem możliwy do zrealizowania przez inwestora.

Istotnym elementem projektu jest kosztorys inwestorski, który powinien dokładnie określać wartość całej inwestycji z podziałem na poszczególne branże, w tym ceny zaproponowanych zabezpieczeń, co pozwala na przejście do następnego etapu, którym jest zaplanowanie wydatków związanych z jego realizacją.

Po zaplanowaniu wydatków przychodzi czas na wybranie wykonawcy systemu technicznych zabezpieczeń. Zajmuje się tym właściwa dla jednostki komórka ds. zamówień publicznych, ściśle współpracująca w tym zakresie z pełnomocnikiem ds. ochrony, który uczestniczy w przygotowaniu dokumentacji technicznej zwanej SIWZ (specyfikacją istotnych warunków zamówienia). W takiej specyfikacji precyzuje się wymagania systemowe, przyrządowe i eksploatacyjne dotyczące systemu technicznych zabezpieczeń bez wskazania systemu konkretnej firmy. Dokumentacja powinna zawierać między innymi:

- projekt technicznego systemu zabezpieczeń,
- wzór umowy,
- wzór instrukcji bezpieczeństwa przemysłowego (przygotowanej przez pełnomocnika ds. ochrony użytkownika),
- wymagania stawiane wykonawcy zamówienia, które dotyczą między innymi:
 - a) koncesji na wykonywanie prac związanych z instalowaniem elektronicznych systemów zabezpieczeń,
 - b) świadectw bezpieczeństwa przemysłowego,
 - c) poświadczeń bezpieczeństwa osobowego lub upoważnień do dostępu do informacji niejawnych oznaczonych klauzulą zastrzeżone.

Właściwe zaprojektowanie technicznych zabezpieczeń oraz przygotowanie specyfikacji do dokumentacji przetargowej wymaga od pełnomocnika wiedzy z zakresu systemów zabezpieczeń. Niejednokrotnie pełnomocnik korzysta z wiedzy podległych mu w pionie ochrony administratorów elektronicznych systemów zabezpieczeń. Jeżeli w jednostce organizacyjnej nie ma osób posiadających fachową wiedzę z tego zakresu, trzeba skorzystać z wiedzy rzeczoznawcy czy eksperta w dziedzinie systemów technicznych zabezpieczeń. Zdarza się, że takiego eksperta należy zatrudnić już na etapie przygotowania inwestycji i wyłonienia wykonawcy projektu. Ekspert powinien występować jako doradca inwestora i wykonawca specjalistycznej

części dokumentacji przetargowej. Może on (w imieniu inwestora) nadzorować przebieg prac instalacyjnych i montażowych. Ekspert lub projektant powinien być obecny także przy odbiorze elektronicznych systemów zabezpieczeń i sprawdzić, czy systemy są wykonane zgodnie z projektem.

Rola pełnomocnika nie kończy się w chwili wykonania technicznego zabezpieczenia obiektu. Uczestniczy on jako gestor systemów zabezpieczeń w ich właściwej eksploatacji, konserwacji oraz w usuwaniu ewentualnych usterek i awarii w celu zapewnienia ciągłości ich działania. Jest odpowiedzialny za umożliwienie modernizacji systemów w przyszłości.

Planowanie, projektowanie i instalowanie systemów technicznych zabezpieczeń jest dziedziną obszerną, wymagającą dużej wiedzy z zakresu inżynierii i znajomości specyfiki prac inwestycyjno-remontowych. Ponadto pełnomocnik musi czuwać nad niejawnością tego procesu, zarówno na etapie planowania, jak i na etapie realizacji. Wykonawcy (osoby fizyczne i prawne) powinni posiadać stosowne poświadczenia bezpieczeństwa (osoby fizyczne) i świadectwa bezpieczeństwa przemysłowego (osoby prawne) – adekwatne do wymaganego poziomu ochrony informacji niejawnych wynikającego z najwyższej przewidywanej klauzuli przetwarzanych danych. Niejawność całości postępowania inwestycyjnego gwarantuje szczelność systemu oraz jego właściwe późniejsze działanie.

Czesław Ćwiek

*Bezpieczeństwo oraz Ochrona Informacji Niejawnych
i Danych Osobowych*

Bibliografia:

1. Decyzja Nr 105/MON z 1 kwietnia 2011 r. w sprawie zatwierdzenia i wprowadzenia dokumentów normalizacyjnych dotyczących obronności i bezpieczeństwa państwa (Dz. Urz. MON z 2011 r., nr 7, poz. 90).
2. Decyzja Ministra Obrony Narodowej nr 7/MON z 20 stycznia 2012 r. w sprawie ochrony systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych w resorcie obrony narodowej (Dz. Urz. MON z 2012 r. poz. 8).
3. *Przepisy prawne regulujące procesy inwestycyjne w obiektach i kompleksach resortu ON*, mat. Szefostwa Infrastruktury Inspektoratu Wsparcia Sił Zbrojnych, Bydgoszcz 2011.
4. Rozporządzenie Rady Ministrów z 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. z 19 czerwca 2012 r., poz. 683).
5. Ustawa o ochronie informacji niejawnych z 5 sierpnia 2010 r. (Dz. U. z 2010 r., nr 182, poz. 1228).
6. Zarządzenie Ministra Obrony Narodowej nr 57/MON z dnia 16 grudnia 2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego (Dz. Urz. MON z 2011 r., nr 25, poz. 402).

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Nowe kamery serii F

Większa liczba efektywnych pikseli
976 (H) x 582 (V)

960H

HLC - funkcja redukująca
efekt oślepienia kamery

Inteligentny IR

Zapewnia zrównoważony poziom jasności obrazu
przy pracy oświetlacza IR
(wybrane modele)



Seria F obejmuje 3 rodzaje kamer:

- Kamery kopułkowe: NVC-FC2310D, NVC-FC2311D/IR, NVC-FC2312D
- Kamery wandaloodporne: NVC-FC4320V/IR, NVC-FDN4321V/IR
- Kamery w obudowie z oświetlaczem IR: NVC-FC3308H/IR, NVC-FC3311H/IR, NVC-FDN3309H/IR, NVC-FDN3310H/IRH-2

- 1/3" CCD SONY Super HAD II
- Mechaniczny filtr podczerwieni lub elektroniczna funkcja dzień/noc
- Rozdzielczość pozioma: do 700 TVL
- Czułość: od 0.01 lx/F=1.2
- HLC - funkcja redukująca efekt oślepienia kamery
- WDR - Szeroki zakres dynamiki
- DNR - Cyfrowa redukcja szumu
- Typy obiektywów: f=3.6 mm/f=2.8~11 mm/f=2.8~12 mm (w zależności od modelu)
- 4 strefy prywatności

- Detekcja ruchu
- 2-, 3-osiowa regulacja położenia modułu kamerowego (kamery wandaloodporne i kopułkowe)
- Obudowa o szczelności IP 65 i IP 66 (kamery wandaloodporne i w obudowie)
- Oświetlacz podczerwieni - 2 dużej mocy 18/24/36/44 (kamery z „IR” w nazwie)
- Smart IR - funkcja zapobiegająca „przepalaniu” w obrazie obiektów silnie oświetlonych podczerwienią
- Temperatury pracy: -30°C~50°C (w zależności od modelu)
- Zasilanie: 12 VDC/24 VAC (w zależności od modelu)

Wyłączny dystrybutor produktów NOVUS® w Polsce:



AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Czujka PIR + kamera w systemie alarmowym niezbędny gadżet?

Daniel Kamiński

W dobie kryzysu wykonanie zabezpieczeń dla klientów prowadzących działalność gospodarczą stanowi spore wyzwanie. Z jednej strony system alarmowy i system telewizji dozorowej powinny dobrze spełniać swoją funkcję, z drugiej zaś przedsiębiorcę dysponującego okrojonym budżetem musi być na nie stać



W związku z tym powstało kilka rozwiązań, które integrują w sobie funkcje alarmowania za pomocą czujki PIR oraz funkcje nadzoru wizyjnego możliwe dzięki wbudowanej kamerze CCTV. Na rynku dostępne są czujki PIR z wbudowaną kamerą, ukryte minikamery wbudowane w czujki PIR oraz kamery z wbudowanymi czujkami PIR.

Każde z rozwiązań ma inną konstrukcję oraz przeznaczenie. W artykule omówione zostaną funkcje poszczególnych rozwiązań integrujących kamery z czujnikami PIR oraz przedstawione zostaną ich zastosowania.

Czujka PIR z wbudowaną kamerą

Nowym elementem systemu alarmowego, promowanym od kilku lat, są czujki PIR z wbudowanymi kamerami. Urządzenia te są stosowane najczęściej w bezprzewodowych systemach alarmowych. Skonstruowano je po to, by użytkownicy mogli uzyskiwać obraz obiektu, co ułatwia ustalenie przyczyny alarmu i zredukowanie fałszywych alarmów. Dziś użytkownicy mogą dodatkowo zażądać przesłania obrazu w celu sprawdzenia, co dzieje się w chronionym obiekcie.

Zaletą takiego rozwiązania jest brak kabli, ponieważ wykrywanie i sygnalizacja alarmowa, a także przekazywanie obrazu odbywa się bezprzewodowo. Dzięki temu instalowanie czujek i wkomponowywanie ich w wystrój wnętrza jest łatwiejsze. Czas montażu skraca się, ponieważ nie trzeba doprowadzać kabli zasilających ani łączyć czujek z centralą alarmową.

Kolejną zaletą jest niski koszt takiego systemu w stosunku do zabezpieczeń wykorzystujących dwa systemy oddzielne, czyli system sygnalizacji alarmu i system telewizji dozorowej. W tym przypadku kamera stanowi integralną część systemu alarmowego, a obraz jest wyświetlany na ekranie smartfonu (dzięki specjalnej aplikacji) oraz w centrum monitorowania alarmów.

Przekaz radiowy ma również wady. Powoduje większy pobór prądu, co skutkuje ograniczeniem liczby transmisji tak, aby wbudowane baterie wystarczyły przynajmniej na rok eksploatacji urządzeń. Dlatego transmisje wizyjne są przekazywane tylko po wywołaniu alarmu i ograniczone do 10–15 sekund. Centrala alarmowa przekazuje zdarzenia za pomocą linii telefonicznej, nadajnika GSM lub karty IP. Czas transmisji zajmuje od jednej do dwóch minut.

W celu ograniczenia czasu transmisji obrazu do telefonu klienta lub do centrum monitorowania alarmów stosuje się systemy, które zamiast obrazu ruchomego przesyłają od jednego do ośmiu zdjęć. W tym przypadku pierwsze zdjęcie jest dostępne po ok. 20 sekundach, co pozwala szybciej podjąć decyzję o sposobie reakcji na zdarzenie. W większości przypadków dwa czy trzy zdjęcia wystarczają do poprawnej oceny sytuacji w chronionym obiekcie.

Zastosowania czujek PIR z wbudowaną kamerą

Z założenia głównym celem stosowania czujek PIR z wbudowaną kamerą jest



weryfikacja alarmów za pomocą obrazu. Na jej podstawie zarówno stacja monitorowania, jak i klient mogą ustalić, czy alarm jest prawdziwy czy fałszywy.

Na szczęście dzięki temu, że system jest mało kosztowny i w razie potrzeby klient może zdalnie sprawdzić, czy w chronionym obiekcie wszystko jest w porządku, czujki PIR z wbudowanymi kamerami mają dodatkowe zastosowania. Można na przykład:

- zweryfikować, kto i o której godzinie otworzył obiekt (czujka z kamerą zainstalowana przy wejściu),
- sprawdzić, ilu jest w danej chwili klientów w sklepie,
- sprawdzić, kto wchodzi po godzinach pracy do magazynu,
- sprawdzić, czy auto stoi w garażu,
- użyć tych czujek wszędzie tam, gdzie nie jest wymagany stały nadzór wizyjny i wystarczy możliwość otrzymania zdjęć w razie alarmu lub po wysłaniu prośby o przesłanie obrazu na żądanie.

Ukryta kamera wbudowana w czujkę PIR

Kamery mogą być ukryte w czujkach dymu, zegarach naciennych, ramkach na zdjęcia, oprawkach żarówek, wizerach w drzwiach i w wielu innych miejscach. Dostępne są również kamery ukryte w czujkach PIR – we wspólnej obudowie znajduje się czujka PIR, przyłączona przewodowo do centrali systemu alarmowego, i minikamera, przyłączona przewodowo do rejestratora systemu telewizji dozorowej.

W systemach wykorzystujących czujki PIR obraz może być nagrywany tylko w razie wykrycia ruchu, przy czym specjalistyczna czujka PIR jest znacznie skuteczniejsza niż algorytm detekcji ruchu kamery. Umożliwia to zmniejszenie wielkości pliku archiwum obrazu (nagrania zawierają tylko te klatki, na których widoczne są postacie), co znacznie upraszcza jego przeszukiwanie. Oczywiście takie rozwiązanie nie wyklucza możliwości nagrywania ciągłego.

Zaletą zastosowania czujek z wbudowanymi kamerami jest także mniejsza liczba nawierceń związanych z montażem czujki i kamery, a także możliwość ukrycia obiektywu przed postronnymi osobami. Trzeba zaznaczyć, że maskowanie kamer i nieinformowanie odwiedzających o nagrywaniu ich wizyt może narazić na kontakt z wymiarem sprawiedliwości i jest moralnie problematyczne.

Utrudnieniem jest duża liczba przewodów (przewody sygnałowe i zasilania do kamery oraz sygnalizacja i zasilanie czujki). Wprawdzie kamery ukrywane w czujkach PIR mają mniejszą czułość i rozdzielczość w stosunku do standardowych kamer stosowanych w zabezpieczeniach, ale jeśli uwzględnimy fakt, że są montowane w pomieszczeniach ze stałym oświetleniem, jakość obrazu uzyskiwanego dzięki nim jest zadowalająca.

