CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 1(95)/2014

ZABEZPIECZENIA

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

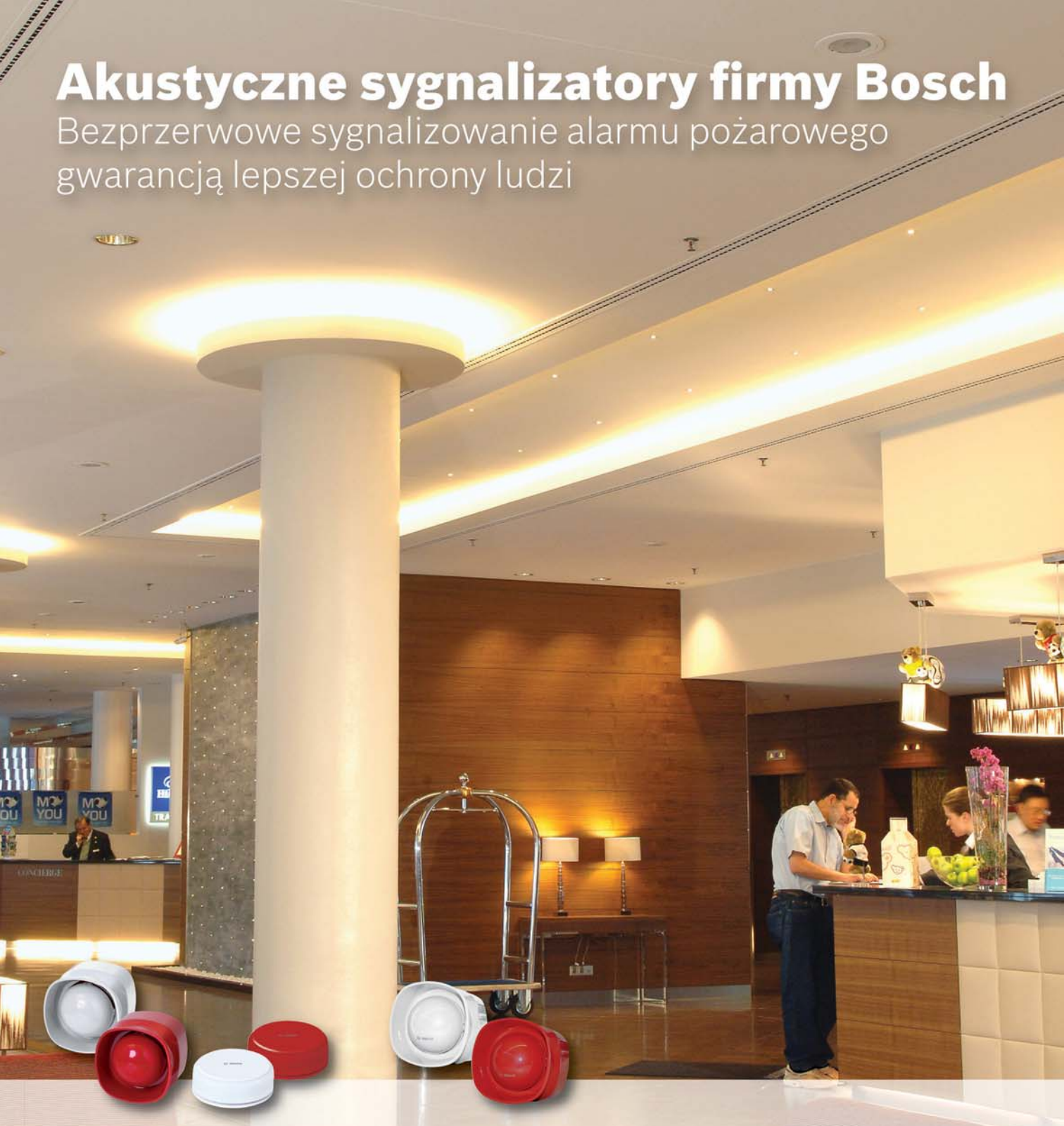
W NUMERZE:

- Termowizja staje się dostępna na co dzień
- Zgoda na przetwarzanie danych osobowych
- Systemy zabezpieczające z rozproszoną inteligencją
- Radiokomunikacja cyfrowa w służbach ochrony i ratownictwa (część 1)

WYDANIE SPECJALNE SECUREX 2014

Akustyczne sygnalizatory firmy Bosch

Bezprzerwowe sygnalizowanie alarmu pożarowego gwarancją lepszej ochrony ludzi



Nowe sygnalizatory adresowalne akustyczne FNM 420U oraz akustyczno-głosowe FNM 420V firmy Bosch zapewniają bezprzerwowe sygnalizowanie alarmu w miejscu wystąpienia pożaru. Sygnalizatory adresowalne są dobrym rozwiązaniem do każdego rodzaju budynków, a możliwość indywidualnego programowania zadziałania każdego urządzenia daje przewagę nad sygnalizatorami konwencjonalnymi. Dodatkowo sygnalizatory akustyczno-głosowe są idealnym rozwiązaniem do obiektów, gdzie potrzebna jest szybka ewakuacja, a system Evac nie jest wymagany.

Więcej informacji u najbliższego przedstawiciela Bosch
lub na naszej stronie **www.boschsecurity.pl**

BOSCH
Technologia bliżej nas

Rejestratory sieciowe i oprogramowanie do rejestracji, zarządzania i nadzoru systemów CCTV

iPOLiS
Your smart security solution

Unrivaled Image Quality
Niezrównana jakość obrazu

Efficient Network Transmission
Wydajna transmisja sieciowa

Komfort użytkowania

Kompleksowe rozwiązania sieciowe

Mądry wybór profesjonalistów

Zero Downtime – zdublowany zasilacz oraz dyski hot swap, pracujące w trybie RAID, zapewniają najwyższy poziom niezawodności systemu.

Heat Map – funkcja pozwalająca na zobrazowanie w postaci kolorowej mapy częstotliwości występowania wyszukiwanych obiektów w analizowanej scenie.

RAID 6 – macierz dysków z podwójną kontrolą parzystości, odporna na jednoczesną awarię 2 dysków.

Dewarping – funkcja umożliwiająca przetworzenie obrazu lub fragmentu obrazu, z kamery z obiektywem „rybie oko", do postaci standardowej.

Klasyfikacja – funkcja analityczna pozwalająca na rozróżnienie typu obiektu, np.: samochód - człowiek.

Hot Swap – możliwość odłączania / podłączania dysków lub zasilaczy bez konieczności wyłączania urządzenia.

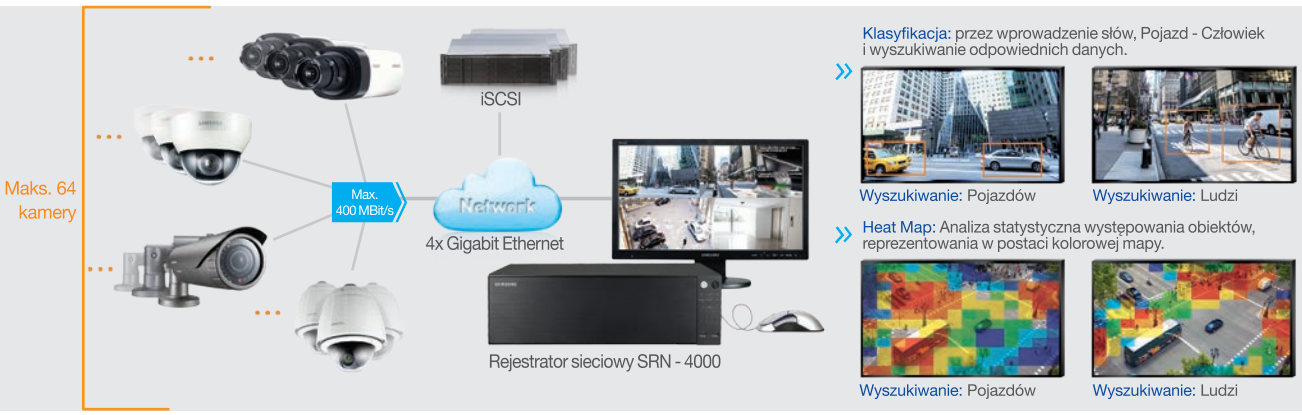
SAMSUNG TECHWIN

SAMSUNG

Rejestrator sieciowy SRN-4000

www.samsung-security.pl

Maks. ilość rejestrowanych strumieni: 64 kamery, rozdzielczość: CIF- 5Mpix
Maks. szybkość zapisu / transmisji sieciowej: 400Mbit/s, (64 kamery 2M real time)
Podgląd lokalny: HDMI / VGA (FHD) - do 16 kamer w różnych podziałach
Maks. szybkość odtwarzania: 100Mbit/s, Odtwarzenie jednoczesne -16 kamer (lokalnie)
Maks. pojemność archiwum wewn.: 12 HDD (Hot Swap) / 36TB, NAS - iSCSI - max 76HDD x 3TB
Porty sieciowe: 4x RJ45 (Gigabit Ethernet)
Liczba użytkowników zdalnych: wyszukiwanie - 3; podgląd - 10/20 (unicast /multicast)
Niezawodności - Zero downtime: 2 redundantne zasilacze (Hot Swap), kontroler RAID 5/6
Inteligentne wyszukiwanie / nagrywanie: klasyfikacja, Heat Map, zaawansowana detekcja ruchu
Zarządzanie użytkownikami: do 100 użytkowników z podziałem na grupy i uprawnienia
Bezpieczeństwo: filtrowanie adresów IP, autentykacja 802.1x, szyfrowanie



Samsung Security Manager

SSM jest kompletną platformą umożliwiającą zarządzanie z maksymalną efektywnością urządzeniami Samsunga, włączając w to kamery sieciowe, enkodery oraz rejestratory analogowe (DVR) i sieciowe (NVR), a także wykorzystanie kamer innych producentów, transmitujących strumienie wideo zgodnie ze standardem Onvif lub w protokole RTSP. Architektura klient-serwer umożliwia elastyczne dostosowanie do pracy w rozproszonej architekturze z wieloma stacjami klienckimi. Dostęp do zarchiwizowanych nagrań lub podglądu "na żywo" jest niezwykle łatwy, również dla zdalnych klientów oraz telefonów komórkowych i tabletów, czyniąc SSM odpowiednim rozwiązaniem dla średnich i dużych instalacji wielostanowiskowych.

SSM Media Gateway

Moduł zapewniający współdzielenie wideo, wielostrumieniowość oraz separację konsoli od urządzeń. Maksymalnie 4 x Media Gateway i 5 konsol w systemie oraz 72 kamery na każdy Media Gatewey. Współpraca z rejstratorami analogowymi i sieciowymi Samsunga.

SSM Console

Moduł umożliwiający podgląd obrazu „na żywo", podgląd zdarzeń alarmowych, wyszukiwanie nagrań. Obsługa maks. 4 monitorów / maks. 64 kamery na monitorze. Wyświetlanie do 100 kamer „na żywo" w różnych układach w tym na mapach. Natychmiastowe odtwarzanie do 16 kamer, zaawansowana oś czasu. Archiwizacja lokalna w formacie AVI lub SEC, de-warping.

SSM System Manager/Configuration Manager

Baza danych systemu umożliwiająca zarządzenie użytkownikami, obsługą i monitoringiem systemu. Konfiguracja urządzeń oraz uprawnień grup i użytkowników, aktualizacja firmware. Konfiguracja skryptów, map, presetów dla różnych zdarzeń i trybów pracy.

SSM-RS10/RS20 - Recording Module

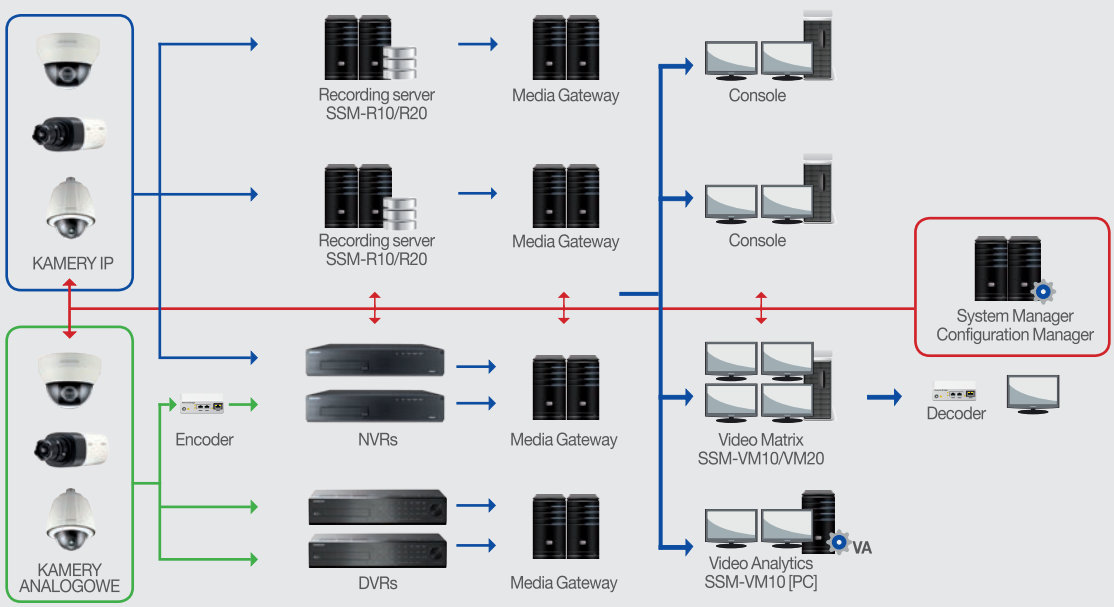
Rejestracja obrazów z 36/72 kamer (Samsung lub Onvif), maks. 24HDD. Zapis do 400Mbit/s. Odtwarzanie jednoczesne 16 strumieni wideo. Zapis logów: systemowych, dostępu użytkowników, archiwizacji, zdarzeń alarmowych.

SSM-VM10/VM20 Virtual Video Matrix

Wyświetlanie obrazu na maksymalnie 16/ 36 monitorach w różnych podziałach. Automatyczna zmiana ustawień dla zdarzeń alarmowych. Sterowanie z pozimu konsoli, Mapy, Virtual Salvo Switching. Obsługa sprzętowych dekoderów wideo.

SSM-VA10 - Video Analytics

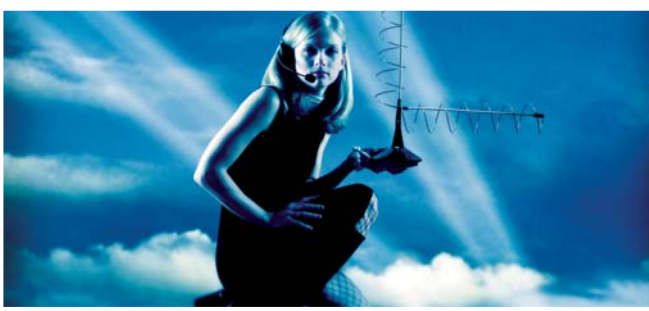
Analiza do 10 kanałów na serwer. Heat Mapping, analiza stref (Ścieżka, Kolejka, Krążenie wokół zdefiniowanego miejsca), statystyki (zliczanie osób).



Spis treści

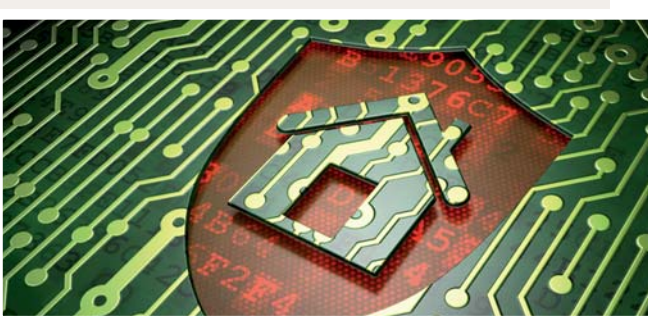
CZASOPISMO ZABEZPIECZENIA 1/2014

Bezpieczeństwo danych w nowoczesnej telemedycynie **20**



Radiokomunikacja cyfrowa w służbach ochrony i ratownictwa. Zarys zagadnień teoretycznych **26**

Systemy zabezpieczające z rozproszoną inteligencją **40**



Systemy automatyki domowej, w których wykorzystuje się komunikację Z-wave **54**

Międzynarodowe Targi Poznańskie

spotkaj przyszłość

20 EDYCJA TARGÓW

securex®
POLAND

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

ZŁOTY MEDAL 2014

RZECZPOSPOLITA
PARTNER MEDIALNY KONKURSU O ZŁOTY MEDAL MTP

Złoty Medal Międzynarodowych Targów Poznańskich – Securex 2014

Prestiż, który zabezpieczy twój sukces podczas SECUREX 2014
– największych targów branży zabezpieczeń w Europie Środkowo-Wschodniej

Tradycja i zaufanie

Złoty Medal to jedna z najbardziej rozpoznawalnych, prestiżowych i cenionych nagród na polskim rynku. Tylko najlepsze, najbardziej innowacyjne i wykonane z użyciem najnowszych technologii produkty są nominowane do konkursu. Oceny dokonuje profesjonalny zespół ekspertów z branży zabezpieczeń. Dzięki swej 30-letniej tradycji konkurs zyskał prawdziwą renomę i zaufanie, co zachęca potencjalnych wystawców – partnerów MTP – do walki o medal.

Pakiet Medalisty – intensywna promocja

Dzięki rozstrzygnięciu konkursu na kilka tygodni przed targami i kompletowi materiałów promocyjnych zwycięzca ma możliwość przygotowania kampanii reklamowej nagrodzonego produktu z dużym wyprzedzeniem. Organizatorzy targów również podejmują działania na rzecz intensywnej promocji – zarówno przed targami, jak i po ich zakończeniu – poprzez swoje nośniki informacji: dotyczące produktów strony internetowe czy magazyn *Securex News*. Informacja o laureatach konkursu jest publikowana w dodatku do *Rzeczpospolitej,* która od lat jest partnerem konkursu. Kampania promocyjna obejmuje także publikację listy laureatów na łamach współpracujących z targami wydawnictw i portali branżowych. W trakcie targów laureaci konkursu eksponują swą ofertę w niezwykłej oprawie, jaką stanowią ekskluzywne, specjalnie przygotowane stoiska zwane „Strefami Mistrza". Dodatkowo po ogłoszeniu wyników rozpoczyna się konkurs konsumencki – zwiedzający targi i osoby zainteresowane mają możliwość oddania głosu na produkt, który ich zdaniem zasługuje na Złoty Medal – Wybór Konsumentów. Głosowanie trwa do miesiąca po zakończeniu ekspozycji. Kompleksowa promocja konkursu daje zatem możliwość dotarcia do tysięcy zainteresowanych osób.

Wsparcie strategii sukcesu

Wystawcy zainteresowani konkursem mogli zgłaszać swoje produkty do końca stycznia 2014 r. Wyniki Sądu Konkursowego będą znane w połowie lutego. Sprawna organizacja konkursu, czytelne procedury i wreszcie zwycięstwo to elementy, które składają się na sukces stającej na podium firmy. Rozpoznawalny i ceniony znak Złotego Medalu MTP jest kojarzony przez klientów z nowoczesnością i wysoką jakością nagrodzonego produktu. Więcej informacji na *www.securex.pl.*

Bezpośr. inf. Marta Rybko
MTP

securex® 2014
POLAND
Międzynarodowe Targi Zabezpieczeń
International Security Fair

Samsung Techwin i MR SYSTEM sponsorami projektu Polskiej Normy prPN-EN 50132-7:2012

Samsung Techwin (kooperant zagraniczny PISA) i **MR SYSTEM** (członek PISA) przeznaczyły ostatnio środki na opracowanie projektu polskiej wersji nowej normy europejskiej prPN-EN 50132-7:2012 *Systemy alarmowe – Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 7: Wytyczne stosowania.*

Stworzyły tym samym warunki, które umożliwiły **Polskiej Izbie Systemów Alarmowych** zawarcie kolejnej już umowy z Polskim Komitetem Normalizacyjnym na opracowanie projektu, wykonanie procedur uzgodnieniowych, zatwierdzenie i publikację dokumentu normalizacyjnego. Zgodnie z umową PISA – PKN norma zostanie opublikowana najpóźniej do końca 2014 r.

Norma EN 50132-7:2012 wprowadza nową jakość do metodyki projektowania systemów CCTV, zwiększa wymagania jakościowe dotyczące systemów CCTV, dostarcza nowych narzędzi do wspomagania procesu projektowego oraz ujednolica wymagania i procedury testowe.

Podstawowe zmiany nowej regulacji normatywnej w stosunku do funkcjonującej w języku polskim normy PN-EN 50132-7:2003 to m.in.: uzupełnienie i doprecyzowanie dotychczasowych wytycznych, rozszerzenie ich o technologie IP, wprowadzenie zagadnień dotyczących ochrony przed dostępem do urządzeń w warstwie fizycznej, wprowadzenie zagadnień dotyczących integracji systemów, nowe pojęcia dla aplikacji, zmiana obiektu testowego i rozmiaru obiektu testowego w polu widzenia, szczegółowe wytyczne dotyczące projektowania stanowiska monitoringu, szczegółowe wytyczne dotyczące testowania systemów dla aplikacji, zmiany w doborze osprzętu.

Europejska Norma EN 50132-7:2012, uznana w 2013 r. przez Polski Komitet Normalizacyjny w języku oryginału, jest kluczowym wyznacznikiem należytej staranności projektowania, instalowania i eksploatowania systemów telewizji dozorowej CCTV – systemów, bez których współcześnie nie można sobie wyobrazić zapewnienia właściwego poziomu bezpieczeństwa obiektów, zwłaszcza tych podlegających obowiązkowej ochronie.

Bezpośr. inf. PISA

MR SYSTEM

SAMSUNG

Kamery Dahua pracują w systemie dozorowym we włoskim parku sportów motorowych

Modena jest starożytnym włoskim miastem, które często jest nazywane stolicą maszyn. Jest to miejsce bardzo lubiane przez entuzjastów sportów motorowych, gdyż są tu zlokalizowane liczne fabryki samochodów, w tym tak sławne zakłady jak Ferrari, De Tomaso, Lamborghini, Pagani i Maserati.

Autodrome di Modena jest parkiem mieszczącym się w słynnej dzielnicy zwanej Motor Valley, w której rozgrywane są wyścigi samochodowe. Jest to wymarzone miejsce dla entuzjastów sportów motorowych, w którym można skorzystać z torów wyścigowych oraz z porad profesjonalnych instruktorów, biorących udział w prawdziwych wyścigach i dzielących się swoimi doświadczeniami podczas treningów. Długość toru wynosi 2,7 km, zaś w alejce serwisowej znajduje się 21 stanowisk. Jest tam zainstalowany nowy system telemetryczny oraz mieści się dobrze wyposażony padok.

Zapewnienie odpowiedniego poziomu bezpieczeństwa na terenie Autodrome di Modena jest trudne, zarówno ze względu na dobrze znane niebezpieczeństwa, z jakimi mamy do czynienia podczas wyścigów samochodowych, jak i ze względu na rozległość terenu. Podczas projektowania systemów dozorowych konieczne było spełnienie wymagań dotyczących bezpieczeństwa użytkowania obiektu oraz wymagań wynikających z procedur startowych podczas wyścigów samochodowych i motocyklowych. Brano także pod uwagę wymagania wynikające z kształtu toru wyścigowego.

Ostatecznie zapadła decyzja o zainstalowaniu 24 stacjonarnych kamer sieciowych w najistotniejszych punktach toru oraz kilku kamer szybkoobrotowych na otwartych przestrzeniach wokół toru. Wybrane zostały konkretne modele urządzeń, w tym kamery stacjonarne **Dahua** typu IPC-HF3200, pracujące w standardzie full HD, i kamery szybkoobrotowe Dahua typu SD6982A-HN, a także jednostki pamięciowe Dahua 128 Channel Super NVR. Do obsługi tak skonfigurowanego systemu służy oprogramowanie Dahua VMS. W efekcie powstał system zapewniający właściwą ochronę całego terenu. Doskonała jakość obrazów z kamer, łatwość obsługi systemu, którego działanie może być elastycznie dostosowywane do specyfiki rozgrywanych wyścigów, a także otwarta architektura rejestratorów NVR umożliwia lepsze wykorzystanie wszystkich zainstalowanych urządzeń.

– Ten projekt udowodnił, że rozwiązania systemowe oferowane przez firmę Dahua mogą sprostać wymaganiom stawianym przez użytkowników – powiedział **Pasquale Totaro**, dyrektor generalny firmy Videotrend będącej lokalnym dystrybutorem produktów Dahua na terenie Włoch. *– Ważne jest, by ceny oferowanych produktów były przystępne dla inwestorów. Z drugiej strony użytkownicy końcowi oczekują długoletniej gwarancji. Partnerstwo z firmą Dahua pozwala spełnić te z pozoru sprzeczne wymagania i gwarantuje nam stabilną pozycję na rynku.*

– Wyścigi samochodowe są symbolem włoskiej kultury. Czujemy się zaszczyceni możliwością zaoferowania naszych rozwiązań i udziałem w realizacji tego projektu – powiedział **Elmer Zhang**, dyrektor handlowy firmy Dahua Technology odpowiedzialny za rynek europejski.

– Jak wiadomo, wyścigi samochodowe są źródłem wielkich emocji i stanowią pasję wielu osób. Niezawodne rozwiązania, jakie proponujemy, umożliwią jeszcze głębsze przeżywanie tych emocji. Jak powiedział nasz lokalny dystrybutor, mamy nadzieję, że udana kooperacja przy realizacji tego projektu będzie stanowić dobry początek wspólnej realizacji podobnych przedsięwzięć w najbliższej przyszłości – dodał Zhang.

Bezpośr. inf. JoJo Li
Dahua Technology

Tłumaczenie: Redakcja

Dahua wprowadza na rynek nową sieciową kamerę szybkoobrotową o rozdzielczości 2 Mpx, przyjazną dla środowiska naturalnego

Firma **Dahua** wprowadza na rynek nowe sieciowe kamery szybkoobrotowe, które pracują w standardzie full-HD, są wyposażone w zmiennoogniskowe obiektywy o krotności 12× (modele SD40/42/42C212S-HN) i spełniają wymagania Eco-Savvy, a więc są przyjazne dla środowiska naturalnego.

W tych niewielkich rozmiarów kamerach szybkoobrotowych znajduje się chipset Ambarella, dzięki któremu odznaczają się one niską przepływnością wyjściowego strumienia danych, niskim zużyciem energii i niskimi wymaganiami dotyczącymi oświetlenia obserwowanych scen. Z tych względów omawiane kamery można zaliczyć do urządzeń przyjaznych dla środowiska naturalnego. Potwierdzają to przeprowadzone testy, z których wynika, że przepływność wyjściowego strumienia danych nie przekracza 4 Mb/s przy pracy w standardzie 1080p i 2 Mb/s przy pracy w standardzie 720p, przy czym w obu przypadkach kodowanych jest 60 ramek na sekundę, co znakomicie ułatwia śledzenie obiektów ruchomych. Ponadto, w porównaniu z poprzednimi modelami, zużycie energii podczas ciągłej eksploatacji tych kamer jest niskie i nie przekracza 50 kWh rocznie.

Nowe kamery szybkoobrotowe mają zwartą, jednoczęściową konstrukcję. We wspólnej obudowie umieszczone są wszystkie niezbędne przyłącza, w tym interfejsy wizyjne, dźwiękowe, alarmowe i sieciowe oraz gniazda służące do instalacji kart pamięci SD.

W trybie dziennym kamery z nowej serii realistycznie reprodukują barwy, a podczas pracy w trybie nocnym obraz jest czysty i ostry. Poziom szumów jest bardzo niski w obu tych trybach.

W kamerach zastosowano obiektywy zmiennoogniskowe o krotności 12×, których kąt widzenia zmienia się w zakresie od 4,64 do 51,3 stopnia. Warto podkreślić, że omawiane urządzenia mogą pracować w trybie *smart eye*, w którym regulacja ostrości obrazu odbywa się automatycznie, bez żadnego opóźnienia, co jest przydatne w sytuacjach, w których konieczne jest szybkie reagowanie na zachodzące wydarzenia. Prędkość obrotowa omawianych kamer w osi pionowej wynosi maksymalnie 300°/s. Wszystkie urządzenia wizyjne firmy Dahua są zgodne z protokołem ONVIF. Ponadto kamery mogą być zasilane metodą PoE+ (IEEE 802.3at).

Szybkoobrotowe kamery Dahua typu SD40/42/42C212S-HN mogą by stosowane na stacjach kolejowych, lotniskach, w dużych salonach sprzedaży, sklepach detalicznych, hotelach i tym podobnych obiektach. Można je zamocować na ścianach, sufitach, pionowych wspornikach oraz w podwieszanych sufitach.

Bezpośr. inf. JoJo Li
Dahua Technology
Tłumaczenie: Redakcja

Dahua wprowadza na rynek interfejs HDCVI

Dahua Technology wprowadza na rynek interfejs HDCVI (*High Definition Composite Video Interface*). HDCVI stanowi przełom technologiczny w branży telewizji dozorowej i stwarza możliwość szybkiego i łatwego podwyższenia rozdzielczości obrazu do poziomu HD w istniejących systemach dozorowych z wykorzystaniem konwencjonalnego okablowania. Technologia HDCVI znajduje zastosowanie w systemach instalowanych wewnątrz budynków i pozwala na transmisję analogowych sygnałów wizyjnych w standardzie HD za pośrednictwem zwykłych kabli koncentrycznych. Koszty modernizacji są niskie, zaś wdrożenie nowej technologii jest łatwe.

Zalety technologii HDCVI

Łatwość modernizacji i zwiększenia rozdzielczości do poziomu HD

Interfejs HDCVI wykorzystuje standardy 1080p i 720p i umożliwia transmisję sygnałów wizyjnych z analogową modulacją za pośrednictwem kabli koncentrycznych, co oznacza, że w nowych rozwiązaniach można stosować te same metody instalacji i uruchomienia systemów co w klasycznych systemach analogowych. Jedyna różnica polega na tym, że obraz ma wysoką rozdzielczość i dzięki temu możliwa jest dokładna reprodukcja szczegółów.

Transmisja sygnału na duże odległości

Dzięki temu, że interfejs HDCVI pozwala na transmisję analogowych sygnałów wizyjnych na znaczne odległości, możliwe jest przekazywanie obrazów w rozległych instalacjach dozorowych bez konieczności stosowania jakichkolwiek urządzeń retransmisyjnych. W przypadku stosowania standardowych kabli koncentrycznych interfejs HD-SDI umożliwia transmisję obrazów co najwyżej na odległość 100 metrów, gdy tymczasem użycie interfejsu HDCVI oraz kabla koncentrycznego 75-3 sprawia, że odległość wzrasta do 500 metrów i nie ma wyraźnych zakłóceń.

Transmisja trzech sygnałów przez jeden kabel

Interfejs HDCVI pozwala na jednoczesną transmisję trzech sygnałów – wizyjnego, akustycznego i sterującego – za pośrednictwem jednego kabla koncentrycznego. Dzięki temu można znacznie uprościć okablowanie systemów dozorowych.

Brak opóźnienia

Interfejs HDCVI umożliwia niezawodną transmisję sygnałów analogowych między dwoma urządzeniami bez zauważalnych opóźnień, co ułatwia sterowanie urządzeniami pracującymi w czasie rzeczywistym. Ze względu na brak kompresji obraz zachowuje wysoką jakość, a barwy zostają znakomicie odwzorowane.

Wprowadzenie na rynek technologii HDCVI stanowi przełomowe wydarzenie w branży wizyjnych systemów dozorowych. Obecnie można transmitować obrazy o rozdzielczości megapikselowej na duże odległości i jednocześnie zachować prostotę instalacji.

Bezpośr. inf. JoJo Li
Dahua Technology
Tłumaczenie: Redakcja

Dahua rozszerza ofertę rejestratorów NVR

Dahua powiększa asortyment oferowanych rejestratorów NVR i wprowadza na rynek trzy serie urządzeń. Na jedną z nich składają się modele podstawowe, a na drugą modele zaawansowane technologicznie.

Profesjonalne rejestratory z serii NVR54

Rejestratory z serii 54 są przeznaczone do pracy w systemach o średniej wielkości, w których kładzie się szczególny nacisk na pojemność pamięci. Znajdą one zastosowanie w branży telekomunikacyjnej, energetycznej, systemach bezpieczeństwa publicznego, na rynku handlu sieciowego itp. W ramach każdej z serii oferowane są modele 8-, 16- i 32-kanałowe oraz wersje, w których kamery są zasilane metodą PoE. Przykładowym przedstawicielem tej serii rejestratorów może być model NVR5416/5432-16P.

Rejestrator NVR5416/5432-16P obsługuje szesnaście kanałów wizyjnych lub trzydzieści dwa kanały wizyjne w standardzie 1080p z możliwością podglądu w czasie rzeczywistym. Może też obsłużyć pięć kamer o rozdzielczości 5 megapikseli, jest w stanie zarejestrować sumaryczny strumień danych wejściowych o przepływności 160 Mb/s i wytworzyć sumaryczny strumień danych wyjściowych o przepływności 128 Mb/s, co pozwala na jednoczesną, płynną rejestrację wielu obrazów z kamer HD i kamer megapikselowych. W rejestratorze można zainstalować cztery dyski SATA, z których każdy może mieć pojemność 4 TB.

Rejestratory z tej serii mogą obsłużyć jednocześnie 128 użytkowników sieciowych. Ważną funkcją, umożliwiającą wykorzystanie krótkich fragmentów zapisanego materiału wizyjnego w celach dowodowych, jest odtwarzanie klatka po klatce. Ponadto rejestratory NVR mogą współpracować z kamerami szybkoobrotowymi firmy Dahua i można za ich pośrednictwem korzystać z podstawowych funkcji kamer PTZ, takich jak regulacja ogniskowej czy regulacja ostrości, co znacznie ułatwia operatorom obsługę systemów dozorowych.

Należy podkreślić, że rejestratory NVR mają 16 portów umożliwiających zasilanie kamer metodą PoE oraz wykorzystanie funkcji IPC UPnP, co upraszcza instalację i konfigurację systemu dozorowego.

Rejestratory z podstawowej serii NVR31/21H

Rejestratory z serii 31/21 odniosły sukces, dlatego firma Dahua uzupełniła tę serię o usprawnione modele przeznaczone do małych i średnich instalacji, takich jak systemy instalowane w sklepach i innych obiektach handlu detalicznego, w hotelach itp.

Rejestratory z serii NVR31H obsługują cztery kanały wizyjne w standardzie 1080p i umożliwiają podgląd obrazów w czasie rzeczywistym, z jednoczesnym ich zapisem, zaś rejestratory z serii NVR21H obsługują cztery kanały wizyjne w standardzie 720p. Ponadto wszystkie te urządzenia pozwalają na dwukierunkową komunikację głosową, realizują funkcje alarmowe i funkcje zdalnego sterowania kamerami. Cechami wyróżniającymi te rejestratory spośród innych jest niskie zużycie energii oraz niski poziom wytwarzanego hałasu, co czyni je przyjaznymi dla środowiska naturalnego.

Wszystkie rejestratory NVR firmy Dahua spełniają wymagania ONVIF i mogą współpracować z kamerami sieciowymi wielu producentów.

