CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 6(70)/2009

ZABEZPIECZENIA

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

W NUMERZE:

Sztuka niewidocznej ochrony przeciwpożarowej

Detektor Plusz

Buildings Editors' Choice TOP 100 PRODUCTS 2005

DESIGNPREIS 2006 NOMINEE

Premio Intel Design 2005 INNOVATION & DESIGN

DETEKTOR INTERNATIONAL AWARD Innovative Achievement 2004

Prize for Innovation in Architecture and Technical Systems

DESIGN PLUS AWARD WINNER 2004

Czujki dymu serii 500. Czasy nieestetycznych i rzucających się w oczy czujek dymu minęły bezpowrotnie. Nowa czujka dymu serii 500 firmy Bosch łączy w sobie płaską, elegancką obudowę z możliwością montażu podtynkowego. Różnokolorowe pierścienie sprawiają, że czujka jest praktycznie niewidoczna na suficie. Wysoka skuteczność wykrywania dymu i nierzucający się w oczy wygląd. A wszystko to dzięki innowacji firmy Bosch. Dodatkowe informacje można uzyskać pod adresem **www.boschsecurity.pl**

BOSCH

Technologia bliżej nas

Robert Bosch Sp. z o.o.
Security Systems
ul. Jutrzenki 105, 02-231 Warszawa
tel.: +48 22 715 41 00, fax: +48 22 715 41 05
securitysystems@pl.bosch.com **www.boschsecurity.pl**

Spis treści

CZASOPISMO ZABEZPIECZENIA 6/2009

Ochrona żeglugi i portów morskich (część I) 26

Wąskie gardła w IP 34

Elektroniczny system sygnalizacji pożarowej dla wagonów pasażerskich, autobusów szynowych i autobusów miejskich 68

Konkurs **Polski Mistrz Techniki Alarmowej** 2010

Stowarzyszenie **POLALARM** zaprasza polskich i zagranicznych producentów i dystrybutorów elektronicznych i elektromechanicznych urządzeń oraz systemów przeznaczonych do ochrony osób i mienia do udziału w XIII edycji konkursu Polski Mistrz Techniki Alarmowej 2010.

Konkurs będzie przeprowadzony w następujących kategoriach przedmiotowych:

1) Urządzenia i systemy sygnalizacji włamania i napadu;
2) Urządzenia i systemy sygnalizacji pożarowej;
3) Urządzenia i systemy nadzoru telewizyjnego i rejestracji obrazów;
4) Urządzenia i systemy kontroli dostępu;
5) Zintegrowane systemy sygnalizacji zagrożeń;
6) Urządzenia i systemy transmisji alarmu oraz monitoringu;
7) Systemy zabezpieczenia przeciwkradzieżowego pojazdów;
8) Systemy zarządzania i bezpieczeństwa transportu;
9) Systemy zarządzania i bezpieczeństwa ładunków;
10) Inne urządzenia i systemy technicznej ochrony oraz wspomagające ochronę fizyczną;

Zgłoszenia będą przyjmowane **do dnia 20 lutego 2010 roku** na drukach wniosku o udział w konkursie, które należy przesłać na adres:

Biuro Zarządu Stowarzyszenia POLALARM
ul. Nowogrodzka 18 lok. 8
00-511 Warszawa
e-mail: polalarm@polalarm.com.pl
tel./faks: (22) 626 90 31, (22) 625 57 43

Ogłoszenie wyników konkursu i uroczystość wręczenia nagród laureatom odbędzie się 26 kwietnia 2010 r., pierwszego dnia Międzynarodowej Wystawy Zabezpieczeń „SECUREX 2010" w Poznaniu.

Regulamin konkursu i wniosek o udział w konkursie są dostępne na stronach www.polalarm.org oraz w Biurze Zarządu Stowarzyszenia POLALARM.

Serdecznie zapraszamy do udziału w konkursie i życzymy sukcesów!

Bezpośr. inf. POLALARM

Informacja o zmianach w prowadzeniu Sekretariatu Komitetu Technicznego Nr 52

Ogólnopolskie Stowarzyszenie **POLALARM** informuje, iż od października 2009 r. nie prowadzi Sekretariatu Komitetu Technicznego Nr 52 ds. Systemów Alarmowych Włamania i Napadu.

Sekretariat KT-52 jest obecnie prowadzony przez Polski Komitet Normalizacyjny, a sekretarzem został mianowany pracownik PKN Piotr Górecki, dotychczasowy konsultant Komitetu.