Zastosowania ukrytych kamer wbudowanych w czujkę PIR

Ukryte kamery służą głównie do zastawiania pułapek na nieuczciwych pracowników oraz klientów. Prowokacje organizuje się za zgodą policji, a materiał wizyjny udostępniany jest tylko kierownictwu firmy oraz policji.

Najczęściej ukryte kamery stosuje się po to, by sprawdzić, który z pracowników jest nieuczciwy, jeżeli nikt postronny nie miał dostępu do mienia firmy, a tymczasem zginęły produkty z magazynu, pieniądze z kasy lub dokumenty z archiwum.

Czasami ukryte kamery stosuje się również do wykrywania kradzieży dokonywanych przez klientów w sklepach, ale w tym przypadku zawsze towarzyszą im kamery zainstalowane w widocznych miejscach. Ukryte kamery mają przeciwdziałać sytuacjom, w których potencjalni złodzieje robią sztuczny tłok, aby zasłonić sobą produkty, którymi się interesują. Z tego względu ukryte kamery stosuje się na przykład wewnątrz stoisk z żywnością (np. z mięsem), aby upewnić się, że produkty nie zostały zabrudzone lub skażone, przy stoiskach z perfumami i kosmetykami, aby chronić drogie produkty przed podmianą lub kradzieżą, a także w innych miejscach, które ze względu na charakter chronionego mienia oraz przeszkody architektoniczne utrudniają stosowanie standardowych kamer.

Ukrytych kamer nie można stosować w miejscach, w których ich wykorzystanie może stanowić naruszenie prawa do prywatności, np. w salach konferencyjnych celem nagrywania spotkań, w szatniach lub przebieralniach, a także w innych miejscach, w których stosowanie kamer jest nieetyczne.

Zastosowania te są wymienione tylko po to, aby uświadomić czytelnikom, że takie rozwiązania istnieją i mogą być stosowane np. przez nieuczciwych konkurentów.

Kamera z wbudowanym detektorem PIR

Na rynku dostępne są kamery, które mogą być substytutem linii dozorowej systemu alarmowego. Kamery te posiadają wbudowane wejścia alarmowe, wyjścia do sterowania innym urządzeniami, a nawet czujki PIR. Mogą być obsługiwane za pośrednictwem strony internetowej lub za pomocą smartfonu z odpowiednią aplikacją. W razie wystąpienia alarmu użytkownicy otrzymują stosowną wiadomość e-mail lub PUSH, a archiwizacja może odbywać się w chmurze. Takie rozwiązania są opłacalne, gdyż umożliwiają uzyskanie funkcji systemu alarmowego przez prosty system telewizji dozorowej.

Wbudowany w kamerę detektor PIR pozwala ograniczyć detekcję ruchu w stosunku do systemu analizy ruchu stosowanego w kamerach. Jest to szczególnie ważne w systemach, które korzystają z usługi zdalnego monitoringu wizyjnego, ponieważ każdy alarm inicjuje transmisję obrazu do centrum monitorowania alarmów. Duża liczba zdarzeń powoduje obciążenie łącza internetowego oraz szybkie zużywanie wykupionych pakietów danych. Zastosowanie czujki PIR znacznie ogranicza liczbę transmisji.

Trzeba zaznaczyć, że czujki PIR działają zarówno w dzień i w nocy, co w przypadku kamer umożliwia oświetlenie sceny dopiero w momencie wykrycia ruchu. Taka właściwość znacznie obniża zapotrzebowanie na prąd. Jest to szczególnie istotne w przypadku zastosowania prostych kamer IP, które mają niższą czułość od standardowych kamer.

Zastosowania kamer z wbudowanym detektorem PIR

Kamery z wbudowanym detektorem PIR rozszerzają zakres zastosowań systemów telewizji dozorowej, wzbogacając je w funkcje systemów alarmowych. Są przeznaczone dla systemów, które wymagają stałego nadzoru w razie wykrycia ruchu przez czujkę PIR.

Z tego względu kamery IP z wbudowanym detektorem PIR można spotkać w systemach pracujących w chmurze służących do samodzielnego monitorowania chronionych obiektów. Znajdą one zastosowanie w:

- punktach usługowych (sprawdzanie liczby klientów),
- kontroli punktualności otwarć i zamknięć obiektów handlowych,
- nadzorowaniu dostępu do kasy w punktach gastronomicznych,
- weryfikacji pracy służb technicznych dokonujących serwisów i napraw,
- w wielu innych przypadkach, w których nie jest potrzebny system telewizji dozorowej i wystarczy kamera IP pracująca w tzw. chmurze.

Kamery z wbudowaną czujką PIR można zastosować również w standardowych systemach obserwacyjnych i w systemach zdalnego monitoringu wizyjnego z głośnikami. Taki system można wykorzystać do komunikacji głosowej oraz nadzoru wizyjnego dostawców, którzy przywieźli towar po godzinach pracy, do nadzoru wizyjnego ogrodzenia parkingu i wydawania intruzom polecenia opuszczenia chronionego terenu, do zdalnych interwencji głosowych w przypadku zaparkowania pojazdu w strefie niedozwolonej (np. zablokowania dojazdu do śmietnika) i w innych sytuacjach, w których niezbędna jest natychmiastowa interwencja.

Podsumowanie

Granica między systemami alarmowymi oraz systemami telewizji dozorowej zaciera się. Systemy alarmowe są wyposażane w kamery wbudowane w czujki, a kamery systemów telewizji dozorowej coraz częściej wykorzystują wbudowane czujki PIR do detekcji ruchu. Ponadto istnieją specjalne aplikacje umożliwiające zdalne sterowanie wymienionymi systemami. W przyszłości obie grupy produktów będą miały podstawowe funkcje kontroli dostępu, np. dzięki zainstalowanej w telefonie funkcji NFC umożliwiającej sterowanie elektrozamkami w firmie.

Można zauważyć, że łączenie czujek PIR i kamer to już nie moda – to część zmian we współczesnym świecie wymuszonych koniecznością oszczędności oraz wykorzystywania systemów zabezpieczeń nie tylko do ochrony, ale również do wspierania biznesu dzięki kontroli pracowników, weryfikacji liczby klientów, nadzorowi dostaw i wielu innym zastosowaniom.

Daniel Kamiński
Ochrona Juwentus



System sygnalizacji pożarowej



CSP

niezawodny system wykrywania i sygnalizacji pożaru

Znajomość potrzeb i oczekiwań rynku, jak również ponad 20 letnie doświadczenie, pozwoliło stworzyć CSP - nowoczesny i zaawansowany w swojej klasie system sygnalizacji pożarowej. Dużym atutem systemu CSP jest system zapewnienia jakości, obejmujący 100% testowanie produkowanych urządzeń dzięki czemu charakteryzują się one wysoką niezawodnością. Atrakcyjne wzornictwo urządzeń powoduje, że doskonale komponują się one zarówno z nowoczesnym, jak i tradycyjnym wystrojem wnętrz.

Zalety systemu CSP:



programowanie za pomocą komputera, ułatwia skonfigurowanie i uruchomienie systemu



wirtualny panel centrali dostępny przez Internet, umożliwia szybkie diagnozowanie systemu na odległość



liczne ułatwienia dla instalatora i personelu konserwującego system, takie jak jednoosobowy test czujek, czy pojedynczy akumulator 12 V zapewniający zasilanie awaryjne

Satel

ul. Franciszka Schuberta 79, 80-172 Gdańsk
tel.: 58 320 94 00, fax: 58 320 94 01
e-mail: satel@satel.pl, www.satel.pl

Monitorowanie pracowników w kontroli operacyjnej firmy

Tytus Andrzej Woźniak

Obecnie nadzór nad pracownikami jest łatwiejszy dzięki nowoczesnemu oprogramowaniu i sprzętowi, które umożliwiają monitorowanie aktywności pracowników w Internecie, kontrolowanie wysyłanych e-maili, rejestrację i przetwarzanie danych dotyczących czasu pracy, geolokalizacji, nadzoru wizyjnego i rejestracji dźwięku. Dostępność rozwiązań technicznych powoduje ich masowe użycie przez menedżerów. Monitorowanie pracowników, tak jak każde rozwiązanie organizacyjne, ma swoją specyfikę. W pewnych zastosowaniach jest szczególnie ważne i umożliwia eliminowanie niekorzystnych zachowań, które w polskim środowisku pracy są nagminne¹. Monitorowanie jest często stosowane w miejscach, w których osiągnięte efekty organizacyjne są nikłe lub nawet odwrotne do planowanych. W takich przypadkach potrzebna jest wiedza z zakresu zarządzania, która pozwoli na selektywne stosowanie rozwiązań teleinformatycznych w monitorowaniu działań pracowników, a co za tym idzie – uzyskanie zamierzonych rezultatów przy zachowaniu możliwie niskich kosztów

1) D. Ambroziak, M. Maj, T. Woźniak, „Anomia i wartości w perspektywie dyrektorów firm 2013”, <http://redwoods.com.pl/materiały-eksperckie.html> (stan z dnia 25 września 2013 r.).



Potężne narzędzia, które nie przynoszą oczekiwanych rezultatów

Problemem wielu menedżerów są niepożądane zachowania pracowników zdarzające się pomimo wprowadzenia procedur kontrolnych. Pracownicy po pewnym czasie dowiadują się, co dokładnie wchodzi w zakres monitorowania, i wykorzystują istniejące luki. W efekcie menedżerowie tracą zaufanie do narzędzi monitorujących i przestają

regularnie je stosować. Zdarza się, że pomimo wdrożenia nowoczesnych metod kontroli następuje wyciek poufnych danych, efektywność pracowników pozostawia wiele do życzenia, zdarzają się kradzieże.

Wyjściem z opisanej sytuacji jest uświadomienie menedżerom zalet i wad zastosowanych rozwiązań oraz przedstawienie możliwych skutków ubocznych.

Monitorowanie pracowników i inne rodzaje kontroli

W praktyce kierowniczej istnieje możliwość stosowania różnych metod kontroli pracowników. W ramach kontroli menedżerskiej² można wyróżnić:

- 1) Monitorowanie zachowań pracowników. Metoda ta polega na poprawnym dostosowaniu się pracowników do wymogów miejsca pracy, norm, procedur;
- 2) Kontrola wyników ekonomicznych pracowników i firmy. Zapewnia ona dane określające, jakie są efekty organizacyjne i finansowe poszczególnych jednostek i całej firmy;
- 3) Kontrola norm społecznych w firmie. Pozwala ona na przeniesienie odpowiedzialności za kontrolę na każdym stanowisku pracy na samych pracowników. Warto podkreślić, że każdy rodzaj pracy bazuje w jakimś stopniu na samokontroli pracowniczej – na dążeniu pracowników do kierowania sobą i kontroli efektów swojej pracy.

Każda z wymienionych metod powinna być stosowana w odpowiednim kontekście sytuacji panującej w danej firmie i spodziewanych efektów. W zależności od specyfiki danej branży, w kontroli menedżerskiej będą przeważały różne metody. W działalności zakładu produkcyjnego, która opiera się na kontraktach długoterminowych, przeważać będzie kontrola zapewniająca powtarzalność i przewidywalność procesów, np. nadzorowanie wypełniania dokumentacji magazynowej w celu zapewnienia jego poprawności i dokładności. Podobnie będzie w dziale likwidacji szkód w zakładzie ubezpieczeniowym. W nim liczy się sprawne stosowanie się do procedur i, co za tym idzie, terminowe rozliczanie każdego kroku likwidacji.

Wszystkie trzy składniki kontroli menedżerskiej są ważne. Nawet na bardzo zruynizowanym stanowisku pracy korzystna jest inicjatywa pracowników przy usprawnianiu istniejących procedur i sposobów współpracy z innymi działami firmy.

Pożądane efekty monitorowania

Monitorowanie zachowania pracowników pomaga w:

- osiągnięciu lepszego bezpieczeństwa firmy, gdy pracownicy mają styczność z wrażliwymi danymi, których wyciek stwarza duże zagrożenie dla organizacji (np. dane finansowe, technologiczne);
- osiągnięciu lepszego wykorzystania zasobów, gdy duża złożoność działania daje możliwość optymalizacji (np. geolokalizacja pozwala kierownikom pełniącym także funkcje logistyków czy sprzedawców na efektywniejsze wykorzystanie czasu i trasy);
- utrzymaniu wysokiej jakości i powtarzalności procesów, np. tych, które mają związek z obsługą klienta (w tym przypadku monitorowanie dostarcza pracownikom informacji zwrotnych o postępach w stosowaniu procedur obsługi);
- likwidacji poczucia bezkarności, które pojawia się, gdy pracownicy mogą mniemać, że za przekroczenie reguł w pewnych obszarach nie spotkają ich konsekwencje (pracownik musi być przekonany, że nie jest bezkarny, ale powinno się dążyć również do tego, by sam postrzegał łamanie wyznaczonych reguł jako złe).