Bezpośr. inf. JoJo Li
Dahua Technology

Tłumaczenie: Redakcja

Terminale kontroli dostępu z panelem dotykowym w ofercie firmy ROGER

Asortyment oferowanych przez firmę **ROGER** terminali kontroli dostępu został poszerzony o nową serię urządzeń o nazwie **QUADRUS**. Nowa seria odzwierciedla aktualne trendy stylistyczne we wzornictwie urządzeń z ekranami dotykowymi.

W skład nowej rodziny urządzeń wejdą czytniki zbliżeniowe, wykorzystujące technologię EM 125 kHz i 13.56 MHz Mifare, oraz, w zależności od modelu, urządzenia wyposażone w dotykowe klawisze funkcyjne lub klawiaturę sensoryczną.

W ramach serii pojawią się również urządzenia funkcjonalnie wykraczające poza systemy kontroli dostępu i przeznaczone do automatyki biurowej, między innymi panel sterowania klimatyzacją, panel przycisków funkcyjnych, graficzny panel dotykowy, panel sygnalizacji akustyczno-optycznej.

Urządzenia serii QUADRUS są przeznaczone do pracy zarówno w znajdującym się obecnie w sprzedaży systemie kontroli dostępu RACS 4, jak i w przygotowywanym do wdrożenia w tym roku systemie RACS 5. Niektóre wersje urządzeń będą

mogły pracować w standardzie Wiegand, więc będzie można je dołączyć do kontrolerów dostępu innych producentów.

Urządzenia będą oferowane w dwóch wersjach kolorystycznych – białej i czarnej.

Bezpośr. inf. ROGER

CEM Systems zabezpiecza nowy kompleks szpitalny w Glasgow

Zintegrowany system zarządzania bezpieczeństwem CEM AC2000 chroni szpital w Glasgow

Firma **CEM Systems,** należąca do grupy Tyco Security Products, ma przyjemność zaanonsować podpisanie umowy na projekt i instalację systemu zabezpieczającego w największym nowo powstającym państwowym obiekcie szpitalnym w Szkocji. Kompleks New South Glasgow Hospitals powstaje w regionie Greater Glasgow and Clyde. Ten finansowany z publicznych pieniędzy projekt pozwoli na stworzenie jednego z najlepszych ośrodków leczenia szpitalnego dla dorosłych w Wielkiej Brytanii oraz największego ośrodka intensywnej terapii w Szkocji.

Boston Networks, autoryzowany dystrybutor produktów firmy CEM Systems, instaluje zintegrowany system inteligentnego zarządzania budynkiem wart miliony funtów, w skład którego wchodzi system zarządzania bezpieczeństwem CEM AC2000, kontrolujący ponad 400 wejść w całym obiekcie. Prace budowlane rozpoczęły się na początku 2010 roku, a ich zakończenie jest planowane na rok 2015. Głównym wykonawcą jest firma Brookfield Multiplex Construction Europe.

Zaawansowany system zarządzania bezpieczeństwem CEM AC2000 będzie stanowił podstawowe zabezpieczenie techniczne w nowym szpitalu dla dorosłych i dla dzieci w Glasgow. W projekcie przewidziano ponad tysiąc łóżek dla pacjentów w czternastopiętrowym kompleksie z nowoczesnym oddziałem ratunkowym, oddziałem intensywnej opieki medycznej, trzydziestoma nowoczesnymi salami operacyjnymi, oddziałami diagnostycznymi wraz z pełną ofertą pediatrycznych usług szpitalnych i ambulatoryjnych.

– Dzięki zastosowaniu systemu AC2000 kompleks szpitalny New South Glasgow Hospitals zostanie wyposażony w wysoce elastyczną i zintegrowaną infrastrukturę zabezpieczeń, powstałą przez połączenie wizyjnego systemu dozorowego Pelco Endura z systemem sygnalizacji włamania i napadu Honeywell Galaxy – wyjaśnia **Philip Verner**, regionalny dyrektor sprzedaży, EMEA, CEM Systems. – *System CEM AC2000 pozwala na integrację urządzeń na wysokim poziomie technologicznym, dzięki czemu możemy zapewnić ośrodkowi szpitalnemu w Glasgow wysoce skuteczny system zarządzania bezpieczeństwem.*

– Ze względu na dużą skalę i złożoność projektu systemu zabezpieczeń w New South Glasgow Hospitals, firma Boston Networks przy wyborze partnerów musiała wziąć pod uwagę wiele różnych czynników, takich jak wybór najlepszej technologii umożliwiającej rozbudowę systemu, dobór odpowiedniego poziomu integracji oraz możliwość spełnienia wszystkich wymagań związanych z warunkami instalacji i eksploatacji systemów w obiektach szpitalnych – komentuje **Paul Goodbrand**, dyrektor ds. inteligentnych budynków w firmie Boston Networks.

Oprócz integracji systemów zabezpieczających platforma CEM AC2000 umożliwia instalację wielu aplikacji usprawniających obsługę obiektu. W ośrodku New South Glasgow Hospitals wykorzystywane będzie oprogramowanie AC2000 VIPPS, które umożliwia projektowanie i wydruk profesjonalnych identyfikatorów, na których można umieszczać tekst, znaki graficzne, zdjęcia, kody kreskowe i podpisy. Będzie wykorzystane także oprogramowanie AC2000 AED, które zapewni bieżącą, dynamiczną wizualizację wszystkich alarmów i zdarzeń zachodzących w obrębie systemu AC2000.

Infrastruktura sieci Ethernet w nowo powstającym budynku szpitalnym jest zaprojektowana tak, że wszystkie urządzenia dostarczane przez firmę CEM Systems mogą być zasilane metodą PoE. Oznacza to, że do każdego z przejść może być doprowadzony tylko jeden kabel Ethernet, co w przypadku instalacji na tak rozległym obszarze upraszcza i przyspiesza montaż urządzeń peryferyjnych.

– Dzięki możliwościom technologicznym, wynikającym z zasilania urządzeń dostarczanych przez firmę CEM Systems metodą PoE, i wyjątkowym właściwościom systemu AC2000. Firma Boston Networks spełniła wymagania postawione przez szpital i stworzyła wydajny system, którego wdrożenie zmieściło się w określonych ramach budżetowych – kontynuuje **Paul Goodbrand**. – *Dzięki pełnej kontroli nad przebiegiem instalacji i ścisłej współpracy z firmą CEM mamy pewność, że spełnimy wymagania projektowe i dotrzymamy terminu realizacji inwestycji.*

W systemie kontroli dostępu wykorzystane zostaną czytniki CEM EtherProx. Są to najmniejsze dostępne w tej branży czytniki kart działające w sieci Ethernet, wyposażone w zintegrowaną klawiaturę i wyświetlacz LCD. Czytniki mają własną bazę danych, która umożliwia walidację kart identyfikacyjnych i inteligentne podejmowanie decyzji dotyczących otwierania przejść w trybie offline, nawet w przypadku chwilowego braku łączności z centralnym serwerem. Czytniki EtherProx umożliwiają wyświetlanie komunikatów z opisem przeznaczonym dla konkretnych użytkowników systemu natychmiast po odczytaniu danych z karty. Na przykład – sanitariusz próbujący wejść do szpitalnej apteki może otrzymać komunikat o odmowie dostępu, potwierdzony zaświeceniem się czerwonej diody LED.

Bezpośr. inf. Rachel Marley
CEM Systems

Bosch łączy alarm pożarowy i dźwiękowe systemy ostrzegawcze za pomocą sieci IP

Nowa centrala sygnalizacji pożaru FPA 5000

Bosch zwiększa skuteczność systemu sygnalizacji pożarowej i łączy go poprzez sieć IP z dźwiękowym systemem ostrzegawczym. Rozwiązanie to zastosowano w najnowszej centrali sygnalizacji pożarowej **FPA 5000**.

Zadaniem priorytetowym w przypadku każdego pożaru jest jak najszybsza ewakuacja osób z zagrożonego budynku lub obszaru. Z tego względu firma Bosch opracowała rozwiązanie, które może skrócić czas trwania tej ewakuacji. W najnowszej wersji modułowej centrali sygnalizacji pożarowej FPA 5000 zastosowano dwukierunkowe połączenie systemu sygnalizacji pożarowej z systemami nagłośnieniowymi.

Panel centrali sygnalizacji pożarowej FPA 5000 wyposażono w interfejs IP z cyfrowym systemem nagłośnieniowym i dźwiękowym systemem ostrzegawczym Praesideo. Dzięki temu zapewniono elastyczne i trwałe połączenie między systemami.

Połączenie centrali alarmu pożarowego z dźwiękowym systemem ostrzegawczym poprzez sieć Ethernet pozwala uniknąć konieczności instalacji dodatkowego okablowania oraz sprzętu, a także znacznie skraca czas i obniża koszt wykonania instalacji. Ponowne okablowanie sprzętu nie będzie konieczne, nawet w przypadku dalszej rozbudowy systemu. Dodatkowo pojedyncze połączenie z siecią Ethernet eliminuje ryzyko wykonania błędów w okablowaniu, które występowało w starszych systemach korzystających z kilku połączeń kablowych.

Interfejs centrali sygnalizacji pożarowej FPA 5000 spełnia wymogi normy EN 54. Może pracować w sieci IP, co czyni go idealnym rozwiązaniem dla dużych instalacji wykorzystujących wiele połączeń, takich jak systemy stosowane na lotniskach czy dworcach kolejowych.

Bezpośr. inf. Bosch Security Systems

Samsung Techwin ogłasza wprowadzenie usługi *Advanced Replacement*

Wprowadzenie przez dział profesjonalnych produktów zabezpieczających usługi *Advanced Replacement* podkreśla zaangażowanie firmy Samsung Techwin w zapewnienie klientom najwyższego poziomu obsługi posprzedażowej.

– Nasze produkty służące do budowy wizyjnych systemów dozorowych mają wysoką niezawodność. Zdajemy sobie jednak sprawę, jakim problemem dla instalatorów i użytkowników jest oczekiwanie na sprawdzenie produktu, odpowiedź na zgłoszenie uszkodzenia i dokonanie wymiany – powiedział **Jason Rou**, European Service Manager w **Samsung Techwin Europe**. *– Wprowadzenie naszej nowej usługi Advanced Replacement spowoduje, że instalatorzy uzyskają pewność, że obsługiwany przez nich system zostanie usprawniony w najkrótszym możliwym czasie i nie będą musieli czekać na dostarczenie sprzętu do jednego z naszych centrów serwisowych.*

Jeśli urządzenie ulegnie uszkodzeniu w ciągu pierwszego roku eksploatacji, w trakcie trzyletniego okresu gwarancji, to w ciągu 48 godzin od zgłoszenia zostanie wysłany sprzęt zastępczy. Ta nowa usługa jest dostępna w przypadku wszystkich produktów do analogowej telewizji przemysłowej oraz telewizji przemysłowej IP, z wyłączeniem akcesoriów, klawiatur operatorskich oraz monitorów.

Instalatorzy, który zostaną przeszkoleni w ramach programu **Samsung Techwin Smart Partners**, uzyskają możliwość korzystania z usługi **Advanced Replacement** przez pierwsze dwa lata w trzyletnim okresie gwarancyjnym.

– Chcemy pomagać profesjonalnym instalatorom systemów bezpieczeństwa w oferowaniu lepszej obsługi serwisowej oraz we współpracy z obecnymi klientami. Rozszerzenie oferowanej przez nas gwarancji samo w sobie jest znaczącym krokiem. Jest ono również uzupełnieniem całego zestawu oferowanych przez nas usług dodatkowych, w tym bezpłatnego projektowania systemu, wsparcia technicznego i szkoleń – powiedział Jason Rou. *– Dzięki naszym dystrybutorom dowiedzieliśmy się, co jest ważne dla naszych klientów. Zaowocowało to wprowadzeniem w ostatnim czasie serii kamer WiseNetIII, w których zaimplementowaliśmy funkcje, jakie według użytkowników produktów Samsung Techwin powinny mieć nasze kamery sieciowe, aby stać się kamerami sieciowymi preferowanymi przez instalatorów i użytkowników końcowych. Jednak w pełni rozumiemy, że doskonałe produkty to nie wszystko i musimy oferować większy zakres usług realizowanych przez nasz specjalny dział wsparcia technicznego.*

Więcej informacji o polityce gwarancyjnej Samsung Techwin oraz procedurach zwrotu sprzętu można znaleźć na stronie internetowej – pod adresem *www.samsungsecurity.co.uk.*

Bezpośr. inf. Samsung Techwin Europe, Poland

Interfejs komunikacyjny GSM/GPRS do systemu kontroli dostępu RACS

Interfejs komunikacyjny **RCI-6** jest nowym, wielofunkcyjnym urządzeniem w ofercie firmy **ROGER**, wykorzystującym technologię GSM/GPRS i przeznaczonym do zastosowania w systemach kontroli dostępu RACS 4 i RACS 5, jak też do pracy poza tymi systemami.

Podstawowym zadaniem interfejsu RCI-6 jest przesyłanie komunikatów o zdarzeniach, które wystąpiły w systemie kontroli dostępu, do stacji monitorowania alarmów lub na zaprogramowane numery abonentów telefonii komórkowej. Powiadamianie może być realizowane z wykorzystaniem popularnych standardów SIA, Contact ID, Ademco Express lub transmisji w technologii SMS/CLIP. Współbieżnie z funkcją powiadamiania interfejs RCI-6 może pełnić rolę terminalu (czytnika) dostępu, przez który użytkownik może zdalnie, przez sieć komórkową, uzyskiwać dostęp na przejściu będącym pod nadzorem systemu RACS.

Użycie interfejsu RCI-6 jako terminalu dostępu stwarza możliwość wykorzystania go jako czytnika dalekiego (globalnego) zasięgu, w którym rolę identyfikatora pełni telefon komórkowy. Zdalne logowanie z poziomu telefonu komórkowego może być realizowane przez GPRS lub poprzez wysłanie wiadomości SMS/CLIP. Do zdalnego logowania służy aplikacja mobilna przeznaczona dla systemu operacyjnego Android, która umożliwia zgłoszenie chęci uzyskania zdalnego dostępu poprzez wygodny interfejs graficzny, bez konieczności manualnego tworzenia wiadomości SMS i zestawiania połączenia telefonicznego.

Jak większość tego typu urządzeń, interfejs RCI-6 jest wyposażony w zestaw trzech linii wejściowych, które mogą być objęte monitorowaniem, oraz dwóch linii wyjściowych z możliwością zdalnego sterowania przez SMS, co dodatkowo zwiększa liczbę możliwości wykorzystania tego wielofunkcyjnego urządzenia.

Bezpośr. inf. ROGER

Polska edycja Commend Roadshow 2013 – podsumowanie

Interkom o wielu możliwościach

Firmy **C&C Partners Telecom** i **Commend International** – producent zaawansowanych systemów interkomowych – zorganizowały w dniach 4–7 listopada br. cykl spotkań pod nazwą **Commend Roadshow 2013**, które odbyły się w Katowicach, Gdańsku, Warszawie oraz we Wrocławiu.

Bloki tematyczne:

1) **Ukryte skarby.** W dotychczasowym dorobku technologicznym firmy Commend znalazło się wiele rozwiązań, które ułatwiają nam codzienne funkcjonowanie. Jednym z nich jest ciągła gotowość interkomów do pełnienia przypisanych im funkcji. Jest ona możliwa dzięki zdalnemu monitorowaniu stanu technicznego interkomów i szybkiemu reagowaniu w sytuacjach uniemożliwiających ich poprawne działanie, np. w momencie zaklejenia gumą do żucia mikrofonu interkomu przeznaczonego do komunikacji alarmowej. Przykładem innego bardzo użytecznego rozwiązania jest rozgłaszanie tzw. automatycznych komunikatów głosowych, które pozwalają np. na poinformowanie kierowcy, chcącego dostać się na teren parkingu, o awarii automatu biletowego lub szlabanu.
2) **Wirtualizacja.** Główną ideą wirtualizacji jest współdzielenie zasobów sprzętowych jednego serwera przez wiele równocześnie uruchomionych systemów operacyjnych oraz aplikacji. Taki kierunek rozwoju został przyjęty również przez firmę Commend, która, wprowadzając do oferty pierwszy na świecie programowy serwer interkomowy VirtuoSIS, wyprzedziła trendy rynkowe w dziedzinie systemów zabezpieczeń. Niezwykle istotną cechą serwera programowego jest możliwość łączenia urządzeń wykorzystujących różne technologie, nawet 30-letni interkom może być dziś podłączony do serwera VirtuoSIS, którego środowiskiem pracy, dzięki kompatybilności ze standardami wirtualizacji, może być również chmura.

3) **Przyszłość interkomów.** Firmy Commend i C&C wspólnie tworzą interkomy, analizując możliwe kierunki rozwoju oraz obecne i przyszłe trendy technologiczne. Biorąc pod uwagę nowoczesne metody pracy różnych aplikacji, wykorzystujące wirtualne serwery, funkcje realizowane przez fizyczne stacje interkomowe mogą zostać przeniesione w obszary dotychczas nieosiągalne. Obecnie największym wyzwaniem technologicznym jest usprawnienie komunikacji głosowej pomiędzy osobami władającymi różnymi językami. Usprawnienie to umożliwiłoby tłumaczenie informacji słownych w czasie rzeczywistym. Kilka firm próbowało już rozwiązać ten problem za pomocą odpowiednich narzędzi programowych, ale nadal nie zapewniają one naturalnej komunikacji głosowej, tak istotnej w sytuacjach zagrożenia życia bądź potrzeby uzyskania informacji.

Commend Roadshow to impreza ogólnoświatowa. Kolejnym krajem, w którym odbędzie się cykl prezentacji, będzie Francja.

Bezpośr. inf. C&C Partners

Samsung wprowadza nową serię kamer 960H z funkcją WDR

Firma **Samsung Techwin** wprowadziła nową serię kamer o rozdzielczości 700 linii TV (960H), wytwarzających kolorowe obrazy nawet w złych warunkach oświetleniowych. Jedną z najbardziej interesujących instalatora funkcji będzie prawdopodobnie *Simple Focus*, ponieważ wydatnie skraca ona czas potrzebny na regulację ostrości.

Dwie kamery kopułkowe i kamera kompaktowa z nowej serii 960H mają zakres dynamiki WDR rozszerzony metodą opracowaną przez firmę Samsung Techwin, dzięki której skutki prześwietlenia fragmentów kadru są likwidowane 128 razy skuteczniej niż w przypadku stosowania standardowej funkcji WDR. Dzięki funkcji progresywnej kompensacji tylnego oświetlenia (SSDR), automatycznie dostosowującej ekspozycję w ciemnych obszarach kadru, a także funkcji redukcji szumów (SSNRIII) możliwe jest uzyskiwanie wysokiej jakości obrazów nawet w trudnych warunkach oświetleniowych. Minimalne, niezbędne do wytworzenia prawidłowego obrazu oświetlenie obserwowanej sceny wynosi 0,1 luksa. Nowe modele mają przetworniki z progresywnym skanowaniem, dzięki czemu prawidłowo reprodukują kształt obiektów znajdujących się w ruchu. Dzięki temu można na przykład łatwo odczytywać numery na tablicach rejestracyjnych pojazdów – nie występuje efekt rozmazania lub przesuniętych linii.

Dzięki funkcji *Simple Focus* pojedyncze naciśnięcie przycisku znajdującego się z tyłu kamery powoduje automatyczne ustawienie ostrości obrazu. Funkcję *Simple Focus* można również inicjować zdalnie – z poziomu rejestratora DVR połączonego z kamerą kablem koncentrycznym. Dodatkową zaletą jest to, że funkcja Simple Focus automatycznie optymalizuje ostrość i pozwala uzyskać wyraźne, ostre obrazy także po zmianie trybu pracy kamery (funkcja dzień/noc) z kolorowego na monochromatyczny, z czym wiąże się przesunięcie filtru podczerwieni.

Modele z serii 960H mają funkcję inteligentnej analizy obrazu (*Intelligent Video Analysis – IVA*), która może być wykorzystana do zliczania osób widocznych na obserwowanym obszarze lub do detekcji ruchu, w tym do wykrywania przekroczenia wirtualnej bariery, wykrywania pojawienia się lub zniknięcia obiektów oraz wykrywania prób sabotażu, dzięki czemu w razie zamalowania obiektywu farbą lub nieautoryzowanej zmiany pola widzenia kamery generowany jest alarm.

Trzy nowe modele kamer są w pełni kompatybilne z serią rejestratorów DVR 960H Samsung Techwin, które po wprowadzeniu na rynek w marcu 2013 r. ustanowiły nowy standard w dziedzinie cyfrowej rejestracji obrazów i zapewniły użytkownikom obserwację obrazów o wysokiej jakości na monitorach o wysokiej rozdzielczości.

Trzy opisywane modele z serii 960H to:
- kamera w obudowie tradycyjnej SCB-3003;
- kamera kopułkowa SCD-3083 z obiektywem zmiennoogniskowym, sterowanym za pomocą silnika o krotności regulacji ×3,6;
- wandaloodporna kamera kopułkowa SCV-3083 z obiektywem zmiennoogniskowym, sterowanym za pomocą silnika o krotności regulacji ×3,6.

Bezpośr. inf. Samsung Techwin Europe, Poland
Opracowanie: Redakcja

Nowa wersja oprogramowania CMS Samsung SmartViewer

Udostępniona niedawno nowa wersja oprogramowania SmartViewer służącego do zarządzania systemem dozoru wizyjnego **Samsung Techwin** obsługuje wszystkie produkty sieciowe Samsung oraz stacjonarne kamery analogowe, głowice szybkoobrotowe i rejestratory cyfrowe.

SmartViewer 4.0 został zaprojektowany dla systemów dozoru wizyjnego składających się z maksymalnie 36 kamer.

Umożliwia uprawnionym użytkownikom dostęp do systemu poprzez sieć komputerową, w celu podglądu bieżących obrazów i przeglądania zarejestrowanego materiału wizyjnego z kamer dołączonych do rejestratorów cyfrowych (DVR) lub rejestratorów sieciowych (NVR) marki Samsung.

Użytkownicy mogą jednocześnie wyświetlać obrazy z maksymalnie 16 kamer, w różnych trybach podziału ekranu, oraz zapisywać ulubione układy obrazów z kamer w celu ich szybkiego przywołania na ekran podglądowy.

Ważnym składnikiem oprogramowania SmartViewer 4.0 jest menadżer urządzeń, który automatycznie wykrywa kamery IP, enkodery i rejestratory podłączone do sieci oraz umożliwia pobieranie plików konfiguracyjnych i przesyłanie zapisanych wcześniej ustawień. Ma on również funkcję zdalnej aktualizacji oprogramowania wewnętrznego, co pozwala na

DIVAR IP – nowa seria sieciowych rejestratorów wizyjnych firmy Bosch

W najnowszej serii sieciowych rejestratorów wizyjnych **DIVAR IP** firma **Bosch Security Systems** zastosowała innowacyjną technologię dynamicznego transkodowania. Dzięki temu możliwy jest natychmiastowy dostęp do nagrań o jakości HD w dowolnym miejscu na świecie, w którym jest dostęp do Internetu.

Technologia dynamicznego transkodowania (*Dynamic Transcoding Technology*) wykorzystana w rejestratorach wizyjnych DIVAR IP gwarantuje transmisję obrazu na żywo oraz odtwarzanie go w rozdzielczości HD. Jakość obrazu jest dostosowywana do dostępnej szerokości pasma, dlatego ograniczenie dostępu do usług sieciowych 3G czy dostęp do sieci przez Wi-Fi przy stale zmieniającej się przepustowości nie będzie już utrudniać śledzenia nagrań.

Rejestratory wizyjne z nowej serii należą do grupy urządzeń określanych mianem „wszystko w jednym" i pozwalają na zarządzanie zarejestrowanym materiałem wizyjnym. Do grupy urządzeń DIVAR IP typu „wszystko w jednym" należą sieciowe rejestratory wizyjne (DIVAR IP 2000, DIVAR IP 3000, DIVAR IP 6000 lub DIVAR IP 7000), macierz dyskowa, i stacja robocza wraz ze zintegrowanym oprogramowaniem.

Sieciowe rejestratory wizyjne serii DIVAR IP umożliwiają nagrywanie, podgląd i eksport obrazów w rozdzielczości HD lub w rozdzielczości standardowej. Możliwa jest równoczesna transmisja obrazów o proporcjach 16: 9 i 4:3. W zależności od modelu rejestratora oglądanie obrazów i zarządzanie obrazami jest możliwe za pomocą zdalnego klienta, zintegrowanego klienta lub zintegrowanej aplikacji sieciowej (aplikacja *Bosch Video Security* pozwala na oglądanie nagrań o jakości HD na iPadach i iPhonach; aplikację można pobrać bezpłatnie ze strony *https://itunes.apple.com/us/app/video-security/id569156417?mt=8*).

Rejestratory wizyjne typu „wszystko w jednym" DIVAR IP 3000 i DIVAR IP 7000 są wyposażone w oprogramowanie *Video Management Software* firmy Bosch i zapewniają zaawansowane przetwarzanie sygnałów alarmowych, które gwarantuje identyfikację zdarzeń o charakterze krytycznym oraz zarządzanie tymi wydarzeniami. Rejestratory mają także funkcję *Forensic Search*, umożliwiającą operatorom systemów szybkie wyszukanie określonych zdarzeń w wielogodzinnym materiale wizyjnym, a po znalezieniu poszukiwanego zdarzenia, dzięki funkcji *Instant Detail Enhancement*, natychmiast wyświetlają obraz o jakości Full HD.

– Wymagania klientów ciągle rosną. Obecnie zależy im na stałym dostępie do wysokiej jakości nagrań z systemów telewizji dozorowej, niezależnie od tego, czy interesuje ich monitoring całej sieci hoteli czy jednej stacji paliw. Użytkownicy przyzwyczajeni do mobilnych rozwiązań oczekują identycznego komfortu w dostępie do nagrań niezależnie od tego, gdzie w danym momencie się znajdują. Wprowadzając na rynek cztery nowe sieciowe rejestratory wizyjne, firma Bosch spełnia oczekiwania klientów i oferuje im proste w obsłudze, a jednocześnie zaawansowane technologicznie rozwiązanie dla małych, średnich i dużych instalacji – powiedział **Michal Biela** z Bosch Security Systems.

W skład serii DIVAR IP wchodzą produkty skalowalne, dzięki czemu możliwe jest dopasowanie ich funkcji do instalacji różniących się wielkością. DIVAR IP 3000 obsługuje maksymalnie 32 kanały wizyjne i ma pamięć o pojemności 4 TB lub 8 TB, co sprawia, że jest idealnym rozwiązaniem dla małych i średnich systemów, instalowanych w takich miejscach jak sklepy, placówki edukacyjne czy banki. Dla dużych systemów przeznaczony jest model DIVAR IP 7000, który w wersji prelicencyjnej ma pamięć 16 TB i obsługuje nawet do 128 kanałów wizyjnych. Pojemność pamięci wszystkich modeli rejestratorów serii DIVAR IP można zwiększyć poprzez dodanie do nich kolejnych urządzeń pamięciowych DIVAR IP 2000 lub DIVAR IP 6000.

Rejestratory wizyjne DIVAR IP są zgodne ze standardem ONVIF, więc łatwo integrują się ze sprzętem i oprogramowaniem firmy Bosch, a także z produktami innych producentów. Decydując się na rejestrator serii DIVAR IP, warto skorzystać z programu Bosch Integration Partner Program, który zapewnia projektantom dostęp do narzędzi sieciowych umożliwiających łatwą integrację oprogramowania do zarządzania i rejestracji, analizy materiału wizyjnego, obsługi systemów wielomonitorowych oraz śledzenia nagrań w chmurze. Więcej informacji na temat programu jest dostępnych na stronie *ipp.boschsecurity.com*.

Bezpośr. inf. Bosch Security Systems
Opracowanie: Redakcja

zaoszczędzenie czasu i pieniędzy, ponieważ instalator nie musi pojawiać się w obiekcie, w którym są zainstalowane urządzenia. Ponadto program umożliwia wybieranie obrazów z kamer za pomocą techniki „przeciągnij i upuść", obsługuje obrazy w formacie H.264, MPEG-4 i MJPEG, udostępnia listę zdarzeń raportowanych przez urządzenia oraz ma interfejs użytkownika w 24 językach.

– Klienci z pewnością dostrzegą, że SmartViewer 4.0 jest łatwy w obsłudze – powiedział **Peter Ainsworth**, Senior Product Manager w Samsung Techwin Europe. – *Nasi inżynierowie odpowiedzialni za oprogramowanie stworzyli produkt stanowiący uproszczoną wersję programu SSM (Samsung Security Manager). Jak wynika z opinii naszych klientów, pomaga on użytkownikom w pełni wykorzystywać możliwości systemów dozoru wizyjnego.*

Bezpośr. inf. Samsung Techwin Europe, Poland

WARSZTATY PROJEKTOWE FIRMY BOSCH

CZWARTEK
PAŹDZIERNIK
23

PODSUMOWANIE

24 października 2013 r. odbyły się warsztaty projektowe zorganizowane przez firmę **Bosch**. Tematy poruszone na warsztatach to:

1) Aktualny status certyfikacji rozwiązań Bosch DSO w CNBOP – certyfikacja urządzeń z zakresu ochrony przeciwpożarowej w świetle Rozporządzenia UE nr 305/2011 (zmiana z CPD na CPR).
2) Integracja centrali SAP FPA-5000 z centralą DSO Praesideo za pomocą nowego interfejsu IP.
3) Zastosowanie urządzeń multimedialnych Bosch w instalacjach nagłośnieniowych oraz konferencyjnych.
4) Integracja automatyki budynkowej oraz systemów bezpieczeństwa różnych producentów za pomocą platformy zarządzającej BIS (Building Integration System).
5) Wykorzystanie standardu 960H w analogowych instalacjach CCTV.
6) Nowa jakość obrazu i zapisu w rejestratorach cyfrowych Divar IP.

Na warsztatach odbył się wykład ekspercki pt. *Kable w instalacjach przeciwpożarowych – zachowanie funkcjonalności w warunkach pożaru*, wygłoszony przez mł. bryg. mgr inż. Edwarda Skiepko.

Warsztaty były przeznaczone przede wszystkim dla projektantów systemów zabezpieczeń budynkowych i instalatorów systemów.

Wejście w życie z dniem 1 lipca br. Rozporządzenia UE nr 305/2011 wpływa znacząco zarówno na certyfikację wyrobów przeznaczonych do stosowania w systemach ochrony przeciwpożarowej, jak i na przepisy dotyczące stosowania materiałów w technice budowlanej. Podczas warsztatów przedstawiono uczestnikom rodzaje świadectw i certyfikatów obowiązujących po wejściu w życie rozporządzenia, systemy oceny i weryfikacji stałości własności użytkowych, zasady i podstawy wydawania deklaracji właściwości użytkowych przez producentów wyrobów budowlanych i inne zmiany wynikające z wejścia w życie wspomnianego rozporządzenia.

Prelegenci przestawili przykłady integracji różnych systemów zabezpieczeń z wykorzystaniem platformy zarządzającej, urządzenia multimedialne w systemach konferencyjnych oraz nowości techniczne w telewizji dozorowej, zarówno cyfrowej, jak i analogowej. Szczegółowo przedstawiono właściwości nowej wersji centrali sygnalizacji alarmów pożarowych FPA 5000 oraz zwiększone możliwości sterowania przez nią systemem DSO typu Praesideo.

Warsztaty zakończył wykład ekspercki na temat kabli w instalacjach przeciwpożarowych, w którym zwrócono uwagę na powszechnie popełniane (również przez rzeczoznawców) błędy przy doborze, prowadzeniu i mocowaniu kabli w tych instalacjach. Najważniejszym zadaniem okablowania w instalacjach przeciwpożarowych jest zachowanie funkcji systemu podczas pożaru i na tym należy skupić się przy opracowywaniu projektu i wykonywaniu instalacji.

Opracowanie: Redakcja

Spotkanie Partnerów firmy Axis Communications – podsumowanie

Dnia 14 listopada 2013 roku w Hotelu Hayatt w Warszawie odbyło się kolejne spotkanie przedstawicieli firmy **Axis Communications** z partnerami biznesowymi. Licznie przybyłych uczestników powitała **Agata Majkucińska**. Następnie głos zabrał **Martin Gren**, jeden ze współzałożycieli firmy Axis oraz współtwórca pierwszej kamery sieciowej tej firmy. Prelekcja, którą wygłosił, dotyczyła oceny obecnej sytuacji rynkowej oraz planów produkcyjnych firmy Axis na najbliższe lata.

Spotkanie miało charakter edukacyjny. Kolejni prelegenci omówili różne zagadnienia techniczne, związane z projektowaniem i instalacją wizyjnych systemów dozorowych, w których wykorzystuje się urządzenia firmy Axis Communications. Zaproszeni goście gromkimi brawami nagrodzili **Jana Gruszkę**, który z typową dla siebie lekkością zaprezentował nowe kamery firmy Axis oraz zapoznał zebranych z metodami badań jakościowych prowadzonych na terenie zakładów wytwórczych w Szwecji. Szczególne zainteresowanie wzbudził opis laboratorium optycznego, w którym testowane są obiektywy stosowane w kamerach Axis.

Głos zabrali również projektanci i instalatorzy systemów dozorowych, którzy podzielili się swoimi doświadczeniami zebranymi podczas wieloletniej współpracy z firmą Axis Communications. Zaprezentowano także liczne eksponaty i tablice poglądowe. Przedstawiono innowacyjny system Axis Camera Companion oraz oprogramowanie służące do zarządzania wizyjnymi systemami dozorowymi wykorzystującymi kamery Axis. Duże zainteresowanie uczestników spotkania wzbudziła zaciemniona komora, w której umieszczona została wysokoczuła kamera Axis. Znakomity obraz, jaki można było obserwować na ekranie monitora, stanowił dowód na przydatność tej kamery w bardzo złych warunkach oświetleniowych.

Spotkanie zakończyło się wręczeniem nagród dla wyróżniających się partnerów firmy Axis oraz losowaniem, w którym główną nagrodą była kamera sieciowa.

Redakcja


AXIS
Experience smarter
Axis Roadshow


AXIS


AXIS Camera Com
easiest way to network video surveillance

Wywiad z Martinem Grenem

członkiem zarządu firmy Axis Communications i jednym z jej współzałożycieli

Powszechnie wiadomo, że firma Axis od samego początku swojego istnienia oferuje kamery sieciowe i nigdy nie produkowała kamer analogowych. Dlaczego?

M.G.: Jeśli znają państwo historię firmy Axis Communications, powinniście także wiedzieć, że w okresie poprzedzającym nasze wejście na rynek wizyjnych systemów dozorowych zajmowaliśmy się produkcją innych urządzeń sieciowych. Doskonale znaliśmy zagadnienia związane z sieciami IP oraz zdawaliśmy sobie sprawę z tego, że prędzej czy później rozwiązania sieciowe zdominują rynek zabezpieczeń. Możliwe, że w początkowym okresie nasze działania były nieco przedwczesne, gdyż wtedy dominowały rozwiązania analogowe, jednak z czasem okazało się, że mieliśmy rację.

Podobno najnowsza kamera PTZ firmy Axis zawiera zaledwie kilka części ruchomych. Czy możemy usłyszeć coś więcej na temat tego modelu?