Bezpośr. inf. Polalarm

Od redakcji:

Informujemy, że w numerze 5/2009, w *Wywiadzie z wiceprezesem stowarzyszenia POLALARM Krzysztofem Ciesielskim* (s. 18), podana została informacja, że POLALARM prowadzi sekretariat KT-52, co było zgodne z prawdą w czasie, gdy wywiad przeprowadzano i gdy czasopismo *Zabezpieczenia* było w druku. Aktualnie, jak podaje stowarzyszenie POLALARM, KT-52 jest prowadzony przez PKN.

Linc zaprasza na **bezpłatne szkolenia**

Firma **Linc** – oficjalny przedstawiciel firmy **Mobotix** w Polsce – ma zaszczyt poinformować, że rozpoczął się **cykl bezpłatnych szkoleń** pt. „Megapikselowe kamery IP Mobotix – i wszystko pod kontrolą...".

Szkolenia są organizowane w większych miastach na terenie całej Polski. Raz w miesiącu zapraszamy między innymi do Warszawy, Poznania i Katowic. Kompletny kalendarz seminariów jest dostępny na stronie *www.mobotix.com.pl*.

Prezentacja składa się z dwóch części: teoretycznej i praktycznej. Druga część umożliwia zapoznanie się „na żywo" z wyjątkowymi możliwościami megapikselowych kamer IP Mobotix (gdyż Mobotix to więcej niż kamera…).

Sieciowe kamery Mobotix to sześć w jednym:

– rejestrator,
– transmisja,
– centrum kontrolne,
– kamera,
– obiektyw,
– obudowa.

Ze względu na swoją innowacyjność i wszechstronność sieciowe kamery Mobotix są z powodzeniem stosowane w wielu bardzo różnych aplikacjach.

Wszystkich zainteresowanych uczestnictwem w szkoleniach prosimy o kontakt e-mailowy – *info@mobotix.com.pl* – lub telefoniczny – (61) 839 19 00.

Bezpośr. inf. Linc

Mobotix Mx2wire

– transmisja danych i zasilanie po dowolnym kablu

Firma **Mobotix** – wiodący producent unikatowych technologicznie megapikselowych kamer IP – wprowadza do oferty całkowicie nowe rozwiązanie **Mx2wire**, które umożliwia transmisję danych i zasilanie nie tylko kamer Mobotix, ale także innych urządzeń (zgodnych ze standardem PoE 802.3af) po miedzianych liniach kablowych.

Jest to autorskie i opatentowane rozwiązanie firmy Mobotix, którego głównym celem jest umożliwienie podłączenia dowolnej kamery Mobotix za pomocą istniejącego już, dostępnego okablowania – w szczególności wtedy, gdy nie jest możliwa (lub jest bardzo trudna i kosztowna) wymiana istniejącego, starego okablowania na aktualnie stosowaną w sieciach komputerowych skrętkę. Możliwe jest użycie do tego celu zarówno kabli koncentrycznych (po kamerach analogowych), jak też kabli telefonicznych lub standardowych kabli zasilających (a także – po testach – każdych innych).

Główne cechy Mx2wire:

– przesyła dane i zasilanie PoE zgodnie ze standardami,

– nie wymaga osobnego zasilania,

– używa istniejącego okablowania (koncentrycznego, telefonicznego lub zasilającego), dzięki czemu znacznie skraca czas i wysiłek potrzebne do wykonania instalacji,

– stwarza możliwość współpracy z urządzeniami dowolnego producenta, które spełniają standardy (dla PoE jest to IEE 802.3af),

– jest wysokiej jakości autorskim rozwiązaniem wykonanym w całości w Niemczech.

Bezpośr. inf. Linc

Źródło: www.mobotix.com.pl

Inteligentne zarządzanie punktem sprzedaży – **LDM II**

Oferta elektronicznych **systemów przeciwkradzieżowych (EAS)** została wzbogacona o nowe urządzenie – Local Device Manager II marki Sensormatic. Zapewnia ono możliwość inteligentnego zarządzania punktami sprzedaży z wykorzystaniem najnowocześniejszych technologii.

Local Device Manager II to nowy produkt należący do grupy rozwiązań SmartEAS, dostępny w ofercie **ADT Fire and Security**. Umożliwia gromadzenie danych nawet ze 124 urządzeń EAS bez konieczności uzyskiwania bezpośredniego połączenia z systemem wybranego punktu sprzedaży. Właściciele sieci handlowych mogą uzyskać dostęp do generowanych informacji poprzez połączenie z bezpieczną witryną internetową za pomocą dowolnego szyfrowanego łącza zabezpieczonego hasłem.