Ograniczenia monitorowania zachowań

Stosowanie monitorowania jest problematyczne, jeżeli menedżer używa danych z systemu (np. z kamer na hali produkcyjnej) jako jedyne czynnika motywującego pracowników do lepszej pracy. Takie działanie jest oparte na założeniu,

2) K. Merchant, W. Van der Stede, „Management Control Systems”, Pearson Education Ltd, 2012.

revizoom IP
Rozwiązania monitoringu IP

Kamery IP
Rejestratory NVR
Kamery IP speeddome
Monitory
Akcesoria

System ReviZOOM^{IP}:

- kamery stacjonarne 1,3MPx; 2MPx; 3MPx oraz 5MPx
- kamery szybkoobrotowe 1,3MPx; 2MPx
- rejestratory sieciowe
- akcesoria do kamer

Możliwości systemu:

- w odróżnieniu od tańszych kamer IP, kamery ReviZOOM^{IP} mogą pracować z rozdzielczością full HD przy 25kl/s z kompresją H.264 i wybieraniem progresywnym
- generują obraz panoramiczny 16:9 (taki jak w telewizji wysokiej rozdzielczości), co w większości przypadków pozwala na redukcję ilości stosowanych kamer
- dwa strumienie H.264 główny i pomocniczy oraz dodatkowy strumień MJPEG pozwalają zoptymalizować zapotrzebowanie na pasmo
- współpraca z innymi urządzeniami zgodnymi z ONVIF 2.2 oraz profilem S
- rejestracja na karcie mikro SD, FTP oraz NAS
- zasilanie PoE

www.revizoom.pl

GDE POLSKA

Włosań, ul. Świątnicka 88, 32-031 Mogiła
tel. 12 256 50 25, 12 256 50 35
fax 12 270 56 96
biuro@gde.pl www.gde.pl

GWARANCJA & GDE POLSKA DOOR-2-DOOR

Infolinia techniczna 693 631 403
Pomoc techniczna techniczny@gde.pl

JOTAKABEL CNB SCOT LonBon tti COMMAX ABAXO revizoom

że kontrola mobilizuje najlepiej. Badania (dot. niewłaściwego wykorzystania komputerów³ czy kradzieży czasu pracy⁴) dowodzą jednak, że najistotniejsza jest zmiana postaw pracowników wobec nieuczciwych zachowań. Na drugim miejscu w tym rankingu plasuje tworzenie się norm w grupach pracowniczych, a dopiero na trzecim utrudnianie wykroczeń.

Stosowanie technicznych rozwiązań nie zastępuje zarządzania. Okazuje się, że w przypadku nadzoru ciągłego częściej zdarza się, że pracownicy oczekują informowania o wynikach kontroli oraz nagradzania za dobre wyniki. Takim oczekiwaniom trudno jest sprostać, więc kontrolujący ograniczają się do rejestrowania nieprawidłowości. W efekcie monitorowanie staje się narzędziem, które służy przede wszystkim do przyłapania na błędzie, a nie do optymalizacji procesu.

Warto wymienić efekty uboczne monitorowania. Są to m.in.:

- opór przed kontrolą (tzw. reakcja) – psychologiczne dążenie do autonomii i niechęć do podlegania kontroli właściwe wszystkim ludziom (w przypadku zbyt intensywnej, drażniącej inwigilacji efektem może być negatywna reakcja pracowników na wszelkie przejawy kontroli w miejscu pracy);
- koncentrowanie się pracowników na ukrywaniu błędów, a nie na poprawie jakości pracy („wy mnie śledzicie, a ja staram się schować”);
- obniżenie satysfakcji pracowników (przez wielu pracowników monitorowanie jest postrzegane jako ingerencja w ich prywatność⁵) i wzmożona rotacja, która jest szczególnie niekorzystna, jeśli odchodzą wykwalifikowani specjaliści.

Znajomość efektów ubocznych pozwala na łagodzenie ich skutków, np. przez wyjaśnianie pracownikom celu kontroli, dostarczanie informacji o efektach pracy i inne działania.

Konieczność odpowiedniego stosowania monitorowania

Powyżej przedstawiono obszary zastosowań monitorowania, a także jego ograniczenia i niepożądane efekty uboczne. Wykorzystując tę wiedzę, menedżerowie powinni dokonywać wyboru i wykorzystywać odpowiednie metody z uwzględnieniem analizy sytuacji w swojej firmie. Należy dostosować rozwiązania do potrzeb kadry kierowniczej i wziąć pod uwagę spodziewane efekty biznesowe. Rezultatem będzie wówczas ograniczenie kosztów zarządzania, czasu poświęcanego na kontrolę, strat wynikających z nieuczciwych zachowań pracowników i jednocześnie wzrost wyników finansowych firmy.

Na koniec pragnę przypomnieć, że istnieje również istotny aspekt prawny monitorowania pracowników⁶.

Tytus Andrzej Woźniak

doradca ds. systemów kontroli menedżerskiej

3) J. D'Arcy, S. Devaraj, *Employee misuse of information technology resources*, *Decision Sciences*, vol. 43, 12/2012.

4) C. Henle, C. Reeve, V. Pitts, „Stealing Time at Work”, *Journal of Business Ethics*, vol. 94, 06/2010.

5) J. Chalykoff, T. Kochan, „Computer-aided Monitoring”, *Personnel Psychology* nr. 42, 2009.

6) M. Szczepanek, „Prawo pracownika do prywatności a monitoring w miejscu pracy”, http://www.hrk.pl/pl/home/moja_kariera/prawo_pracy/Prawo_pracownika_do_prywatno%C5%9Bci_a_monitoring_w_miejscu_pracy.aspx (stan z dnia 23 września 2013 r.).



RACS 4.5

System Kontroli Dostępu

- kontynuacja popularnego systemu RACS 4
- nowa centrala systemu z wbudowanym interfejsem TCP/IP
- bezpieczna komunikacja szyfrowana AES 128 CBC
- współpraca z czytnikiem linii papilarnych RFT1000 (ROGER)
- obsługa zamków mechatronicznych systemu SALLIS (SALTO)
- integracja z centralami alarmowymi serii INTEGRA (SATEL)
- integracje CCTV: Hikvision, Dahua, Geovision



www.roger.pl

roger[®]

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



ME-5 - obudowa systemowa

Efektywny sposób instalacji kontroli dostępu i redukcji jej kosztu

Kontrolery, zasilacz oraz akumulator widoczne na zdjęciu nie wchodzą w skład ME-5



Lotnisko w Krakowie jest bezpieczne dzięki kamerom Axis Communications

Axis Communications



Fot. 1. Międzynarodowy Port Lotniczy
im. Jana Pawła II Kraków-Balice

Misja

W swojej działalności krakowskie lotnisko dba o zachowanie najwyższych standardów bezpieczeństwa, porównywalnych ze standardami innych europejskich lotnisk. Misją spółki Kraków Airport jest osiągnięcie czołowej pozycji wśród europejskich portów regionalnych, dbanie o wysoki poziom obsługi pasażerów, a co za tym idzie – o ich satysfakcję. Do zadań spółki należy rozbudowa, modernizacja i eksploatacja Międzynarodowego Portu Lotniczego Kraków-Balice oraz podejmowanie wszelkich działań związanych z obsługą lotniczego ruchu pasażerskiego i towarowego (między innymi międzynarodowego przejścia granicznego na terenie portu) w celu promocji Krakowa i regionu. Zarząd spółki stawia na sprawdzone rozwiązania technologiczne, które służą usprawnieniu pracy lotniska. Dotyczy to również systemu nadzoru wizyjnego, którego zadaniem jest strzeżenie bezpieczeństwa pasażerów i personelu krakowskiego lotniska.

Rozwiązanie

Partner Axis Communications – firma DG ELPRO (przy współpracy z firmami KABE Systemy Alarmowe, Carboautomatyka i INTERBUD) wzięła udział w planowaniu modernizacji i digitalizacji systemu nadzoru wizyjnego. Proces był podzielony na cztery etapy. Pierwszy z nich – etap testowy – miał na celu stworzenie systemu nadzoru nowej generacji w nowo powstałym wielopoziomowym parkingu. Z pozoru proste zadanie okazało się nie lada wyzwaniem dla projektantów, instalatorów i sprzętu. Poszczególne poziomy parkingu są słabo oświetlone i odbywa się tam ciągły ruch pojazdów, których światła oślepiają kamery. Kolejne trzy etapy budowy systemu były prowadzone jednocześnie. Istniejący analogowy system monitorowania miał ograniczenia i nie dysponował takimi możliwościami jak system wykorzystujący technologię IP. Z drugiej strony był skomplikowany i kosztowny, a jakość obrazu uzyskiwana na niektórych

obszarach była wystarczająca. Wymiana tego systemu na nowy mogłaby wiązać się z poniesieniem zupełnie niepotrzebnych kosztów i z ogromnym nakładem pracy. Dlatego podjęto ekonomicznie uzasadnioną decyzję – postanowiono zmodernizować istniejący system i przystosować go do integracji z systemem IP. Do tego celu wykorzystano kodery wizyjne Axis.

– *Wybierając rozwiązanie dostosowane do wymogów krakowskiego lotniska, nie mieliśmy wątpliwości co do wyboru partnera technologicznego. Współpracujemy z Axis Communications od kilku lat i jesteśmy świadomi zalet urządzeń dostarczanych przez tego producenta i ich możliwości technicznych. Dla nas najważniejsze jest dobro klienta. Jesteśmy pewni, że zastosowanie stabilnej i otwartej platformy Axis Communications jest właściwym rozwiązaniem* – powiedział Krzysztof Durlak – dyrektor DG ELPRO.

DG ELPRO

Rezultat

Dzięki wielu możliwościom swobodnej konfiguracji i innowacyjnym funkcjom urządzenia Axis umożliwiły uzyskanie satysfakcjonującego obrazu. Duża dynamika kamer pozwala uchwycić każde zagrożenie na parkingu. Z budynku obserwowany jest również teren przyległy. Zastosowano kamery PTZ, które mają bardzo precyzyjny mechanizm obrotowy i doskonałą optykę. Wytworzone obrazy o wymaganej jakości powinny być odpowiednio rejestrowane. Do realizacji tego zadania wybrano platformę duńskiej firmy Milestone. Ze względów bezpieczeństwa rejestracja obrazów odbywa się w strefie zamkniętej, oddalonej od parkingu. Do transmisji strumieni wizyjnych wytwarzanych przez kamery Axis nie jest wymagane szerokie pasmo sieciowe, a objętość zapisywanych plików nie jest duża. Do cyfryzacji istniejącego systemu analogowego wykorzystano kodery wizyjne Axis przetwarzające analogowe sygnały wizyjne na strumienie danych cyfrowych, które są przesyłane do systemu Milestone celem rejestracji. Stary system rejestracji pozostał nienaruszony i działa jako rezerwowany. Digitalizacja pozwoliła zwiększyć możliwości eksploracji archiwum i zarządzania systemem. Efektem jest również możliwość tworzenia wielu stanowisk dozorowych dla uprawnionych pracowników lotniska. Dotychczas niełatwe było dozоровanie płyty postojowej lotniska. Kamery musiały obserwować olbrzymi obszar, często w trudnych warunkach atmosferycznych, dostarczając szczegółowy obraz przez całą dobę. Podobny problem dotyczył ogrodzenia – utrudnieniem były duże odległości i złe warunki oświetleniowe w nocy.

– *Jesteśmy bardzo zadowoleni z realizacji tego projektu. Udało nam się wykorzystać wcześniejsze inwestycje związane z budową systemu analogowego i przejść na wyższy poziom – poziom cyfrowego systemu nadzoru, który umożliwi nam również dalszą rozbudowę i modernizację. Nowe narzędzie umożliwi nam wczesne wykrywanie incydentów i proaktywne reagowanie* – powiedziała Urszula Podraza – rzecznik prasowy spółki Kraków Airport.

Wybrane rozwiązanie spełniło oczekiwania zarządu spółki, a kompetencja partnera przelożyła się na sukces realizacji całego projektu.



FARGO DTC4000 – profesjonalna drukarka kart plastikowych

Idealna dla firm, urzędów i szkół



FARGO®

Profesjonalna drukarka termosublimacyjna dla firm potrzebujących prostego, elastycznego sposobu na kolorową personalizację i kodowanie kart procesorowych. Dzięki modułowej budowie umożliwia łatwą modernizację w miarę rosnących potrzeb.

Elegancka i kompaktowa, zajmuje mało miejsca, a jej obsługa jest bardzo prosta - nie wymaga szkolenia. Drukarka posiada wyświetlacz graficzny Smart Screen pozwalający na łatwą diagnostykę oraz prosty system instalacji taśm, które są umieszczone w kartridżu z funkcją samooczyszczania karty.

Współpracuje z dowolnym programem graficznym działającym w środowisku Windows. Daje świetny nadruk na karcie: wyraźny, kontrastowy o głębokiej barwie, wielokolorowy lub jednokolorowy.

Drukarka posiada dwuletnią gwarancję firmy HID Global, światowego lidera w dziedzinie rozwiązań do weryfikacji tożsamości.

Drukarka oferowana jest wraz z autoryzowanym serwisem gwarancyjnym i pogwarancyjnym Fargo HID realizowanym przez CONTROL SYSTEM FMN

Dane techniczne

- Rodzaj nadruku: termotransfer
- Rozdzielczość wydruku: 300 dpi
- Kolory: 16,7 mln/256 odcieni na piksel
- Prędkość nadruku: 24 s dla taśmy YMCKO
- Obsługiwane karty: PVC, karty wielokrotnego nadruku, rozmiary ISO CR-80, samoprzylepne
- Podajnik na 100 kart
- Odbiornik na 100 kart
- Interfejs do PC: USB, opcjonalnie Ethernet
- Pamięć RAM: 32 MB
- Sterowniki: Windows XP, Vista (32 i 64 bity), Server 2003 i 2008, Windows 7, Linux
- Oprogramowanie: wbudowana aplikacja Swift ID oraz program diagnostyczny FARGO Workbench
- Zabezpieczenia: dostęp za pomocą hasła, kompatybilność z Kensington lock
- Wymiary drukarki jednostronnej:
249 mm × 460 mm × 234 mm/3,63 kg
- Gwarancja: 2 lata

Taśmy

- Kolorowe: YMCKO, półówkowa YMCKO, YMCKOK, YMCFKO, YMCFKOK
- Czarna: rezinowa KO, sublimacyjna BO, standardowa i premium K
- Monochromatyczne: zielona, niebieska, czerwona, biała, srebrna i złota 1000 wydruków
- Nadruk wielokrotny

Opcje dodatkowe

- Moduł dwustronny
- Kodery: kart stykowych i bezstykowych
- Koder paska magnetycznego
- Podajnik wejściowy na 200 kart
- Złącze Ethernet z wewnętrznym serwerem wydruków

Dystrybucja:



CONTROL SYSTEM FMN Sp. z o.o.
Al. Komisji Edukacji Narodowej 96 lok. U-15
02-777 Warszawa

tel./faks 22 855 00 17 do 19, 855 24 33,34
e-mail: cs@cs.pl
<http://www.cs.pl>, <http://www.cpk.com.pl>

FARGO DTC4500 – profesjonalna drukarka kart plastikowych idealna dla dużych firm i organizacji, np. wojska



FARGO®

Profesjonalna drukarka termosublimacyjna przeznaczona do dużych obciążeń produkcyjnych i do ciężkich warunków pracy. Spełnia najbardziej rygorystyczne wymagania bezpieczeństwa w dużych organizacjach.