M.G.: Tak, to prawda. Nasza najnowsza kamera PTZ nie zawiera ani kół zębatych, ani pasków klinowych. Ruchome części są napędzane bezpośrednio przez dwa silniki krokowe, dzięki czemu uzyskaliśmy bardzo wysoką precyzję i powtarzalność pozycjonowania kamery. Poza tym tego typu napęd jest niezawodny i nie ulega szybkiemu zużyciu.

Panuje opinia, że firma Axis nie tylko dba o dobór odpowiednich rozwiązań technicznych, ale także przywiązuje wagę do estetyki swoich wyrobów.

M.G.: Faktycznie, zwracamy uwagę na estetykę naszych wyrobów. W dniu dzisiejszym Agata Majkucińska zabrała mnie na krótki spacer po Warszawie. Z przykrością stwierdziłem, że dostrzeżone przeze mnie kamery PTZ zainstalowane na elewacjach budynków nie są ich ozdobą. Dotyczyło to niestety wszystkich kamer, z modelami Axisa włącznie. Nasze obecne wyroby są wolne od tej wady. Wyszliśmy z założenia, że niemal wszystkie kamery, w tym także kamery PTZ, są instalowane na ścianach, dlatego najnowszy model ma odpowiednie mocowanie. Obudowa kamery składa się z dwóch części, przy czym jedną z nich przykręca się bezpośrednio do ściany, zaś druga jest mocowana na zawiasie. Podczas montażu kamerę można odchylić od ściany i podłączyć kable. Taki sposób mocowania jest bardzo wygodny dla instalatora. Poza tym wszystkie zewnętrzne części obudowy można łatwo zdemontować i pomalować na dowolny kolor. W efekcie kamery Axis wtapiają się w otoczenie i nie szpecą elewacji budynków.

Kamery firmy Axis słyną z dobrego obrazu. W znacznym stopniu przyczynia się do tego optyka. Z jakiego źródła pochodzą obiektywy montowane w waszych kamerach?

M.G.: Są to japońskie obiektywy, pochodzące od kilku różnych producentów. Elementy optyczne są dobierane odpowiednio do roli, jaką mają pełnić. Inne obiektywy stosujemy w kamerach PTZ, inne w kamerach stacjonarnych. Przy okazji chciałbym podkreślić, że dysponujemy własnym rozbudowanym laboratorium optycznym, w którym jesteśmy w stanie wnikliwie przebadać obiektywy oferowane przez poddostawców i wybrać te, które nam najlepiej odpowiadają.

Firma Axis jest jednym z niewielu, jeżeli nie jedynym dostawcą kamer termowizyjnych produkowanych z myślą o cywilnych systemach dozorowych. Co skłoniło firmę do ich produkcji?

M.G.: Faktycznie, kamery termowizyjne stanowiły dotychczas domenę rynku wojskowego. Były dwa powody, dla których wprowadziliśmy je do naszej oferty. Po pierwsze, w pewnych rejonach w Szwecji obowiązuje zakaz instalowania kamer dozorowych, a nie dotyczy to kamer termowizyjnych. Po drugie zauważyliśmy, że w wielu dużych instalacjach oprócz kamer pracujących w widmie widzialnym można spotkać kamery termowizyjne. Pełnią one rolę detektorów wykrywających ludzi i pojazdy mechaniczne nawet w zupełnych ciemnościach, czyli wspomagają pracę klasycznych kamer, szczególnie w nocy. Wprowadziliśmy na rynek własne kamery termowizyjne, gdyż istniało zapotrzebowanie na tego typu urządzenia.

Dotychczas rozmawialiśmy o najbardziej wyrafinowanych rozwiązaniach technicznych. Pomówmy jeszcze o dolnym segmencie rynku, czyli o systemach dozorowych powszechnego użytku. Jakie są plany firmy Axis w tej dziedzinie?

M.G.: Firma Axis nie lekceważy żadnego z segmentów rynku i ma w swojej ofercie kamery przeznaczone do pracy w małych instalacjach, służących do ochrony sklepów, biur, obiektów mieszkalnych. Znane wszystkim prawo Moore'a przewiduje, że zarówno moc obliczeniowa mikroprocesorów, jak i pojemność pamięci rośnie wykładniczo wraz z upływem czasu. Na tej podstawie doszliśmy do wniosku, że bez obaw o przyszłość można zbudować system dozorowy nie zawierający żadnej jednostki centralnej, a całą moc obliczeniową niezbędną do realizacji funkcji systemowych oraz całą pamięć niezbędną do rejestracji obrazów można zawrzeć wewnątrz kamer. W ten sposób powstał system Axis Camera Companion, który wykorzystuje sieć IP i nie wymaga użycia żadnych dodatkowych urządzeń poza samymi kamerami. Do zarządzania systemem i obserwacji obrazów wykorzystuje się dowolnie zlokalizowane komputery PC lub smartfony.

Faktycznie, to bardzo ciekawe rozwiązanie. Czy system Axis Camera Companion pozwala na archiwizację obrazów na innych nośnikach lub w chmurze internetowej?

M.G.: Oczywiście, to jest możliwe, jednak nie jest konieczne. Sumaryczna pojemność pamięci zainstalowanych we wszystkich kamerach pracujących w danym systemie wystarczy do wielotygodniowej archiwizacji obrazów. Pamiętajmy, że są to małe, lokalne systemy dozorowe, od których nie oczekuje się profesjonalnej archiwizacji obrazów. Prawo Moore'a pozwala nam przypuszczać, że wkrótce pojemność pamięci wzrośnie na tyle, że problem długoterminowej archiwizacji obrazów zostanie ostatecznie rozwiązany.

Na koniec porozmawiajmy o planach firmy Axis dotyczących szkolenia projektantów i instalatorów systemów dozorowych. Możemy prosić o kilka słów na ten temat?

M.G.: Jak państwu wiadomo, od jakiegoś czasu działa Akademia Axis, powołana w celu popularyzacji wiedzy na temat naszych wyrobów i sposobów ich wykorzystania. W każdym z krajów Europy, a także na innych rynkach mamy swoich trenerów prowadzących intensywną działalność szkoleniową. Większą część naszego budżetu marketingowego przeznaczamy na szkolenia. Staramy się przełamać opory projektantów i instalatorów systemów dozorowych wynikające z braku obycia z zagadnieniami sieciowymi. Program szkoleń w siedemdziesięciu pięciu procentach dotyczy ogólnej wiedzy na temat telewizji i sieci IP, a jedynie dwadzieścia pięć procent dotyczy konkretnych rozwiązań firmy Axis. Przewidujemy stworzenie w najbliższej przyszłości profesjonalnych ośrodków treningowych, gdzie uczestnicy szkoleń mogliby zdobywać wiedzę i doświadczenie, a na koniec zdawać egzaminy certyfikacyjne potwierdzające ich przygotowanie zawodowe. Podobnie organizują szkolenia inne wiodące firmy informatyczne.

To wszystko z naszej strony. Dziękujemy za interesujący wywiad. Wypada życzyć pomyślnej realizacji planów, o których mówiliśmy.

M.G.: Również dziękuję i zapraszam do dalszej współpracy z firmą Axis.

Bezpieczeństwo danych w nowoczesnej telemedycynie (część 1)

Marek Blim, Jerzy Mikulik

1. Wprowadzenie do telemedycyny

Telemedycyna – czyli medycyna „na odległość" – to najnowsza forma świadczenia usług medycznych i opieki zdrowotnej, łącząca w sobie elementy telekomunikacji, informatyki oraz medycyny. Wykorzystanie nowych technologii umożliwia przełamywanie geograficznych barier i wymianę specjalistycznych informacji. Przesyłanie najwyższej jakości zdjęć EKG, USG i MRI umożliwia dokonanie diagnozy w miejscu odległym od tego, w którym badano pacjenta (dotyczy głównie to radiologii, kardiologii i dermatologii). Telemedycyna jest wykorzystywana w chirurgii, podczas zabiegów – w celu tzw. robotyzacji zabiegu. Nowoczesna technologia, wykorzystująca szybkie procesory i algorytmy do cyfrowego przetwarzania i kompresji sygnałów, umożliwia przesyłanie obrazów o wysokiej rozdzielczości, a także interaktywną transmisję audiowizualną z wyjątkową dokładnością i w czasie rzeczywistym. Systemy wideokomunikacyjne (kodery wizyjne) pracują na ogólnodostępnych cyfrowych liniach transmisyjnych ISDN, w ogólnoświatowej sieci Internet, a także na liniach satelitarnych, w ramach celowo zestawionych, czasowo trwałych, łączy abonenckich o dobrych parametrach przesyłu pakietów danych medycznych.

Przykładowe zastosowania telemedycyny w życiu są skutkiem „kompresji odległości" między badanym a lekarzem (zachowanie „jedności miejsca i czasu badania") i obejmują:

– konsultacje specjalistyczne,
– badania,

– okresowe przeglądy,
– długotrwałe leczenie,
– monitorowanie pacjentów i wyników leczenia,
– asystowanie przy trudnych zabiegach chirurgicznych,
– medycyna powypadkowa,
– ratownictwo medyczne.

Konkretne zalety telemedycyny to przede wszystkim:
– ułatwienie mieszkańcom małych miast i wsi dostępu do specjalistycznej opieki medycznej,
– pomoc w specjalistycznych usługach i konsultacjach dla mniejszych ośrodków medycznych,
– polepszenie opieki zdrowotnej na odizolowanych lub odległych obszarach,
– szybka diagnoza i pomoc medyczna w ratownictwie,
– ułatwiony dostęp do pomocy medycznej w poważnych, nagłych przypadkach lub w trakcie katastrofy naturalnej,
– ograniczenie hospitalizacji i koniecznych dojazdów pacjentów,
– zmniejszone ogólne koszty leczenia i opieki zdrowotnej w kraju,
– zwiększone możliwości podnoszenia kwalifikacji personelu medycznego,
– oszczędności wynikające z usprawnień administracyjnych,
– ułatwienie prowadzenia badań naukowych, dotychczas wymagających czasochłonnych dojazdów oraz scalania danych rozproszonych po różnych jednostkach służby zdrowia,
– zmniejszenie barier komunikacyjnych pomiędzy ośrodkami służby zdrowia.

2. Specjalizacja informacji medycznej w obszarze e-zdrowia

Informacja medyczna jest obecnie podstawą komunikowania się w dziedzinie e-zdrowia (*e-health*). Chodzi o komunikowanie się lekarzy, aptekarzy, pielęgniarzy i laborantów z pacjentami, a także o komunikację systemową, tzn. wymianę danych tekstowych (diagnozy, opisy stanu/choroby, dane pacjenta itp.) lub graficznych (zdjęcia RTG i RMI, wykresy EKG i EEG itp.) w ramach urządzeń/systemów informatyki medycznej. Odpowiednie specjalistyczne zasoby słownikowe, czyli wybrany i zaakceptowany ogólnie zakres i format stosowanego nazewnictwa, tworzą obszar pojęć, na jakim opiera się taka wymiana informacji (osobowa i/lub systemowa) w danej dziedzinie telemedycyny.

W medycynie i ochronie zdrowia słownictwo pochodzi z medycyny, farmacji, epidemiologii i innych pokrewnych dziedzin, więc jest zrozumiałe tylko dla pewnej grupy ludzi. Na dodatek zdarza się, że osoby wywodzące się z różnych środowisk czy szkół medycznych posługują się różnymi terminami na określenie tych samych zjawisk lub określają tym samym terminem inne zjawiska. W celu wyeliminowania wynikających z tego nieporozumień i niespójności zaczęto tworzyć i katalogować słownictwo, przypisując poszczególnym terminom określone, z założenia jednoznaczne znaczenie. W ten sposób powstały zbiory terminów cechujące się w określoną logiką i strukturą, o cechach klasyfikacji, oraz takie, które tych cech nie posiadają. W przypadku opieki zdrowotnej w praktyce w użyciu są w szczególności klasyfikacje dotyczące:
– chorób i problemów zdrowotnych,
– procedur, w tym procedur chirurgicznych, diagnostycznych i innych,
– leków i materiałów medycznych, w tym sprzętu medycznego,
– jednostek opieki zdrowotnej,
– zawodów i specjalności medycznych.

Klasyfikacje i systemy kodowania są podstawową częścią składową rozwijanej w ostatnim piętnastoleciu informatyki medycznej. Są elementami metasystemu e-zdrowie, dla którego poszczególne normy i standardy są określone przez zapisy normalizacyjnych organizacji międzynarodowych (ISO), regionalnych (CEN) i krajowych (ANSI, AFNOR, BSI, DIN, PKN i in.). Opierając się na wiedzy medycznej obejmują nie tylko systemy pojęć, ale także przyjęte, umowne formy dokumentacji chorób/pacjentów wraz z aplikacjami obsługującymi te dokumentacje.

Standaryzacja obejmuje także (na przykładzie USA[1]) klasyfikowanie chorób i problemów zdrowotnych (ICD-10), procedur chirurgicznych i innych procedur zabiegowych (ICD-9-CM, OPS-301), a także samych chorych/pacjentów (DRG). Zwieńczeniem tej piramidy standardów jest *Unified Medical Language System* (UMLS)[2] – metatezaurus łączący wiele różnych systemów kodowania i klasyfikacji, funkcjonujący pod egidą National Library of Medicine.

Istnieje wiele ośrodków, które wytworzyły i upowszechniły systemy kodowanego słownictwa dla różnych celów w ochronie zdrowia. Charakteryzując systemy kodowania w ochronie zdrowia, należy wskazać cechę związaną z zasięgiem terytorialnym ich oddziaływania.

Lokalne systemy i klasyfikacje (quasi-standardy) są tworzone z myślą o konkretnym odbiorcy informacji w danym kraju. Bardzo często są one narzędziem służącym do dokonywania rozliczeń finansowych i (jako takie) powstały z inspiracji płatników usług medycznych, np.:
– CPT – *Current Procedural Terminology*[3] – klasyfikacja procedur medycznych stworzona przez American Medical Association, mająca na celu dostarczanie informacji na temat świadczeń zrealizowanych na rzecz pacjenta; odbiorcami tych informacji są głównie płatnicy usług zdrowotnych, np. firmy i fundusze ubezpieczeń zdrowotnych;
– *International Classification of Diseases – 9th Revision – Clinical Modification* – Procedures[4] – klasyfikacja

1) za: Josef Ingenerf, Medizinische Universität zu Lübeck (MUL), Institut für Medizinische Informatik (IMI), http://www.medinf.mu-luebeck.de.

2) National Library of Medicine, http://www.nlm.nih.gov/research/umls/.

3) Physicians' Current Procedural Terminology, AMA, 4th ed., 2003.

4) International Classification of Diseases – 9th Revision – Clinical Modification – Procedures, St. Anthony Publishing Inc, Virginia, USA, 1991.

utworzona w USA (mimo iż jest nazwana międzynarodową), na zlecenie Health Care Financing Administration, z myślą o rozliczaniu procedur chirurgicznych w USA;
– *Read Codes*[5] – system stworzony w Center for Coding and Classification na potrzeby National Health Service w Wielkiej Brytanii;
– *Internationale Klassifikation der Prozeduren in der Medizin*[6] – niemiecka klasyfikacja procedur służąca rozliczeniom Kas Chorych.

Systemy i klasyfikacje międzynarodowe są tworzone przez międzynarodowe gremia, często związane ze Światową Organizacją Zdrowia, których głównym zadaniem jest ujednolicenie terminologii odnoszącej się do zjawisk, które mają być porównywane w skali międzynarodowej. Przykłady takich klasyfikacji:
– ICD-9, ICD-10 – *International Classification of Diseases and Health Related Problems*[7] – podstawowa klasyfikacja, będąca standardem nazewnictwa i kodowania chorób, wydana przez Światową Organizację Zdrowia (WHO);
– ICPC – *International Classification for Primary Care*[8] – opracowana przez Światową Organizację Lekarzy Rodzinnych (WONCA) – umożliwia odnotowywanie zjawisk w celu określania stanu zdrowia populacji i potrzeb zdrowotnych oraz oceny jakości usług medycznych w opiece podstawowej;
– ICHA – *International Classification for Health Accounts*[9] – opracowana pod patronatem Organizacji Współpracy Gospodarczej i Rozwoju (OECD), we współpracy z WHO i Eurostatem, dla celów klasyfikowania wydatków na ochronę zdrowia.

Wiele z systemów stworzonych lokalnie i na potrzeby konkretnych odbiorców z biegiem czasu umiędzynarodowiło się i stanowi obecnie nieformalny standard światowy. Przykładem może być ECRI (Nomenklatura Urządzeń Medycznych) czy zdobywające coraz więcej użytkowników ICD-9-CM-Procedures.

Pamiętajmy, że opisane powyżej systemy kodowania nie zapewniają bezpieczeństwa informacji medycznej, a jedynie ujednolicają jej rozumienie i wykorzystanie.

2.1. Dane medyczne pacjenta w lecznictwie zamkniętym

Obecnie informatyka medyczna w ramach lecznictwa zamkniętego posiłkuje się dwoma przyjętymi standardami:
– HL7 v.3.0 – jako standardem wymiany wiadomości tekstowych (ISO/HL7 21731:2006) współpracującym ze standardem UN/EDIFACT (ISO 9735:1987);
– DICOM – jako standardem wymiany obrazów medycznych.

2.1.1. Standard HL7

Health Level Seven International (HL7) to nazwa powstałej w 1987 roku w USA (Michigan) organizacji zajmującej się

5) NHS Information Authority, http://www.nhsia.nhs.uk/terms/pages/default.asp (stan z dnia 13.08.2003).

6) Internationale Klassifikation der Prozeduren in der Medizin, Deutschen Institut für Medizinische Dokumentation und Information, Berlin 2000.

7) International Classification of Diseases and Health Related Problems – 10th Revision, Volume I–III, WHO Geneva, 1992.

8) International Classification for Primary Care, WONCA.

9) System of Health Accounts, OECD, Paris, France, 2000.

rozwojem interoperacyjności w zakresie wymiany informacji szpitalnej. Jest to organizacja akredytowana przez ANSI, co daje jej pełne prawo do stanowienia standardów. Polem działania HL7 jest przetwarzanie danych klinicznych oraz administracyjnych.

Zgodnie ze statutem organizacji jej celem jest „zapewnienie standardów wymiany i integracji danych, które wspomagają opiekę kliniczną nad pacjentem oraz zarządzanie, dostarczanie i użytkowanie usług medycznych. W szczególności chodzi tutaj o stworzenie elastycznych i ekonomicznych podejść do różnych standardów, wytycznych, metodyk oraz powiązanych z nimi usług kooperujących, związanych z różnorodnymi systemami informacji wykorzystywanymi w służbie zdrowia".

HL7 v.1.0 został zaakceptowany przez ANSI jako standard 26 lipca 1999 roku. Obecnie standardem jest wersja 3.0, zaakceptowana przez ANSI w 2005 roku oraz przyjęta na drodze szybkiej akceptacji jako norma międzynarodowa ISO/HL7 21731:2006, a od kwietnia 2013 r. specyfikacja tego standardu jest dostępna bezpłatnie pod adresem *www.hl7.org* (łącznie 15 rozdziałów i 4 dodatki). Definiując jedynie model/moduł podstawowy tworzenia wiadomości wersja 3.0 umożliwia zapisywanie wiadomości w różnych popularnych formatach, takich jak np. XML czy popularne w medycynie EDIFACT i ER7. Również w Polsce przygotowano formaty dokumentów zgodnie z normą UN/EDIFACT (ISO 9735:1987) dla potrzeb ich elektronicznej wymiany (EDI[10]) pomiędzy placówką służby zdrowia (szpitalem) a NFZ-em (Karta Leczenia Szpitalnego – ZDR100 oraz ZDR200).

HL7 3.0 wprowadza szereg modeli jednostek i aktywności występujących w służbie zdrowia i na tej podstawie odwzorowuje je w postaci zapisywanej wiadomości. Podstawowym opracowanym przez HL7 modelem jest obiektowy model informacji w służbie zdrowia, określony jako referencyjny, o nazwie RIM (*Reference Information Model*). Model ten, poprzez zastosowanie języka modelowania obiektowego UML (*Uniform Modeling Language*), przedstawia 123 klasy obiektów, możliwe stany oraz relacje pomiędzy obiektami. Uproszczeniem tego modelu jest model informacyjny wiadomości MIM (*Message Information Model*) ujmujący te klasy, których obiekty są odwzorowywane.

Wraz z opracowywaniem nowego standardu wiadomości, modelu referencyjnego oraz typów dokumentów XML dla wiadomości organizacja HL7 postanowiła opracować architekturę elektronicznych kart pacjenta. Bazując na modelu referencyjnym RIM, opracowano szereg form dokumentów DTD oraz procedur ich wymiany. Przedsięwzięcie to nazwano PRA – *Patient Record Architecture*. Dokumenty PRA są implementacją XML, więc stanowią opracowania niezależne od urządzeń czy rozwiązań sprzętowo-programowych. Umożliwiają one przepływ wiadomości na temat pacjenta pomiędzy różnymi jednostkami organizacji medycznych, także z wykorzystaniem normy EDIFACT zintegrowanej z HL7.

Konstrukcja wiadomości jest tworzona na podstawie normy ISO 9735 (EDI) opisującej reguły składni. Podsumowując, można powiedzieć, że zastosowanie normy EDIFACT jest łatwe, niemniej przebrnięcie przez całą dokumentację jej opisu (ponad 2700 stron) stanowi poważną przeszkodę.

Ograniczenia normy EDIFACT, ze względu na uniwersalność jej zastosowania, uniemożliwiają przesyłanie różnych danych medycznych, na przykład obrazów czy sygnałów czynności elektrycznej. Dlatego norma EDIFACT przyjęła się w medycynie jako norma wykorzystywana w celach sprawozdawczych i administracyjnych (np. w relacji dostawca usług medycznych – ubezpieczyciel lub NFZ).

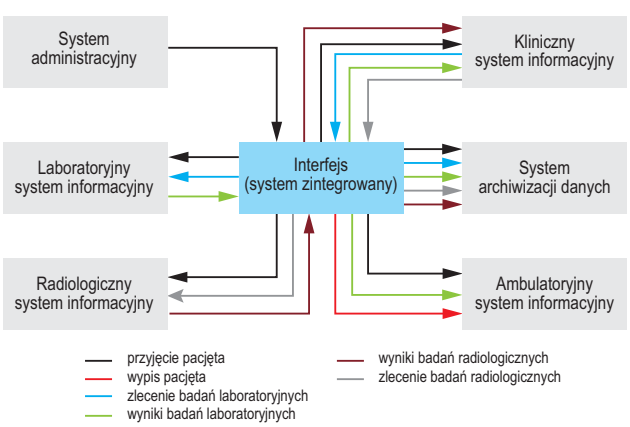
Należy zwrócić uwagę na fakt, że pliki HL7 oraz EDIFACT zawierają komplet danych tekstowych dotyczących pacjenta, więc mamy pełne podstawy do wymagania spełnienia warunków ochrony tych danych, co wiąże się nie tylko z bezpieczną identyfikacją użytkownika tych informacji (PN-EN 12251:2005P – *Informatyka medyczna – Bezpieczna identyfikacja użytkownika w ochronie zdrowia – Zarządzanie i bezpieczeństwo uwierzytelniania z użyciem haseł*), ale i z ochroną samych informacji (PN-ISO/IEC 17799:2007 – *Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji*; PN-ISO/IEC 27001:2007 – *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*; PN-EN ISI 27799:2010 – *Informatyka w ochronie zdrowia – zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002*).

2.1.2. DICOM

W informatycznych systemach medycznych oprócz danych tekstowych niejednokrotnie trzeba przesyłać dane graficzne, takie jak zdjęcia rentgenowskie czy zapisy badań USG. Z tego powodu opracowano standard DICOM. Twórcą tego standardu jest ACR/NEMA (American College of Radiology/National Electrical Manufacturers Association), a jego pierwsza wersja została opublikowana w roku 1993. Obecnie obowiązująca wersja standardu została zaakceptowana w roku 2004.

Standard DICOM definiuje obiekty informacji oraz zakresy usług (funkcje serwisów) dostępnych dla danych obiektów informacji. Określony jest szereg usług/funkcji, które pełnią role usługodawcy i usługobiorcy w danej klasie obiektów. Nowe obiekty są definiowane na bieżąco, w miarę pojawiania się na rynku medycznym nowych urządzeń diagnostycznych. Obiekty te są przypisywane do takich klas jak CT (*Computed Tomography* – tomografia komputerowa), MRI (*Magnetic Resonance Image* – obraz rezonansu magnetycznego) czy CR (*Computed Radiology* – radiologia komputerowa). Najważniejszą zaletą standardu DICOM jest integracja danych wizualnych z danymi medycznymi w pojedynczym pliku, więc istotne jest złożenie pliku/pakietu DICOM.

10) EDI (ang. „Electronic Data Interchange") – elektroniczna wymiana informacji.



Rys. 1. Model przepływu informacji wg UN/EDIFACT (ISO 9735:1987)

Pojedynczy plik standardu DICOM zawiera w sobie zarówno nagłówek (w którym zapisane są dane pacjenta, typ obrazu, jego wymiary itp.), jak również sam obraz, który może zawierać informacje w trzech wymiarach. Obraz przechowywany w pliku może być skompresowany z zastosowaniem kompresji stratnej (JPEG) lub bezstratnej (TIFF).

Należy zwrócić uwagę na fakt, że plik DICOM zawiera komplet danych tekstowych i obrazowych dotyczących pacjenta, więc mamy pełne podstawy do wymagania spełnienia warunków ochrony tych danych, co wiąże się z bezpieczną identyfikacją użytkownika tych informacji (PN-EN 12251:2005P – *Informatyka medyczna – Bezpieczna identyfikacja użytkownika w ochronie zdrowia – Zarządzanie i bezpieczeństwo uwierzytelniania z użyciem haseł*), jak i ochroną samych informacji (PN-ISO/IEC 17799:2007 – *Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji*; PN-ISO/IEC 27001:2007 – *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*; PN-EN ISI 27799:2010 – I*nformatyka w ochronie zdrowia – zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002*).

2.1.3. Zarządzanie bezpieczeństwem danych w lecznictwie zamkniętym

Dla administratorów zarządzających infrastrukturą informatyczną w lecznictwie zamkniętym (klinika, szpital, sanatorium itp.) istotnym zadaniem jest stworzenie polityki bezpieczeństwa, czyli utworzenie spójnego, precyzyjnego i zgodnego z obowiązującym prawem zbioru przepisów, reguł i procedur, zgodnie z którymi będą zbudowane, zarządzane i udostępniane zasoby projektu e-zdrowie.

Polityka bezpieczeństwa powinna też być zgodna z obowiązującymi normami, które obejmują takie zagadnienia jak:

– bezpieczeństwo przesyłania danych osobowych w opiece zdrowotnej,
– bezpieczne przesyłanie elektronicznego rekordu medycznego w sieciach IT,
– bezpieczna identyfikacja użytkownika danych w systemie ochrony zdrowia,
– bezpieczeństwo i uwierzytelnianie wszystkich udostępnianych danych dot. stanu zdrowia.

Podsumowanie części pierwszej

Sama znajomość norm dotyczących informatyki medycznej nie wystarczy do opracowania dobrej (zapewniającej odpowiedni poziom bezpieczeństwa) polityki bezpieczeństwa, ale bez ich znajomości nie jest możliwe wdrożenie właściwej polityki ochrony systemów medycznych i przetwarzanych w nich danych.

dr hab. inż. Jerzy Mikulik prof. nadzw. AGH
AGH Akademia Górniczo-Hutnicza
im. Stanisława Staszica w Krakowie

dr inż. Marek Blim

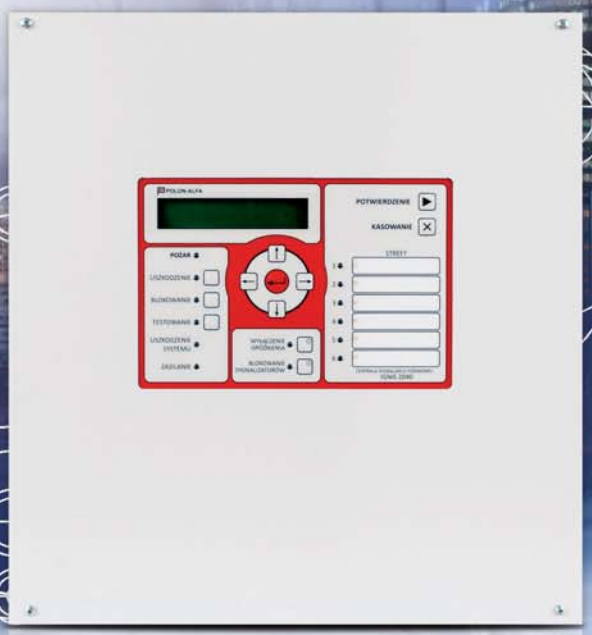
Bibliografia:

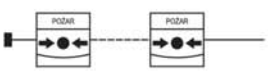
1. International Classification of Diseases – 9th Revision – Clinical Modification – Procedures, St. Anthony Publishing Inc, Virginia, USA, 1991.
2. International Classification of Diseases and Health Related Problems – 10th Revision, Volume I–III, WHO Geneva, 1992.
3. International Classification for Primary Care, WONCA, 1997.
4. Internationale Klassifikation der Prozeduren in der Medizin, Deutschen Institut für Medizinische Dokumentation und Information, Berlin 2000.
5. ISO 9735:1987, baza normatywna EDIFACT.
6. ISO/HL7 21731:2006, Informatyka medyczna. HL7 model referencyjny v.3.
7. Krzyminiewski R., *Projekt MONTE*, http://www.monte.amu.edu.pl.
8. Physicians' Current Procedural Terminology, AMA, 4th ed., 2003.
9. PN-EN 12251:2005P – I*nformatyka medyczna – Bezpieczna identyfikacja użytkownika w ochronie zdrowia – Zarządzanie i bezpieczeństwo uwierzytelniania z użyciem haseł.*
10. PN-EN 14484:2005 – *Informatyka medyczna – Międzynarodowy przekaz medycznych danych osobowych objętych dyrektywą UE dotyczącą ochrony danych – Wysoki poziom polityki bezpieczeństwa.*
11. PN-EN 14485:2005 – *Informatyka medyczna – Wskazania dla operowania medycznymi danymi osobowymi w międzynarodowych aplikacjach z uwzględnieniem dyrektywy UE dotyczącej ochrony danych.*
12. PN-EN ISO 13606-1:2013 – *Informatyka w ochronie zdrowia – Przesyłanie elektronicznej dokumentacji zdrowotnej – Część 1: Model referencyjny.*
13. PN-EN ISO 13606-4:2009 – *Informatyka w ochronie zdrowia – Przesyłanie elektronicznej dokumentacji zdrowotnej – Część 4: Bezpieczeństwo.*
14. PN-EN ISO 13606-5:2010 – *Informatyka w ochronie zdrowia – Przesyłanie elektronicznej dokumentacji zdrowotnej – Część 5: Specyfikacja interfejsu.*
15. PN-EN ISO/IEC 27799:2010 – *Informatyka w ochronie zdrowia – zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002.*
16. PN-ENV 13608-1:2003 – *Informatyka w ochronie zdrowia – Bezpieczeństwo przesyłanych danych w opiece zdrowotnej – Część 1: Pojęcia i terminologia.*
17. PN-ENV 13608-2:2003 – *Informatyka w ochronie zdrowia – Bezpieczeństwo przesyłanych danych w opiece zdrowotnej – Część 2: Bezpieczne obiekty danych.*
18. PN-ENV 13608-3:2003 – *Informatyka w ochronie zdrowia – Bezpieczeństwo przesyłanych danych w opiece zdrowotnej – Część 3: Bezpieczne kanały przesyłania danych.*
19. PN-ISO/IEC 17799:2007 – *Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji.*
20. PN-ISO/IEC 27001:2007 – *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.*
21. Rozporządzenie Ministra Zdrowia z dnia 28 marca 2013 r. w sprawie wymagań dla Systemu Informacji Medycznej, Dz. U. z 2013 r., poz. 463.
22. System of Health Accounts, OECD, Paris, France, 2000.
23. Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, Dz. U. z 2011 r., nr 113, poz. 657 z późn. zm.

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

IGNIS 2040

OCHRONA PRZECIWPOŻAROWA MAŁYCH OBIEKTÓW



WEJŚCIA	IGNIS 2040	WYJŚCIA
 do 32 czujek punktowych		→ przekaźniki alarmu i uszkodzenia
 do 10 ręcznych ostrzegaczy pożarowych		→ zasilanie urządzeń zewnętrznych (24 V)
 czujka liniowa		→ linie sterujące sygnalizatorami
 czujki iskrobezpieczne	• od 4 do 6 linii dozorowych • 2 linie sterujące sygnalizatorami (zamiennie z liniami dozorowymi) • 5 lat gwarancji	→ odczyt pamięci zdarzeń

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.

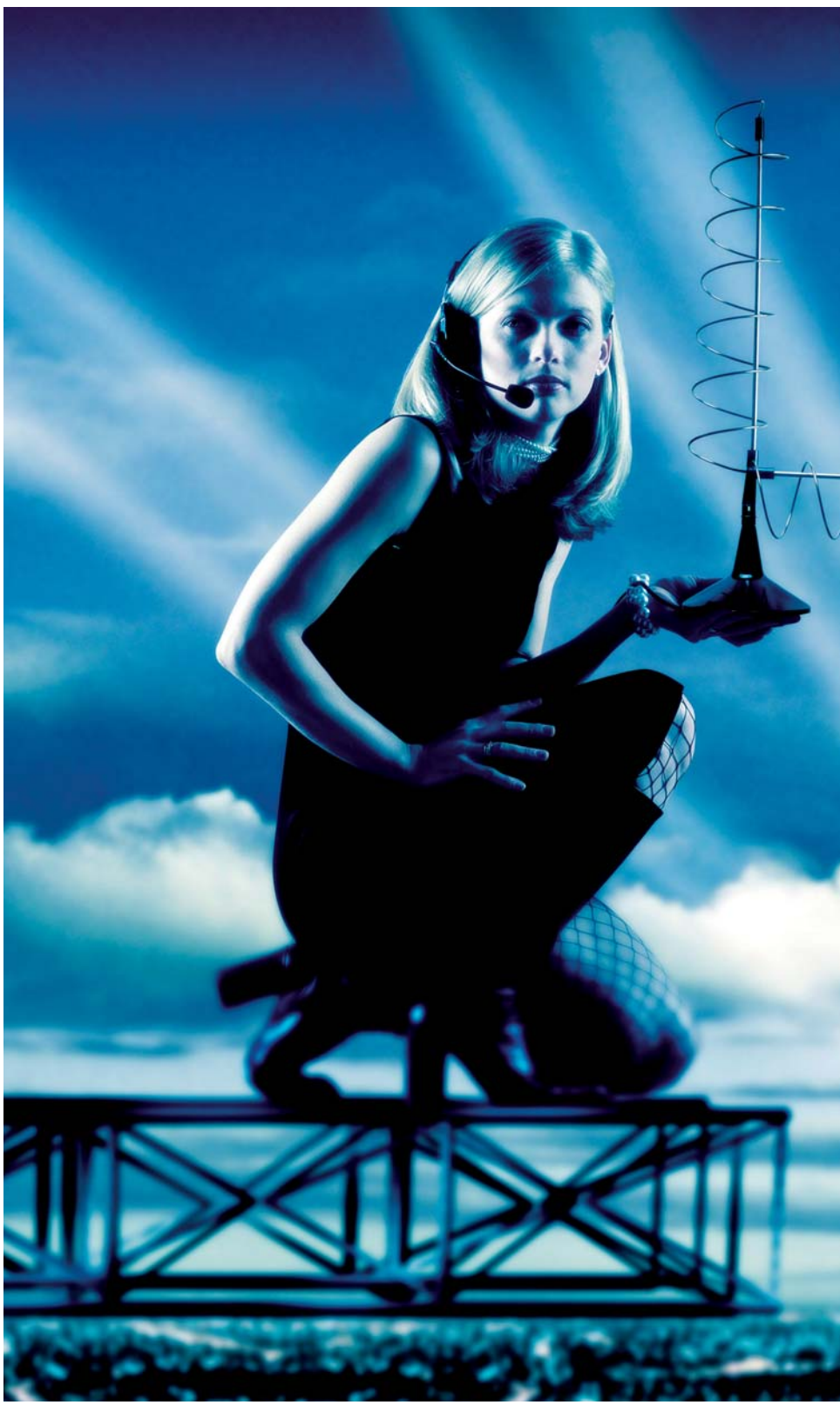
85-861 Bydgoszcz, ul. Glinki 155, www.polon-alfa.pl

Radiokomunikacja cyfrowa w służbach ochrony i ratownictwa (część 1)

Zarys zagadnień teoretycznych

Andrzej Walczyk

W ostatnich latach mamy do czynienia z szybkim rozwojem systemów alarmowych oraz wizyjnych systemów dozorowych, jednakże nawet najdoskonalsze z nich nie są w stanie podwyższyć poziomu bezpieczeństwa na chronionych obszarach bez udziału ludzi



Telefonia komórkowa – iluzja niezawodnej łączności

Użytkownikami profesjonalnych środków łączności są służby mundurowe, prawnie zobligowane do budowy własnych sieci radiokomunikacyjnych, jednakże, ze względu na swój specyficzny charakter, nie dzielą się one doświadczeniami ze służbami cywilnymi. Tymczasem firmy zajmujące się fizyczną ochroną obiektów cywilnych wykorzystują do komunikacji najczęściej telefony komórkowe.