LDM II umożliwia zdalną współpracę z urządzeniami systemu EAS, a także podgląd statusu wszystkich podłączonych do systemu przeciwkradzieżowego urządzeń poprzez generowanie raportów. W przypadku wystąpienia ewentualnych zakłóceń w pracy któregokolwiek z elementów systemu autoryzowany serwis, dzięki zastosowaniu LDM II, może uzyskać zdalny dostęp do ustawień i konfiguracji systemu EAS oraz zdiagnozować i usunąć usterkę zdalnie, praktycznie z dowolnego miejsca na świecie. W systemie przeciwkradzieżowym zainstalowanym w punkcie sprzedaży można także szybko zaimplementować nowe funkcje poprzez zdalne wgrywanie nowych wersji oprogramowania i ustawianie opcji kontrolera przez sieć.

Jedną z funkcji LDM II umożliwiających inteligentne zarządzanie obiektem jest zliczanie osób odwiedzających punkt handlowy. Raporty zliczeń pozwalają na uzyskanie informacji o natężeniu ruchu klientów w ciągu dnia. Dzięki uzyskanej w ten sposób wiedzy zarządzający pracą sklepu mogą ustalić czas najwyższej i najniższej koncentracji odwiedzających. Pozwala to na prostsze i bardziej skuteczne planowanie pracy personelu tak, aby zapewnić klientom sprawny poziom obsługi. Dzięki temu możliwe jest skrócenie czasu zakupów, co wpływa pozytywnie na wizerunek sklepu, gdyż pozwala na zmniejszenie/wyeliminowanie kolejek do kas. Ponadto, dzięki wykorzystaniu funkcji zliczania klientów, jak również liczby transakcji, można określić wydajność punktu handlowego przez porównanie natężenia ruchu odwiedzających i wielkości sprzedaży.

LDM II umożliwia zarządzanie energią elektryczną w taki sposób, aby koszty jej zużycia były zminimalizowane. Dzięki zastosowaniu LDM II określone urządzenia mogą być przełączane w tryb niskiego zużycia energii (tryb czuwania) poza godzinami pracy. Pozwala to na mniejsze zużycie energii przez urządzenia EAS w sklepie w ustalonych godzinach. Możliwe jest również ręczne włączenie lub wyłączenie trybu czuwania. W przypadku ewentualnej utraty połączenia systemu EAS z LDM II na ponad 15 minut wbudowana funkcja zabezpieczenia przywróci pełną sprawność działania.

Wykorzystując dane pochodzące ze wszystkich działających w środowisku danego punktu handlowego systemów EAS, detaliści mogą przeglądać informacje dotyczące wydajności operacyjnej wszystkich podłączonych systemów oraz zwiększać przychody poprzez poprawę skuteczności systemu przeciwkradzieżowego.

Bezpośr. inf. ADT Fire and Security

Czujka IVORY
– nowe spojrzenie na bezpieczeństwo

W siedzibie firmy **Satel** najlepsi specjaliści co dzień starają się wyznaczać nowe standardy jakości produktów alarmowych. Efektem tych działań jest stale rozszerzająca się oferta producenta inteligentnych systemów alarmowych z Gdańska.

IVORY – nowa czujka firmy Satel – wykorzystuje sprawdzoną technologię zastosowaną w popularnej czujce **GRAPHITE**. Nowością jest zastosowany w czujce układ optyczny, który wykorzystuje precyzyjne zwierciadło segmentowe zamiast najczęściej stosowanej soczewki Fresnela. Lepsze ogniskowanie energii przez zwierciadło umożliwiło zwiększenie siły sygnału docierającego do piroelementu.

Nowa czujka firmy Satel jest jednakowo czuła w całym obszarze jej działania. Rozwiązanie to pozwala na wykrywanie osób przechodzących bezpośrednio pod czujką, likwidując tym samym tzw. martwą strefę.

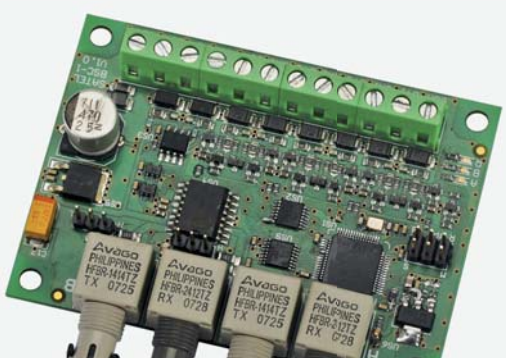
Monitorowanie napięcia zasilania oraz poprawności zadziałania toru sygnałowego gwarantuje natychmiastowe ostrzeżenie w razie nieprawidłowego funkcjonowania systemu lub sabotażu. Jeśli napięcie zasilania spadnie poniżej 9 V na czas dłuższy niż dwie sekundy albo zostanie stwierdzona usterka toru sygnałowego, czujka IVORY poinformuje o tym.