Szybko i sprawnie wykonuje duże serie identyfikatorów. Jednoczesna dwustronna laminacja oszczędza cenny czas.

Drukarka świetnie współgra ze wszystkimi urządzeniami w sieci dzięki możliwości drukowania i kodowania za pomocą pojedynczego kabla Ethernet.

Posiada prosty system instalacji taśm umieszczonych w kartridżu z funkcją samooczyszczania karty.

Współpracuje z dowolnym programem graficznym działającym w środowisku Windows. Daje piękny nadruk na karcie: wyraźny, kontrastowy o głębokiej barwie, wielokolorowy lub jednokolorowy.

Drukarka oferowana jest wraz z autoryzowanym serwisem gwarancyjnym i pogwarancyjnym Fargo HID realizowanym przez CONTROL SYSTEM FMN

Dane techniczne

- Rodzaj nadruku: termotransfer
- Rozdzielczość wydruku: 300 dpi
- Kolory: 16,7 mln/256 odcieni na piksel
- Prędkość nadruku: 7 s dla taśmy K, 12 s dla taśmy KO, 24 s dla taśmy YMCKO, 31 s dla taśmy YMCKOK
- Obsługiwane karty: PVC, poliestrowe z wykończeniem PVC, karty wielokrotnego nadruku, rozmiary ISO CR-80 oraz samo-przylepne CR-79 o grubości od 0,229 mm do 1,016 mm
- Podajnik na 200 kart
- Odbiornik na 100 kart
- Interfejs do PC: USB, opcjonalnie Ethernet
- Pamięć RAM: 32 MB
- Sterowniki: Windows XP, Vista (32 i 64 bity), Server 2003 i 2008, Windows 7, Linux
- Oprogramowanie: wbudowana aplikacja Swift ID oraz program diagnostyczny FARGO Workbench
- Zabezpieczenia: dostęp za pomocą hasła, kompatybilność z Kensington Lock
- Wymiary drukarki jednostronnej: 249 mm × 460 mm × 234mm/9,1 kg
- Gwarancja: 2 lata

Taśmy

- Kolorowe: YMCKO, półkolorowa YMCKO, YMCKK YMCKOK, YMCFKO, YMCFKOK
- Czarne: rezinowa KO, sublimacyjna BO, standardowa i premium K
- Monochromatyczne: zielona, niebieska, czerwona, biała, srebrna i złota
- Nadruk wielokrotny

Opcje dodatkowe

- Moduł dwustronny
- Kodery: kart stykowych i bezstykowych
- Koder paska magnetycznego
- Podajnik wejściowy na 200 kart
- Złącze ethernet z wewnętrznym serwerem wydruków
- Moduł laminacyjny

Dystrybucja:



CONTROL SYSTEM FMN Sp. z o.o.
Al. Komisji Edukacji Narodowej 96 lok. U-15
02-777 Warszawa

tel./faks 22 855 00 17 do 19, 855 24 33,34
e-mail: cs@cs.pl
<http://www.cs.pl>, <http://www.cpk.com.pl>

Rejestrator NVR5416/5432-16P



Sieciowy rejestrator wizyjny 16/32 kanałów, 1.5U 16PoE

Podstawowe dane techniczne

- Obsługa 16/32 kamer sieciowych
- Obsługa jednego monitora (w trzech standardach)
- Rejestrator współpracuje z kamerami 5 Mp, 3 Mp, 1080p, 720p, D1 i innymi
- Wyjścia HDMI, VGA w standardzie 1080P i wyjście TV
- 16 wejść alarmowych i 6 wyjść przekaźnikowych, interfejsy RS485, RS232
- 4 interfejsy SATA, 3 interfejsy USB, jeden interfejs Ethernet RJ45 (1Gb/s)
- Maksymalny wejściowy strumień danych: 160 Mb/s
- Opcja plug & play, 16 portów PoE

Model	DH-NVR5416-16P	DH-NVR5432-16P
Wizja i fonia		
Kamery IP	16 kanałów wejściowych	32 kanały wejściowe
Dwukierunkowa komunikacja głosowa	jeden kanał wejściowy i jeden kanał wyjściowy, BNC	
Wyświetlanie obrazów		
Interfejs	1 HDMI, 1 VGA, 1TV	
Rozdzielczość	1920×1080, 1280×1024, 1280×720, 1024×768	
Zapis obrazów		
Kompresja	H.264 / MJPEG	
Rozdzielczość	5 Mpix (2560×1920)/3 Mpix (2048×1536)/1080p (1920×1080)/720p (1280×720)/D1 (704×576/704×480)	
Prędkość zapisu	maks. 128 Mb/s (16 kanałów 5 Mpix po 8 Mb/s, 32 kanały 1080P po 4 Mb/s)	
Odtwarzanie i archiwizacja obrazów		
Odtwarzanie	co 1/4/9/16 klatek	co 1/4/9/16 klatek
Tryb wyszukiwania	czas/data, alarm, wyrwykowe (z dokładnością do sekundy),	
Funkcje odtwarzania	odtwarzanie, pauza, stop, przewijanie, szybkie odtwarzanie, wolne odtwarzanie, następny plik, poprzedni plik, następna kamera, poprzednia kamera, tryb pełnoekranowy, powtarzanie, przeszukiwanie, wybór archiwum, cyfrowe powiększenie	
Tryb archiwizacji	pamięć USB/pamięć eSATA/wewnętrzny napęd optyczny SATA/ pamięć sieciowa	
Dodatkowe interfejsy		
USB	trzy porty USB (dwa na tylnym panelu), USB2.0	
RS232	jeden port do komunikacji z PC i klawiaturą	
RS485	jeden port do sterowania kamer PTZ	
Dane ogólne		
Wymiary (szer.×dl.×wys.)	1.5U, 440mm×460mm×68mm	
Masa	5 kg (bez dysków HDD)	

Producent:



Dahua Technology Co., Ltd.
1199 BinAn Road, Binjiang District
Hangzhou, China

tel.: +86-571-87688883, faks +86-571-87688815
e-mail: overseas@dahuatech.com
www.dahuasecurity.com

Kamery z nowym kodekiem H.265 HEVC



Aventura Technologies Inc., lider w branży zaawansowanych technologii bezpieczeństwa i systemów dozoru wizyjnego, jako pierwszy na świecie wprowadził na rynek produkty wykorzystujące najnowszy kodek **H.265 HEVC** (High Efficiency Video Coding solution). H.265 HEVC został zatwierdzony jako standard kompresji sekwencji wizyjnych opracowany przez ISO oraz ITU-T. Ta następna generacja kodeka zmniejsza nawet o 50% ilość danych niezbędnych do zakodowania sekwencji obrazów o wysokiej jakości w porównaniu do swojego poprzednika H.264. Producent posiada w swojej ofercie serię kamer wykorzystujących kodek H.265 HEVC.

Dane techniczne kamery CAM-IPM-2X5-DNP

- Przetwornik: 1/2.8" CMOS, skanowanie progresywne
- Rozdzielczość: 3 MPx (2048×1536)
- Zamocowanie obiektywu: C/CS
- Min. oświetlenie: 0.5 lx @ F1.2, 0.1 lx @ F1.2 (funkcja sens-up aktywna)
- WDR: Tak
- Elektroniczna migawka: 1/25 (1/30 ~1/100,000 s)
- Synchronizacja: wewnętrzna
- Kompresja obrazu: H.265 HEVC / MJPEG
- Generowany strumień: 32Kbps ~8Mbps, potrójny strumień
- Liczba klatek na sekundę: 1920×1080/1280×720 @ 30 FPS
- Kompresja dźwięku: Ogg Vorbis
- Obsługiwane protokoły sieciowe: TCP/IP, HTTP, DHCP, DNS, RTP/RTCP, PPPoE (FTP, SMTP, NTP, SNMP opcjonalnie)
- Kompatybilność: ONVIF, PSIA, CGI
- Interfejsy komunikacyjne: RJ45 Ethernet, RS485
- Redukcja szumów: 3D DNR
- BLC (Back Light Compensation): tak
- BFA(Back Focus Adjustment): tak
- AWB (Auto White Balance): tak
- Zapis wewnętrzny: karta SDXC, do 64 GB
- Środowisko pracy: wewnątrz budynków
- Temperatura składowania: -20~60° C
- Temperatura pracy: -10~60° C
- Wilgotność pracy: ≤ 95% bez kondensacji
- Zasilanie: 24 V_{AC}, 12V_{DC}, PoE
- Pobierana moc: 6 W
- Masa: 830 g
- Wymiary: 69 x 65 x 145 mm
- Certyfikaty: CE, FCC, UL
- Gwarancja: 3 lata

Dystrybutor:

ZBAR

ZBAR PHU Mariusz Popenda
ul. Krakowska 60
94-214 Łódź

tel. 42 611 12 97, faks 42 611 12 98
e-mail: zbar@zbar.com.pl
www.zbar.com.pl

Kamera IP XWA-502V



revizoom

W ofercie kamer marki RevIZOOM dostępne są kamery kompaktowe o rozdzielczości 5 MPx. Duża rozdzielczość i własny oświetlacz o dużej mocy to cechy, które sprawiają że jest to idealna kamera do pracy w systemach dozorowych, gdzie wymagana jest lepsza jakość niż oferują popularne kamery o rozdzielczości 2 MPx. Kamery RevIZOOM mogą wytwarzać obrazy o rozdzielczości 2592 x 1920 z prędkością 10 kl./s, 2048 x 1536 z prędkością 20 kl./s oraz 1920 x 1080 z prędkością 30 kl./s. Kamery mają nowoczesne przetworniki Aptina CMOS o rozmiarach 1/2,5". Kamera ma wbudowany oświetlacz pracujący w podczerwieni, w którym wykorzystane zostały nowatorskie diody świecące Super Flux, dzięki czemu w porze nocnej możliwa jest obserwacja obiektów oddalonych od kamery nawet o 40 m. Podobnie jak wszystkie kamery RevIZOOM, model IP XWA-502V ma wbudowany odsuwany filtr podczerwieni oraz może być zasilany metodą PoE. Obiektyw o ogniskowej regulowanej w zakresie od 3,3 mm do 12 mm pozwala na precyzyjną regulację pola widzenia kamer. Wszystkie kamery mają taki sam firmware co pozwala na jego równoczesną aktualizację w wielu różnych kamerach, poza tym nie może zaistnieć pomyłka polegająca na wczytaniu do danej kamery firmware'u przeznaczonego dla innego modelu.

Cechy kamery

- Progresywne skanowanie – wybieranie kolejno-liniowe (progresywne) wraz prędkością 25 kl./s gwarantuje płynność ruchu bez smużeń czy zniekształceń krawędzi
- Trzy strumienie wizyjne: dwa z kompresją H.264 oraz dodatkowy strumień z kompresją MJPEG – zróżnicowane strumienie wizyjne pozwalają na transmisję obrazów różniących się jakością poprzez sieci o różnych przepustowościach
- Zgodność z ONVIF 2.2 oraz ONVIF profil S
- Obsługa za pomocą przeglądark Internet Explor, Firefox i innych, z zainstalowanym dodatkiem Flash Player
- Dwukierunkowa komunikacja głosowa
- Analogowe, wizyjne wyjście serwisowe – pozwala na równoczesne udostępnianie obrazów z kamery zarówno w sieci IP jak poprzez wyjście analogowe
- Możliwość nagrywania materiału wizyjnego na karcie pamięci mikro SD o pojemności do 64 GB
- Możliwość nagrywania obrazów na serwerze FTP oraz sieciowej pamięci NAS (w udostępnionym katalogu)
- Podgląd obrazu za pomocą smartfonów
- Odporność mechaniczna IK5
- Klasa szczelności obudowy IP66
- Zasilanie metodą PoE – (Power over Ethernet, IEEE 802.3af)

Dane techniczne

- Kamera kompaktowa zewnętrzna
- Rozdzielczość: 2592 x 1920, 5 MPx
- Przetwornik: CMOS 1/2,5" Aptima
- Obiektyw: ogniskowa od 3,3 mm do 12 mm, DC Iris
- Czułość: 0,5 lx (kolor), 0,0 lx (IR włączony)
- Doświetlenie: 25 sztuk diod świecących Super Flux IR, 850nm, zasięg do 40 m
- Filtr IR: mechanicznie odsuwany filtr podczerwieni TDN
- Maks. strumień wizyjny:
 - 1: 50 kb/s – 12 Mb/s
 - 2: 10 kb/s – 6 Mb/s
 - 3: MJPEG – 50 Mb/s
- Wymiary: 377 x 110 mm
- Masa: 1,65 kg
- Obudowa: IP66/IK5
- Zasilanie: 12 V_{DC} maks. 10 W; 0,84 A, PoE IEEE 802.3af

Dystrybucja:

&GDE
POLSKA

GDE Polska
Włosań, ul. Świątnicka 88
32-031 Mogiła

tel./faks 12 256 50 35, 256 50 25
faks 12 270 56 96
e-mail: biuro@gde.pl

Monitor wideodomofonowy CDV-70UM



COMMAX
SmartHome & Security

Oferta firmy rozszerzyła się o nowy model monitora COMMAX **CDV-70UM**. Monitor ma szklany przedni panel i szarą obudowę. Oprócz standardowych cech modelu CDV-70U (7" ekran, sensoryczne przyciski, obsługa dwóch wejść, funkcja interkomu) model ten ma także gniazda służące do obsługi kamer CCTV, realizuje funkcję PIP (obraz w obrazie) oraz ma moduł pamięci umożliwiający zapis zdjęć i sekwencji obrazów na karcie Micro SD. Dodatkową funkcją jest tzw. ramka cyfrowa, umożliwiającą sekwencyjne wyświetlanie zdjęć zapisanych na karcie. Kamery są połączone z monitorem za pomocą czterożyłowego przewodu.