Ta z pozoru prosta metoda komunikacji ma tę zaletę, że jest tania, jednak ma także poważne wady. Proces zestawiania połączeń głosowych jest czasochłonny, gdyż wymaga wybierania numerów konkretnych abonentów. Nie ma funkcji wywołania grupowego, więc trudno jednocześnie wydawać polecenia wielu osobom. Często zdarza się, że sieć komórkowa jest przeciążona i w ogóle nie można nawiązać żadnego połączenia – na przykład w noc sylwestrową, gdy wiele osób jednocześnie próbuje wysłać życzenia noworoczne do swoich znajomych. Na dodatek stacje przemiennikowe telefonii komórkowej są wyłączane w przypadku jakiegokolwiek podejrzenia o atak terrorystyczny, by nie można było tą drogą odpalić ładunków wybuchowych. W przypadku klęsk żywiołowych infrastruktura odpowiedzialna za działanie telefonii komórkowej ulega szybkiemu zniszczeniu. Tak więc telefonia komórkowa nie zapewnia niezawodnej łączności i może zawieść w krytycznych sytuacjach.

Najtańsze rozwiązanie – radiotelefony PMR

W handlu dostępne są tanie radiotelefony ręczne, przeznaczone do prywatnego użytku, jednak mają one zbyt mały zasięg, by mogły znaleźć profesjonalne zastosowanie w służbach ochrony czy ratownictwie. Te radiotelefony należą do kategorii PMR. Skrót jest zapożyczony z języka angielskiego i pochodzi od słów *Private Mobile Radio.*

Dla użytkowników radiotelefonów PMR wydzielony został specjalny zakres częstotliwości w paśmie 446 MHz, z którego korzystanie nie wymaga żadnych zezwoleń. Radiotelefony PMR mają tylko osiem kanałów a chętnych do prowadzenia rozmów jest wielu, co oznacza, że panuje spory tłok w eterze.

Radiotelefony PMR są chętnie wykorzystywane przez firmy budowlane do łączności z operatorami dźwigów. Gdy znajdują się na wysokich dźwigach, mają duży zasięg, ale dla ich użytkowników nie ma to znaczenia – większy zasięg sprzyja jedynie zwiększeniu poziomu zakłóceń na dużym obszarze.

Wszystkie te czynniki wykluczają możliwość stosowania radiotelefonów PMR w profesjonalnych sieciach łączności radiowej.

Rozwiązania profesjonalne – radiotelefony DMR

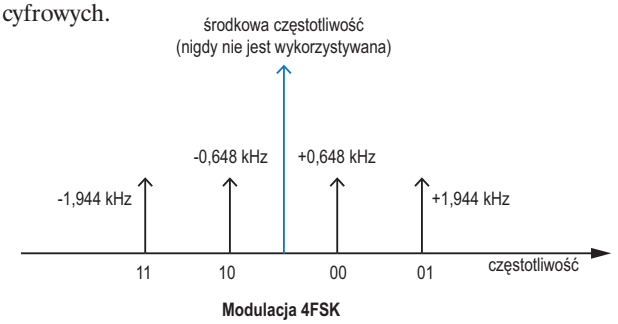
Z myślą o użytkownikach profesjonalnych systemów łączności radiowej stworzony został standard DMR. Skrót jest zapożyczony z języka angielskiego i pochodzi od słów *Digital Mobile Radio*. DMR jest otwartym standardem, opracowanym i zatwierdzonym przez Europejski Instytut Norm Telekomunikacyjnych. Tak więc wszystkie urządzenia DMR są wzajemnie kompatybilne i mogą ze sobą współpracować.

Standard DMR został opracowany z myślą o dotychczasowych użytkownikach analogowych systemów łączności, to znaczy o tych wszystkich osobach i instytucjach, które już kiedyś wystąpiły o przydział częstotliwości i uzyskały zezwolenia na korzystanie z określonych kanałów radiokomunikacyjnych. Podstawowe parametry urządzeń DMR, takie jak odstęp międzykanałowy, szerokość zajmowanego pasma, moc nadajnika, są zgodne z tymi samymi parametrami urządzeń analogowych. Dlatego zastępowanie starszych, analogowych systemów radiokomunikacyjnych współczesnymi, cyfrowymi systemami DMR nie wymaga ponownego ubiegania się o przydziały częstotliwości i uzyskiwania zezwolenia na ich użytkowanie.

Najistotniejsze cechy urządzeń DMR – modulacja cyfrowa ze zwielokrotnieniem w dziedzinie czasu

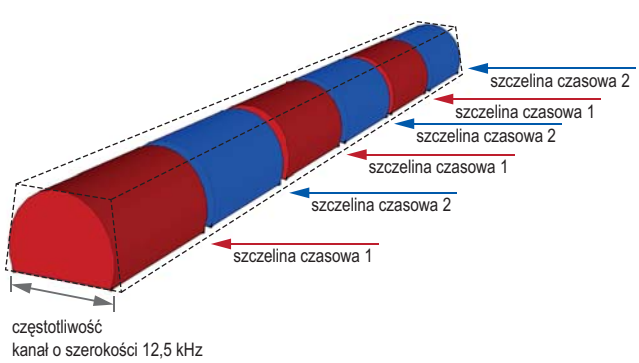
Jedną z cech urządzeń DMR, odróżniających je od stosowanych dotychczas urządzeń analogowych, jest czterowartościowa, cyfrowa modulacja częstotliwości ze zwielokrotnieniem w dziedzinie czasu. Te dziwnie brzmiące określenia mogą być obce dla wielu osób i dlatego zostaną wyjaśnione.

Czterowartościowa, cyfrowa modulacja częstotliwości jest w literaturze określana jako 4FSK. W istocie jest to zwykła modulacja FM, tyle że częstotliwość nośna nadajnika nie może się dowolnie zmieniać, lecz przyjmuje jedną z czterech ściśle określonych wartości. Tym wartościom są przyporządkowane dwubitowe symbole, które można traktować jak litery jakiegoś alfabetu. Czyli w systemie radiokomunikacyjnym z modulacją 4FSK operuje się czterema symbolami, które jak litery można układać w ciągi, dzięki czemu możliwa jest transmisja danych cyfrowych.



Modulacja 4FSK

Drugi z wymienionych terminów, czyli zwielokrotnienie w dziedzinie czasu, oznacza, że w tym samym kanale radiowym mogą być jednocześnie nawiązane dwa niezależne połączenia głosowe, lub mogą być jednocześnie przekazywane informacje głosowe i dane cyfrowe. Zwielokrotnienie w dziedzinie czasu jest określane w literaturze jako TDMA. Skrót pochodzi od słów *Time Division Multiple Access*. Zastosowanie TDMA oznacza, że radiotelefon na przemian nadaje i odbiera dane cyfrowe. Dzieje się to na tyle szybko, że użytkownik nie zdaje sobie z tego sprawy, jednak w systemie radiokomunikacyjnym zachodzi cykliczne przełączanie z nadawania na odbiór i z odbioru na nadawanie. Poszczególne interwały czasowe, w których odbywa się nadawanie i odbiór, są w literaturze określane jako szczeliny czasowe. W każdej ze szczelin czasowych można transmitować inne informacje i właśnie na tym polega zwielokrotnienie w dziedzinie czasu.



Najistotniejsze cechy urządzeń DMR – zastosowanie wokodera

Można powiedzieć, że w analogowym systemie radiokomunikacyjnym dźwięk jest przekazywany w swojej klasycznej, niezakodowanej postaci. Fala nośna emitowana przez nadajnik jest zmodulowana dźwiękiem, czyli *de facto* przenosi ten dźwięk bez jakiejkolwiek modyfikacji. W cyfrowym systemie radiokomunikacyjnym transmitowane są informacje na temat dźwięku, a nie sam dźwięk. Za przekształcenie dźwięku z postaci analogowej na postać cyfrową, czyli za wytworzenie informacji o dźwięku, odpowiada wokoder.

Wokoder został wynaleziony kilkadziesiąt lat temu i początkowo stanowił niezależne urządzenie elektroniczne. Rozwój technologii półprzewodników pozwolił na miniaturyzację wokodera i jego zamknięcie w pojedynczym układzie scalonym, przy czym zasada działania nie uległa zmianie.

Podstawową i najważniejszą częścią składową wokodera stosowanego w radiotelefonach DMR jest dwuwymiarowa matryca o rozmiarach około 30×30 elementów, czyli, mówiąc językiem matematyki, macierz zawierająca około 1000 pozycji. W każdej z tych pozycji jest zapisany określony dźwięk stanowiący fragment mowy ludzkiej. Innymi słowy jest to zbiór elementów fonetycznych, bardziej przypominających szelesty, trzaski czy piski niż jakiekolwiek artykułowane dźwięki, jednak przez odpowiednie uszeregowanie tych elementów można syntetycznie stworzyć głos ludzki o brzmieniu zbliżonym do naturalnego.

Zasada transmisji dźwięku w radiotelefonach DMR polega na analizie sygnału akustycznego dostarczanego przez mikrofon, na podziale tego sygnału na elementarne fragmenty odpowiedzialne za poszczególne dźwięki i na wyszukiwaniu takich elementów fonetycznych w jego matrycy, które są podobne do tych dźwięków. Tak więc w wokoderze sygnał akustyczny wytwarzany przez mikrofon zostaje zamieniony na ciąg liczb określających położenia wybranych elementów fonetycznych w matrycy wokodera. Ten ciąg liczb jest przekazywany do nadajnika, gdzie z użyciem modulacji 4FSK jest wysyłany w eter.

W odbiorniku następuje odwrotny proces. Odebrany ciąg liczb wskazuje na wybrane elementy w tablicy wokodera, które są pobierane, ustawiane kolejno jeden za drugim i w procesie syntezy łączone w jedną całość. W ten sposób na wyjściu wokodera odbiorczego uzyskuje się sygnał akustyczny bardzo zbliżony do tego, który występował w nadajniku na wyjściu mikrofonu.

Jaka korzyść wynika z tak skomplikowanego procesu transmisji dźwięku? Chodzi o to, że ilość informacji niezbędnych do wskazywania wybranych elementów w matrycy wokodera jest znacznie mniejsza niż ilość informacji, jaka byłaby niezbędna do przekazania właściwego dźwięku. Cały ten proces można porównać do posługiwania się szyfrem książkowym, gdy dwie korespondujące osoby zaopatrzone w egzemplarze tej samej książki nie przekazują sobie całych wyrazów, a jedynie odpowiednie numery stron i numery wyrazów. Osoba, która otrzymała tak zakodowany list, jest w stanie po kolei odtworzyć wszystkie wyrazy, czyli jest w stanie odczytać przekazywaną informację. Ciąg liczb zapisany w liście zajmuje o wiele mniejszą przestrzeń niż zajęłyby właściwe wyrazy, więc można mówić o silnej kompresji przekazywanych informacji.

Na tym kończy się zarys zagadnień teoretycznych związanych z transmisją dźwięku w radiotelefonach DMR. W drugiej części zostaną omówione zagadnienia praktyczne związane z budową cyfrowych systemów radiokomunikacyjnych.

Andrzej Walczyk

Światło i dźwięk
dla bezpieczeństwa

Sygnalizatory wewnętrzne do sygnalizacji Pożaru
z dokumentami CNBOP-PIB

SO-Pd13 sygnalizator optyczny

- optyka - diody led
- < 38 mA@24V DC
- zgodny z PN-EN 54-23: 2010

SA-K7N sygnalizator akustyczno - optyczny

- 16 wzorów syreny
- regulacja natężenia dźwięku
- część optyczna zgodna z PN-EN 54-23:2010

SA-K5N sygnalizator akustyczny

- 4 wzory syreny
- < 20 mA@24V DC
- regulacja natężenia dźwięku
- zgodny z PN-EN 54-3:2003/A2:2007

www.w2.com.pl

W2 Włodzimierz Wyrzykowski - ul. Czajcza 6, 86-005 Białe Błota, NIP: 953-180-16-19, tel./fax (+4852) 584 01 92, tel. (+4852) 345 45 00, biuro@w2.com.pl

Firmy Samsung i Securitec Systems tworzą wysokiej jakości wizyjny system dozorowy w sortowniach APC Overnight

Samsung Techwin Europe

Securitec Systems utrzymuje partnerskie kontakty z działem profesjonalnych zabezpieczeń w firmie Samsung Techwin. Ta współpraca zaowocowała stworzeniem sieciowego systemu dozorowego w nowo budowanej sortowni APC Overnight w Cannock

Fot. 1. Sortownia APC Overnight w Cannock

Jeszcze niewiele lat temu jedynym celem stosowania wizyjnych systemów dozorowych w sortowniach i centrach dystrybucyjnych było odstraszanie potencjalnych złodziei i przeciwdziałanie kradzieżom przesyłek. Mimo to, nawet w przypadku właściwej lokalizacji oraz poprawnej regulacji kamer analogowych, jakość obrazów uzyskiwanych tradycyjnymi metodami była niewystarczająca do rzetelnej oceny sytuacji w obiekcie, a z całą pewnością nie pozwalała na identyfikację osób podejrzanych o udział w niedozwolonych działaniach. W tamtym okresie od kamer zainstalowanych w sortowniach i centrach dystrybucyjnych nie oczekiwano niczego więcej.

Fot. 2. Kamera SND-5061

Wraz z pojawieniem się tanich kamer megapikselowych oraz dzięki możliwości sterowania tymi kamerami za pośrednictwem sieci IP zwiększył się zakres zastosowań wizyjnych systemów dozorowych. Najlepszym przykładem może być nowa sortownia APC Overnight wybudowana w Cannock w West Midlands. Sieciowy system dozorowy dostarczony przez firmę Samsung nie tylko odstrasza potencjalnych złodziei paczek, lecz także stanowi użyteczne narzędzie usprawniające pracę pracowników sortowni, przez których ręce przechodzi miesięcznie półtora miliona przesyłek. Ponadto system dozorowy umożliwia sprawdzanie, czy w sortowni przestrzega się zasad bezpieczeństwa.

APC Overnight jest największą brytyjską siecią kurierską dostarczającą paczki w trybie jednodniowym, w skład której wchodzi 115 lokalnych sortowni. Ostatnio firma zainwestowała 16,5 milionów funtów w budowę nowego centrum dystrybucyjnego o powierzchni 138 000 stóp kwadratowych, zlokalizowanego w Cannock. Zastosowanie najnowszych rozwiązań technologicznych zostało wymuszone przez ciągle rosnące wymagania rynkowe i przez konieczność utrzymania wysokiego poziomu usług kurierskich.

W projekcie nowego centrum dystrybucyjnego APC Overnight przewidziano możliwość pełnego wykorzystania zalet kamer megapikselowych wytwarzających czytelne obrazy o bardzo wysokiej jakości. Kamery zostały umieszczone w punktach, w których wymagane jest uzyskiwanie obrazów o jakości dowodowej, takich jak miejsca przeładunku paczek przenoszonych przez taśmociągi czy rampy wyładowcze. Wykorzystanie obiektywów zmiennoogniskowych umożliwia powiększanie wybranych fragmentów obrazów obserwowanych miejsc w celu dokładnej oceny przeprowadzanych tam operacji.

– Jedną z podstawowych korzyści wynikających z zastosowania sieciowych systemów dozorowych jest możliwość sterowania kamerami oraz obserwacji obrazów w dowolnym miejscu, w którym jest dostęp do sieci – powiedział Colin Dicken, dyrektor do spraw bezpieczeństwa w firmie APC Overnight. – *Oznacza to, że możliwość obserwacji na bieżąco obrazów z kamer oraz obrazów zapisanych w jednostkach pamięciowych systemu ma nie tylko personel pracujący na terenie obiektu, lecz także wszyscy moi współpracownicy, którzy mają dostęp do zasobów systemu za pośrednictwem komputerów PC, laptopów, a nawet smartfonów i innych urządzeń przenośnych. Mogą oni nadzorować prace przeładunkowe nawet wtedy, gdy przebywają z dala od obiektu.*

APC Overnight przykłada wagę do możliwości śledzenia poszczególnych przesyłek, które przechodzą przez sortownię w Cannock. – *Troszczymy się o powierzone nam przesyłki. Dbamy o to, by dotarły one do odbiorców w stanie nienaruszonym i we właściwym czasie* – powiedział Colin Dicken. – *Dlatego bardzo ważna jest możliwość identyfikacji każdej z paczek przechodzących przez naszą sortownię. Osiągamy ją dzięki powiązaniu wizyjnego systemu dozorowego z naszym wewnętrznym systemem odczytu kodów paskowych. Reklamacje dotyczące zaginięcia lub uszkodzenia paczek mogą być łatwo przeanalizowane. Dostarczone przez firmę Samsung kamery o wysokiej rozdzielczości odgrywają istotną rolę w tym procesie, gdyż umożliwiają zgromadzenie materiału, z którego jasno wynika, jak troskliwie obchodzimy się z przesyłkami od momentu, w którym przekroczą one granicę sortowni w Cannock.*

Fot. 3. Colin Dicken

Na terenie sortowni w Cannock zainstalowano w sumie 124 kamery Samsung. Dokonała tego firma Securitec Systems, która jest certyfikowanym partnerem Samsunga, w ramach kontraktu na projekt i instalację wizyjnego systemu dozorowego. Kamery zostały rozmieszczone w taki sposób, by zarówno na terenie sortowni, jak i w jej najbliższym otoczeniu nie występowały martwe pola nie objęte obserwacją. – *Jak zwykle w przypadku tego rodzaju inwestycji bardzo istotne są etapy badań wstępnych i projektowania instalacji* – powiedział Martin Kadir, pracownik firmy Securitec Systems. – *Przed podjęciem decyzji dotyczącej wyboru rodzaju i liczby kamer poświęciliśmy wiele czasu na zbadanie obiektu. Musieliśmy przewidzieć, jakie funkcje będą pełnić kamery zainstalowane w poszczególnych punktach oraz na jakie warunki oświetleniowe i środowiskowe natrafią te kamery. Należy pamiętać, że część z nich obserwuje tereny wokół sortowni.*

61 spośród wszystkich zainstalowanych kamer należy do serii Samsung LiteNet, z czego 36 to kamery kopułkowe typu SND-7061 o rozdzielczości 3 megapiksele, przy czym mogą one pracować w standardzie Full HD. Kolejnych 25 kamer to modele kopułkowe SND-5061 o rozdzielczości 1.3 megapiksela. Wszystkie z wymienionych kamer mają obiektywy o ogniskowej regulowanej w zakresie od 3 mm do 8 mm i mogą być zasilane metodą PoE. Mają one także typowe funkcje maskowania stref prywatności, detekcji ruchu, detekcji sabotażu oraz automatycznej zmiany trybu pracy z kolorowego na monochromatyczny i odwrotnie, w zależności od zmieniających się warunków oświetleniowych. Wszystkie modele są zgodne ze specyfikacją ONVIF i wykorzystują metody kompresji obrazu H.264 i MJPEG, dzięki czemu możliwa jest jednoczesna transmisja obrazów różniących się poklatkowością i kompresją do różnych lokalizacji.

Do grupy pozostałych 124 kamer należą zarówno kamery stacjonarne, jak i szybkoobrotowe kamery kopułowe PTZ. Parametry każdej z nich zostały odpowiednio dobrane do specyfiki miejsca instalacji i do wymagań użytkowych stawianych przez APC Overnight. Do zapisu obrazów ze wszystkich kamer wykorzystywane są rejestratory sieciowe Samsung, które mogą być obsługiwane za pomocą darmowego oprogramowania Samsung Security Manager. Operatorzy systemu mogą przeglądać zarówno bieżące obrazy z kamer, jak i obrazy archiwalne.

Samsung Techwin Europe, Poland
e-mail: marcin.kucharski@samsung.com
tel.: +48 222 050 777
http://www.samsung-security.pl

20th MOSCOW INTERNATIONAL PROTECTION & SECURITY EXHIBITION & CONFERENCE

ufi Approved Event

Mips MOSCOW

14–17 APRIL 2014

PAVILION 75, VVC, MOSCOW

It's our 20th birthday!

CCTV & Surveillance

Security Technologies & Solutions

Perimeter protection systems. Fencing.

Fire safety. Rescue equipment. Safety at work

Smart Cards

Organiser:

ITE

Martyna Michalska

T: +48 61 6627244

F: +48 61 6627246

E: michalska@ite-poland.com

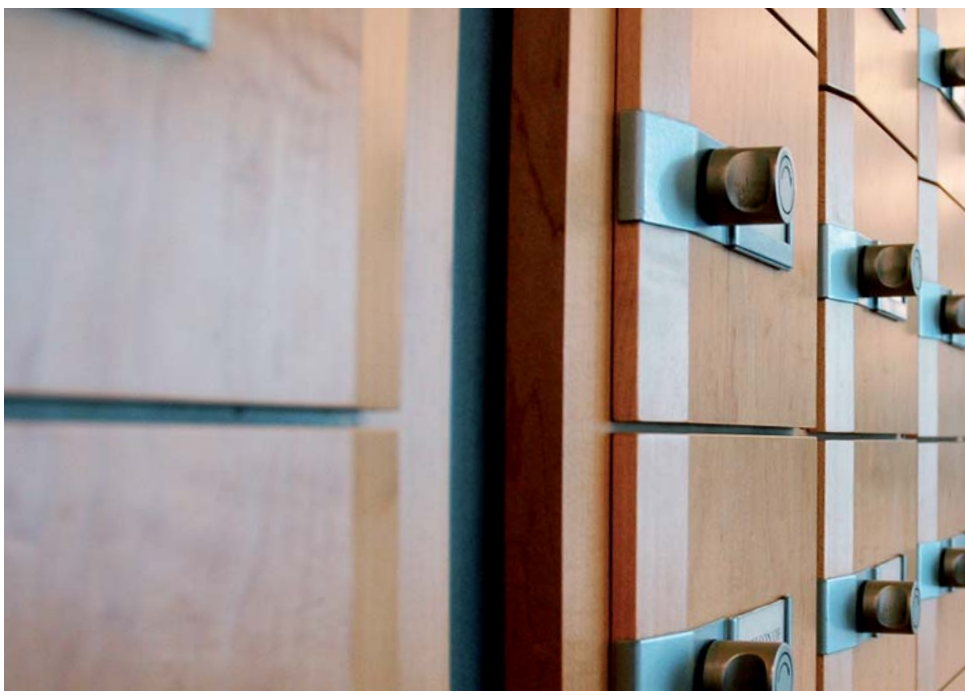
Supported by:

Ministry of the Interior of the Russian Federation

www.mips.ru

Większe możliwości dzięki centrali
INTEGRA 256 Plus

Michał Konarski



Stosowanie systemów sygnalizacji włamania i napadu w obiektach użyteczności publicznej jest w wielu przypadkach narzucone przez przepisy. Dotyczą one głównie tych obiektów, w których ryzyko związane z włamaniem jest szczególnie wysokie, lub takich, w których straty wynikające z kradzieży wartościowych przedmiotów, czy z nieuprawnionego dostępu do informacji niejawnych byłyby szczególnie dotkliwe. Przepisy te regulują sposoby zabezpieczania takich obiektów jak banki, kancelarie tajne, mennice czy muzea

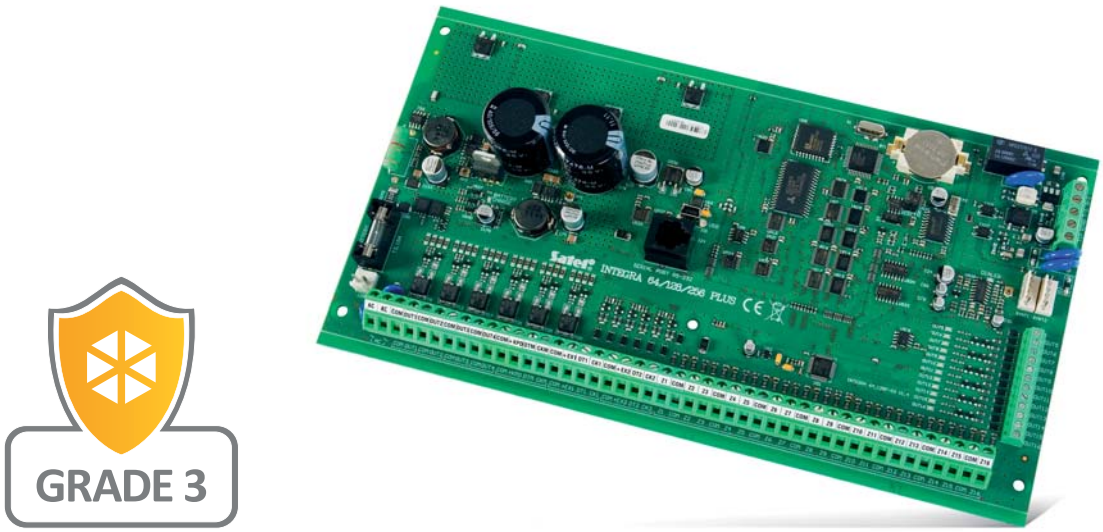
Jakość systemów zabezpieczających ważne obiekty, a także klasa urządzeń wchodzących w skład tych systemów jest regulowana normami branżowymi. W przypadku systemów sygnalizacji włamania i napadu najbardziej aktualne są europejskie normy serii EN50131, które wprowadzają spójną klasyfikację systemów i urządzeń. Jest ona czterostopniowa – od stopnia 1 (*Grade 1*), w przypadku obiektów najniższego ryzyka, aż po stopień 4 (*Grade 4*), którym oznacza się obiekty najwyższego ryzyka. W praktyce systemy odpowiadające stopniom 1 i 4 spotykane są rzadko. Większość odpowiada stopniowi 2 (systemy niezaawansowane) oraz stopniowi 3 (systemy zaawansowane).

Odpowiedzią firmy SATEL na rosnące zapotrzebowanie na urządzenia, które mogą być stosowane w systemach podwyższonego ryzyka, było wprowadzenie central rodziny INTEGRA Plus zaliczanych do stopnia 3 według normy EN50131.

Nowością w rodzinie INTEGRA Plus jest centrala INTEGRA 256 Plus. Umożliwia ona stworzenie systemu, w którym pracuje maksymalnie 256 czujek, a więc dwa razy więcej niż w przypadku starszych modeli central. Jest to istotne w przypadkach tworzenia rozległych systemów alarmowych w średnich i dużych obiektach, które wymagają kompleksowego zabezpieczenia.

Konstrukcja wszystkich central INTEGRA Plus wywodzi się ze sprawdzonych i uznanych central INTEGRA, jednak nowe urządzenia wyraźnie różnią się od poprzednich. Przede wszystkim zasilacz stosowany w centralach INTEGRA Plus został dostosowany do rygorystycznych wymagań dotyczących urządzeń stopnia 3 – zastosowano niezależne obwody służące do zasilania urządzeń oraz ładowania akumulatora, a także wprowadzono wiele wymaganych zabezpieczeń. Centrale serii INTEGRA Plus obsługują linie wejściowe w konfiguracji 3EOL, dzięki czemu sygnały naruszenia, sabotażu i maskowania czujek mogą być przekazane do centrali za pomocą jednej pary przewodów. Wprowadzono również udogodnienia dla instalatora, m.in. możliwość połączenia centrali z komputerem za pomocą kabla USB czy nowe funkcje programowe.

Dużą zaletą systemów bazujących na centralach z serii INTEGRA Plus jest ich modułowa budowa. Oznacza to,



Fot. 1. Dzięki spełnieniu wymagań zawartych w EN50131 (stopień 3) centrale serii INTEGRA Plus doskonale sprawdzą się w zaawansowanych systemach zabezpieczających obiekty szczególnie zagrożone włamaniem, np. banki, sklepy jubilerskie czy budynki użyteczności publicznej. Centrale te mają wiele funkcji, więc można stosować je również w systemach kontroli dostępu, a nawet w inteligentnych budynkach

że w skład systemu, oprócz samej centrali, wchodzi szereg podzespołów, które umożliwiają dostosowanie działania urządzeń peryferyjnych do aktualnych potrzeb. Modułowość central pozwala na rozbudowę systemu, jeżeli w przyszłości pojawi się taka potrzeba, bez konieczności wymiany wielu urządzeń.

Centrale INTEGRA Plus mają wszechstronne zastosowanie. Mogą służyć zarówno do sygnalizacji włamania i napadu, jak i do budowy systemu kontroli dostępu. W tym celu należy zastosować dedykowane moduły kontroli przejść, które umożliwiają wykorzystanie klawiatur i czytników kart zbliżeniowych do weryfikacji tożsamości osób. Elektroniczna kontrola dostępu stanowi więc dodatkowe zabezpieczenie chronionego obszaru – sygnalizacja włamania utrudnia nieuprawniony dostęp intruzom z zewnątrz, natomiast kontrola dostępu ma na celu poprawę bezpieczeństwa osób normalnie przebywających na terenie obiektu. Połączenie tych dwóch systemów jest korzystne także dla inwestora, ponieważ nie tylko obniża koszty inwestycji, ale także ułatwia administrowanie całą instalacją.

W newralgicznych obiektach, w których konieczne jest utrzymanie wysokiego poziomu bezpieczeństwa, stosowane są zaawansowane systemy alarmowe. Oferują one elastyczne narzędzia ułatwiające administrowanie wszystkimi urządzeniami wchodzącymi w skład tych systemów. Stosowane dawniej tradycyjne tablice synoptyczne zastępowane są obecnie interfejsami graficznymi, które zapewniają bardziej uporządkowany i kompleksowy dostęp do informacji. W przypadku systemów INTEGRA Plus rolę tę pełni przede wszystkim oprogramowanie GuardX umożliwiające kontrolę stanu obiektu w czasie rzeczywistym poprzez korzystanie z graficznych map, odczytywanie na bieżąco listy zdarzeń czy sprawdzanie przyczyn awarii zgłoszonych przez system. Innym narzędziem ułatwiającym zarządzanie systemem jest program DloadX, który umożliwia wykwalifikowanym technikom zmianę konfiguracji systemu czy diagnozowanie jego usterek.

Dzięki możliwościom komunikacyjnym centrale INTEGRA Plus mogą być wykorzystywane także przez organizacje, które mają wiele oddziałów wymagających scentralizowanego zarządzania. W praktyce łączność TCP/IP oferowana przez moduły ETHM-1 umożliwia pełne, zdalne zarządzanie z jednej lokalizacji z wykorzystaniem oprogramowania GuardX. W przypadku zarządzania większą liczbą oddziałów jeszcze lepiej sprawdzi się oprogramowanie STAM-2 Pro, które przeznaczone jest do zbiorczego nadzorowania wielu obiektów. Umożliwia ono nawiązanie połączenia z wybranym systemem i zarządzanie jego składnikami bez konieczności opuszczania miejsca pracy przez personel zajmujący się bezpieczeństwem.

Centrale INTEGRA Plus można połączyć również z innymi instalacjami w obiekcie. Dzięki specjalistycznym modułom INT-RS Plus, z otwartym protokołem komunikacyjnym, można stworzyć zintegrowany system zarządzania wszystkimi instalacjami w obiekcie, obejmujący m.in. systemy: wykrywania pożaru, sterowania automatycznymi urządzeniami przeciwpożarowymi, dozoru wizyjnego czy też kontroli dostępu.

Zalety nowych central INTEGRA 256 Plus, tak jak całej rodziny urządzeń INTEGRA Plus, docenią przede wszystkim ci, którzy poszukują skutecznych rozwiązań dla rozległych obiektów o wysokim ryzyku włamania.

Michał Konarski
Kierownik Działu Badań
SATEL

Systemy alarmowe **Satel**

INTEGRA 256 Plus

bezkompromisowe bezpieczeństwo

Gwarancją najwyższego bezpieczeństwa oferowanego przez centralę **INTEGRA 256 Plus jest pełna zgodność sprzętu z wymaganiami zawartymi w normach z serii EN50131 dla urządzeń Stopnia 3 (Grade 3)**.

Możliwość rozbudowy systemu do 256 wejść dostępna w nowej centrali, doskonale sprawdza się w rozległych systemach ochrony obiektów podwyższonego ryzyka.

Dodatkowe, innowacyjne rozwiązania, które zostały zastosowane w konstrukcji central INTEGRA 256 Plus to:

- dwusekcyjny układ zasilania z rozbudowaną autodiagnostyką,
- obsługa sygnałów maskowania z użyciem linii trójparametrycznych o programowalnej rezystancji EOL,
- obsługa czujek wibracyjnych i roletowych z analizą impulsów,
- port USB do łatwego i szybkiego programowania centrali.

GRADE 3

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

Zasysająca punktowa czujka dymu

Andrzej Obłój

Czyżby błąd w tytule?

Na pierwszy rzut oka coś się nie zgadza – zasysające czujki dymu nie są czujkami punktowymi! A jednak od niedawna i taka kombinacja jest możliwa. Po raz kolejny firma XTRALIS wprowadziła na rynek produkt, na pomysł którego wcześniej nikt inny nie wpadł. Dlaczego? Żeby połączyć zalety czujek punktowych z zaletami czujek zasysających, żeby zaoferować niedrogi, a jednocześnie zaawansowany technologicznie i wygodny w użytkowaniu system dostosowany do małych przestrzeni.

Zalety czujek punktowych

Około połowy kosztów systemów sygnalizacji pożarowej stanowią punktowe czujki dymu. Czujki te są podstawowymi elementami niemal wszystkich systemów sygnalizacji pożarowej. Mają szereg niepodważalnych zalet: wykrywanie pożaru na stosunkowo wczesnym etapie jego rozwoju, dobrze opracowane i opanowane reguły ich rozmieszczania, łatwa instalacja, niski koszt jednostkowy. Ale mają też wady – wymagają dostępu serwisowego do każdej czujki, nie pracują dobrze w silnych strumieniach powietrza, nie można ich instalować w różnych położeniach i dowolnych odległościach od sufitu, nie współpracują ze sobą.

Właściwości czujek zasysających

Tak się dobrze składa, że zalety czujek zasysających kompensują wady czujek punktowych. Czujki zasysające potrafią dobrze pracować w silnych strumieniach powietrza, otwory zasysające mogą „patrzeć" w różnych kierunkach i być umieszczone niemal wszędzie tam, gdzie spodziewamy się źródła zagrożenia, a orurowanie można wykonać tak, że dostęp do poszczególnych otworów zasysających nie będzie potrzebny. Ponadto efekt kumulacyjny silnie wspomaga wczesne wykrywanie dymu, a kilka progów alarmowania, które można ustawić w sensownych odstępach na skali wzrostu zadymienia, to chyba najskuteczniejszy sposób walki z opieszałością obsługi i traktowaniem wszystkich alarmów jako fałszywe.

Podstawowe wady czujek zasysających to duży pobór prądu, wysoka cena i… ciągle jeszcze mało rozpowszechniona wiedza na temat ich zalet i możliwych zastosowań.

Zasysająca punktowa czujka dymu VESDA VLQ

Obecnie wprowadzana na rynki czujka zasysająca VESDA VLQ (fot. 1) byłaby rzeczywiście czujką punktową, gdyby w rurze zasysającej wywiercić tylko jeden albo kilka otworów tuż obok siebie. Jest to możliwe, ale tracimy wtedy efekt kumulacyjny. Dlatego VLQ została opracowana tak, aby mogła pracować zarówno jako czujka punktowa, jak i wielopunktowa – klasyczna czujka zasysająca – ale w małej przestrzeni.

Podstawowe parametry czujki VLQ

Czujka VLQ jest przeznaczona do pracy w obiektach/pomieszczeniach o powierzchni nie większej niż 100 m^2. Ma dwa wejścia rur zasysających, które muszą być wykorzystane (obie rury przyłączone). W zależności od konfiguracji rury mogą mieć od 2×15 cm do 2×9 m długości. Każda rura musi mieć dwa otwory zasysające o średnicy 4,5 mm. Dwa progi wykrywcze można zaprogramować tak, żeby wykrywanie następowało w klasie A, B lub C. Zasilanie jest typowe – 24 V_{DC} zgodnie z EN54-4. Maksymalny pobór prądu wynosi 190 mA. Czujka VLQ ma trzy przekaźniki wyjściowe: *Prealarm, Alarm, Awaria*. Jak każde urządzenie XTRALIS, czujka VLQ ma pamięć – do 1000 zdarzeń, przydatną zwłaszcza dla instalatora – w razie wystąpienia błędów i usterek. Parametry czujki VLQ można programować zarówno lokalnie, przełącznikiem DIP, lub z komputera. Czujka jest większa od czujki punktowej (260×228×110 mm), ale na tyle mała, że nie powinno być problemów ze znalezieniem dla niej miejsca. Możliwa jest instalacja pozioma, na suficie, i pionowa, na ścianie. Możliwy jest montaż zarówno powierzchniowy, jak i wpuszczany, co pozwoli schować rury nad sufitem podwieszonym.

Fot. 1. Punktowa zasysająca czujka dymu VESDA VLQ

Obiekty, które czekały na czujkę VLQ:

1) Niewielkie obiekty telekomunikacyjne w kontenerach. Rozwój telekomunikacji powoduje, że jest coraz więcej obiektów bezobsługowych, rozmieszczonych w terenie. Są małe, ważne i drogie. Ilość wydzielanego w nich ciepła stale rośnie, a wentylacja jest coraz silniejsza. Stosowanie w nich czujek zasysających powinno być naturalnym wyborem. Największe kontenery – 45-stopowe, które mogą być użyte jako pojemniki na takie obiekty – mają wewnętrzną długość nieco ponad 13 m. Stąd maksymalna długość rurek czujki VLQ.
2) Komory transformatorowe o maksymalnych wymiarach 10 m×10 m. Kluczowa jest w tym przypadku możliwość wyniesienia czujki poza miejsce niebezpieczne. Sześciometrowa rura powinna wystarczyć do umieszczenia otworów zasysających mniej więcej na środku takiej komory transformatorowej.
3) Małe serwerownie. Niemal każda firma zatrudniająca kilkanaście lub nieco więcej osób ma dziś swoją serwerownię. Są to na ogół pomieszczenia o powierzchni od kilku do kilkunastu metrów kwadratowych, z szafami wentylowanymi tradycyjnie – do góry. Coraz częściej spotyka się takie serwerownie także w dużych domach jednorodzinnych. Czujka VLQ doskonale sprawdzi się w obu zastosowaniach. Wykorzystanie dwóch czujek VLQ pozwoli uruchamiać gaszenie.

Podsumowanie

Czujka VESDA VLQ to produkt idealnie wpisujący się w opisane wyżej zastosowania. Obiektów wymienionych wyżej rodzajów jest bez liku. Instalacja czujki VLQ jest niewiele trudniejsza niż zamontowanie zwykłej czujki punktowej. Projekt sprowadza się do wyznaczenia miejsc, w których chcemy mieć punkty zasysające.

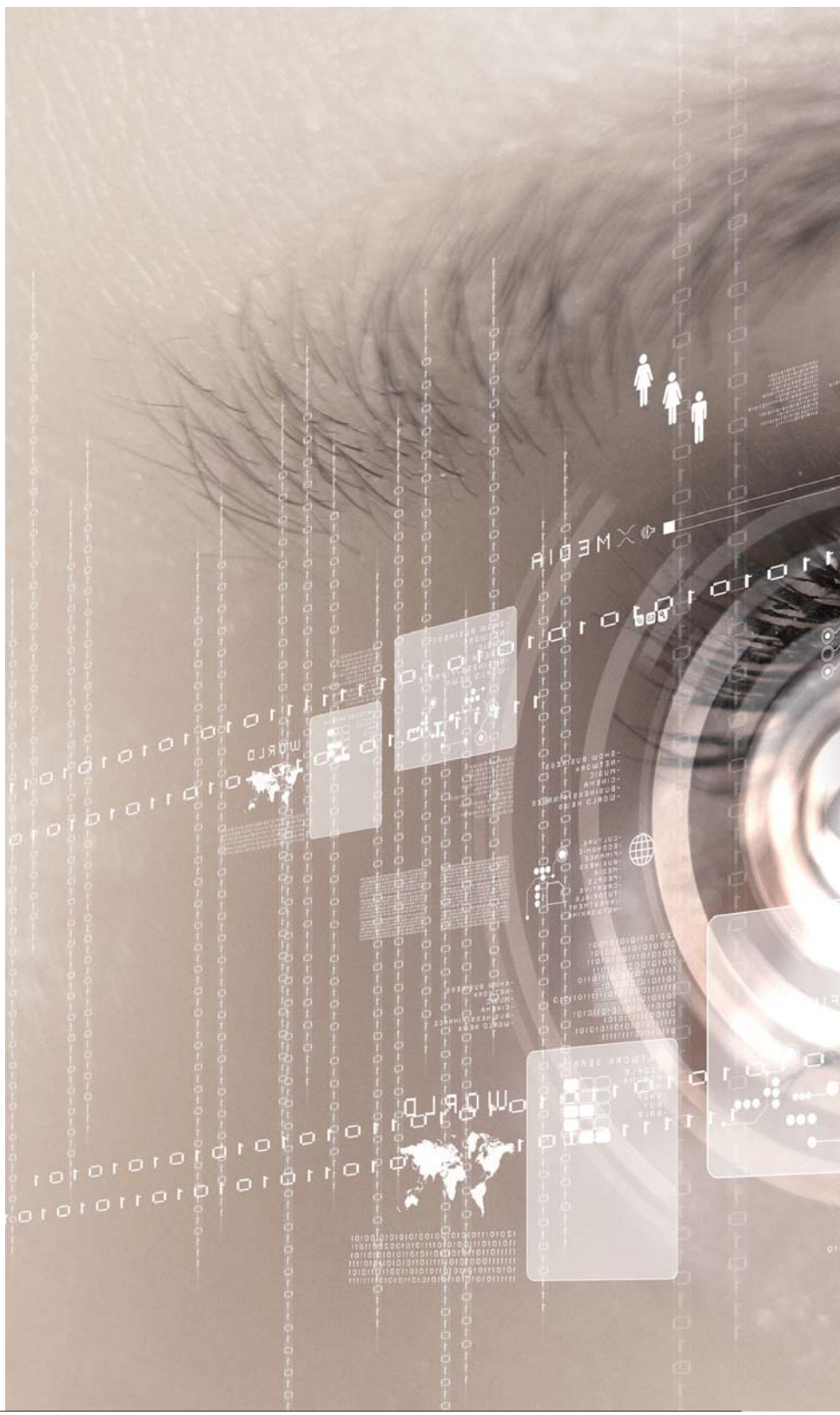
Autoryzowanym dystrybutorem produktów VESDA, OSID i XCC firmy Xtralis w Polsce jest Vision Polska (ul. Unii Lubelskiej 1, 61-249 Poznań, *www.visionpolska.pl*, e-mail: *biuro@visionpolska.pl*).

Andrzej Obłój
dyrektor techniczny na Europę Centralną i Wschodnią w firmie Xtralis

Systemy zabezpieczające z rozproszoną inteligencją

Czesław Półtorak

Firma CEM Systems, należąca do grupy Tyco Security Products, jest przodującym dostawcą systemów kontroli dostępu oraz zintegrowanych systemów zabezpieczających. Stworzony przez nią system AC2000 chroni wiele prestiżowych obiektów, zapewniając niezawodne, wyrafinowane rozwiązania w dziedzinach kontroli dostępu i zarządzania bezpieczeństwem



System CEM AC2000 pełni rolę scentralizowanego systemu zarządzania bezpieczeństwem, w którym z jednego stanowiska dowodzenia możliwe jest sprawowanie nadzoru nad chronionym obiektem i sterowanie wszystkimi zintegrowanymi składnikami – systemem kontroli dostępu, systemem dozoru wizyjnego, systemem sygnalizacji włamania i napadu, systemem ochrony obwodowej oraz innymi systemami zabezpieczającymi. Firma CEM Systems współpracuje z takimi partnerami jak Milestone, Bosch, IndigoVision, Salto i Assa Abloy.

CEM Systems jest światowym liderem w dziedzinie produkcji urządzeń zabezpieczających i wiele z nich wprowadziła na rynek jako pierwsza, np. ręczne przenośne czytniki kart, czytniki kart pracujące w sieci Ethernet czy sieciowe kontrolery przejść zasilane metodą PoE+. Najnowszym, innowacyjnym produktem, wprowadzonym ostatnio na rynek, jest emerald – wielofunkcyjny, „inteligentny" terminal z ekranem dotykowym.

Czym jest emerald?

emerald to wielofunkcyjny, „inteligentny" terminal dostępowy, którego konstrukcja stanowi przełom technologiczny w tej dziedzinie przemysłu. Ten wyróżniający się stylowym wyglądem i innowacyjnym dotykowym ekranem LCD produkt łączy w sobie zaawansowane funkcje czytnika kart i kontrolera przejścia, a także zintegrowanego interkomu VoIP. Obsługuje także wiele aplikacji uruchomionych na zdalnym serwerze. Terminal emerald jest przystosowany do współpracy ze scentralizowanym systemem zarządzania bezpieczeństwem CEM AC2000, w którym pełni rolę kontrolera przejść, a także realizuje pewne „inteligentne" funkcje systemowe, przeniesione z jednostki centralnej do urządzenia peryferyjnego.

Co czyni terminal emerald produktem tak odmiennym od rozwiązań konkurencyjnych?

Terminal emerald należy do kolejnej generacji produktów firmy CEM Systems pracujących w sieci Ethernet. Jego konstrukcja stanowi przełom technologiczny w tej dziedzinie przemysłu. Unikatowe właściwości terminalu emerald są następujące:

– **Spersonalizowany, dotykowy ekran LCD**
Terminal emerald ma jasny pojemnościowy ekran dotykowy LCD o przekątnej 4,3", pokryty powłoką przeciwodblaskową i umieszczony za szybą wykonaną z hartowanego szkła. Obudowa terminalu ma stopień szczelności IP65, zaś jej konstrukcja jest na tyle wytrzymała, że terminal można montować zarówno wewnątrz, jak i na zewnątrz budynków. Czytelny i intuicyjny graficzny interfejs użytkownika wyświetla animowane komunikaty dla posiadaczy kart, zależne od ich uprawnień dostępu.

– **Zintegrowany czytnik i kontroler przejścia**
Terminal emerald to znacznie więcej niż tradycyjny czytnik kart identyfikacyjnych. Jest to zintegrowany sieciowy czytnik kart i kontroler przejścia, który komunikuje się z serwerem-hostem AC2000 za pośrednictwem sieci Ethernet, co eliminuje konieczność stosowania dodatkowych urządzeń. Terminal ma obszerną wewnętrzną bazę danych, która umożliwia pracę w trybie offline w razie chwilowej utraty połączenia z serwerem-hostem.

– **Zintegrowany interkom VoIP zapewniający komunikację głosową**
Terminal emerald ma wbudowany mikrofon i głośnik, dzięki czemu pełni rolę interkomu VoIP zapewniającego dwukierunkową komunikację głosową pomiędzy użytkownikami systemu a pracownikami ochrony.

– **Obsługa zdalnych aplikacji**
Aplikacje zdalne to aplikacje sieciowe, zainstalowane na serwerze systemowym AC2000, które umożliwiają bezpieczny dostęp do centralnej bazy danych bezpośrednio z terminalu dostępowego zainstalowanego przy kontrolowanym przejściu.

Dlaczego firma CEM Systems stworzyła terminal emerald?

Firma CEM Systems nieustannie wprowadza na rynek innowacyjne produkty służące do budowy systemów kontroli dostępu. Jednym z ostatnich zadań było opracowanie nowych urządzeń pracujących na wspólnej platformie programowej, wykorzystujących różne technologie teleinformatyczne. Celem była poprawa komfortu obsługi terminali dostępowych i stworzenie platformy programowej, która będzie lepiej odpowiadać biznesowym potrzebom klientów. Podczas prac nad terminalem emerald uwzględnione zostały wyniki wieloletnich doświadczeń projektowych oraz badań rynkowych prowadzonych przez firmę CEM Systems.

Jest wiele powodów, dla których nowe opracowania firmy CEM Systems zmierzają w kierunku komplikacji urządzeń peryferyjnych. Składa się na to rozwój sieci TCP/IP, upowszechnienie rozwiązań bazujących na interfejsach sieciowych oraz standaryzacja protokołów komunikacyjnych. Współczesne sieci IP są na tyle sprawne, że za pośrednictwem połączeń ethernetowych możliwa jest szybka wymiana danych miedzy serwerami a urządzeniami peryferyjnymi. Ponadto duży wpływ na konstrukcję urządzeń peryferyjnych ma postępująca standaryzacja protokołów komunikacyjnych. W przypadku terminalu emerald wykorzystany został protokół SIP/VoIP, dzięki czemu możliwe jest nawiązywanie interkomowych połączeń głosowych, zaś wybór interfejsu sieciowego jako platformy zapewniającej komunikację terminali z zewnętrznymi aplikacjami, zainstalowanymi na serwerze, pozwala na bezpieczną obsługę tych aplikacji z poziomu terminali. Zastosowanie terminali emerald przyczynia się do podwyższenia poziomu bezpieczeństwa obiektów, a także do ich efektywniejszego wykorzystania.

Czym są zdalne aplikacje?

Dzięki wykorzystaniu bezpiecznego interfejsu sieciowego oraz protokołu SSL służącego do transmisji szyfrowanych strumieni danych zdalne aplikacje umożliwiają dostęp do informacji

Fot. 1. Szyfrowana klawiatura emerald TS300

Fot. 2. Zdalne aplikacje emerald

zgromadzonych w bazie danych systemu CEM AC2000. Terminale pełnią rolę bezpiecznych, „inteligentnych" punktów dostępowych, których działanie dostosowuje się do uprawnień poszczególnych okazicieli kart identyfikacyjnych. Na ekranach terminali wyświetlane są bieżące informacje dotyczące stanu bezpieczeństwa obiektu oraz dane statystyczne, na przykład dotyczące uprawnień gości odwiedzających dany obiekt, alarmów systemowych oraz ostatnich alarmów związanych z danym terminalem. Inne aplikacje mogą udostępniać informacje dotyczące ostatnio użytych kart identyfikacyjnych, co może być wykorzystane do rejestracji czasu pracy poszczególnych pracowników, mogą informować użytkowników o poziomie uprawnień i okresie ważności ich kart identyfikacyjnych, a także wyświetlać na ekranach terminali dodatkowe informacje, na przykład dotyczące bezpieczeństwa i higieny pracy w zakładzie. Ponadto zewnętrzne aplikacje mogą być wykorzystane do zmiany kodów PIN poszczególnych kart identyfikacyjnych bez udziału operatora systemu. Zakres zastosowań aplikacji zewnętrznych może być rozszerzony i dostosowany do indywidualnych wymagań użytkowników. Firma CEM Systems stale poszerza swoją ofertę w tej dziedzinie.

Czesław Półtorak

CEM Systems
tel.: +44 (0) 28 9045 6767
e-mail: cem.info@tycoint.com
www.cemsys.com

System komunikacji wewnętrznej VoIP

Inteligentny terminal dotykowy

Zdalne aplikacje

Kontroler i czytnik IP

emerald™

Świat możliwości na wyciągnięcie ręki

emerald™ to wielofunkcyjny inteligentny terminal dostępowy rewolucjonizujący przemysł zabezpieczeń.

Dzięki eleganckiej konstrukcji i specjalnie zaprojektowanemu nowoczesnemu ekranowi dotykowemu urządzenie emerald stanowi wydajny czytnik kart i kontroler w jednym, oferujący w pełni zintegrowany system komunikacji wewnętrznej Voice over IP (VoIP) oraz asortyment zdalnych aplikacji, zapewniających różnorodne możliwości kontroli dostępu. System emerald otwiera świat niezliczonych możliwości umieszczając system kontroli dostępu CEM w awangardzie przyszłości.

emerald™ — najbardziej wielofunkcyjny inteligentny terminal dostępowy w branży.

Jeśli potrzebujesz więcej informacji, prosimy o kontakt:
T: +44 (0)28 9045 6767
E: cem.info@tycoint.com
lub odwiedź nas na stronie www.cemsys.com/emerald

CEM SYSTEMS
From Tyco Security Products

BMS sięgnął chmur

Johnson Controls

Dzięki działającym w chmurze systemom zarządzania budynkami (ang. *Building Management System* – BMS) właściciele i zarządcy budynków mogą lepiej zarządzać swoimi obiektami. Systemy zarządzania budynkami z powodzeniem funkcjonują na świecie od wielu lat, od parunastu także w Polsce. Stanowią one bezcenne narzędzie do optymalizacji wykorzystania energii w budynkach. W Polsce systemy BMS dopiero się rozwijają, ale istnieją już zaawansowane rozwiązania w tej dziedzinie

Johnson Controls, światowy lider w dziedzinie systemów i usług podnoszących efektywność wykorzystania energii w budynkach, poszedł o krok dalej, umieszczając system BMS w tzw. chmurze obliczeniowej. Rozwiązanie o nazwie Panoptix daje ogromne możliwości użytkownikom systemów BMS.

Czym dokładnie jest BMS działający w chmurze? Zasadniczą rolą systemu BMS jest integracja wszystkich systemów elektrycznych i elektronicznych znajdujących się w budynku i przetwarzanie spływających z nich danych. BMS działający w chmurze można natomiast zdefiniować jako system zarządzania systemami zarządzania. Innymi słowy, łączy on wiele niezależnych od siebie systemów BMS, często znajdujących się w różnych lokalizacjach, w celu przetwarzania danych pochodzących z tych systemów.

Czy z wdrożenia takiego systemu wynikają jakieś korzyści? Przeanalizujmy kompleks budynków Politechniki Warszawskiej, które są rozrzucone na terenie Warszawy w promieniu pięciu kilometrów od gmachu głównego. Uczelnia ma także filię w Płocku – 100 kilometrów od gmachu głównego. Chcąc zarządzać wydatkiem cieplnym czy zużyciem energii elektrycznej w tak odległych od siebie budynkach, moglibyśmy napotkać wiele trudności. Mając kontrolę nad wszystkimi budynkami – zarówno akademikami, jak i budynkami wydziałowymi – centralny system monitorujący mógłby dostosować nastawy central wentylacyjnych lub natężenie oświetlenia do warunków zewnętrznych na danej szerokości geograficznej, w zależności od pory roku czy dnia. Dzięki systemowi BMS pracującemu w chmurze wszystkie te nastawy byłyby możliwe do wykonania centralnie, z jednego miejsca i przez jedną osobę.

W ramach prac nad rozwiązaniem Panoptix firma Johnson Controls zapytała swoich klientów, co myślą o systemach BMS i jak systemy te mogłyby rozwiązywać ich problemy w zakresie zarządzania budynkami. Okazało się, że większość użytkowników wskazała na te same obszary trudności związanych z obecnymi systemami.

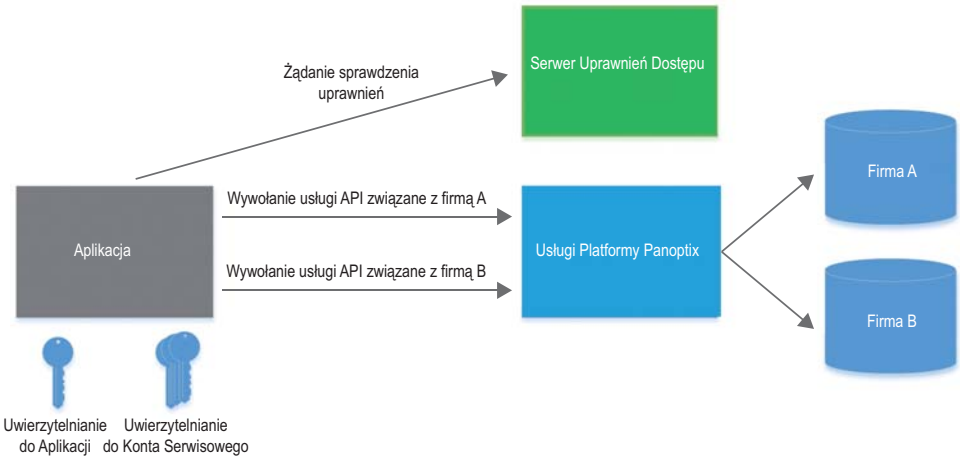
Po pierwsze, takie systemy BMS wytwarzają ogromną ilość informacji zbieranych przez tysiące punktów pomiarowych – są to stale zmieniające się wartości temperatury, wilgotności, ciśnienia, wydajności urządzeń, poboru energii elektrycznej i inne dane, które sygnalizują zagrożenia i alarmy. Przy tak dużej bazie danych wyzwaniem staje się ich umiejętna obróbka. Wiele firm nie ma zasobów ludzkich dysponujących wystarczającą wiedzą ekspercką, umożliwiającą interpretację tych danych. Można oczywiście zlecić zarządzanie systemem BMS wyspecjalizowanym firmom zewnętrznym, ale wiąże się to z dużym nakładem finansowym.

Miliardy obliczeń

Z pomocą przychodzą narzędzia systemu Panoptix, które w trybie ciągłym sporządzają diagnozy stanu obiektu, które następnie można poddać analizie. Skomplikowane algorytmy bezustannie badają prawdopodobieństwo różnych zdarzeń. Co może się zdarzyć, jeśli temperatura wody w twoim agregacie spadnie o dwa stopnie? Jak przełoży się to na działanie obiektu? Co stanie się, jeśli wcześniej wyłączymy klimatyzatory, oświetlenie etc.? Jaki dałoby to efekt? Możemy uzyskać odpowiedzi na takie pytania.

Proces diagnostyczny trwa nieprzerwanie i w momencie pojawienia się jakiejkolwiek nieprawidłowości system identyfikuje odchylenie od normy. Narzędzia Panoptix cały czas wykonują miliardy obliczeń, sprawdzając i analizując systemy i procesy, podpowiadając użytkownikowi, w jaki sposób można zoptymalizować pracę budynku czy zaoszczędzić na kosztach wymiany urządzeń.

Panoptix pozwolił nam lepiej dostosować nasze rozwiązania do potrzeb klientów, gdyż pomaga nam skoncentrować się na sposobie wykorzystania informacji o obiektach. Za pomocą interfejsu API (Application Programming Interface) system Panoptix pozwala zebrać dane z różnych obiektów i systemów różnych producentów.



Rys. 1. Struktura zabezpieczeń i komunikacji systemu

Zmniejsza to koszty związane z integracją systemów i oznacza, że zasoby właściciela czy zarządcy obiektów, angażowane zazwyczaj do działań związanych z integracją systemów, mogą być kierowane do innych obszarów biznesu generujących zysk – powiedział Michael Murray, prezes firmy Lucid zajmującej się tworzeniem oprogramowania do zarządzania budynkami, której aplikacja działa w ramach platformy Panoptix.

Konsultanci Live Guides

Poza szybkim dostępem do przeanalizowanych informacji użytkownicy systemów BMS działających w chmurze na pewno docenią możliwość kontaktu z grupą ekspertów, tzw. *live guides* („konsultanci na żywo"), którzy mają ogromną specjalistyczną wiedzę z zakresu zarządzania budynkami i są do dyspozycji w razie potrzeby konsultacji lub rozwiązania problemów na terenie naszego budynku.

Są to eksperci bardzo dobrze zaznajomieni z infrastrukturą swoich klientów, dzięki czemu są w stanie wskazać obszary zagrożeń i doradzić, jakie działania należy podjąć, aby zapobiec problemom w przyszłości. Mając dane z pierwszej ręki, zebrane i przekazywane przez system w formie raportu, na życzenie klienta dokonują analizy tych danych i przedstawiają możliwości rozwiązania problemu. Raporty są stale generowane przez system, więc na przykład zarządca budynku, który otrzymuje taki raport, może od razu podjąć działanie i zaoszczędzić na kosztach zużycia energii. Oczywiście konsultanci *live guides* nie udają się osobiście do żadnego z obiektów. Konsultacja odbywa się on-line lub telefonicznie.

Rys. 2. Panel operatorski użytkownika

Wspólna przestrzeń

Kolejną zaletą takiego systemu jest możliwość komunikacji z tysiącami innych użytkowników, których systemy także pracują w chmurze. Z tego względu Panoptix jest więc także swego rodzaju platformą społecznościową, w ramach której użytkownicy systemów mogą porozumiewać się pomiędzy sobą, wymieniając się doświadczeniami oraz analizując, w jaki sposób można zwiększyć efektywność wykorzystania energii w swoich budynkach. Tutaj również z pomocą przychodzą konsultanci *live guides*.

Podsumowanie

Klient, który podejmuje decyzję o przystosowaniu swojego systemu BMS do pracy w chmurze, podpisuje umowę serwisową uwzględniającą indywidualne cechy i funkcje budynku. Następnie wyznaczeni przez klienta pracownicy uzyskują dostęp do grupy ekspertów *live guides*, z którymi w każdym momencie można się kontaktować e-mailowo lub telefonicznie. Poza usługami serwisowymi związanymi z eksploatacją urządzeń użytkownik otrzymuje darmową usługę doradztwa.

System BMS działający w chmurze to bardzo ekonomiczna metoda przechowywania danych w jednym, bezpiecznym ośrodku informatycznym. Wdrożenie tego rozwiązania wymaga bezpiecznej infrastruktury sieciowej z możliwością podłączenia indywidualnej sieci VPN – aby nikt nie mógł w sposób nieautoryzowany uzyskać dostępu do danych zgromadzonych w systemie.

Aplikacje pracujące w chmurze dają wgląd w działanie każdego systemu, podsystemu, a nawet każdego urządzenia. Można je zastosować w budynku o dowolnej powierzchni, w którym pracuje dowolnego rodzaju system BMS, a obsługiwać za pomocą dowolnego komputera, tabletu czy smartfonu. Opisany w artykule system Panoptix zapewnia nie tylko agregację i wstępną analizę danych przychodzących z obiektów, ale także możliwość konsultacji ze specjalistami w dziedzinie systemów budynkowych oraz wymiany doświadczeń z innymi użytkownikami systemu. Podobne systemy pojawiają się w branży automatyki już od jakiegoś czasu, jednak jeszcze nigdy nie były one tak funkcjonalne i kompleksowe. W dziedzinie systemów automatyki budynkowej system BMS działający w chmurze to ważny wkład w rozwój całej branży.

Johnson Controls
ul. Krakowiaków 50, 02-255 Warszawa
tel.: +48 22 518 19 00, faks: +48 22 811 61 01
www.johnsoncontrols.pl/be

dahua TECHNOLOGY

i ♥ HDCVI

High Definition Composite Video Interface (HDCVI) is an eye-catching technology breakthrough in the industry, providing a new HD solution on the market besides IP and HD-SDI. HDCVI is an optimal solution for megapixel high definition application, featuring non-latent long-distance transmission at lower cost.

Highlights

- Fast and Fabulous to HD
- Long-distant Transmission
- Zero Video Lose/Real-time Preview
- 3 Signals (Video/Audio/Control) in 1 Coaxial Cable

Recommended models:

4/8/16 All Channel 1080P 2U Standalone DVR
HCVR7804/08/16S

4/8 All Channel 720P Mini 1U Standalone DVR
HCVR5104/08H

720P/1080P Water-proof IR HDCVI Mini Dome Camera
HAC-HDW2100S/2200S

720P/1080P Water-proof IR HDCVI Camera
HAC-HFW2100S/2200S

1.3Mp HD HDCVI IR PTZ Dome Camera
SD6C120I-HC

1.3Mp HD HDCVI PTZ Dome Camera
SD63120I-HC

CE FC UL RoHS ISO 9001:2000

ISC WEST
ISE WEST 2014
02–04 Apr 2014 Las Vegas
Booth: NO.22089

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

www.dahuasecurity.com

IS VENO

PLATFORMA INTEGRUJĄCA

Połączyliśmy nasze doświadczenie i wiedzę o czterech systemach bezpieczeństwa:
przeciwpożarowym, alarmowym, CCTV oraz kontroli dostępu, by stworzyć jeden system nadzoru, integrujący wszystkie zabezpieczenia obiektu.
Tak powstała **PLATFORMA INTEGRUJĄCA VENO.**

Wyłączny dystrybutor 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

Efektywne zarządzanie bezpieczeństwem obiektu

Każdy system bezpieczeństwa zainstalowany w obiekcie dostarcza innych informacji o jego stanie. Kompletny obraz sytuacji można uzyskać dopiero po połączeniu informacji przychodzących ze wszystkich systemów. Zestawienie i zsynchronizowanie tak dużej ilości danych bywa często bardzo trudne, zwłaszcza w przypadku bardziej zaawansowanych instalacji. Oprogramowanie VENO integruje systemy CCTV, SSWiN, PPOŻ oraz KD, dzięki czemu zapewnia wyższy stopień ochrony obiektu, niż każdy z tych systemów z osobna.

Wspólny interfejs dla wszystkich systemów

Jeden program nadzorczy to większa efektywność w zarządzaniu bezpieczeństwem całego obiektu. Operator, dysponując danymi ze wszystkich urządzeń i instalacji jednocześnie, może precyzyjnie określić przyczynę alarmu i podjąć działania stosowne do danej sytuacji. Wspólny interfejs i ujednolicony sposób informowania o alarmach pozwala osobom odpowiedzialnym za bezpieczeństwo obiektu szybciej podejmować trafne decyzje.

Elastyczna konfiguracja, możliwość realizowania nietypowych funkcjonalności

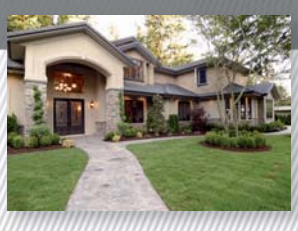
Każdy obiekt ma inną charakterystykę, a co za tym idzie, specyficzne potrzeby. Zaletą oprogramowania VENO jest duża elastyczność. Program można łatwo konfigurować pod kątem indywidualnych wymagań, a także charakteru i przeznaczenia konkretnego obiektu. Liczba możliwych konfiguracji jest praktycznie nieograniczona. Za zarządzanie całym systemem odpowiada administrator, który przydziela uprawnienia poszczególnym operatorom.




Szeroki wachlarz zastosowań

Oprogramowanie VENO nie narzuca żadnych ograniczeń co do wielkości systemu – nie ma limitów liczby urządzeń pracujących w systemach CCTV, SSWiN, PPOŻ i KD, ani limitów liczby operatorów. VENO doskonale sprawdza się zarówno w dużych, rozproszonych obiektach, jak też w mniejszych instalacjach. Program dedykowany jest do każdego typu obiektów – budynków mieszkalnych, komercyjnych, użyteczności publicznej i dużych kompleksów przemysłowych.



VENO

platforma integrująca elektroniczne systemy zabezpieczeń

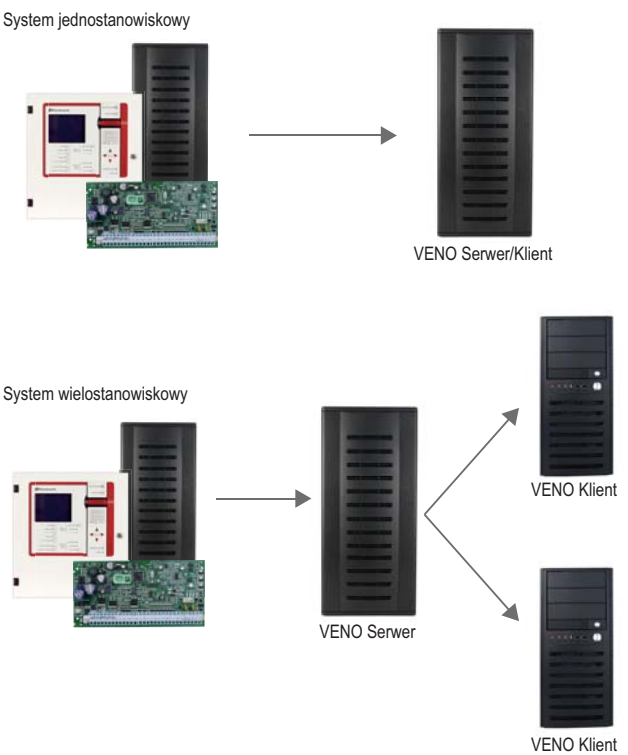
Patryk Gańko

W wielu obiektach oprócz wymaganych systemów przeciwpożarowych instalowane są również dodatkowo systemy alarmowe, kontroli dostępu oraz telewizji dozorowej IP. Napływające z poszczególnych systemów informacje muszą być stale analizowane przez pracowników ochrony. Dopiero ich powiązanie zwiększa prawdopodobieństwo podjęcia trafnej decyzji w przypadkach wystąpienia określonych zdarzeń w obiekcie

Pozyskiwanie i synchronizowanie danych z różnych systemów jest często bardzo kłopotliwe, szczególnie w przypadku rozbudowanych instalacji. Przy dużej rotacji pracowników ochrony umiejętność obsługi każdego z tych systemów, nawet na podstawowym poziomie, wymaga częstych i rozbudowanych szkoleń. W wielu przypadkach realizacja procedur szkoleniowych jest kosztowna i nie zawsze jest możliwa, dlatego istnieje potrzeba wdrożenia rozwiązań, które w przypadku wystąpienia określonego typu zdarzeń automatycznie powiążą informacje pochodzące z wielu systemów oraz pomogą podjąć właściwą decyzję co do dalszego postępowania. Do tej pory integracja systemów ograniczała się do połączenia bloków wejść/wyjść alarmowych współpracujących instalacji. Wraz ze wzrostem znaczenia technik cyfrowych w systemach telewizji dozorowej (telewizja IP) oraz w systemach kontroli dostępu i sygnalizacji włamania ten poziom integracji stał się niewystarczający. Rynek oczekuje integracji elektronicznych systemów zabezpieczających nie na poziomie sprzętowym, ale programowym. W niniejszym artykule chciałbym przedstawić czytelnikom oprogramowanie VENO, które powstało w odpowiedzi na oczekiwania integratorów systemów zabezpieczeń. Opiszę najważniejsze funkcje tego oprogramowania, a w kolejnym artykule omówię przypadki konkretnych wdrożeń na przykładzie obiektów, w których to oprogramowanie zostało wykorzystane do integracji istniejących systemów.