Charakterystyka

- Rodzaj ekranu: kolor LCD-LED
- Przekątna ekranu: 7"
- Rozdzielczość ekranu: 800×480 px
- Liczba obsługiwanych wejść: 2
- Funkcja interkomu: tak (monitor-monitor, monitor-unifon)
- Rodzaj monitora: głośnomówiący
- Moduł pamięci: tak (na karcie microSD)
- Standard sygnału wizyjnego: PAL/NTSC
- Regulacja głośności wywołania: tak
- Regulacja głośności rozmowy: tak
- Regulacja kontrastu: tak
- Regulacja jasności obrazu: tak
- Zasilanie: 230 V_{AC}
- Pobór mocy (praca/czuwanie): 16/3,9 VA
- Wymiary (szer.×wys.×gt.): 276×185×33 mm

Dystrybucja:

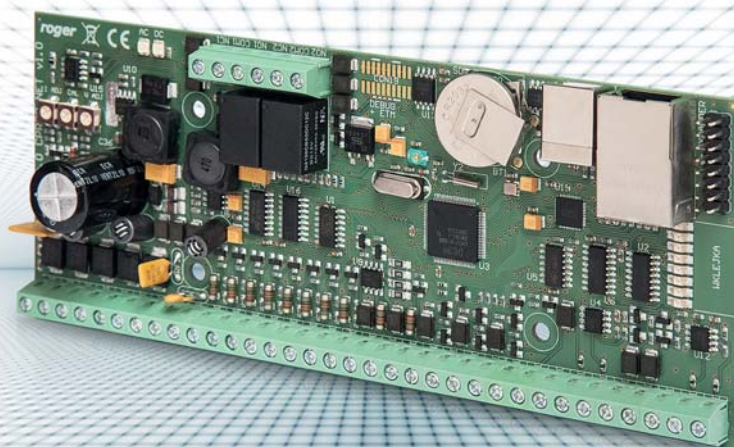
&GDE
POLSKA

GDE Polska
Włosań, ul. Świątnicka 88
32-031 Mogiła

tel./faks 12 256 50 35, 256 50 25
faks 12 270 56 96
e-mail: biuro@gde.pl

Centrala CPR32-NET

Centrala systemu kontroli dostępu RACS 4 z interfejsem IP/Ethernet



Centrala systemu kontroli dostępu **CPR32-NET** stanowi kolejną, rozwojową wersję oferowanej od kilku lat centrali CPR32-SE. Ten nowy produkt realizuje wszystkie funkcje swojego poprzednika, a dodatkowo oferuje szereg nowych możliwości, z których najważniejsze to możliwość programowej integracji z centralami alarmowymi INTEGRA (wymagany jest interfejs INT-RS) oraz możliwość współpracy z bezprzewodowymi zamkami systemu SALLIS (firmy SALTO). Zrealizowana w centrali CPR32-NET koncepcja integracji z systemem INTEGRA umożliwia sterowanie czuwaniem stref alarmowych zarówno z poziomu manipulatorów systemu alarmowego jak i czytników systemu kontroli dostępu. Ponadto system kontroli dostępu pobiera i wyświetla w swoim logu zdarzeń pewne krytyczne zdarzenia pochodzące z systemu alarmowego w wyniku czego operator systemu może się ograniczyć do monitorowania jednego wspólnego logu zdarzeń. Nowa centrala oferuje także opcję zapisu zdarzeń na wymiennej karcie pamięci co umożliwia w praktyce zabezpieczenie bufora zdarzeń na kilka lat pracy systemu bez zagrożenia jego przepełnieniem. Komunikacja z nową centralą odbywa się przez sieć komputerową WAN/LAN z wykorzystaniem standardu szyfrowania AES128 CBC.

Charakterystyka

- Obsługa 32 kontrolerów serii PRxx1/PRxx2
- Osiem wejść NC/NO
- Sześć wyjść tranzystorowych 15 V_{DC}/1 A
- Dwa wyjścia przekaźnikowe 30 V/1,5 A
- Zarządzanie harmonogramami czasowymi i kalendarzami
- Wbudowany interfejs komunikacyjny Ethernet-RS485
- Synchronizacja czasu z serwerami czasu NTP
- Szybka, szyfrowana transmisja danych pomiędzy centralą a komputerem zarządzającym
- Wbudowany nieulotny bufor pamięci o pojemności 250 tys. zdarzeń z możliwością rozszerzenia o dodatkową kartę pamięci o pojemności 33 mln zdarzeń
- Realizacja funkcji globalnych (Strefy Alarmowe, Globalny Antipassback itd.)
- Integracja programowa z centralami alarmowymi INTEGRA (SATEL)
- Integracja programowa z zamkami bezprzewodowymi SALLIS (SALTO)
- Zasilanie 18 V_{AC} lub 12 V_{DC}
- Wbudowany zasilacz impulsowy z wyjściem 12 V_{DC}/1 A
- Aktualizacja oprogramowania wbudowanego (firmware)

Producent:

roger®

Roger Sp.j.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

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

RFT1000

Czytnik linii papilarnych



Czytnik biometryczny **RFT1000** jest wyposażony w wysokiej jakości optyczny skaner linii papilarnych oraz czytnik zbliżeniowy kart standardu ISO/IEC 14443A Mifare. Rozpoznawanie użytkowników może następować przez porównanie zeskanowanego odcisku palca ze wzorcami przechowywanymi w wewnętrznej bazie danych czytnika (tzw. tryb 1:N) lub ze wzorem odcisku palca wczytanym z karty zbliżeniowej (tzw. tryb 1:1). Pamięć czytnika może pomieścić do 1900 wzorów linii papilarnych przy zachowaniu relatywnie szybkiego procesu rozpoznania. Zastosowanie trybu 1:1 pozwala na zapewnienie najwyższej, trzeciej klasy rozpoznania w systemie kontroli dostępu, a dodatkowo wychodzi naprzeciw niektórym regulacjom prawnym, które wymagają aby w systemach rejestracji czasu pracy dane biometryczne były przechowywane na nośnikach danych należących do pracownika. Czytnik może być podłączony do kontrolerów dostępu wyposażonych w interfejs RACS CLK/DTA (kontrolery Roger) lub innych, akceptujących transmisję w popularnym formacie Wiegand. Komunikacja z czytnikiem jest szyfrowana przy użyciu standardu AES128 CBC, który gwarantuje wysoką odporność urządzenia na ataki cybernetyczne. Konfiguracja i zarządzanie wzorcami odcisków palców mogą być przeprowadzone z poziomu programu narzędziowego RogerVDM lub z poziomu oprogramowania PR Master. Dla celów integracji czytnika w innych systemach lub aplikacjach udostępniany jest pakiet SDK.

Charakterystyka

- Optyczny skaner linii papilarnych
- Czytnik kart standardu ISO/IEC 14443A Mifare
- Rozpoznanie użytkownika na podstawie danych biometrycznych odczytanych z karty (tzw. tryb 1:1)
- Rozpoznanie użytkownika na podstawie danych biometrycznych zapisanych w pamięci czytnika (tzw. tryb 1:N)
- Pamięć 1900 wzorów linii papilarnych
- Interfejsy wyjściowe RACS CLK/DTA oraz Wiegand
- Program do konfiguracji czytnika i zarządzania użytkownikami (RogerVDM)
- Zarządzanie użytkownikami bezpośrednio z poziomu programu PR Master (system RACS 4)
- Szyfrowany protokół komunikacyjny AES128 CBC
- Konfiguracja przez port RS485 lub Ethernet/UDP
- SDK dla celów integracji

Producent:

roger®

Roger Sp.j.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

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

Pożarowy sygnalizator optyczny SO-Pd13

Sygnalizator **SO-Pd13** jest sygnalizatorem optycznym przeznaczonym do stosowania w systemach sygnalizacji pożarowej. Sygnalizator spełnia wymagania normy EN 54-23:2010. *Systemy sygnalizacji pożarowej. Część 23: Pożarowe urządzenia alarmowe. Sygnalizatory optyczne.*

Innowacyjna konstrukcja urządzenia zapewnia uzyskanie znacznego obszaru pokrycia (obszar w którym natężenie oświetlenia na powierzchni jest większe od 0,4 lx zgodnie z EN 54-23) przy niewielkim poborze prądu. Pionierski układ optyczny kształtuje bryłę fotometryczną sygnalizatora (umowna przestrzeń, w której natężenie światła osiąga zadeklarowaną wartość katalogową) tak, aby w zależności od wysokości montażu uzyskać maksymalny obszar pokrycia. Sygnalizator generuje impulsowy sygnał optyczny koloru czerwonego. Jako źródło światła zastosowano diody LED mocy.

Zgodnie z normą EN 54-23 sygnalizator SO-Pd13 jest sygnalizatorem należącym do kategorii O, co sprawia, że można go montować zarówno na ścianie jak i suficie. SO-Pd13 występuje w trzech wersjach różniących się maksymalną wysokością montażu: SO-Pd13/3m, SO-Pd13/6m oraz SO-Pd13/9m. W zależności od wersji sygnalizatora zmienia się kształt i rozmiar obszaru pokrycia (wykres oraz plik z bryłą fotometryczną sygnalizatora zamieszczono na stronie internetowej producenta).

Jeśli sygnalizujemy alarm w pomieszczeniach, w których mogą znajdować się osoby wrażliwe na migotanie światła (np. osoby ze skłonnościami do napadów epileptycznych), można stworzyć sieć sygnalizatorów pracujących synchronicznie. Sieć sygnalizatorów może działać jak fala świetlna, wskazując np. kierunek ewakuacji.

W celu doboru liczby sygnalizatorów można skorzystać z programów komputerowych bazujących na bryłach fotometrycznych sygnalizatora zamieszczonych na stronie internetowej producenta lub z prostych obliczeń wykorzystujących dane podane na wykresach.



Najważniejsze cechy

- Zgodność z normą EN 54-23:2010, certyfikat zgodności nr 1438/CPD/0287 wydany przez CNBOP-PIB
- Bardzo mały pobór prądu (<38 mA) przy zapewnieniu znacznego obszaru pokrycia
- Zaawansowany układ optyczny poszerzający zasięg działania urządzenia
- Kategoria O zgodnie z wymaganiami normy EN 54-23
- Trzy wersje wyrobu dostosowane do wysokości pomieszczenia: SO-Pd13/3m, SO-Pd13/6m, SO-Pd13/9m
- Możliwość tworzenia sieci sygnalizatorów pracujących synchronicznie lub w trybie fali
- Synchronizacja z wykorzystaniem linii zasilającej
- Współpraca z dowolnym systemem SAP, dostarczającym napięcie w zakresie 16-32,5 V_{DC}

Zgodnie z postanowieniami Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2010 r. sygnalizator uzyskał świadectwo dopuszczenia do stosowania w ochronie przeciwpożarowej nr 1345/2012, wydane przez CNBOP-PIB.

Producent:



W2 Włodzimierz Wyrzykowski
ul. Czajcza 6
86-005 Białe Błota

tel. /faks 52 584 01 92
www.w2.com.pl
biuro@w2.com.pl

HD-PR0810DNW – kamera IP 5 MPx z serii HD-PRO do pracy na zewnątrz budynków



Jest to kamera IP o bardzo wysokiej rozdzielczości równej 5 megapikseli, uzupełniająca serię kamer HD-PRO. Kamera ma mechanicznie odsuwany filtr podczerwieni, bardzo wydajny system redukcji szumów SPQ+3DNR oraz funkcję WDR rozszerzającą zakres dynamiki, dzięki czemu dobrze radzi sobie z pracą w trudnych warunkach oświetleniowych. Wbudowane funkcje analizy obrazu umożliwiają wykrywanie ruchu w wielu strefach, z różną czułością detekcji. Kamera ma funkcję wykrywania sabotażu (np.: przez zasłonięcie obiektywu, czy gwałtowne przekierowanie kamery na inny plan obserwacji). Standardowo kamera ma wejście i wyjście alarmowe, system zasilania PoE oraz diody podczerwieni zapewniające doświetlenie sceny na odległość do 25 metrów. Obudowa ma klasę szczelności IP66, w komplecie jest dostarczany daszek i uchwyt z prowadzeniem kabli. Oprócz wersji standardowej, kamera ta może być dostarczona w kilku opcjonalnych wersjach, tj. z dodatkowym systemem podgrzewania, z elektrycznie sterowanym obiektywem z funkcją autofocus i auto-iris o ogniskowej regulowanej w zakresie od 3,6 mm do 9 mm (zamiast standardowego obiektywu z ręczną regulacją ogniskowej w zakresie od 3,6 mm do 9 mm z funkcją auto-irys).

Kamera ta, jak każda z grupy HD-PRO, spełnia wymagania ONVIF i może współpracować z systemami zbudowanymi w oparciu o otwarte oprogramowanie takie jak IVTVision, NUUO, exacqVision, Milestone itp.