System jedno- i wielostanowiskowy

Przed użyciem oprogramowania VENO, integrującego systemy zabezpieczające w danym obiekcie, należy zastanowić się nad strukturą systemu, który powstanie w wyniku integracji. Oprogramowanie VENO może posłużyć do budowy zarówno prostego systemu jednostanowiskowego, jak i rozbudowanego systemu złożonego z serwera oraz wielu podłączonych do niego stacji klienckich. Jeśli oprogramowanie VENO pracuje w trybie serwer/klient, wszystkie dane wychodzące z różnych urządzeń są doprowadzane do jednej stacji roboczej, na której są wizualizowane i archiwizowane. W trybie wielostanowiskowym funkcje archiwizacji danych są oddzielone od procesów wizualizacji, co znacznie podwyższa poziom bezpieczeństwa systemu i daje możliwość podglądu stanu poszczególnych podsystemów na niezależnych stanowiskach operatorskich. W tego typu aplikacjach serwer może być umieszczony w osobnym, klimatyzowanym pomieszczeniu, do którego fizyczny dostęp jest ograniczony, i można się z nim komunikować poprzez sieć domenową za pośrednictwem stacji operatorskich.



Rys. 1. Schemat systemu jedno- i wielostanowiskowego

Interfejs graficzny

Po pierwszym uruchomieniu aplikacji klienckiej użytkownik zobaczy pusty, biały ekran. To administrator sytemu, poprzez tryb edycji, ustawia tła, nanosi ikony i obiekty powiązane z poszczególnymi systemami. Wizualizacje związane z poszczególnymi podsystemami mogą być ze sobą powiązane i równocześnie wyświetlane na wielu monitorach, w zależności od wydajności kart graficznych poszczególnych jednostek klienckich. Najważniejszą zaletą tak powstałego graficznego interfejsu jest możliwość naniesienia informacji ze wszystkich systemów na jeden ekran. Operator, dysponując danymi ze wszystkich urządzeń i instalacji jednocześnie, może precyzyjnie określić przyczynę alarmu. Wspólny interfejs i ujednolicony sposób informowania o zdarzeniach pozwalają na szybsze podejmowanie decyzji. System integrujący jest przystosowany do pracy z wykorzystaniem monitorów dotykowych, m.in. dzięki dużym ikonom oraz wygodnemu sposobowi ich przenoszenia („przeciągnij i upuść"). Aplikacja umożliwia dodanie dwuwymiarowych i trójwymiarowych map oraz planów w formacie PNG. Poziom uszczegółowienia wizualizacji zależy od potrzeb i preferencji operatorów – program nie narzuca żadnych ograniczeń.

Niezależne panele użytkowników

Wielostanowiskowy tryb pracy systemu umożliwia scentralizowane zarządzanie uprawnieniami użytkowników stacji klienckich. Zarówno administrator, jak i poszczególni użytkownicy mogą mieć niezależnie skonfigurowane panele. Za konfigurację oprogramowania (m.in. programowanie scenariuszy alarmowych, tworzenie harmonogramu) oraz ustalenie uprawnień operatorów odpowiada administrator. Takie rozwiązanie jest bezpieczne, ponieważ operator korzysta z gotowych ustawień i nie może ich modyfikować (brak trybu edycji). Operator otrzymuje tylko te informacje, które administrator uznał za niezbędne do jego codziennej pracy.

Niezawodność działania

VENO integruje działanie systemów bezpieczeństwa wykorzystujących różne technologie i mających różne funkcje w chronionym obiekcie, nie zmieniając przy tym ich pierwotnych funkcji. Każdy z systemów pracuje autonomicznie, a VENO jedynie ułatwia i usprawnia ich obsługę. Poszczególne systemy działają niezależnie i awaria jednego z nich nie wpływa na pracę innego. Również ewentualna awaria serwera z oprogramowaniem VENO nie wpływa na pracę autonomicznych systemów.

Rys. 2. Przykładowy graficzny panel użytkownika

Scenariusze reakcji

Użytkownik może tworzyć rozbudowane scenariusze reakcji programu na alarmy. Schematy reakcji na alarm mogą zostać przypisane do zdefiniowanych stanowisk operatorskich. Automatyczne scenariusze umożliwiają usprawnienie pracy operatorów. Przykładową reakcją na zdarzenie alarmowe może być wyświetlenie obrazów z pojedynczej kamery lub grupy kamer i weryfikacja rzeczywistych przyczyn alarmu przez operatora, zmiana lub otwarcie dodatkowego panelu na wybranym monitorze lub uruchomienie innej, zewnętrznej aplikacji. Scenariusze mogą być bardzo złożone i dlatego w aplikacji została dodana funkcja pseudokodu, która ułatwia analizę i weryfikację poprawności zaprogramowanych scenariuszy. Zdefiniowane logiczne związki między elementami są zapisywane w postaci tekstowej w plikach PDF.

Unikatową funkcją jest możliwość stosowania komunikatów głosowych. Po zainstalowaniu w jednostce klienckiej dowolnego syntezatora mowy głos lektora może informować o alarmach i innych zdarzeniach.

Archiwum zdarzeń

Informacje o zdarzeniach ze wszystkich systemów (CCTV, SWiN, ppoż. oraz KD) są automatycznie rejestrowane w jednej bazie danych. Dzięki temu operator widzi pełną historię alarmów, awarii oraz logowania użytkowników. Po podaniu kryteriów zaawansowany moduł wyszukiwania filtruje informacje o zdarzeniach i dzieli zdarzenia na kategorie. Całą bazę danych lub jej wybraną część można eksportować do pliku PDF.

Aktualnie system VENO umożliwia integrację systemów telewizji dozorowej NMS, systemów alarmowych DSC i SATEL, systemów kontroli dostępu KaDe i Kantech oraz systemów sygnalizacji pożarowej Polon Alfa. Dzięki otwartej architekturze możliwe jest dodawanie kolejnych systemów i ich integracja.

Oprogramowanie serwerowe VENO działa tylko wtedy, gdy do komputera podłączony jest na stałe klucz zabezpieczający. Jeśli klucz ten nie jest aktywny, serwer będzie pracował przez godzinę w trybie demo, a następnie samoczynnie wyłączy się.

Dostępne są cztery wersje oprogramowania VENO: Standard, Professional, Enterprise oraz Infinity, w zależności od liczby integrowanych elementów. Niezależnie od wersji, oprogramowanie obsługuje maksymalnie cztery stacje robocze.

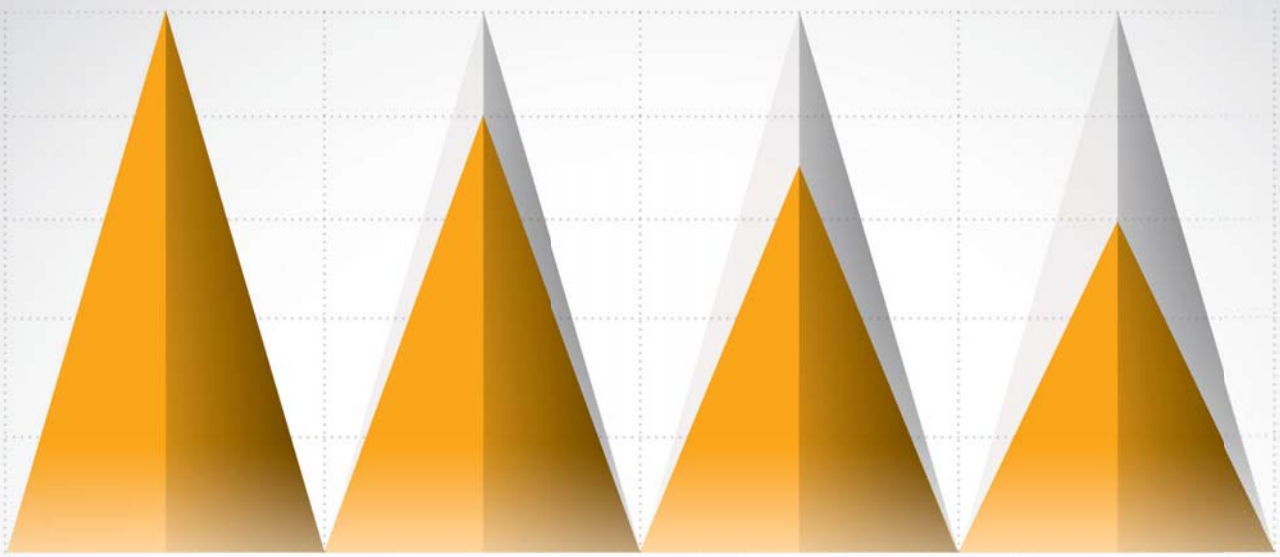
Oprogramowanie VENO doskonale sprawdza się zarówno w małych, jak i w rozległych obiektach. Przykładowo, może być stosowany do integracji systemów zabezpieczających w budynkach mieszkalnych, komercyjnych, użyteczności publicznej i w dużych kompleksach przemysłowych. Ze względu na wzrost znaczenia rozwiązań integrujących na rynku zabezpieczeń oraz złożoność i dynamiczny rozwój opisywanego oprogramowania należy oczekiwać, że jeszcze często będziemy się spotykali z tematyką VENO na łamach *Zabezpieczeń*.

Patryk Gańko
AAT Holding

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

4 NOWE SERIE KAMER
poziomy zaawansowania



800 SERIA

- **Przetwornik 960H**
- Czułość od 0.00002 lx
- Do 700 TVL
- DSS - wydłużona migawka
- OSD - menu ekranowe w j. polskim
- Sterowanie RS-485 (wybrane modele)
- WDR - szeroki zakres dynamiki
- HLC - redukcja oślepiania
- DNR - cyfrowa redukcja szumu
- Strefy prywatności
- Zoom cyfrowy
- Detekcja ruchu
- DIS - cyfrowa stabilizacja obrazu
- LPR - rozpoznawanie tablic rejestracyjnych (wybrane modele)
- Oświetlacz podczerwieni (wybrane modele)
- Obiektyw f=2.5-12 mm, f=3.5-16 mm, f=6-50 mm (wybrane modele)
- Smart IR
- Grzałka (wybrane modele)

600 SERIA

- **Przetwornik 960H**
- Czułość od 0.00001 lx
- Do 750 TVL
- DSS - wydłużona migawka
- OSD - menu ekranowe
- WDR - szeroki zakres dynamiki
- HLC - redukcja oślepiania
- DNR - cyfrowa redukcja szumu
- Strefy prywatności
- Zoom cyfrowy
- Smart zoom
- Detekcja ruchu
- DIS - cyfrowa stabilizacja obrazu
- Oświetlacz podczerwieni (wybrane modele)
- F-DNR - niweluje zakłócenia spowodowane mgłą, opadami śniegu lub deszczu
- Obiektyw f=3.6 mm, f=2.8-12 mm (wybrane modele)
- Smart IR

400 SERIA

- **Przetwornik 960H**
- Czułość od 0.001 lx
- Do 700 TVL
- OSD - menu ekranowe
- WDR - szeroki zakres dynamiki
- HLC - redukcja oślepiania
- DNR - cyfrowa redukcja szumu
- Strefy prywatności
- Detekcja ruchu
- Oświetlacz podczerwieni (wybrane modele)
- Obiektyw f=2.8-11 mm, f=2.8-12 mm, f=3.6 mm (wybrane modele)
- Smart IR
- Grzałka (wybrane modele)

200 SERIA

- Czułość od 0.05 lx
- Do 700 TVL
- Oświetlacz podczerwieni (wybrane modele)
- Obiektyw f=2.8-11 mm, f=3.5-8 mm, f=3 mm (wybrane modele)

Wyłączny dystrybutor produktów NOVUS® w Polsce:

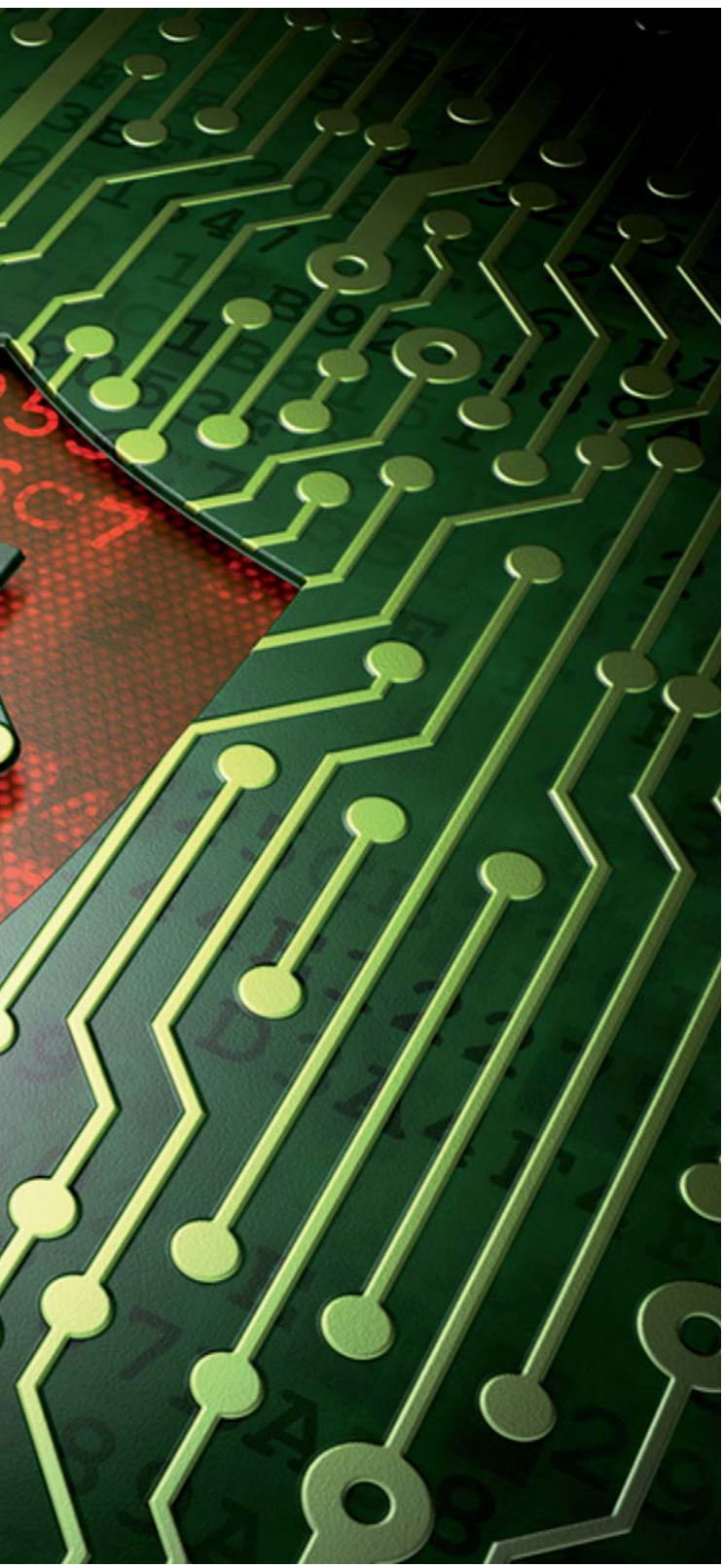
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Systemy automatyki domowej,
w których wykorzystuje się komunikację Z-wave

Daniel Kamiński

Produkty ułatwiające sterowanie i automatyzację oświetlenia, klimatyzacji, wentylacji, ogrzewania, podlewania ogrodu, sterowania bramami i roletami, a także integrujące systemy zabezpieczeń, takie jak systemy alarmowe, systemy kontroli dostępu czy wizyjne systemy dozorowe, są dostępne w Polsce od ponad dwudziestu lat. Określa się je wspólnym mianem systemów zintegrowanych. Obiekty, w których są zainstalowane, to tak zwane inteligentne budynki

W ostatnich latach odczuwalny stał się wpływ nowych technologii na życie przeciętnego człowieka. Po prostu trudno uwierzyć, że w ciągu ostatnich trzydziestu lat dokonała się rewolucja technologiczna, dzięki której pojawiły się komputery osobiste, laptopy, telefony komórkowe, tablety, smartfony, stworzony został Internet, a w nim portale społecznościowe i wiele innych usług, bez których dziś trudno nam się obyć. Rozwój technologii jest tak szybki, że wprawia w zakłopotanie przeciętnych mieszkańców tego świata.



Niestety tak szybki postęp powoduje, że pojęcia takie jak *cloud computing, web 2.0 software as a service* czy *next generation networks* niewiele wyjaśniają zwykłemu zjadaczowi chleba. Z tego względu producenci tworzą też rozwiązania, dzięki którym urządzenia – pomimo technologicznego zaawansowania – są przyjazne dla użytkownika, np. *plug and play*.

Powyższe trendy mają też odbicie w rozwiązaniach przeznaczonych dla gospodarstw domowych. Szczególnie przydatne są systemy, które ułatwiają wykonywanie powtarzalnych czynności (takich jak: otwieranie bram, podlewanie ogrodów, zamykanie rolet itp.) lub zmniejszają zużycie energii (np. sterowanie ogrzewaniem, wentylacją, klimatyzacją itp.), co ma przełożenie na korzyści finansowe. Internet umożliwia sterowanie poszczególnymi systemami, nawet wtedy, gdy nikogo nie ma w budynku.

Idea inteligentnego budynku

Systemy automatyki budynkowej są znane w Polsce od wielu lat. Kojarzone są z systemami drogimi, w których zintegrowane urządzenia są połączone przewodami i komunikują się za pomocą protokołów LON lub EIB/KNX. Jednym z najkosztowniejszych składników takich systemów jest instalacja kablowa. Na kolejnych miejscach plasują się są sterowniki i konwertery protokołów. Niestety w przypadku małego domu system automatyki, w którym wykorzystywane są wymienione wcześniej protokoły, może kosztować nawet kilkadziesiąt tysięcy złotych.

Komunikacja Z-wave

Rozwój technologii doprowadził do tego, że producenci systemów automatyki budynkowej znaleźli tańsze rozwiązania umożliwiające integrację systemów korzystających z energii elektrycznej. Jedną z wiodących technologii jest Z-wave, która wykorzystuje komunikację radiową (pasmo 868 MHz). Dzięki temu systemy wykorzystujące Z-wave można uruchamiać bez potrzeby zmiany wyposażenia domów czy mieszkań. Wystarczy korzystać z urządzeń zgodnych z wymienionymi protokołami lub zastosować specjalne adaptery zamontowane w urządzeniach lub gniazdkach elektrycznych. W ten sposób do instalacji oświetleniowej można podłączyć centralę, która umożliwia realizację zaprogramowanych scenariuszy oraz zdalne sterowanie odbiornikami energii elektrycznej.

Technologia Z-wave powstała dwanaście lat temu w Danii, a spopularyzowano ją około pięciu lat temu w USA. W rozwój Z-wave zaangażowały się międzynarodowe koncerny, takie jak GE, Honeywell, Samsung, Danfoss i inne. Urządzenia są produkowane z myślą o masowych zastosowaniach, więc ich cena szybko spada i stają się coraz bardziej popularne. Dzięki standaryzacji protokołu Z-wave jeden system może składać się z komponentów różnych producentów. Dostępne są także polskie urządzenia wykorzystujące technologię Z-wave, a niektóre z nich zdobyły nawet międzynarodowe nagrody za wzornictwo.

Zarządzanie energią

Jedną z głównych korzyści wynikających ze stosowania automatyki budynkowej jest możliwość ograniczenia zużycia energii elektrycznej. Z tego względu systemy automatyki budynkowej

Rys. 1. Przykład rozwiązania „Inteligentny Dom"

są najczęściej wykorzystywane do sterowania urządzeniami elektrycznymi, m.in. systemami oświetlenia oraz kontroli temperatury, których działanie zostaje uzależnione od obecności domowników i ich zwyczajów.

W przypadku nieobecności domowników instalacja oświetleniowa oraz urządzenia zużywające prąd nawet w trakcie czuwania (telewizor, komputer, kuchenka mikrofalowa itp.) są wyłączane, a temperatura w pomieszczeniach jest obniżana do pewnego ustalonego poziomu, np. 18°C. W ten sposób można ograniczyć zużycie prądu.

Przed powrotem domowników system może uruchomić pewne wybrane urządzenia (np. ekspres do kawy) i podwyższyć temperaturę w domu do 22°C. Scenariusz może być realizowany na podstawie założonego harmonogramu lub na podstawie ustalanej za pomocą GPS pozycji pojazdu użytkownika, który wraca z pracy lub wakacji i znajduje się w niewielkiej odległości od domu.

W przypadku obecności domowników w domu system będzie wyłączał oświetlenie w pomieszczeniach, w których nikt nie przebywa, sprawdzał, czy brama garażowa jest zamknięta, czy nie ma czynników powodujących wychłodzenie lub nadmierne nagrzanie domu itd. Dodatkowo system zaalarmuje użytkowników, gdy któreś z urządzeń zacznie zużywać więcej energii niż powinno, a także umożliwi zdalne odłączenie tego urządzenia.

To tylko niektóre z możliwych scenariuszy. Ich liczba zależy od potrzeb i wyobraźni użytkowników. Przy odpowiednim doborze scenariuszy użytkownicy mogą zoptymalizować korzystanie z urządzeń elektrycznych.

Należy spodziewać się, że wkrótce polscy dostawcy energii, wzorem dostawców z innych krajów europejskich, przygotują specjalne taryfy dla użytkowników systemów automatyki budynkowej i będą oferować swoim klientom urządzenia umożliwiające zdalne monitorowanie zużycia energii oraz zdalne wyłączanie urządzeń, które niepotrzebnie pobierają energię.

Automatyka domowa

Systemy automatyki budynkowej umożliwiają komfortowe korzystanie z wielu urządzeń elektrycznych, które normalnie działają niezależnie od siebie, ale w przypadku ich zintegrowania mogą być centralne zarządzane. Zaangażowanie się międzynarodowych korporacji w rozwój technologii Z-wave przyczyniło się do zwiększenia liczby kompatybilnych urządzeń dostępnych na rynku.

Główne zastosowania Z-wave:

1) Sterowanie oświetleniem. W przeciętnym domu jest ponad sto elementów oświetleniowych, więc do realizowania scenariuszy potrzebne są czujki obecności wykrywające nawet niewielki ruch (na przykład ruch osoby czytającej książkę), włączniki grupujące żarówki i reflektory, ściemniacze dostosowujące natężenie oświetlenia do pory dnia oraz adaptery gniazdkowe do sterowania pracą lampek biurkowych.
2) Kontrola temperatury. Praktycznie wszystkie domy są wyposażone w piecyki, podgrzewacze wody, klimatyzatory oraz wentylatory. Za pomocą termometrów, czujek wilgotności oraz stacji pogodowych można kontrolować temperaturę i dostosowywać ją do aktualnych potrzeb

Fot. 1. Przykładowy ekran aplikacji internetowej „Inteligentny Dom"

Fot. 2. Przykładowe ekrany aplikacji mobilnej „Inteligentny Dom"

użytkowników. W przypadku słonecznych dni albo wietrznych nocy można posłużyć się systemem sterowaniem rolet.

3) Sterowanie urządzeniami elektrycznymi. Do kontroli zużycia energii elektrycznej oraz sterowania urządzeniami elektrycznymi, takimi jak monitory, komputery, telewizory, służą uniwersalne przełączniki gniazdkowe. Część przełączników jest wyposażona w liczniki zużycia energii.
4) Zarządzanie bezpieczeństwem. Obecne systemy automatyki budynkowej pełnią też rolę systemów alarmowych. Mogą być wyposażone w czujki ruchu, czujki kontaktronowe w oknach i drzwiach, czujki zalania, czujki dymu oraz sygnalizatory. Do zarządzania systemem alarmowym służą klawiatury, piloty oraz aplikacje mobilne. Do ochrony mienia wykorzystywane są kamery IP z podstawowymi algorytmami analizy obrazu (zliczanie osób, detekcja pojawienia się albo zniknięcia obiektu, detekcja przekroczenia wyznaczonej linii).
5) Sterowanie systemami kontroli dostępu. Do sterowania systemami KD wykorzystywane są wideodomofony, zdalnie sterowane zamki oraz siłowniki. System steruje zamkami w drzwiach i bramach i automatycznie je otwiera albo zamyka – w zależności od scenariusza. Działanie takiego systemu jest podobne do działania zamka centralnego w samochodzie – po rozbrojeniu systemu alarmowego zamek w drzwiach od strony kierowcy zostaje automatycznie otwarty. W przypadku inteligentnego domu, otwierając bramę, można np. rozbroić system alarmowy i otworzyć zamek w drzwiach między garażem i domem, włączyć oświetlenie w garażu i obejrzeć obraz z kamer wokół domu na wyświetlaczu wmontowanym w klawiaturę.

Integracja systemów alarmowych

Wiele osób ma już systemy alarmowe. Część z nich nie chce w pełni integrować systemu alarmowego z systemem automatyki budynkowej, a jedynie korzystać z wybranych funkcji. Można jednak zintegrować oba systemy tak, by system automatyki mógł odczytywać status systemu alarmowego, zaś system alarmowy mógł inicjować wybrane scenariusze w systemie automatyki budynkowej.

Zestawy do samodzielnego montażu

Rozwój techniki pozwala na tworzenie urządzeń, które działają od razu po włączeniu zasilania. W przypadku technologii Z-wave uruchomienie i obsługa urządzeń jest na tyle prosta, że na rynku są dostępne zestawy do samodzielnego montażu, nazywane z angielska DIY (*do it yourself*). Urządzenia wchodzące w skład zestawów są zgrupowane tematycznie. Służą do zarządzania oświetleniem, sterowania urządzeniami elektrycznymi czy też zabezpieczenia domu przed włamaniem. Do sterownika systemu automatyki budynkowej wprowadzone są domyślne scenariusze, a część producentów umożliwia również zdalne zarządzanie poprzez udostępnianie zasobów systemowych w tak zwanej chmurze.

Zarządzanie systemem automatyki budynkowej

System automatyki budynkowej pozwala zarządzać wszystkimi zintegrowanymi systemami za pomocą jednej platformy programowej. Dzięki temu użytkownicy nie muszą uczyć się obsługi wielu różnych aplikacji. W praktyce, po przygotowaniu scenariuszy, system nie wymaga dodatkowej obsługi za pomocą komputera. Aplikacja jest wykorzystywana do wizualizacji stanu poszczególnych systemów oraz do podglądu obrazów z kamer.

W systemie automatyki budynkowej możliwe jest korzystanie z dobrodziejstw „chmury". Można umieszczać w niej dane dotyczące konfiguracji całego systemu oraz dzienniki systemowe. Zwiększa to niezawodność systemu i ułatwia jego odtworzenie w przypadku awarii, np. po przepięciach powstałych na skutek wyładowań atmosferycznych w trakcie burzy.

Kolejną zaletą nowoczesnych systemów automatyki budynkowej jest możliwość sterowania wszystkimi systemami w budynku za pomocą telefonu komórkowego lub tabletu. Wystarczy mieć dostęp do Internetu mobilnego, aby np. przed powrotem z urlopu włączyć w domu wybrane urządzenia, zwiększyć temperaturę w pomieszczeniach i uruchomić jacuzzi.

Podsumowanie

Omówione rozwiązania mają być przyjazne dla użytkowników, dlatego zintegrowane urządzenia są proste i wygodne w obsłudze. Aby je stworzyć, wykorzystuje się zaawansowane technologie komunikacji bezprzewodowej, platformy komunikacyjne, algorytmy analizy danych i wiele innych elementów. Systemy automatyki budynkowej są tak przygotowane, że użytkownik nie musi wykazywać się znajomością techniki – wystarczy, że potrafi obsługiwać telefon. Systemy te będą ciągle udoskonalane. Główny wpływ na ich rozwój będą miały firmy telekomunikacyjne oraz dostawcy energii elektrycznej. Możliwe, że kolejny krok milowy w rozwoju tej dziedziny techniki postawi firma Google, wdrażając projekt Android@Home wykorzystujący protokół komunikacyjny ZigBee. Przodujący producenci sprzętu już dziś umożliwiają sterowanie urządzeniami za pomocą tego protokołu, ale o tym napiszę innym razem.

Daniel Kamiński
Ochrona Juwentus

Technologia inteligentnej, dynamicznej redukcji szumów iDNR

Bosch Security Systems

Innowacyjne technologie wykorzystane w kamerach HD i kamerach megapikselowych firmy Bosch umożliwiają zmniejszenie wymagań dotyczących pasma sieciowego, a tym samym obniżenie kosztów transmisji, zapisu i przechowywania materiału wizyjnego w systemach dozorowych, i jednocześnie zachowanie dobrej rozróżnialności szczegółów i wysokiej jakości obrazu

Technologie przyczyniające się do zmniejszenia kosztów

Kamery megapikselowe wytwarzają użyteczne obrazy, na których można rozróżnić bardzo wiele szczegółów, lecz wiąże się to z pewnymi kosztami. Ilość danych niezbędnych do transmisji i zapisu obrazów rośnie wraz ze wzrostem ich rozdzielczości. Wynikający z tego wzrost obciążenia infrastruktury sieciowej oraz konieczność rozbudowy jednostek pamięciowych przekłada się na znaczny wzrost kosztów wdrożenia sieciowych systemów dozorowych. Przestrzeń dyskowa jest jednym z najkosztowniejszych składników takich systemów. W efekcie firmy oferujące kamery megapikselowe mają niewielkie szanse na pokonanie konkurentów podczas realizacji dużych projektów.

Najłatwiej zmniejszyć koszty transmisji i zapisu obrazów w miejscu, w którym te obrazy powstają, czyli w kamerach. Firma Bosch rozwiązuje problem ograniczenia ilości wytwarzanych danych kilkoma metodami:

– przez zastosowanie technologii obróbki obrazu opartej na analizie jego treści,
– przez wyznaczenie priorytetowych fragmentów obrazu, z których pochodzą najistotniejsze informacje,
– przez optymalizację pracy koderów w celu zapewnienia skuteczniejszej kompresji obrazu.

Jednoczesne zastosowanie tych trzech metod powoduje poprawę jakości obrazu w stosunku do przepływności strumienia wizyjnego, co bezpośrednio przekłada się na zmniejszenie kosztów infrastruktury sieciowej i jednostek pamięciowych.

Technologia obróbki obrazu oparta na analizie jego treści (CIBT) ma kluczowe znaczenie dla redukcji szumów

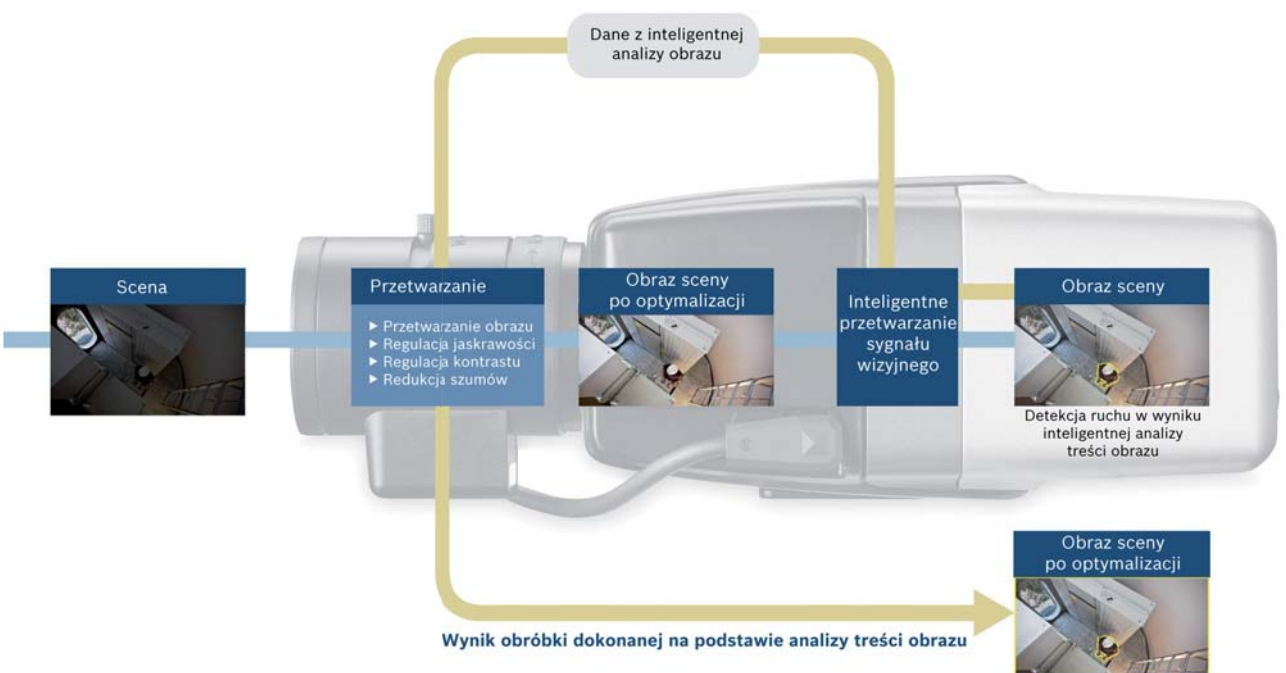
Szumy mają postać przypadkowych zmian w rozkładzie pikseli tworzących obraz telewizyjny i występują we wszystkich układach elektronicznych służących do wytwarzania, transmisji i rejestracji sygnałów wizyjnych. Nie można ich uniknąć. Można tylko zmniejszyć ich poziom. Szumy stanowią niepożądany produkt powstający w przetworniku optycznym podczas tworzenia obrazu i mają szkodliwy wpływ na dalszy przebieg procesu kodowania i transmisji sygnału wizyjnego. Ich obecność prowadzi do niczym nie uzasadnionego wzrostu przepływności wyjściowego strumienia wizyjnego. Kamery megapikselowe są bardziej podatne na wpływ szumów niż kamery o standardowej rozdzielczości, gdyż w ich przetwornikach piksele mają małe rozmiary, przez co mają ograniczoną zdolność do absorbowania światła. Sygnał wizyjny musi być silniej wzmacniany, co powoduje dalszy wzrost poziomu szumów. Obserwacja słabo oświetlonych scen wiąże się z zauważalnym wzrostem zaszumienia obrazu.

Firma Bosch jako pierwsza w branży opracowała nową technologię sterowania procesem obróbki obrazów, opartą na analizie treści tych obrazów. Zastosowana metoda sterowania pozwala na wytworzenie informacji zwrotnej i przekazanie jej do procesora sygnałowego DSP, dzięki czemu możliwa jest optymalizacja parametrów procesu obróbki sygnału wizyjnego.

Obecnie firma Bosch jest jedynym producentem kamer, w których sterowanie procesem obróbki obrazów odbywa się z wykorzystaniem metody inteligentnej analizy sygnału wizyjnego IVA i metody inteligentnej detekcji ruchu Motion+. Opracowanie innowacyjnej technologii CBIT umożliwiło stworzenie zintegrowanego układu scalonego, łączącego funkcje przetwornika obrazowego, cyfrowego procesora sygnałowego oraz modułu inteligentnej analizy sygnału wizyjnego. Technologia CBIT umożliwia radykalną poprawę jakości obrazu. Jej stosowanie przynosi jeszcze lepsze efekty, gdy jest wykorzystywana wraz z innymi technologiami zmniejszającymi poziom szumów w sygnale wizyjnym, takimi jak iDNR.

Metoda inteligentnej, dynamicznej redukcji szumów iDNR

Istnieją dwa klasyczne sposoby redukcji szumów – w wymiarze przestrzennym i w wymiarze czasowym. Z natury rzeczy szumy mają charakter losowy i wszelkie próby uśredniania sygnału wizyjnego prowadzą do ich redukcji. Redukcja



Rys. 1. Technologia obróbki obrazu oparta na analizie jego treści (CBIT)

szumów w wymiarze przestrzennym następuje dzięki uśrednianiu sygnałów z poszczególnych pikseli w obrębie jednej ramki telewizyjnej. Redukcja szumów w wymiarze czasowym następuje dzięki agregacji sygnałów z poszczególnych pikseli w obrębie kilku ramek telewizyjnych.

Do stworzenia metody inteligentnej, dynamicznej redukcji szumów iDNR wykorzystane zostały oba sposoby. Ich proporcjonalny udział w procesie redukcji szumów jest dynamicznie dostosowywany do poziomu oświetlenia obserwowanej sceny oraz do rozkładu ruchomych obiektów, wykrywanych w wyniku analizy treści obrazu metodą CBIT.

Fot. 1. Porównanie obrazu, na którym widoczne są wyraźne szumy (u góry), z obrazem, na którym poziom szumów został zredukowany (na dole)

Redukcja szumów w wymiarze czasowym jest bardzo skuteczna w przypadku nieruchomych obrazów, jednak może sprawić kłopoty w przypadku obserwacji obiektów ruchomych. W tym drugim przypadku na obrazie mogą wystąpić smugi, ruchome obiekty mogą ulec rozmyciu lub rozdwojeniu. Dzięki analizie treści obrazu metodą CBIT możliwe jest wykrywanie klatek, na których występują obiekty ruchome, i przekazywanie informacji zwrotnej do procesora DSP, który modyfikuje sposób redukcji szumów dla tych klatek.

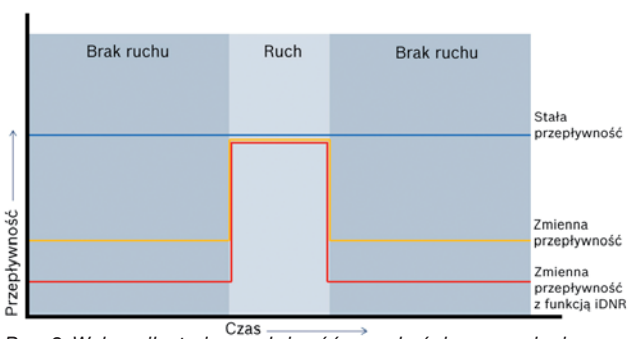
Podczas redukcji szumów metodą iDNR brane są pod uwagę trzy czynniki wpływające na proporcje redukcji w wymiarze przestrzennym i w wymiarze czasowym:

– wynik detekcji ruchu podczas analizy treści obrazów metodą CBIT,
– poziom oświetlenia obserwowanej sceny,
– ustawienia dokonywane przez użytkownika.

Dzięki wszystkim wymienionym czynnikom i zastosowaniu metody iDNR pasmo sieciowe jest wykorzystane w optymalny sposób. Stopień redukcji szumów jest dostosowany do bieżącej treści obrazu. Jeśli obraz jest nieruchomy lub intensywność ruchu jest niewielka, pasmo sieciowe jest wykorzystywane jedynie w niewielkim stopniu. Gdy w obserwowanej scenie pojawiają się obiekty ruchome, szerokość wykorzystywanego pasma wzrasta w celu zapewnienia dobrej reprodukcji szczegółów obrazu. W praktyce, podczas obserwacji pewnego rodzaju scen, zaawansowany algorytm detekcji ruchu stosowany w metodzie iDNR pozwala na zmniejszenie przepływności strumienia wizyjnego i ograniczenie wymaganej przestrzeni pamięciowej o około 50% – bez pogorszenia jakości obrazu.

Jaka jest zależność między zastosowaniem inteligentnej metody dynamicznej redukcji szumów iDNR a pracą kamery w trybie stałej lub zmiennej przepływności?

Kamery megapikselowe z zasady wykorzystują szerokie pasmo sieciowe, gdyż jest to niezbędne do transmisji obrazów o wysokiej rozdzielczości. W szczególności dotyczy to pracy kamer w trybie stałej przepływności CBR, w którym przepływność jest ustalana arbitralnie i utrzymywana na stałym poziomie. W przypadku sieci wąskopasmowych, przepływność spada i następuje wyraźne pogorszenie jakości obrazu.



Rys. 2. Wykres ilustrujący zależność szerokości pasma sieciowego od zastosowanych metod redukcji szumów

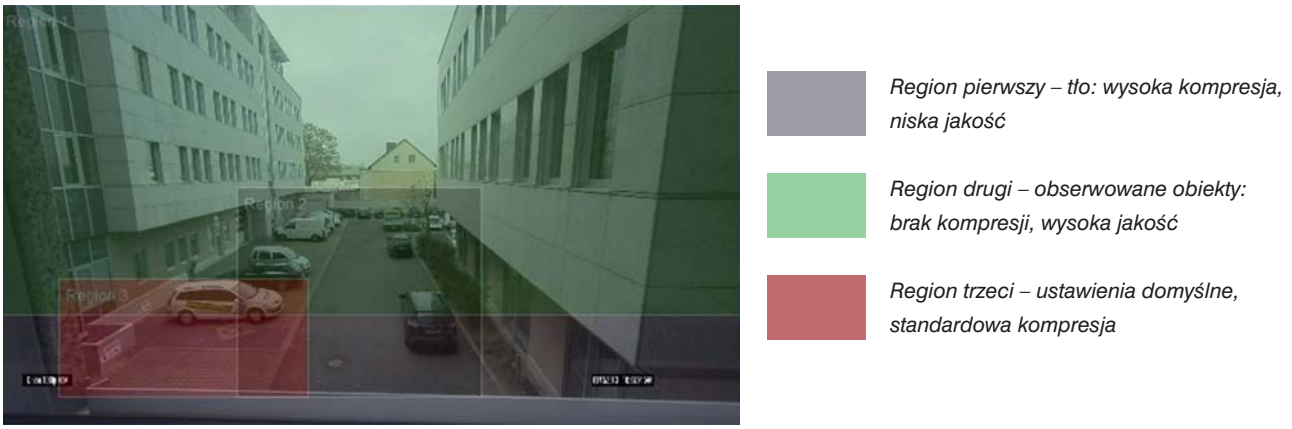
Z drugiej strony, podczas pracy kamery w trybie zmiennej przepływności VBR ustalany jest stały poziom jakości obrazu, który zostaje zachowany niezależnie od tego, czy obraz jest nieruchomy, czy w obserwowanej scenie występuje ruch. Pasmo sieciowe jest wykorzystywane w stopniu zależnym od intensywności tego ruchu.

W przypadku stosowania metody iDNR używany jest tryb pracy zbliżony do VBR, jednak podczas regulacji przepływności podejmowane są decyzje oparte na wynikach inteligentnej analizy treści obrazu. Regulacja przepływności w przypadku zastosowania metody iDNR jest lepsza, skuteczniejsza niż w trybie VBR.

Podział obrazu na fragmenty

Poza zmniejszeniem przepływności strumienia wizyjnego, uzyskanym dzięki zastosowaniu metody iDNR, możliwe jest dalsze jej zmniejszenie przez zróżnicowanie stopnia kompresji poszczególnych fragmentów obrazu.

Nieistotne fragmenty obrazu mogą podlegać silnej kompresji, co spowoduje znaczne zmniejszenie przepływności wyjściowego strumienia wizyjnego. Z kolei ważne fragmenty mogą w ogóle nie podlegać kompresji lub poziom kompresji może być niski, dzięki czemu będzie można



Fot. 2. Rozmieszczenie istotnych obszarów obrazu z podziałem na fragmenty różniące się sposobem kodowania oraz wymaganym pasmem sieciowym

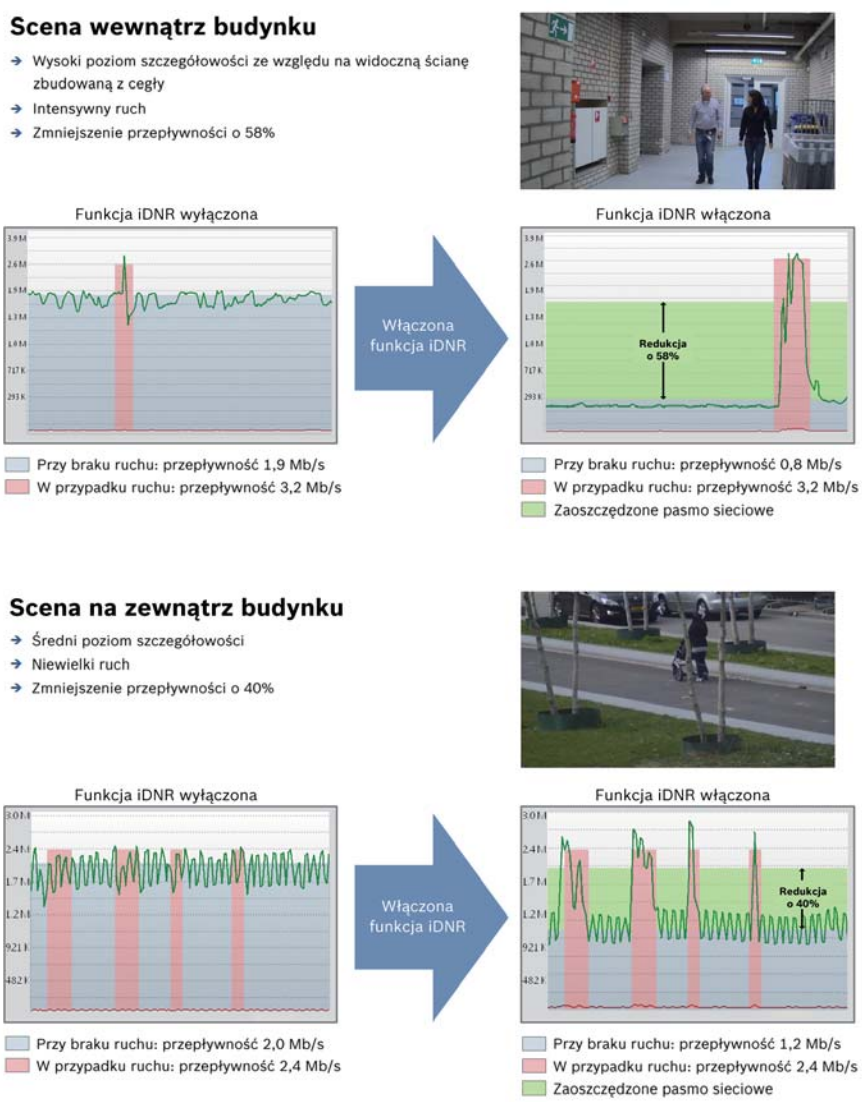
rozróżnić drobne szczegóły, zaś sumaryczna przepływność strumienia wizyjnego wzrośnie jedynie w niewielkim stopniu. Przez odpowiedni dobór wielkości i rozkładu poszczególnych fragmentów obrazu oraz przez przypisanie tym fragmentom odpowiednich poziomów kompresji można uzyskać znaczne obniżenie sumarycznej przepływności strumienia wizyjnego.

Wyniki

Korzystne efekty wynikające ze stosowania metody inteligentnej, dynamicznej redukcji szumów iDNR oraz ze zróżnicowania poziomów kompresji różnych fragmentów obrazu kumulują się, dzięki czemu wynikowy obraz odznacza się bardzo dobrą jakością, zaś sumaryczna przepływność strumienia wizyjnego jest niska. Wyniki uzyskane dzięki tej metodzie obróbki obrazów można prześledzić na rys. nr 3.

Jakie realne oszczędności można uzyskać dzięki metodzie iDNR?

Oszczędności uzyskiwane dzięki metodzie iDNR można łatwo obliczyć. Z przeprowadzonych testów wynika, że przepływność strumieni wizyjnych podczas obserwacji jednej z przykładowych scen zmalała o 58%. W dużych systemach dozorowych zależność kosztów związanych z zapotrzebowaniem na jednostki pamięciowe od sumarycznej przepływności zapisywanych strumieni wizyjnych jest w przybliżeniu liniowa. Oznacza to, że można obniżyć koszty zakupu jednostek pamięciowych w przybliżeniu o połowę, przy czym jakość zapisywanych obrazów i rozróżnialność szczegółów nie ulegnie zmianie.



Rys. 3. Na wykresie widoczne są obszary o zwiększonej przepływności, odpowiadające fragmentom obrazu, w których występuje intensywny ruch. W przypadku braku ruchu następuje znaczne zmniejszenie przepływności. Górne zdjęcie: wzrost przepływności następuje jedynie wtedy, gdy widoczne są osoby przechodzące przez korytarz; dolne zdjęcie: wzrost przepływności następuje jedynie wtedy, gdy widoczne są samochody przejeżdżające ulicą

Przykładowa scena: *budynki*
Opis sceny: *mała liczba szczegółów, brak ruchu*
Obniżenie przepływności: *48%*

Przykładowa scena: *wentylator*
Opis sceny: *duża liczba szczegółów, intensywny ruch*
Obniżenie przepływności: *33%*

Przykładowa scena: *ceglana ściana*
Opis sceny: *duża liczba szczegółów, intensywny ruch*
Obniżenie przepływności: *58%*

Przykładowa scena: *alejka*
Opis sceny: *średnia liczba szczegółów, intensywny ruch*
Obniżenie przepływności: *40%*

Konkluzja

Dzięki metodzie iDNR firmy Bosch możliwe jest uzależnienie sposobu obróbki sygnału wizyjnego od treści przekazywanego obrazu. W efekcie stopień redukcji szumów będzie zależny od poziomu oświetlenia i intensywności ruchu w obserwowanej scenie. Dzięki temu w przypadku nieruchomych obrazów przepływność wyjściowego strumienia wizyjnego może być o 50% mniejsza niż w trybie VBR. Analiza treści obrazów metodą CBIT pozwala na dalsze zmniejszenie przepływności, więc wymagana przestrzeń dyskowa jest o połowę mniejsza i potrzebnych jest mniej jednostek pamięciowych. Kolejne konsekwencje to mniejsze zużycie energii i ograniczenie emisji ciepła, co również ma przełożenie na oszczędności i oczywiście korzystny wpływ na środowisko naturalne.

Należy pamiętać, że w każdej kamerze można zmniejszyć przepływność wyjściowego strumienia wizyjnego, lecz w przypadku klasycznych rozwiązań powoduje to pogorszenie jakości obrazu. Podstawową korzyścią wynikającą z zastosowania metody iDNR oraz podziału obrazu na mniej i bardziej istotne fragmenty jest ograniczenie przepływności wyjściowego strumienia wizyjnego bez pogorszenia jakości obrazu.

Dzięki zachowaniu równowagi między jakością obrazu a zajmowanym pasmem sieciowym kamery firmy Bosch są dla użytkowników końcowych bardzo atrakcyjnym produktem, gdyż umożliwiają dobrą reprodukcję szczegółów obserwowanych scen i zarazem ograniczenie kosztów wdrożenia i eksploatacji systemów dozorowych.

Bosch Security Systems

Arecont Vision

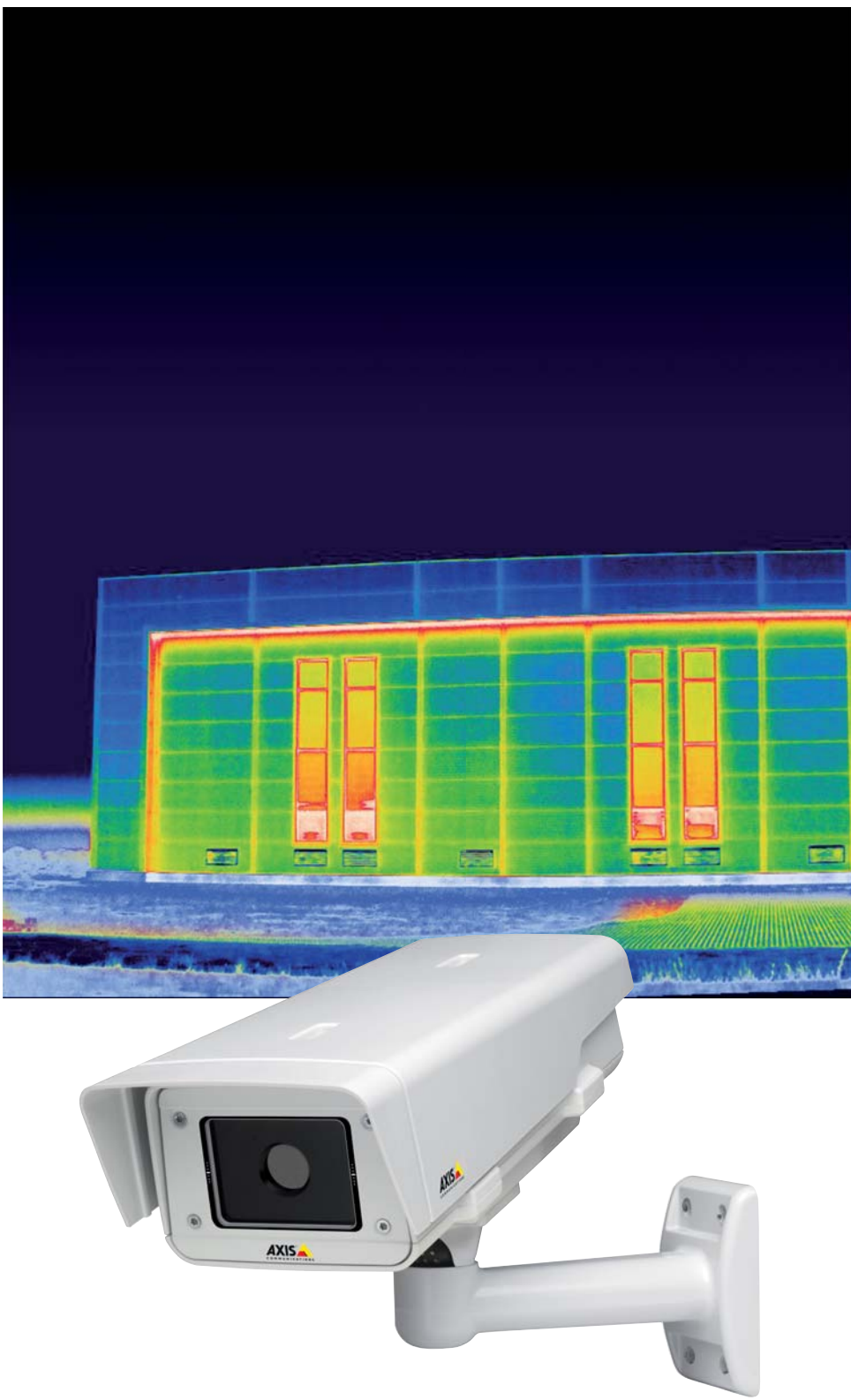
1,3 MP | 2 MP | 3 MP | 5 MP | 10 MP | 20 MP | 40 MP

zamów najnowszy katalog 2014

Termowizja staje się dostępna na co dzień

Martin Gren

Technika termowizyjna w różnych odmianach była dotychczas wykorzystywana jedynie przez wojsko, służby specjalne oraz służby ratownictwa. Pokazywane czasami w telewizyjnych programach informacyjnych obrazy termowizyjne pochodzą przeważnie z kosztownych kamer umieszczanych na helikopterach biorących udział w działaniach operacyjnych. Przykładem może być maraton w Bostonie. W trakcie tego maratonu napastnik strzelał do ludzi, a następnie ukrył się w łodzi wyciągniętej na zimę na nabrzeże. Nie zdawał sobie sprawy z tego, że nie może czuć się bezpiecznie, gdyż zostanie wykryty przez kamery termowizyjne i w następstwie tego schwytany



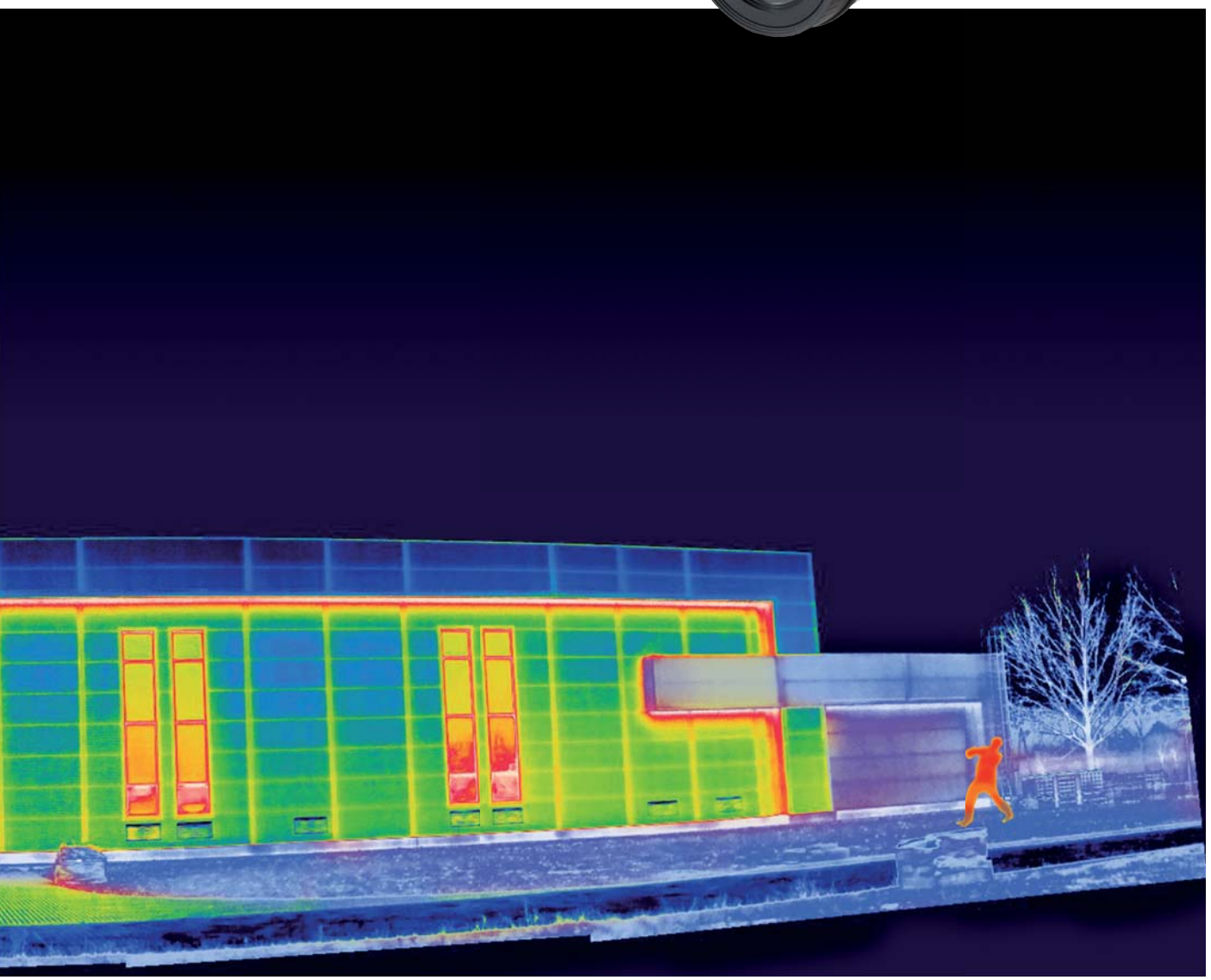
Fot. 1. Kamera AXIS Q1921-E widziana z lewej strony

W przeszłości jedynymi obszarami cywilnych zastosowań termowizji były systemy zabezpieczające gazociągi i rafinerie naftowe oraz obiekty infrastruktury krytycznej. Obecnie, dzięki usprawnieniu konstrukcji kamer termowizyjnych oraz obniżeniu kosztów ich produkcji, termowizja stała się naturalnym składnikiem wizyjnych systemów dozorowych.

Fot. 2. Sieciowa kamera termowizyjna AXIS Q1931-E przymocowana do ściany

Dlaczego termowizja jest skuteczna?

Podstawową zaletą termowizyjnych systemów dozorowych jest to, że trudno się przed nimi ukryć. Zespół Mythbusters, występujący w programie „Crime and Myth-Demeanors" na kanale Discovery, podjął trud oszukania czujników termicznych. Uczestnicy programu zakładali na siebie czarne ubrania, pokrywali swoje ciała grubą warstwą błota, ubierali się w kombinezony służące do nurkowania, a nawet wkładali stroje upodabniające ich do gigantycznych kurczaków. Nie pozwoliło to oszukać kamer termowizyjnych. Jedyną metodą na ukrycie się było zastosowanie dużych szklanych tarczy, jednak nawet one nie zapobiegły alarmowi, gdyż kamery termowizyjne wykrywały obecność dziwnych czarnych przedmiotów, wyraźnie odróżniających się od tła.



Ceny kamer termowizyjnych są nadal bardzo wysokie, jednakże korzyści, jakie wynikają z ich stosowania, rekompensują koszty, dlatego wykorzystuje je wielu profesjonalistów.

W przypadku kamer termowizyjnych z wewnętrznym, wbudowanym procesorem analizującym treść obrazu ilość błędów, a tym samym liczba nieuzasadnionych alarmów, jest znacznie niższa niż w przypadku kamer pracujących w widmie optycznym. Przed kamerami termowizyjnymi trudno się ukryć, dlatego znajdują one zastosowanie w wielu dziedzinach gospodarki.

Transport kolejowy

Zastosowanie kamer termowizyjnych stwarza zupełnie nowe możliwości wykrywania ludzi w miejscach, w których nikt niepowołany nie powinien przebywać. Na przykład można w ten sposób wykrywać wandali malujących graffiti na wagonach stojących na bocznicy. Na podobnej zasadzie można wykrywać

Fot. 3. Sieciowa kamera termowizyjna AXIS Q1931-E przymocowana do sufitu

próby kradzieży miedzianych przewodów trakcji elektrycznej, gdyż kamery termowizyjne wyposażone w długoogniskowe obiektywy mogą obserwować torowiska na wielokilometrowych odcinkach i wykrywać intruzów przez cała dobę i przez siedem dni w tygodniu.

Infrastruktura krytyczna

Kamery termowizyjne są wykorzystywane w systemach zabezpieczających takie obiekty jak zbiorniki wodne, elektrownie wodne i atomowe, rurociągi i inne instalacje podatne na sabotaż. Dzięki funkcjom detekcji ruchu kamery termowizyjne mogą na przykład uruchamiać oświetlenie na wybranych obszarach, dzięki czemu możliwa jest weryfikacja przyczyn alarmów z wykorzystaniem klasycznych kamer pracujących w widmie optycznym.

Handel detaliczny

Do dużego obiektu handlowego najłatwiej włamać się, przechodząc przez okna umieszczone na suficie, tymczasem do zabezpieczenia każdej z krawędzi dachu wystarczy użyć dwóch kamer termowizyjnych. Koszty są znacznie niższe niż w przypadku zastosowania innego rodzaju czujników, zabezpieczających indywidualnie poszczególne okna. Ponadto często zdarza się, że obiekty handlowe pozostają oświetlone przez całą noc w celu odstraszenia potencjalnych włamywaczy. Stosując kamery termowizyjne, można zmniejszyć koszt oświetlenia – światło może być włączane dopiero po wykryciu intruzów na chronionym obszarze.

Szkolnictwo

W tej dziedzinie także można znaleźć wiele zastosowań dla kamer termowizyjnych. Dotyczy to szczególnie Skandynawii, gdzie uzyskanie zezwoleń na instalację kamer pracujących w widmie optycznym na terenie szkół bywa trudne lub nawet niemożliwe. Przyczyną są restrykcyjne przepisy dotyczące ochrony prywatności. Z drugiej strony często mamy do czynienia z aktami wandalizmu, nielegalnym malowaniem graffiti na ścianach budynków szkolnych, podpaleniami czy mobbingiem, co stanowi trudną do zwalczenia plagę oraz naraża placówki szkolne na znaczne wydatki. Sposobem przeciwdziałania jest zastosowanie kamer termowizyjnych, które mają niską rozdzielczość i nie umożliwiają identyfikacji osób, więc nie naruszają przepisów dotyczących ochrony prywatności. W jednej ze szkół na terenie Szwecji wielokrotnie dochodziło do podpaleń. Problemu nie można było rozwiązać przez siedem miesięcy. Dopiero zainstalowanie kamer termowizyjnych odstraszyło podpalaczy i położyło kres temu procederowi.

Wykorzystanie kamer termowizyjnych

W jaki sposób można najlepiej wykorzystać kamery termowizyjne? Jeśli chcemy polegać na ich zdolnościach analitycznych, należy pamiętać, że nawet najlepsza technika detekcji ruchu nie daje stuprocentowej pewności wykrywania intruzów. Należy stosować kamery termowizyjne o jak najwyższej jakości. Użyteczny obraz powinien mieć możliwie wysoką rozdzielczość i wysoki kontrast. Wykrywanie obecności ludzi może być trudne, jeżeli kamery będą rozgrzewać się za dnia i stygnąć o zmierzchu.

Należy pamiętać, że najlepszym uzupełnieniem kamery termowizyjnej jest dobra, czuła kamera pracująca w widmie optycznym. Podstawową zaletą sieciowych kamer termowizyjnych jest możliwość podłączenia ich do sieci, w której pracują klasyczne kamery dozorowe. Umożliwia to integrację wszystkich kamer i tworzenie zespolonych, centralnie zarządzanych systemów obserwacyjnych.

Inne istotne cechy kamer termowizyjnych to inteligentna analiza treści obrazu, możliwość lokalnej rejestracji materiału wizyjnego, możliwość zasilania metodą PoE, prostota instalacji.

Możliwość integracji kamer termowizyjnych i kamer pracujących w widmie optycznym ma decydujący wpływ na działanie systemów dozorowych. Dotychczas kamery termowizyjne były rzadko stosowane i jeśli w ogóle są wykorzystywane w danym systemie, to stanowią zaledwie 10% ogólnej liczby pracujących w nim kamer. Ich główną funkcją jest generowanie alarmów, których przyczyny są weryfikowane za pomocą kamer pracujących w widmie optycznym, zatem istotna jest możliwość podłączenia wszystkich kamer do jednej sieci i centralnego zarządzania całym systemem. Jeśli już dochodzi do stosowania kamer termowizyjnych, funkcje analityczne powinny być realizowane przez procesory i oprogramowanie wbudowane w te kamery. W ten sposób uzyskuje się znacznie lepsze rezultaty niż w przypadku realizacji funkcji analitycznych na serwerach sterujących pracą całych systemów.

Jaka przyszłość czeka kamery termowizyjne?

Firma Axis wstępnie zakłada, że w przyszłości na jedną sprzedaną kamerę termowizyjną będzie przypadać pięćdziesiąt kamer pracujących w widmie optycznym. Obecnie ta proporcja wynosi jeden do dwustu. Można jednak spotkać specyficzne profesjonalne instalacje, w przypadku których proporcja wynosi jeden do dziesięciu. Dotyczy to takich obiektów jak budynki użyteczności publicznej, centra handlowe, budynki szkolne i oczywiście obiekty penitencjarne i więzienia, w których stosowanie kamer termowizyjnych stało się już normą.

Wkrótce kamery termowizyjne będą stanowiły istotny składnik wszystkich dużych systemów dozorowych i będą obiektem zainteresowania projektantów tych systemów.

Fot. 4. Kamera AXIS Q1922-E widziana od przodu

Martin Gren
współzałożyciel firmy Axis Communications

Zgoda na przetwarzanie danych osobowych
Wszystko, co trzeba wiedzieć

Monika Brzozowska-Pasieka

W ostatnim czasie coraz częściej pojawiają się kwestie związane z udzielaniem zgody na przetwarzanie danych osobowych. Klienci kancelarii pytają m.in. o przedstawiane do podpisu oświadczenia w formie cyfrowej, na przykład w Internecie, a także o to, czy można wycofać zgodę na przetwarzanie danych osobowych, która została wyrażona w ten sposób. Przedsiębiorcy są zainteresowani informacjami dotyczącymi warunków uzyskania czyjejś zgody (np. pytają o to, czy połączenie przedstawianego do podpisu oświadczenia mającego na celu uzyskanie czyjejś zgody na przetwarzanie danych osobowych z innymi oświadczeniami będzie poprawne)

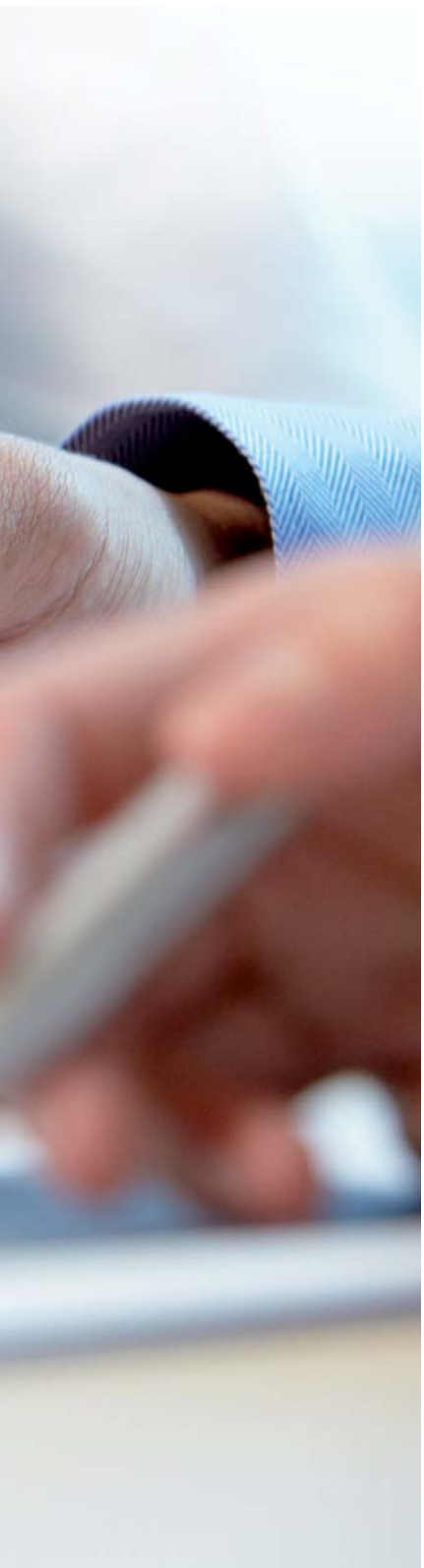
Należy rozprawić się z kilkoma mitami dotyczącymi zgody na przetwarzanie danych osobowych w świetle ustawy o ochronie danych osobowych.