Urządzenie		HD-PR0810DNW
Kamera 5-Megapikselowa Dzień/Noc		
Przetwornik		1/2,5" 5MPx CMOS Progressive Scan
Rozdzielczość przetwornika		2592(H) × 1944 (V)
Mechanicznie odsuwany filtr IR		Tak
Obiektyw		
		3 mm – 9 mm/F1.2 (opcjonalnie sterowany elektrycznie z autofocus)
		103,5° (Wide); 34,3° (tele)
Pozostałe		
Kompresja obrazu		H.264/MJPEG
Strumieniowanie		Maks. 4 strumienie (4 × H.264 lub 3 × H.264 + 1 × MJPEG)
Rozdzielczość		5M (2592 × 1944)/3M (2048 × 1536)/Full HD 1080p/SXGA/HD 720p/XGA/SVGA/D1/VGA/CIF
Ustawienie obrazu	WDR	Tak
	SPQ+3DNR	Tak
	Zoom cyfrowy	Tak
	Detekcja ruchu	Włączona/Wyłączona
	Strefy prywatności	Włączone/Wyłączone
Dźwięk	Wykrywanie sabotażu	Tak (zasłonięcie, przekierowanie)
	Dwukierunkowa komunikacja głosowa	Wyjście liniowe, Wejście liniowe/Wejście mikrofonowe
	Kodowanie dźwięku	G.711/G.726
Oświetlacz IR		Zasięg do 25 m
Złącza	Zasilanie	Trójkońcówkowe złącze
	Sieć IP	RJ45
	Pamięć Micro SD	SDHC (maks. 32 GB)
	Dźwięk	Line in/Line out
	Alarm	Czterokońcówkowe złącze 1 wyj. (optoizolacja 300 V _{DC} /V _{AC}) + 1 wej. (5 V 10 kΩ)
	Analogowe wyjście wizyjne	1.0 V _{p-p} /75 Ω, BNC
Warunki pracy	Temperatura pracy	-15°C ~ -50°C -40°C ~ 50°C (z grzałką – opcja)
	Wilgotność	10% do 90%, bez kondensacji
Zasilanie		DC 12 V/AC 24 V/PoE
Pobór mocy		Kamera: 5 W (oświetlacz IR: +3 W; grzałka: +12 W; zmotoryzowany obiektyw: +3,6 W)
Certyfikaty		CE, FCC, RoHS
Wymiary		Ø84 × 180 mm (z daszkiem 193 mm)
Masa		940 g
Klasa szczelności		IP66

Producent:

urmet
MIWI

MIWI-URMET Sp. z o.o.
ul. Pojezierska 90a
91-341 Łódź

tel. +48 42 616 21 00, faks +48 42 616 21 13
e-mail: miwi@miwiurmet.com.pl
www.miwiurmet.com.pl

**AAT Holding sp. z o.o.**

ul. Puławska 431
02-801 Warszawa
tel. 22 546 05 46
faks 22 546 05 01
e-mail: aat.warszawa@aat.pl
www.aat.pl

Oddziały:

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

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

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

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

ul. Mieszczkańska 18/1, 30-313 **Kraków**
tel./faks 12 266 87 95, 266 87 97
e-mail: aat.krakow@aat.pl

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

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

ul. Raclawicka 82, 60-302 **Poznań**
tel./faks 61 662 06 60/62
e-mail: aat.poznan@aat.pl

Al. Niepodległości 659, 81-855 **Sopot**
tel./faks 58 551 22 63, 551 67 52
e-mail: aat.sopot@aat.pl

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

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

**ACS ID Systems Sp. z o.o.**

ul. Karola Miarki 20C
01-496 Warszawa
tel. 22 832 47 44
faks 22 832 46 44
e-mail: biuro@acss.com.pl
www.acss.com.pl

**AGIS Fire & Security Sp. z o.o.**

ul. Palisadowa 20/22
01-940 Warszawa
tel. 22 430 83 01
faks 22 430 83 02
e-mail: agisfs.pl@agisfs.com
www.agisfs.pl

**ALARMNET Borkiewicz Sp. J.**

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

**ALARMTECH POLSKA Sp. z o.o.**

Oddział:
ul. Kielnieńska 115
80-299 **Gdańsk**
tel. 58 340 24 40
faks 58 340 24 49
e-mail: info@alarmtech.pl
www.alarmtech.pl

**ALKAM SYSTEM Sp. z o.o.**

ul. Bydgoska 10
59-220 **Legnica**
tel. 76 862 34 17, 862 34 19
faks 76 862 02 38
e-mail: alkam@alkam.pl
www.alkam.pl

**ALPOL Sp. z o.o.**

ul. Scigaly 10
40-208 **Katowice**
tel. 32 790 76 16
faks 32 790 76 60
e-mail: katowice@e-alpol.com.pl
www.e-alpol.com.pl

Oddziały:

ul. Warszawska 56, 43-300 **Bielsko-Biała**
tel. 32 790 76 21
faks 32 790 76 64
e-mail: bielsko@e-alpol.com.pl

ul. Łęczycka 55, 85-737 **Bydgoszcz**
tel. 32 720 39 65
faks 32 790 76 85
e-mail: bydgoszcz@e-alpol.com.pl

ul. Uszczyka 11, 44-100 **Gliwice**
tel. 32 790 76 23
faks 32 790 76 65
e-mail: gliwice@e-alpol.com.pl

ul. Sandomierska 105, 25-324 **Kielce**
tel. 32 720 39 82
faks 32 790 76 94
e-mail: kielce@e-alpol.com.pl

ul. Pachońskiego 2a, 31-223 **Kraków**
tel. 32 790 76 46
faks 32 790 76 73
e-mail: krakow@e-alpol.com.pl

ul. Grenadierów 13, 20-331 **Lublin**
tel. 32 790 76 50
faks 32 790 76 74
e-mail: lublin@e-alpol.com.pl

ul. Senatorska 31, 93-192 **Łódź**
tel. 32 790 76 25
faks 32 790 76 66
e-mail: lodz@e-alpol.com.pl

ul. T. Kutrzeby 16G/112, 61-719 **Poznań**
tel. 32 790 76 37
faks 61 826 63 36
e-mail: poznan@e-alpol.com.pl

ul. Rzemieślnicza 13, 81-855 **Sopot**
tel. 32 790 76 43
faks 32 790 76 72
e-mail: sopot@e-alpol.com.pl

ul. Dąbrowskiego 25, 70-100 **Szczecin**
tel. 32 790 76 30
faks 32 790 76 68
e-mail: szczecin@e-alpol.com.pl

ul. Rzymowskiego 34, 02-697 **Warszawa-Mokotów**
tel. 32 790 76 34
faks 32 790 76 69
e-mail: warszawa2@e-alpol.com.pl

ul. Floriana 3/5, 04-664 **Warszawa-Praga**
tel. 32 790 76 33
faks 32 790 76 71
e-mail: warszawa2@e-alpol.com.pl

ul. Stargardzka 7-9, 54-156 **Wrocław**
tel. 32 790 76 27
faks 32 790 76 67
e-mail: wroclaw@e-alpol.com.pl

Oddziały Alpol Express:

ul. Nowodworska 23, 59-200 **Legnica**
tel. 32 750 30 66
faks 32 750 30 67
e-mail: legnica@e-alpol.com.pl

ul. Oleska 99, 45-222 **Opole**
tel. 32 750 30 36
faks 32 750 30 38
e-mail: opole@e-alpol.com.pl

ul. Odolanowska 49a, 63-400 **Ostrów Wlkp.**
tel. 32 750 30 25
e-mail: ostrow@e-alpol.com.pl

ul. Zbrowskiego 100, 26-600 **Radom**
tel. 32 750 30 33
faks 32 750 30 35
e-mail: radom@e-alpol.com.pl

ul. Polna 65, 87-100 **Toruń**
tel. 32 750 30 80
faks 32 750 30 73
e-mail: torun@e-alpol.com.pl

ul. Strzelecka 20/14, 65-452 **Zielona Góra**
tel. 32 750 30 70
faks 32 750 30 71
e-mail: zielona@e-alpol.com.pl

**ASSA ABLOY POLAND Sp. z o.o.**

ul. Jana Olbrachta 94
01-102 Warszawa
tel. 22 751 53 54
faks 22 751 53 56
e-mail: biuro@assaabloy.com.pl
www.assaabloy.com.pl



FIRMA ATLine Sp. J.
Stawomir Pruski
 ul. Franciszkańska 125
 91-845 Łódź
 tel. 42 231 38 49, 236 30 19
 faks 42 655 20 99
 e-mail: handel@atline.pl
 www.atline.pl



CBC (Poland) Sp. z o.o.
 ul. Krasińskiego 41A
 01-755 Warszawa
 tel. 22 633 90 90
 faks 22 633 90 60
 e-mail: info@cbcpoland.pl
 www.cbcpoland.pl



Dahua Technology Co., Ltd.
 No. 1199, Bin an Road, Bin jiang District
 Hangzhou
 P.R. China
 P.C. 310053
 e-mail: overseas@dahuatech.com
 www.dahuasecurity.com



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



CMA MONITORING
Spółka z ograniczoną odpowiedzialnością Sp. k.
 ul. Puławska 359
 02-801 Warszawa
 tel. 22 546 0 888
 faks 22 546 0 619
 e-mail: info@cma.com.pl
 www.cma.com.pl



DG ELPRO Sp. J.
 ul. Wadowicka 6
 30-415 Kraków
 tel. 12 263 93 85/86
 faks 12 263 93 85
 e-mail: biuro@dgelpro.pl
 www.dgelpro.pl



P.W.H. BRABORK-LABORATORIUM Sp. z o.o.
 ul. Ratuszowa 11
 03-450 Warszawa
 tel. 22 619 29 49
 faks 22 619 25 14
 e-mail: brabork@braborklab.pl
 www.braborklab.pl

Oddziały:
 ul. Świętochłowska 3, 41-909 Bytom
 tel. 32 388 0 950
 faks 32 388 0 960
 e-mail: bytom@cma.com.pl

ul. Zatorska 36, 51-215 Wrocław
 tel. 71 340 0 209
 faks 71 341 16 26
 e-mail: wroclaw@cma.com.pl

Biura handlowe:
 ul. Mieszkańska 18/1, 30-313 Kraków
 tel. 12 260 13 96
 tel. kom. 665 380 677
 faks 12 260 13 95

ul. Pałacza 127, 60-279 Poznań
 tel./faks 61 861 40 51
 tel. kom. 601 203 664
 e-mail: poznan@cma.com.pl

Al. Niepodległości 659, 81-855 Sopot
 tel. 58 345 23 24
 tel. kom. 693 694 339
 e-mail: sopot@cma.com.pl



DYSKRET POLSKA
Spółka z ograniczoną odpowiedzialnością Sp. k.
 ul. Mazowiecka 131
 30-023 Kraków
 tel. 12 423 31 00
 faks 12 423 44 61
 e-mail: office@dyskret.com.pl
 www.dyskret.com.pl



bt electronics sp. z o.o.
 ul. Dukatów 10
 31-431 Kraków
 tel. 12 429 36 16
 faks 12 410 85 11
 e-mail: saik@saik.pl
 www.saik.pl



EBS Sp. z o.o.
 ul. B. Czecha 59
 04-555 Warszawa
 tel. 22 812 05 05
 faks 22 812 62 12
 e-mail: sales@ebs.pl
 www.ebs.pl



LEGRAND POLSKA Sp. z o.o.
 ul. Domaniewska 50
 Tulipan Hause
 02-672 Warszawa
 Infolinia 801 133 084
 faks 22 843 94 51
 e-mail: info@legrand.com.pl
 www.legrandgroup.pl



CONTROL SYSTEM FMN
 Al. KEN 96 lok. U-15
 02-777 Warszawa
 tel. 22 855 00 17
 faks 22 855 00 18
 e-mail: biuro@cs.pl
 www.cs.pl



EL-MONT
 ul. Wyzwolenia 15
 44-200 Rybnik
 tel. 32 423 07 28, 422 38 89
 faks 32 423 07 29
 e-mail: el-mont@el-mont.com
 www.el-mont.com



CAMSAT
Gralak Przemysław
 ul. Ogrodowa 2a
 86-050 Solec Kujawski
 tel. 52 387 36 58
 faks 52 387 54 66
 e-mail: camsat@camsat.com.pl
 www.camsat.com.pl



D-MAX Polska Sp. z o.o.
 ul. Obornicka 276
 60-693 Poznań
 tel./faks 61 822 60 52
 e-mail: biuro@dmxpolska.pl
 www.dmxpolska.pl



PHU ELPROMA Sp. z o.o.
 ul. Syta 177
 02-987 Warszawa
 tel. 22 398 96 53/54
 faks 22 398 96 54
 e-mail: elproma@elproma.pl
 www.elproma.pl

**EUREKA SOFT & HARDWARE**

ul. Rynek 13
62-300 Września
tel. 61 437 90 15
e-mail: biuro@eureka.com.pl
www.eureka.com.pl

**EUROPEAN SECURITY TRADING POLSKA Sp. z o.o.**

Al. Jerozolimskie 133 lok. 13
02-304 Warszawa
tel./faks 22 115 71 50
e-mail: kontakt@estpolska.pl
www.estpolska.pl

**FES Trading Sp. z o.o.**

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

**GDE POLSKA**

Włosań, ul. Świątnicka 88
32-031 Mogilany
tel. 12 256 50 25, 256 50 35
faks 12 270 56 96
e-mail: biuro@gde.pl
www.gde.pl

**ICS POLSKA**

ul. Poleczki 82
02-822 Warszawa
tel. 22 646 11 38
faks 22 849 94 83
e-mail: biuro@ics.pl
www.ics.pl

**INSAP Sp. z o.o.**

ul. Ładna 4-6
31-444 Kraków
tel. 12 411 49 79
faks 12 411 94 74
e-mail: insap@insap.pl
www.insap.pl

**JANEX INTERNATIONAL Sp. z o.o.**

ul. Piomyka 2
02-490 Warszawa
tel. 22 863 63 53
faks 22 863 74 23
e-mail: janex@janexint.com.pl
www.janexint.com.pl