Mit pierwszy

Na przetwarzanie danych osobowych zawsze potrzebna jest zgoda. Jeżeli nie ma zgody – nie można ich przetwarzać.

Nic bardziej błędnego. Zgodnie bowiem z art. 23 ust. 1 przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych;
2) jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
3) jest to konieczne do realizacji umowy – gdy osoba, której dane dotyczą, jest jej stroną – lub niezbędne do podjęcia działań przed zawarciem umowy (na żądanie osoby, której dane dotyczą);
4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
5) jest to niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.



Oznacza to, że jest aż pięć warunków legalnego przetwarzania danych osobowych, zaś zgoda osoby zainteresowanej jest tylko jednym z nich.

Mit drugi

Zgoda raz dana nie może być odwołana.

Nieprawda. Zgodnie z art. 7 pkt 5 ustawy zgoda to oświadczenie woli, którego treścią jest przyzwolenie na przetwarzanie danych osoby, która składa oświadczenie. Zgoda nie może być domniemana ani dorozumiana z oświadczenia woli o innej treści i może być odwołana w dowolnym momencie.

Mit trzeci

Zgoda może być wyrażona jedynie na piśmie z własnoręcznym podpisem. Brak wyrażonej w ten sposób zgody (zgoda ustna, zgoda wyrażona w e-mailu, SMS-ie lub na stronie WWW poprzez kliknięcie odpowiedniego miejsca) oznacza, że nie można przetwarzać danych osobowych.

Nic bardziej błędnego. Samo pojęcie „oświadczenie woli" nie jest nigdzie w ustawie zdefiniowane, co jest plusem tej regulacji. Ustawodawca doszedł bowiem do wniosku, że zostało ono dostatecznie zdefiniowane w kodeksie cywilnym i nie ma konieczności tworzenia jakichkolwiek nowych definicji. Zgodnie z art. 60 kodeksu cywilnego: „Z zastrzeżeniem wyjątków w ustawie przewidzianych, wola osoby dokonującej czynności prawnej może być wyrażona przez każde zachowanie się tej osoby, które ujawnia jej wolę w sposób dostateczny, w tym również przez ujawnienie tej woli w postaci elektronicznej (oświadczenie woli)".

Mit czwarty

Nie trzeba podawać celu przetwarzania. Wystarczy formułka „Wyrażam zgodę na przetwarzanie moich danych osobowych" oraz podpis.

Warto pamiętać, że upoważnienia do przetwarzania danych osobowych nie można podpisać *in blanco* – wyrażający zgodę powinien mieć świadomość, jakie dane, w jakim celu i gdzie będą przetwarzane (gdzie jest siedziba administratora danych), a także wiedzieć, czy będą one poddawane dalszemu przetwarzaniu. Wydaje się, że jeżeli administrator nie uzyskał zgody na udostępnienie danych innemu administratorowi, nie będzie mógł ich udostępnić na podstawie uzyskanego oświadczenia woli – konieczna jest dodatkowa zgoda osoby, której dane dotyczą. Za innego administratora nie uznaje się podmiotu przetwarzającego dane na zlecenie administratora.

Mit piąty

Wystarczy „ukryć" zapis wyrażający zgodę na przetwarzanie danych osobowych w innych oświadczeniach przedstawianych do podpisu (lub np. w odrębnym regulaminie, zapisie itp.), aby uzyskać czyjąś zgodę.

Zgoda musi być wyraźna. Nie może być ani domniemana, ani dorozumiana z oświadczeń woli o innej treści. Klauzula o zgodzie powinna być tak wyodrębniona, by można było jednocześnie odmówić wyrażenia zgody na przetwarzanie danych osobowych i zgodzić się na inne warunki. Często pod oświadczeniami przedstawianymi do podpisu (np. mającymi na celu uzyskanie zgody na przesyłanie korespondencji o charakterze reklamowym, na wykorzystanie wizerunku itp.) widnieje miejsce na podpis osoby zainteresowanej (lub „okienko", które trzeba zaznaczyć w przypadku oświadczeń w postaci cyfrowej). Zgodą na przetwarzanie danych osobowych nie jest niewyrażenie sprzeciwu.

Mit szósty

Nie można udzielić zgody na przetwarzanie danych w przyszłości.

Powyższe zdanie – często przytaczane przez naszych Klientów – jest dość nieprecyzyjne. Zgoda może być wyrażona na przyszłość – zgodnie z art. 23 ust. 2 zgoda może dotyczyć

również przetwarzania danych w przyszłości, jeżeli nie zmieni się cel przetwarzania.

Mit siódmy

Nawet na wykasowanie danych trzeba mieć zgodę osoby zainteresowanej.

Powyższe stwierdzenie jest nieprawdziwe. Nie jest wymagana zgoda na usunięcie danych – w przypadku usuwania danych osobowych nie trzeba mieć zgody osoby, której dane dotyczą.

W Internecie wysłanie odpowiedniego formularza z zaznaczonym polem przy sformułowaniu typu „Wyrażam zgodę na przetwarzanie moich danych" jest równoznaczne z udzieleniem zgody na przetwarzanie danych osobowych. W razie wątpliwości administrator będzie musiał udowodnić, że taką zgodę posiada – zgodnie z rozkładem ciężaru dowodowego z art. 6 kc.

Zupełnie inaczej jest w przypadku wrażliwych danych osobowych (do takich danych należą dane o zdrowiu, nałogach itp. – opisane szeroko w art. 27). Ustawa wprowadza bowiem konieczność uzyskania zgody pisemnej (na równi ze zgodą pisemną będzie uznawana zgoda z podpisem cyfrowym). Oznacza to, że opisany wyżej sposób wyrażania i otrzymywania zgody nie jest w tym przypadku właściwy – chyba że formularz zostanie opatrzony podpisem cyfrowym.

W kontekście „cyfrowych" form wyrażania zgody pojawia się szereg wątpliwości dotyczących weryfikacji podmiotu udzielającego zgody, rozumienia wad oświadczenia woli w cyberprzestrzeni czy też możliwości odwołania zgody. Weryfikacja udzielającego zgody może być w wielu przypadkach znacznie utrudniona lub nawet niemożliwa, co oczywiście może doprowadzić do zaprzeczenia wyrażeniu zgody przez daną osobę. W takich sytuacjach podmiot przetwarzający dane najczęściej broni się, wysyłając potwierdzenie zgody na podany adres e-mailowy, ale to nie zawsze wystarczy. Trzeba zauważyć, że w wielu portalach internetowych do zalogowania wystarczy imię i nazwisko oraz adres e-mailowy, co nie jest równoznaczne z weryfikacją tożsamości użytkownika.

Podsumowanie

Zgoda osoby zainteresowanej jest tylko jednym z warunków legalnego przetwarzania danych osobowych. Zgoda może być wyrażona na wiele sposobów – także „cyfrowo". W przypadku danych wrażliwych ważna jest tylko zgoda na piśmie lub z cyfrowym podpisem.

Przedstawiane do akceptacji sformułowania mające na celu uzyskanie czyjejś zgody na przetwarzanie danych osobowych muszą być wyraźnie wyodrębnione – nie mogą być ukryte.

Wyrażenie zgody w formie cyfrowej może rodzić wątpliwości co do możliwości weryfikacji osoby, która taką zgodą wyraziła, lub być wadliwym oświadczeniem woli.

Monika Brzozowska-Pasieka
dyrektor Departamentu Danych Osobowych
w kancelarii Pasieka, Derlikowski, Brzozowska i Partnerzy,
ekspert Instytutu Sobieskiego

Security Products SINCE 1991 roger

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

Wprowadzono do oferty RCI-2 – nowy interfejs komunikacyjny USB-RS485

- zaprojektowany dla systemu kontroli dostępu RACS
- separacja galwaniczna magistrali RS485 od portu USB PC
- oprogramowanie emulujące port szeregowy COM
- obudowa z tworzywa sztucznego do montażu na szynie DIN

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

roger®

FARGO C50

Profesjonalna drukarka do kart plastikowych za rozsądną cenę

FARGO®

Niedroga i prosta w obsłudze drukarka kart plastikowych przeznaczona dla małych przedsiębiorstw, szkół i lokalnych urzędów, potrafi w krótkim czasie drukować identyfikatory, karty lojalnościowe, legitymacje pracownicze itp.
Gotowa do druku od razu po wyjęciu z pudełka. Dzięki nowoczesnej, kompaktowej konstrukcji, drukarka nie wymaga praktycznie żadnej konserwacji i można ją łatwo dopasować nawet do najmniejszych pomieszczeń biurowych.
Zaprojektowana z myślą o wydajności, drukarka C50 jest wyposażona we wbudowane oprogramowanie do tworzenia identyfikatorów, automatyczne narzędzia diagnostyczne i prosty system instalacji taśm umieszczonych w kartridżu z funkcją samooczyszczania karty.
Drukarka posiada dwuletnią gwarancją 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: termosublimacja, termotransfer
- Rozdzielczość wydruku: 300 dpi
- Kolory: 16,7 mln/256 odcieni na piksel
- Prędkość nadruku: nadruk jednostronny mono 500 kart/h, kolor 150 kart/h.
- Obsługiwane karty: PVC, poliestrowe z wykończeniem PVC, karty wielokrotnego nadruku, rozmiary ISO CR-80 oraz samoprzylepne CR-79 o grubości od 0,229 mm do 1,016 mm
- Podajnik na 50 kart
- Odbiornik na 30 kart
- Interfejs do PC: USB
- Pamięć RAM: 32 MB
- Sterowniki: Windows XP, Vista (32 i 64 bity), Server 2003 i 2008, Windows 8 (32 i 64 bity), MAC OS X 10.5/10.6/10.7/10.8, Linux
- Oprogramowanie: wbudowana aplikacja Swift ID oraz program diagnostyczny FARGO Workbench
- Zabezpieczenia: kompatybilność z Kensington lock
- Wymiary drukarki jednostronnej: 224×348×201 mm/3,4 kg
- Gwarancja: 2 lata

Taśmy

- Taśmy standardowe w kasetach z rolką czyszczącą (EZ): kolorowa YMCKO, monochromatyczne: czarna rezinowa K, zielona, niebieska, czerwona, biała, srebrna i złota
- Bardziej ekonomiczne i ekologiczne, taśmy wymienne bez kasety (ECO): kolorowa YMCKO, czarna rezinowa K
- Nadruk wielokrotny – nie wymaga taśmy

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.ckp.com.pl

FARGO HDP8500

Drukarka retransferowa – grawerowanie kart, praca ciągła

Jedyna na rynku drukarka retransferowa **przeznaczona do pracy ciągłej z możliwością laserowego grawerowania kart**. Posiada znakomite parametry techniczne, wyposażona jest w moduły i rozwiązania niespotykane w innych drukarkach. Daje najwyższej jakości nadruk na kartach plastikowych. Przeznaczona dla wyspecjalizowanych centrów personalizacji kart, banków, wyższych uczelni, organizacji państwowych, wojska i dużych korporacji.

W połączeniu z rozbudowanym oprogramowaniem Assure ID do nadruku, personalizacji, kodowania i zarządzania kartą stanowi kompletny system, kompatybilny z wieloma bazami danych.

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

Charakterystyka

- Wielowątkowy tryb pracy – symultaniczne kodowanie, drukowanie i laminowanie. Dodatkowe dwa tryby: wysoka wydajność lub jakość nadruku
- W standardzie posiada: serwer ethernetowy, moduł dwustronny oraz dwa zamykane podajniki o łącznej pojemności 400 kart
- Solidna metalowa obudowa ze specjalnymi zamknięciami ograniczającymi dostęp do kaset z materiałami eksploatacyjnymi
- Dotykowy wyświetlacz LCD z możliwością wprowadzenia kodu PIN
- Wydłużony 3 letni okres gwarancyjny
- Zabezpieczenie nadruku wytrzymałymi materiałami eksploatacyjnymi
- System przepływu i filtracji powietrza
- Dwa moduły czyszczące i pełen wgląd w ścieżkę transportu karty we wnętrzu drukarki
- Szyfrowanie danych przesyłanych do drukarki oraz wymazywanie danych osobowych z panelu K.
- **Moduł do prostowania kart**
- **Moduł do laserowego grawerowania kart**

Parametry techniczne

- Rodzaj nadruku: dwustronny, termosublimacja retransferowa
- Rozdzielczość wydruku: 300 dpi
- Kolory: 16,7 mln/256 odcieni na piksel
- Szybkość nadruku: YMCK do 1000 kart/8 godzin ciągłej pracy; YMC do 1200 kart/8 godzin ciągłej pracy; YMCKK do 720 kart/8 godzin ciągłej pracy
- Obsługiwane karty: rozmiar – CR-80 (85,6×54 mm), grubość – 0,762~1,27 mm
- Pamięć: 32 MB
- Sterowniki: Windows XP, 7 (32 i 64 bity), Server 2003 i 2008 R2 (64 bity), Vista (32 i 64 bity), Mac OS X v10.4/v10.5, Linux
- Interfejs: USB 2.0 i Ethernet w standardzie
- Wyświetlacz: dotykowy, pełnokolorowy LCD 3,2"
- Podajnik: 400 kart, dodatkowa sygnalizacja braku kart w podajniku
- Odbiornik: 200 kart
- Oprogramowanie: FARGO Workbench – program diagnostyczny z asystentem punktowego dopasowania koloru
- Moduł czyszczący 2 sztuki
- Wymiary: wersja podstawowa: 39,4×71,6×35,6 cm/27,7 kg
- Obsługiwane taśmy: YMC, YMCK, YMCKK, ymcKT, filmy retransferowe, taśmy fluorescencyjne/UV
- Dodatkowe opcje: korektor odkształceń kart, laser grawerujący, laminator, laminatom dwustronny, wskaźniki świetlne do zdalnego nadzoru pracy urządzenia
- Opcje koderów: koder paska magnetycznego, kodery kart stykowych i zbliżeniowych

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.ckp.com.pl

Kamera kopułkowa DH-HAC-HDW2100M z wyjściem HDCVI

Rozdzielczość 1,3 megapiksela, standard 720p, wodoszczelna, z oświetlaczem IR

Dane techniczne kamery

- Przetwornik CMOS 1/3" 1,3 megapikseli
- Poklatkowość 25/30/50/60 w standardzie 720p
- Szybka transmisja obrazu na duże odległości
- Przełączany tryb pracy HD-SD
- Menu ekranowe, sterowanie za pośrednictwem kabla koncentrycznego
- Tryby pracy: dzień/noc, automatyczny balans bieli, automatyczna regulacja wzmocnienia, kompensacja tylnego oświetlenia, dynamiczna redukcja szumów
- Obiektyw stałoogniskowy 3,6 mm (opcjonalnie 2,8 mm, 6 mm, 8 mm)
- Zasięg oświetlenia IR równy 20 m, automatyczna regulacja oświetlenia IR
- Stopień szczelności obudowy IP66
- Zasilanie 12 V_{DC}

Model	DH-HAC-HDW2100MP	DH-HAC-HDW2100MN
Podstawowe właściwości		
Przetwornik	CMOS 1/3" 1,3 megapikseli	
Efektywna liczba pikseli	1280(H)×720(V)	
Migawka elektroniczna	1/25 s~1/45,000 s	1/30 s~1/54,000 s
Poklatkowość	25 kl./s przy 1280×720 50 kl./s przy 1280×720	30 kl/s przy 1280×720 60 kl/s przy 1280×720
Synchronizacja	Wewnętrzna	
Minimalny poziom oświetlenia	0,01 lx przy F1.2 (AGC włączone), 0 lx przy włączonym oświetleniu IR	
Wyjście wizyjne	BNC - wyjście sygnału HDCVI o wysokiej rozdzielczości lub sygnału CVBS o standardowej rozdzielczości (przełączane)	
Inne właściwości		
Zasięg oświetlenia IR	20 m, automatyczna regulacja oświetlenia IR	
Tryb dzień/noc	Automatyczne lub ręczne przełączanie między pracą w trybie kolorowym a pracą w trybie monochromatycznym	
Redukcja szumów	Metodą 3D lub 2D	
Menu ekranowe	Tak	
Obiektyw		
Ogniskowa	3,6 mm (opcjonalnie 2.8 mm, 6 mm, 8 mm)	
Zamocowanie	M12	
Warunki pracy		
Zasilanie	12 V_{DC} ±10%	
Pobór mocy	maks. 6 W	
Warunki środowiskowe	temp. od -30°C do 60°C wilgotność względna poniżej 95% bez kondensacji	
Transmisja obrazów	na odległość do 500 m za pomocą kabla koncentrycznego	
Stopień szczelności obudowy	IP66	
Wymiary zewnętrzne	Średnica 94,0 mm, długość 98 mm	
Masa	0,33 kg	

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

Rejestratory NUUO NVR SOLO

Rejestratory NUUO NVR SOLO są urządzeniami sieciowymi typu *stand-alone* zbudowanymi w oparciu o niezawodny system operacyjny Linux. Można obsługiwać je tak samo, jak rejestratory analogowe (tj. z użyciem myszki komputerowej podłączonej do złącza USB) i wyświetlać obraz na monitorze podłączonym do lokalnego portu HDMI/VGA, a także zarządzać ze stacji klienckiej poprzez sieć komputerową. Lista kamer kompatybilnych z rejestratorami SOLO obejmuje obecnie ponad 2300 modeli blisko 100 producentów i systematycznie się powiększa. Rejestratory SOLO mają specjalną funkcję nazywaną ezNUUO, pozwalającą na dostęp do rejestratora poprzez sieć Internet (zarówno przez klientów komputerowych, jak i mobilnych) z pominięciem konfiguracji przekierowań na ruterach dostępowych. Urządzenia te mogą współpracować z punktami POS i innymi systemami zewnętrznymi, dzięki czemu możliwe jest nakładanie danych (np. z kas fiskalnych) na obraz z kamer oraz na późniejsze szybkie wyszukiwanie odpowiednich nagrań po ciągach tekstowych. Rejestratory SOLO należą do rodziny MainConsole, w związku z czym można nimi zarządzać tak jak innymi rejestratorami IP+ oraz NVRmini poprzez jeden spójny system CMS. Do urządzeń z tej rodziny należą rejestratory 16 kanałowe NS-8060 oraz NS-8065, w których można zamontować nawet 8 dysków po 4TB każdy.

Model	NS-8060	NS-8065
Maksymalna liczba kanałów	16	
Wyjście wizyjne	HDMI/VGA	
Rozdzielczość obrazu	1920×1080, 1280×1024, 1280×720, 1024×768	
Możliwość dekodowania	120fps @1080p lub 240fps @720p (H.264/MPEG4)	
System operacyjny	Embedded Linux	
Kompresja	H.264, MPEG-4, MJPEG (zależnie od kamery IP)	
Liczba dysków	8×3,5" (do 4TB każdy)	
RAID	Brak	0, 1, 5, 10
Transmisja dźwięku	jednokierunkowa	
Porty Ethernet	2×Gigabit Port, RJ-45	
Złącza USB	4×USB 2,0	
Klient zdalny	Remote Live Viewer (oprogramowanie) Remote Live Viewer (strona internetowa) iViewer (urządzenia mobilne iOS/Android)	
Zasilanie	100 V_{DC} ~ 240 V_{AC}, 3,5 A~1,5 A, 60-50 Hz	

Dystrybutor: 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

Kamera IP XHA-201Z

reVizoom

Kamera szybkoobrotowa XHA-201Z wyróżnia się wysoką rozdzielczością 2 Mpx oraz obiektywem zapewniającym bardzo duże, bo aż 22-krotne powiększenie optyczne. Kamera wytwarza obrazy o rozdzielczości 1920×1080 z prędkością 25 lub 30 kl./s. Kamera ma nowoczesny przetwornik CMOS 1/2,8" Exmor zaś do podświetlenia obserwowanej sceny wykorzystuje dwanaście diod HP Super Flux pracujących w podczerwieni, co zapewnia zasięg podświetlenia do 100 m. Adaptacyjne sterowanie jasnością świecenia diod zapobiega prześwietleniu sceny obserwowanej w małej odległości. Podobnie jak wszystkie modele ReviZOOM kamera IP XHA-201Z jest wyposażona w odsuwany filtr IR.

Obiektyw o zmiennej ogniskowej mieszczącej się w granicach od 4,7 mm do 103 mm (zoom ×22) pozwala na precyzyjną regulację pola widzenia kamery. Funkcje WDR oraz *de-fog* poprawiają jakość obrazu w trudnych warunkach oświetleniowych.

Do kamer szybkoobrotowych dostępna jest pełna gama uchwytów przeznaczonych do mocowania: do ściany, sufitu, sufitu podwieszanego, słupa oraz narożnika muru.

Cechy kamery

- Progresywne skanowanie z prędkością 25 kl./s gwarantuje płynną reprodukcję obiektów ruchomych bez smużeń czy zniekształceń
- Trzy wyjściowe strumienie wizyjne: dwa z kompresją H.264 oraz jeden z kompresją MJPEG
- Zgodność z ONVIF 2.2 profil S
- Obsługa za pomocą Internet Explorera, Firefoxa i innych przeglądarek obsługujących Flash Player'a
- Dwukierunkowa komunikacja głosowa
- Analogowe wyjście serwisowe wizyjne – pozwala na równoczesne udostępnianie obrazów z kamery zarówno w sieci IP jak poprzez wyjście analogowe
- 7 wejść i 2 wyjścia alarmowe
- 255 presetów, 6 tras
- Możliwość rejestracji obrazów na karcie mikro SD o pojemności do 64 GB
- możliwość rejestracji obrazów na serwerze FTP oraz w pamięci NAS
- Podgląd obrazu na smartfonach
- Odporność mechaniczna IK5
- Dtopień szczelności obudowy IP66

Dane techniczne

- Kamera IP: szybkoobrotowa zewnętrzna
- Rozdzielczość: 1920×1080, 2 MPx
- Przetwornik: CMOS 1/2,8" Exmor
- Obiektyw: f=4,7-103 mm DC Iris
- Czułość: 0,1 lx przy F1,2 (kolor); 0,01 lx przy F1,2 (B/W); 0,0 lx przy włączonym oświetleniu IR
- Doświetlenie: 12 diod HP Super Flux IR LED 850nm, zasięg do 100 m
- Filtr IR: mechanicznie odsuwany filtr podczerwieni TDN
- Maks. przepływność: strumień wizyjny:
  1: 50 kb/s – 12 Mb/s
  2: 10 kb/s – 6 Mb/s
  3: MJPEG, 1Mb/s – 10 Mb/s
- Wymiary: 237×368 mm, średnica 155 mm
- Masa: 6 kg
- Obudowa: IP66/IK10
- Zasilanie: $24V_{AC}$ maks. 30 W

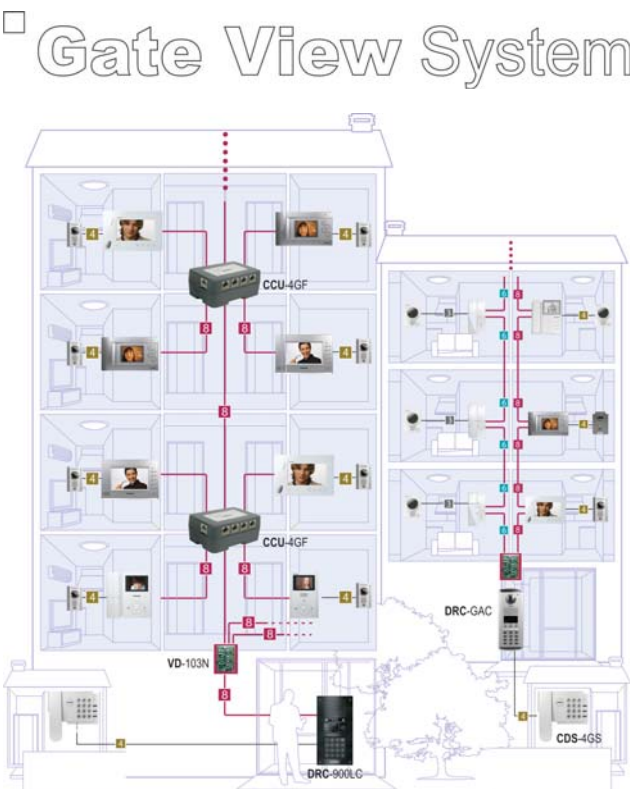
Dystrybucja: &GDE POLSKA

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

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

Wideodomofonowy system wieloabonentowy serii „Gate View”

COMMAX
SmartHome & Security



System wieloabonentowy serii „Gate View” przeznaczony jest zarówno do instalacji w blokach mieszkalnych jak i na osiedlach domów jednorodzinnych. Każdy lokator może posiadać kilka odbiorników wideodomofonych pozwalających na obsługę systemu z kilku miejsc.

Połączenia pomiędzy elementami systemu realizowane są przy użyciu kabla z parami skrętnymi UTP. Przy minimalnej konfiguracji do prawidłowego funkcjonowania niezbędne są jedynie panele zewnętrzne i odbiorniki (monitory). Dodatkowe elementy (wzmacniacze, rozdzielacze) pozwalają na rozbudowę systemu (kilka pionów, większa elastyczność).

Zastosowanie w systemie powszechnie dostępnego kabla sieciowego, wykorzystywanego w technice komputerowej jako medium transmisji sygnałów oraz separacja poszczególnych sygnałów na oddzielne pary przewodu pozwala osobom instalującym system w prosty sposób połączyć wszystkie jego elementy oraz szybko zlokalizować błędne połączenia czy uszkodzenia.

Dzięki połączeniu funkcjonalności monitorów analogowych z urządzeniami cyfrowymi system może być w prosty sposób rozbudowany przez dodanie indywidualnych paneli wejściowych lub dodatkowych kamer obserwacyjnych. Jeżeli na terenie obiektu znajduje się pomieszczenie ochrony, może ono być również wyposażone w stację portierską umożliwiającą kontakt ze wszystkimi użytkownikami oraz gośćmi. Lokatorzy korzystający z paneli bramowych mają możliwość otwarcia wejścia indywidualnymi kodami lub opcjonalnie kartą zbliżeniową. Różnorodność monitorów i paneli zewnętrznych pozwala dopasować wygląd sprzętu do wymogów architektonicznych projektowanych lub modernizowanych budynków.

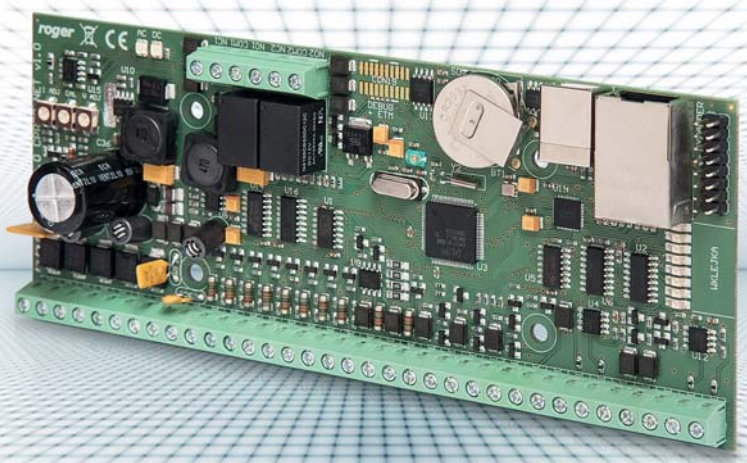
Dystrybucja: &GDE POLSKA

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

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

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. Mieszczańska 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. Racławicka 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

ACSS 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. Ścigały 10
40-208 Katowice
tel. 32 790 76 56
faks 32 790 76 61
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 67
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. Opolska 18 klatka C parter, 31-323 **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: warszawa@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

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.
Sławomir 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

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

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

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

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

Oddziały:
ul. Świętochłowicka 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. Mieszczańska 18/1, 30-313 **Kraków**
tel. 12 260 13 96
tel. kom. 665 380 677
faks 12 260 13 95

ul. Palacza 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

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

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

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

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

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

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

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

D-MAX Polska Sp. z o.o.
ul. Obornicka 276
60-693 Poznań
tel./faks 61 822 60 52
e-mail: biuro@dmaxpolska.pl
www.dmaxpolska.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 35
faks 12 270 56 96
e-mail: biuro@gde.pl
www.gde.pl

GORKE ELECTRONIC Sp. z o.o.
ul. Staromiejska 31 B
43-200 Pszczyna
tel. 32 326 30 70
faks 32 447 73 30
e-mail: biuro@gorke.com.pl
www.gorke.com.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, 411 57 47
faks 12 411 94 74
e-mail: insap@insap.pl
www.insap.pl

JANEX INTERNATIONAL Sp. z o.o.
ul. Płomyka 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 Łapczyca
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.rettopol.com.pl

SAMSUNG TECHWIN EUROPE LTD.
Biuro 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

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 53
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. Wierzbięcice 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. Roździeńskiego 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 Chełmińska 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. 61 674 62 00
faks 61 674 62 01
e-mail: biuro@visionpolska.pl
www.visionpolska.pl

ZBAR PHU
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

PTK5507 - dotykowa klawiatura serii POWER

DSC

- Nowoczesny design • 7” dotykowy wyświetlacz o wysokiej rozdzielczości (800 x 480) • Intuicyjne menu
- Możliwość personalizacji ekranu głównego • Wbudowany slot kart SD • Funkcja ramki elektronicznej
- Funkcja wirtualnej klawiatury • Diody LED sygnalizujące stan systemu
- Kompatybilna z centralami PC1864, PC1832, PC1616

Z dotykową klawiaturą PTK5507 obsługa systemu alarmowego jest jeszcze prostsza. Intuicyjne ikony menu oraz przesuwany ekran pozwalają łatwo zarządzać systemem. Aby uruchomić wybraną funkcję, wystarczy jedno dotknięcie ekranu palcem!

Klawiatura jest elegancką ozdobą każdego pomieszczenia. Zintegrowana ramka elektroniczna umożliwia wyświetlanie na ekranie klawiatury zdjęć z karty pamięci.

Wyłączny dystrybutor produktów DSC 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	TAK	TAK	TAK	TAK	TAK
DG Elpro	–	TAK	TAK	TAK	–
Dyskret	–	TAK	TAK	TAK	–
EBS	TAK	TAK	TAK	–	–
El-Mont	TAK	–	–	TAK	–
Elproma	–	TAK	–	TAK	–
Eureka	–	TAK	–	TAK	–
EST POLSKA	–	–	TAK	–	TAK
FES	–	TAK	TAK	TAK	TAK
GDE Polska	–	TAK	TAK	–	TAK
GORKE	TAK	–	–	–	–
ICS POLSKA	–	TAK	TAK	–	TAK
Insap	–	TAK	TAK	TAK	TAK
Janex International	–	TAK	TAK	–	TAK

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
KATON	–	–	TAK	–	TAK
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	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	–	–
ZBAR	–	TAK	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 nagłośnień
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	–	–	–	–	–	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	–	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								
El-Mont	TAK	TAK	TAK	–	–	TAK	TAK	TAK	TAK
Elproma	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	–
GORKE	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

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 nagłośnień
KATON	–	TAK	TAK	–	–	TAK	–	–	–
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	–	TAK	–	–	–
ZBAR	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 Końka

Redaguje zespół
Krzysztof Białek
Marek Blim
Patryk Gańko
Norbert Góra
Daniel Kamiński
Paweł Karczmarzyk
Adam Rosiński
Ryszard Sobierski
Waldemar Szulc
Adam Wojcinowicz

Współpraca
Marcin Buczaj
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

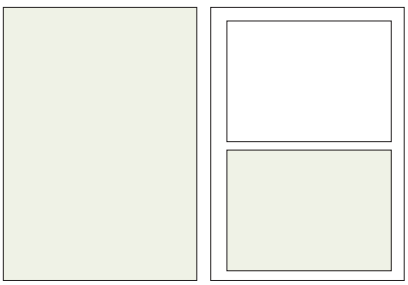
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

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

Cennik reklam

Reklama wewnątrz czasopisma:

cała strona, pełny kolor	4600 zł
cała strona, czarno-biała	2400 zł
1/2 strony, pełny kolor	2900 zł
1/2 strony, czarno-biała	1600 zł
1/3 strony, pełny kolor	2000 zł
1/3 strony, czarno-biała	1100 zł
1/4 strony, pełny kolor	1500 zł
1/4 strony, czarno-biała	900 zł
karta katalogowa, 1 strona	1000 zł

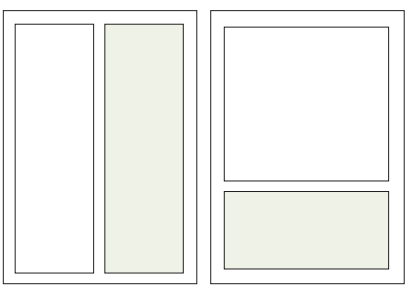


cała strona (200 x 282 mm + 3mm spad)

1/2 strony (170 x 125 mm)

Artykuł sponsorowany:

Cena za stronę artykułu sponsorowanego w czasopiśmie to 1600 zł (forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)

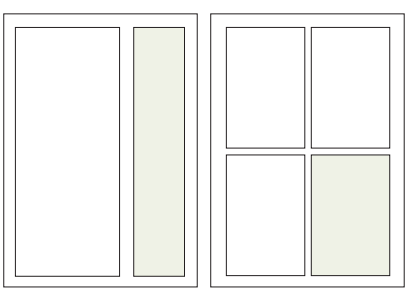


1/2 strony (83 x 260 mm)

1/3 strony (170 x 80 mm)

Reklama na okładkach:

pierwsza strona	indywidualne negocjacje
druga strona	5200 zł
przedostatnia strona	5200 zł
ostatnia strona	5200 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

WiseNet III

SAMSUNG TECHWIN

FUTURE PROOF YOUR BUSINESS

...AND **SAVE MONEY** WITH OUR WISENETIII IP SOLUTION

At Samsung we understand that the decision for when and how you migrate to an IP security solution is a complex one, influenced by many factors. Our new range of WiseNetIII network cameras have both an analogue and IP output, as well as onboard SD card recording. This gives you complete control and flexibility to make the right decision to suit your business. Integrate WiseNetIII onto an existing analogue system, whilst recording Full HD onto the SD card, or take advantage of the dual output and record locally to your analogue recorder whilst simultaneously viewing remotely utilising the IP output. You don't have to throw away the investment you made in your existing equipment – helping to improve Total Cost of Ownership!

Contact us for further information **E** stesecurity@samsung.com **W** www.samsungsecurity.co.uk/WiseNetIII

iCLASS SE®
Najnowocześniejsza platforma kontroli dostępu

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/iclass-se-platform-zab