**KATON Sp. z o.o.**

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

**KOLEKTOR****K. Mikiciuk i R. Rutkowski Sp. J.**

ul. Obrońców Westerplatte 31
80-317 Gdańsk
tel./faks 58 553 67 59
e-mail: info@kolektor.pl
www.kolektor.pl

**MICROMADE****Gałka i Drożdż Sp. J.**

ul. Wieniawskiego 16
64-920 Piła
tel./faks 67 213 24 14
e-mail: mm@micromade.pl
www.micromade.pl

**MICRONIX Sp. z o.o.**

ul. Spółdzielcza 10
58-500 Jelenia Góra
tel. 75 755 78 78
faks wew. 28
e-mail: info@micronix.pl
www.micronix.pl

**NOVATEL Sp. z o.o.**

ul. Turystyczna 1
43-155 Bieruń
tel. 32 201 17 04
faks 32 201 15 10
e-mail: novatel@novatel.pl
www.novatel.pl

**NUUXE – RADIOTON Sp. z o.o.**

ul. Olszańska 5
31-513 Kraków
tel. 12 393 58 00
faks 12 393 58 02
e-mail: cctv@jvcpro.pl
www.jvcpro.pl
www.nuuxe.com

**OBIS CICHOCKI ŚLĄZAK Sp. J.**

ul. Rybnicka 64
52-016 Wrocław
tel./faks 71 343 16 76
e-mail: obis@obis.com.pl
www.obis.com.pl

**OMC INDUSTRIAL Sp. z o.o.**

ul. Rzymowskiego 30
02-697 Warszawa
tel. 22 651 88 61
faks 22 651 88 76
e-mail: sprzedaz@omc.com.pl
www.omc.com.pl

Przedstawicielstwo:

ul. Markiefki 32, 40-213 Katowice
tel./faks 32 202 55 82
e-mail: katowice@omc.com.pl

ul. Murawa 37B/L-6, 61-655 Poznań
tel./faks 61 657 93 60
e-mail: poznan@omc.com.pl

ul. Różyckiego 1c, 51-608 Wrocław
tel./faks 71 347 91 91
e-mail: wroclaw@omc.com.pl

**POINTEL Sp. z o.o.**

ul. Fordońska 199
85-739 Bydgoszcz
tel. 52 371 81 16
faks 52 342 35 83
e-mail: biuro@pointel.pl
www.pointel.pl



POL-ITAL Sp. z o.o.
ul. Irysowa 11
02-660 Warszawa
tel. 22 831 15 35
faks 22 831 73 36
e-mail: biuro@polital.pl
www.polital.pl



PULSAR K. Bogusz Sp. J.
Siedlec 150
32-744 Łąpczyca
tel. 14 610 19 40
faks 14 610 19 50
e-mail: norbert@pulsar.pl
www.pulsar.pl



RISCO GROUP POLAND Sp. z o.o.
ul. 17 Stycznia 56
02-146 Warszawa
tel. 22 500 28 40
faks 22 500 28 41
e-mail: sales-pl@riscogroup.com
www.riscogroup.com



POLON-ALFA
Spółka z ograniczoną odpowiedzialnością Sp. k.
ul. Glinki 155
85-861 Bydgoszcz
tel. 52 363 92 61
faks 52 363 92 64
e-mail: polonalfa@polon-alfa.com.pl
www.polon-alfa.pl



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



ROPAM Elektronik s.c.
Os. Tysiąclecia 6A/1
32-400 Myślenice
tel. 12 341 04 07
faks 12 272 39 71
e-mail: biuro@ropam.com.pl
www.ropam.com.pl
www.ropam.eu



PROFICCTV Sp. z o.o.
ul. Obornicka 276
60-693 Poznań
tel. 61 842 29 62
faks 61 842 29 62
e-mail: biuro@proficctv.pl
www.proficctv.pl
www.dmaxcctv.pl
www.samsungcctv.pl



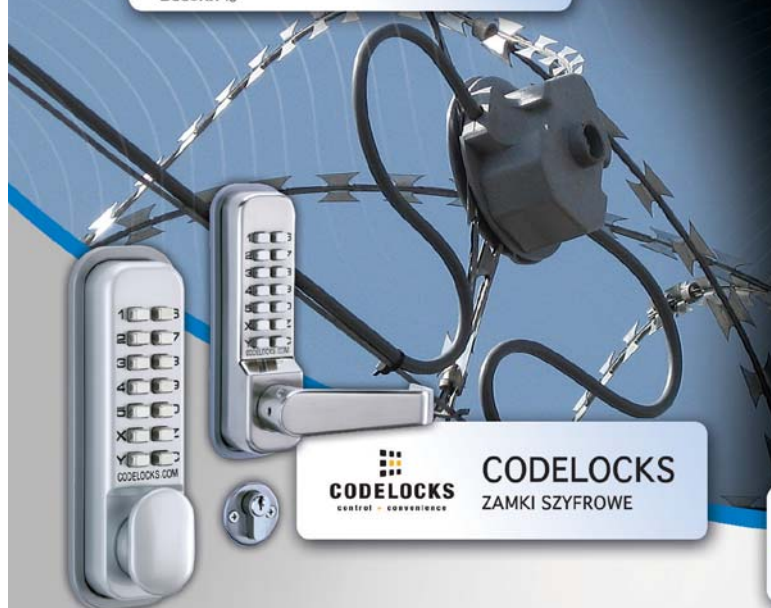
RETT-POL
Bogusław Godlewski
ul. Podmiejska 21
01-498 Warszawa
tel./faks 22 632 72 22
e-mail: biuro@rettpol.pl
www.rettpol.com.pl



SAMSUNG TECHWIN EUROPE LTD.
Biurowo w Polsce
ul. Marynarska 15
02-674 Warszawa
tel. 22 205 07 77
faks 22 205 07 63
e-mail: STESecurity@samsung.com
www.samsungsecurity.com



SERIR
SYSTEM DETEKCJI
NA OGRODZENIA METALOWE



CODELOCKS
ZAMKI SZYFROWE



FLIR
KAMERY TERMOWIZYJNE



Firma ATLine sp.j. Sławomir Pruski
ul. Franciszkańska 125, 91-845 Łódź, tel. +48 422 313 849
fax +48 426 552 099, e-mail: info@atline.pl, handel@atline.pl

zobacz więcej na:
www.atline.pl



SATEL Sp. z o.o.
ul. Schuberta 79
80-172 Gdańsk
tel. 58 320 94 00
faks 58 320 94 01
e-mail: satel@satel.pl
www.satel.pl



SAWEL
Systemy Bezpieczeństwa
ul. Lwowska 83
35-301 Rzeszów
tel. 17 857 80 60
faks 17 857 79 99
e-mail: sawel@sawel.com.pl
www.sawel.com.pl



SCHNEIDER ELECTRIC POLSKA Sp. z o.o.
ul. Iłżecka 24
02-135 Warszawa
tel. 22 313 24 15
faks 22 313 24 10
e-mail: poland.helpdesk@schneider-electric.com
www.schneider-electric.pl

Oddziały:
ul. Arkońska 6 bud. A2
80-387 Gdańsk
tel. 58 782 00 01
faks 58 782 00 04

ul. Rzymowskiego 13
02-697 Warszawa
tel. 22 313 24 10
faks 22 313 24 11

ul. Muchoborska 18
54-424 Wrocław
tel. 71 711 09 19
faks 71 711 09 20

ul. Krakowska 280
32-080 Zabierzów k. Krakowa
tel. 12 257 60 80
faks 12 257 60 81



SCHRACK SECONET POLSKA Sp. z o.o.
ul. Domaniewska 44a
02-672 Warszawa
tel. 22 33 00 620 ÷ 623
faks 22 33 00 624
e-mail: warszawa@schrack-seconet.pl
www.schrack-seconet.pl

Oddziały:
CH Manhattan, III piętro
Al. Grunwaldzka 82, 80-244 Gdańsk
tel./faks 58 767 70 10
e-mail: gdansk@schrack-seconet.pl

ul. Wierzbęćce 1, 61-569 Poznań
tel. 61 833 31 53
faks 61 833 50 37
e-mail: poznan@schrack-seconet.pl

ul. Mydlana 1, 51-520 Wrocław
tel./faks 71 345 00 95
e-mail: wroclaw@schrack-seconet.pl



**PRZEDSIĘBIORSTWO TECHNICZNO- HANDLOWE
SECURAL**
ul. Gen. K. Pułaskiego 4
41-205 Sosnowiec
tel. 32 291 86 17
faks 32 291 88 10
e-mail: info@secural.com.pl
www.secural.com.pl



SMA Sp. z o.o.
ul. Rzymowskiego 30
02-697 Warszawa
tel. 22 651 88 61
faks 22 651 88 76
e-mail: sma@sma.biz.pl
www.sma.biz.pl

Oddziały:
ul. Markiefki 32, 40-213 Katowice
tel./faks 32 202 55 82
e-mail: katowice@sma.biz.pl

ul. Murawa 37B/L-6, 61-655 Poznań
tel./faks 61 657 93 60
e-mail: poznan@sma.biz.pl

ul. Różyckiego 1C, 51-608 Wrocław
tel. 71 347 91 91
tel./faks 71 348 04 19
e-mail: sma@sma.wroclaw.pl



SPS Electronics Sp. z o.o.
ul. Krakowiaków 80/98
02-255 Warszawa
tel. 22 518 31 50
faks 22 518 31 70
e-mail: warszawa@spselectronics.pl
www.spselectronics.pl

Biura Handlowe:
ul. Drożyny 6, 80-302 Gdańsk
tel. 58 624 83 04
faks 58 668 59 20
e-mail: gdansk@spselectronics.pl

al. Różdzieńskiego 188a, 40-203 Katowice
tel. 32 255 64 27
faks 32 255 64 52
e-mail: katowice@spselectronics.pl

ul. Polska 60, 60-595 Poznań
tel. 61 852 19 02
faks 61 825 09 03
e-mail: poznan@spselectronics.pl

pl. Gen. Wróblewskiego 3a, 50-413 Wrocław
tel. 71 348 44 64
faks 71 348 36 35
e-mail: wroclaw@spselectronics.pl

Biuro Partnerskie SPS Partner
ul. Przybyszewskiego 199/205, 93-120 Łódź
tel. 42 617 00 32
e-mail: lodz@spspartner.pl

ul. Szosa Chelmińska 217A, 87-100 Toruń
tel. 56 653 99 43
faks 56 653 90 81
e-mail: torun@spspartner.pl



TAP- Systemy Alarmowe Sp. z o.o.
Os. Armii Krajowej 125
61-381 Poznań
tel. 61 876 70 88
faks 61 875 03 03
e-mail: tap@tap.com.pl
www.tap.com.pl



TECHNOKABEL S.A.
ul. Nasielska 55
04-343 Warszawa
tel. 22 516 97 97
faks 22 516 97 91
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl



UNICARD S.A.
ul. Łagiewnicka 54
30-417 Kraków
tel. 12 398 99 19
faks 12 398 99 01
e-mail: biuro@unicard.pl
www.unicard.pl



W2 Włodzimierz Wyrzykowski
ul. Czajcza 6
86-005 Białe Błota
tel. 52 345 45 00
faks 52 584 01 92
e-mail: biuro@w2.com.pl
www.w2.com.pl



VISION POLSKA Sp. z o.o.
ul. Unii Lubelskiej 1
61-249 Poznań
tel. 61 623 23 05
faks 61 623 23 17
e-mail: biuro@visionpolska.pl
www.visionpolska.pl



ZBAR PHU
Mariusz Popenda
ul. Krakowska 60
94-214 Łódź
tel. 42 611 12 97
faks 42 611 12 98
e-mail: zbar@zbar.com.pl
www.zbar.com.pl

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Nowe kamery serii C

**Bardzo wysoka rozdzielczość
do 700 TVL**



Wydłużona żywotność LED
stabilizacja prądu diod
zapobiegająca ich uszkodzeniu

Ergonomiczne obudowy

3-osiowa regulacja położenia modułu kamerowego,
uchwyt z przepustem kablowym w zestawie,
wygodna regulacja obiektywu

(wybrane modele)



Seria C obejmuje 3 rodzaje kamer:

- Kamery kopułkowe: NVC-CDN2110D/IR, NVC-CC2111D
- Kamery wandaloodporne: NVC-CDN4120V/IR, NVC-CDN4121V/IR
- Kamery w obudowie: NVC-CDN3110H/IR, NVC-CDN3111H/IR, NVC-CDN3112H/IR, NVC-CDN3113H/IR

- Matryca 1/4" CMOS
- Funkcja dzień/noc - filtr IR
- Rozdzielczość pozioma do 700 TVL
- Czułość od 0.05 lx/F=1.4 (0 lx z włączonym IR)
- Typ obiektywu: standardowy, f=3 mm, ze zmienną ogniskową, f=3.5~8 mm lub f=2.8~11 mm
- Wbudowany oświetlacz podczerwieni - 18/24/36/42/76 diod LED

- Duży zasięg oświetlacza podczerwieni - do 25 m
- Klasa szczelności: IP 65 (kamery wandaloodporne) lub IP 66 (kamery w obudowie)
- Temperatura pracy: -30°C~40°C
- Zasilanie: 12 VDC
- Łatwa instalacja - stałe, optymalne ustawienia parametrów pracy



Wyłączny dystrybutor produktów NOVUS® w Polsce:



AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
AAT Holding	–	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	TAK
AGIS Fire & Security	–	TAK	TAK	TAK	TAK
Alarmnet	–	–	TAK	–	–
Alarmtech Polska	TAK	TAK	–	–	–
Alkam System	TAK	TAK	–	TAK	–
Alpol	–	–	TAK	–	TAK
ASSA ABLOY	–	–	TAK	–	TAK
FIRMA ATLine	–	TAK	TAK	TAK	–
BOSCH	TAK	–	–	–	–
P.W.H. Brabork - Laboratorium	–	TAK	TAK	TAK	–
bt electronics	TAK	TAK	TAK	TAK	TAK
CAMSAT	TAK	–	TAK	–	–
CBC (Poland)	TAK	–	TAK	–	TAK
CMA	TAK	TAK	–	TAK	–
CONTROL SYSTEM FMN	TAK	–	TAK	TAK	–
D-MAX	–	–	TAK	–	–
Dahua Technology Co.	TAK	TAK	TAK	TAK	TAK
DG Elpro	–	TAK	TAK	TAK	–
Dyskret	–	TAK	TAK	TAK	–
EBS	TAK	TAK	TAK	–	–
EI-Mont	TAK	–	–	TAK	–
Elproma	–	TAK	–	TAK	–
Eureka	–	TAK	–	TAK	–
EST POLSKA	–	–	TAK	–	TAK
FES	–	TAK	TAK	TAK	TAK
GDE Polska	–	–	TAK	–	TAK
ICS POLSKA	–	TAK	TAK	–	TAK
Insap	–	TAK	TAK	TAK	TAK
Janex International	–	TAK	TAK	–	TAK
KATON	–	–	TAK	–	TAK

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Kolektor	–	TAK	TAK	TAK	–
Legrand Polska	TAK	TAK	TAK	–	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	–	TAK	–	–
Novatel	TAK	TAK	TAK	TAK	TAK
Nuuxe – Radioton	–	TAK	TAK	TAK	TAK
OBIS	–	TAK	–	TAK	–
OMC INDUSTRIAL	–	–	TAK	–	TAK
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	–	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	–	–	–
Ramar	–	–	TAK	TAK	TAK
RETT-POL	–	–	TAK	TAK	–
RISCO	TAK	–	–	–	TAK
ROPAM Elektronik	TAK	–	TAK	–	TAK
Samsung	TAK	–	TAK	–	–
Satel	TAK	TAK	–	–	–
Sawel	–	TAK	TAK	TAK	TAK
Schneider Electric Buildings Polska	TAK	–	TAK	–	–
Schrack Seconet Polska	TAK	TAK	TAK	–	TAK
Secural	TAK	TAK	TAK	–	TAK
SMA	–	TAK	–	TAK	–
SPS Electronics	–	TAK	TAK	–	TAK
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Technokabel	TAK	TAK	–	–	TAK
UNICARD	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	–	–
Vision Polska	–	–	TAK	–	TAK
ZBAR	–	TAK	TAK	TAK	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizyjnej dozоровej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnienia
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, karty magnetyczne i zbliżeniowe								
AGIS Fire & Security	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Alarmnet	–	TAK	TAK	–	–	TAK	–	–	–
Alarmtech Polska	TAK	–	TAK	–	–	–	–	–	–
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
ASSA ABLOY	–	–	TAK	–	TAK	–	–	TAK	–
FIRMA ATLine	TAK	–	TAK	–	TAK	TAK	–	TAK	–
BOSCH	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	–	–	–	–	–	–	TAK
bt electronics	–	–	TAK	–	–	TAK	–	TAK	–
CAMSAT	TAK	TAK	TAK	–	–	–	TAK	–	–
CBC (Poland)	–	TAK	–	–	–	–	–	–	–
CMA	–	–	–	–	–	–	TAK	–	–
CONTROL SYSTEM FMN	drukarki kart plastikowych, kontrola dostępu, zamki elektromagnetyczne								
D-MAX	–	TAK	–	–	–	–	TAK	–	–
Dahua Technology Co.	–	TAK	TAK	–	–	–	–	–	–
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Dyskret	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
EBS	transmitery GSM/GPRS/IP, systemy RFID i GPS, zabezpieczenia dla bankowości, energetyki, produkcja OEM/ODM								
EI-Mont	TAK	TAK	TAK	–	–	TAK	TAK	TAK	TAK
Elpoma	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
EST POLSKA	TAK	TAK	TAK	–	TAK	–	TAK	–	–
FES	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
GDE Polska	–	TAK	TAK	–	–	–	–	TAK	–
ICS POLSKA	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Janex International	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
KATON	–	TAK	TAK	–	–	TAK	–	–	–

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnienia
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MicroMade	–	–	TAK			rejestracja czasu pracy			
Micronix	TAK	TAK	TAK	–	–	–	–	TAK	–
Novatel	–	TAK	TAK	–	–	TAK	TAK	–	TAK
Nuuxe – Radioton	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	TAK	TAK	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	TAK	–	–	–	TAK	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	–	–	–	–	–	–	–	TAK	–
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	TAK	TAK	TAK	–	–	–
RETT-POL	TAK	TAK	TAK	TAK	–	–	TAK	–	–
RISCO	TAK	–	–	–	–	–	–	–	–
ROPAM Elektronik	TAK	TAK	TAK	–	–	TAK	TAK	–	–
Samsung	–	TAK	TAK	–	–	–	–	–	–
Satel	TAK	–	TAK	TAK	–	–	TAK	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Schneider Electric Buildings Polska	TAK	TAK	TAK	–	–	TAK	–	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SMA	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
SPS Electronics	TAK	TAK	TAK	TAK	–	–	TAK	–	–
Tap – Systemy Alarmowe	TAK	TAK	TAK	–	–	TAK	–	–	–
Technokabel	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK	TAK
UNICARD	TAK	TAK	TAK	TAK	–	TAK	–	TAK	–
W2	TAK	–	–	TAK	–	–	–	–	–
Vision Polska	–	–	–	TAK	–	–	–	–	–
ZBAR	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końska

Redaguje zespół
Krzysztof Białek
Marek Blim

Patryk Gańko
Norbert Góra
Daniel Kamiński

Paweł Karczmarzyk
Adam Rosiński
Ryszard Sobierski
Waldemar Szulc
Adam Wojcinowicz

Współpraca

Marcin Buczał
Adam Bułaciński
Piotr Czernoch
Marcin Pyclik
Sławomir Wagner
Andrzej Wójcik

Skład i łamanie

Tomasz Kaczmarczyk

Adres redakcji

ul. Puławska 359, 02-801 Warszawa
tel. 22 546 0 951, 953
faks 22 546 0 959
www.zabezpieczenia.com.pl

Wydawca

AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

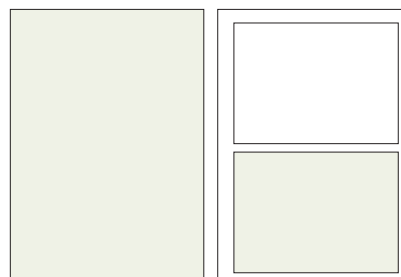
Druk

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

Cennik reklam

Reklama wewnątrz czasopisma:

cała strona, pełny kolor	4200 zł
cała strona, czarno-biała	2200 zł
1/2 strony, pełny kolor	2700 zł
1/2 strony, czarno-biała	1500 zł
1/3 strony, pełny kolor	1900 zł
1/3 strony, czarno-biała	1000 zł
1/4 strony, pełny kolor	1400 zł
1/4 strony, czarno-biała	800 zł
karta katalogowa, 1 strona	900 zł

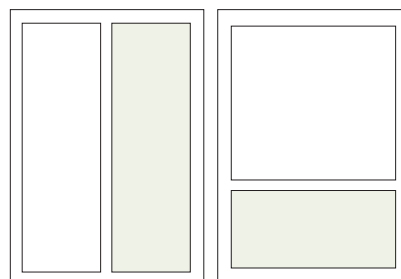


cała strona
(200 x 282 mm + 3mm spad)

1/2 strony
(170 x 125 mm)

Artykuł sponsorowany:

Cena za stronę artykułu sponsorowanego w czasopiśmie to 1500 zł (forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)

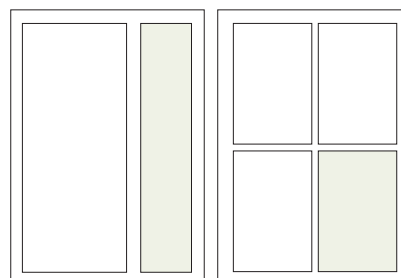


1/2 strony
(83 x 260 mm)

1/3 strony
(170 x 80 mm)

Reklama na okładkach:

pierwsza strona	indywidualne negocjacje
druga strona	5000 zł
przedostatnia strona	5000 zł
ostatnia strona	5000 zł



1/3 strony
(54 x 260 mm)

1/4 strony
(83 x 125 mm)

Spis teleadresowy:

jednorazowy wpis 70 zł

Redakcja przyjmuje zamówienia na
6 kolejnych emisji

Podane ceny nie uwzględniają podatku VAT (23%)

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

Spis reklam

AAT Holding	58, 71, 97	HSK Data	57
ADI	49	MIPS	29
ATline	95	MTP	5
Axis Communications	33, 103	OPTEX Security	41
Bosch Security Systems	53	Polon-Alfa	67
Dahua Technology Co.	45	Roger	79
Euroalarm	63	Satel	37, 75
GDE Polska	78	Videotec	2
Gunnebo	52	ZBAR	1
HID	104		

CZASOPISMO BEZPŁATNE ISSN: 1608-9419 DWUMIESIĘCZNIK NR 6(34) 2013
ZABEZPIECZENIA
 WWW.ZABEZPIECZENIA.COM.PL • E-MAIL: ZABEZPIECZENIA@ZABEZPIECZENIA.COM.PL

ochrona
OBWODOWA OBIEKTÓW

15 lat
Zabezpieczenia

W NUMERZE:

- 2 numerarni wlotów zewnętrznych
- Projektowanie instalacji z zasilającymi czujkami dymu
- Systemy automatycznego rozpoznawania śladów najeżdżających
- Czujka PIR - kamery w systemie alarmowym - niezbędny gadżet?

Redakcja nie zwraca materiałów nie zamówionych oraz zastrzega sobie prawo do skrótu i redakcyjnego opracowania tekstów przyjętych do druku. Za treść reklam, ogłoszeń, tekstów sponsorowanych oraz kart katalogowych redakcja nie odpowiada. Wszelkie prawa zastrzeżone. Przedruk tekstów, zdjęć i grafiki bez zgody redakcji zabroniony.



Inaczej rozumiana
jakość obrazu to jego
użyteczność.

Jakość obrazu jest zawsze ważna, lecz rzeczywiste korzyści jakie czerpiemy z zastosowania systemów nadzoru wideo zależne są od tego jak wykorzystujemy dane obrazy. Czy będą one ogólnie przeglądane czy też będziemy szukać detali? Czy będziemy chronić zadany obszar czy też rozpoznawać tablice rejestracyjne? Przeglądanie, nagrywanie czy też obydwie funkcje jednocześnie? Czy materiał wizyjny jest zoptymalizowany do naszych potrzeb?

Ułatwiamy pracę naszym klientom, gdyż koncentrujemy się na użyteczności materiału wizyjnego. Dzielimy się naszym doświadczeniem i kompetencjami, oferujemy szeroki zakres funkcjonalności związanych z poszerzaniem możliwości obrazu wideo takich jak zbliżanie,

ogniskowanie, technologia megapikselowa i HDTV. Mogą oni w pełni korzystać z najszerszego na rynku portfolio produktów do sieciowego nadzoru wizyjnego.

W celu zapewnienia dostępu do istotnych ekspertyz dotyczących nadzoru IP w zakresie instalacji i wsparcia technicznego, dysponujemy siecią 55 000 partnerów, specjalistów Axis na całym świecie. Jako światowy lider w sieciowych systemach wizyjnych, mamy na celu pomoc w uzyskaniu maksymalnych możliwości systemów nadzoru wizyjnego naszych klientów.

**Przyjmij punkt widzenia Axis.
Bądź zawsze o krok do przodu.**
Odwiedź stronę www.axis.com/imageusability



Kamera sieciowa AXIS Q1755:
H.264, zoom i jakość obrazu HDTV.

AXIS[®]
COMMUNICATIONS

iCLASS SE®

Najnowocześniejsza platforma kontroli dostępu

OBSŁUGUJE WIELE TECHNOLOGII KART

ZDALNA KONFIGURACJA CZYTNIKA

OBSŁUGUJE WIELE RODZAJÓW URZĄDZEŃ

WIĘKSZE BEZPIECZEŃSTWO DANYCH UWIERZYTELNIAJĄCYCH

NAJWYŻSZY POZIOM BEZPIECZEŃSTWA KART MIKROPROCESOROWYCH

Technologia przyszłości zapewniająca bezpieczeństwo danych identyfikacyjnych do szerokiego zakresu zastosowań (od kontroli dostępu po zabezpieczenie danych). Ewolucja w kwestiach bezpieczeństwa, użyteczności i wydajności.



Technologia HID i niezależna od nośnika platforma iCLASS SE®, przygotowana do zastosowań mobilnych, stanowią rozwiązanie bezpiecznej identyfikacji dla kontroli dostępu fizycznego oraz największego asortymentu aplikacji i środowisk. W celu osiągnięcia maksymalnej interoperacyjności platforma iCLASS SE wspiera najwięcej technologii kart dostępu, umożliwiając efektywne kosztowo i bezproblemowe unowocześnienie systemu i zwiększenie poziomu bezpieczeństwa oraz wydajności. Platforma iCLASS SE jest przystosowana do obsługi technologii przyszłości, w tym dostępu za pomocą urządzeń mobilnych w technologii NFC, zapewniając wygodny dostęp oraz bezprecedensowy poziom bezpieczeństwa.

Aby dowiedzieć się więcej, odwiedź witrynę hidglobal.com

© 2013 HID Global Corporation/ASSA ABLOY AB. Wszelkie prawa zastrzeżone. HID, HID Global, oraz logo HID Blue Brick, jak również Chain Design są znakami towarowymi lub zastrzeżonymi znakami towarowymi należącymi do firmy HID Global lub jej licencjodawców/dostawców w Stanach Zjednoczonych i innych krajach. Znaki nie mogą być wykorzystywane bez uzyskania zgody.