Dzięki szczelnej, odpornej na kurz konstrukcji komory optycznej lustro czujki IVORY nie wymaga czyszczenia. Czujka posiada także pamięć alarmów. Dzięki temu nawet jeśli podłączymy kilka czujek do jednego wejścia w centrali, jesteśmy w stanie zidentyfikować, z której pochodził sygnał. Możliwość zdalnego kontrolowania diody LED pozwala na wygodne przetestowanie działania czujki w trakcie prac serwisowych.

Więcej informacji na temat czujki IVORY i innych elementów inteligentnych systemów alarmowych firmy Satel można znaleźć na stronie *www.satel.pl*.

Bezpośr. inf. Satel

Satel wprowadza na rynek nowy **moduł INT-FI**
– światłowodowy konwerter danych



Firma **Satel** wprowadza na rynek nowe urządzenie, które ułatwia budowę funkcjonalnych i rozległych systemów alarmowych oraz usprawnia działanie tych, które pracują w niesprzyjających warunkach. W ofercie tego znanego producenta pojawił się **moduł INT-FI**, który jest światłowodowym konwerterem magistrali danych.

Do przesyłania informacji pomiędzy urządzeniami systemu alarmowego (manipulatorami, modułami rozszerzeń) wykorzystywane są magistrale. Dotychczas sygnał mógł być transmitowany wyłącznie przez kabel miedziany na odległość do 1 km. Zdarzało się jednak, szczególnie w dużych instalacjach i obiektach przemysłowych, że ta forma połączenia zawodziła. W skrajnych przypadkach przekaz danych za pośrednictwem kabla miedzianego mógł ulec zakłóceniu pod wpływem działania innych urządzeń elektrycznych, skutkując generowaniem fałszywych alarmów.

Aby rozwiązać ten problem, firma Satel stworzyła moduł INF-FI. Umożliwia on konwersję sygnału elektrycznego na sygnał optyczny. Pozwala to na galwaniczne odseparowanie urządzeń, eliminując tym samym problemy zakłóceń transmisji, znane z systemów komunikujących się za pomocą kabla miedzianego. Dzięki modułom INT-FI możliwe jest także zwiększenie dystansu, jaki dzieli urządzenia rozszerzające system od centrali. Dzięki zastosowaniu nowego produktu Satela odległość ta może wynosić nawet do 4 km (w przypadku kaskadowego łączenia modułów).

Kompletny system transmisji składa się z dwóch urządzeń – nadajnika i odbiornika. Wykorzystanie dwóch modułów INT-FI umożliwi zamianę sygnału elektrycznego na sygnał optyczny i przekazanie go za pomocą wielomodowego kabla światłowodowego do drugiego modułu INT-FI. W nim ponownie nastąpi konwersja sygnału, jednak tym razem sygnał optyczny zostanie zamieniony na sygnał elektryczny.

Urządzenia INT-FI doskonale sprawdzają się np. w rozległych sieciach przemysłowych.

Bezpośr. inf. Satel

Nowa kamera sieciowa **HDTV** z 18-krotnym zoomem optycznym

od Axis Communications

Axis Communications, lider światowego rynku sieciowych rozwiązań wizyjnych, prezentuje kamerę **AXIS P5534 PTZ** przeznaczoną do instalacji wewnętrznych na lotniskach, stacjach kolejowych, w magazynach, sklepach i szkołach. Nowy model oferuje obraz klasy HDTV, 18-krotny zoom optyczny z autofokusem i 12-krotny zoom cyfrowy.

– *Chcemy wprowadzić standard HDTV do branży monitoringu. Zaprezentowaliśmy już kamery stałopozycyjne HDTV, teraz poszerzamy ofertę o modele PTZ wysokiej rozdzielczości* – powiedział **Erik Fränlid**, dyrektor ds. zarządzania produktami w Axis Acommunications.

AXIS P5534 koduje obraz HDTV 720p zgodnie ze standardem SMPTE 296M. Oznacza to rozdzielczość 1280×720 pikseli, przesyłanie 30 klatek na sekundę, wierne odwzorowanie kolorów i proporcje 16:9. Kamera może równocześnie wysyłać strumienie wideo w formacie H.264 oraz Motion JPEG, z których każdy jest indywidualnie konfigurowany. Zastosowanie kompresji H.264 optymalizuje wykorzystanie pasma sieciowego i pamięci masowej bez obniżania jakości obrazu, natomiast obsługa formatu Motion JPEG zwiększa elastyczność i kompatybilność rozwiązania.

Kamera ma 18-krotny zoom optyczny z autofokusem i 12-krotny zoom cyfrowy. Obraca się też o 360° dzięki unikatowej funkcji Auto-flip, pozwalającej symulować ciągły ruch poza punktem mechanicznego zatrzymania. Umożliwia to nieustanną obserwację nawet szybko przemieszczającego się obiektu. Dzięki mechanizmowi Advanced Gatekeeper kamera automatycznie obraca się i steruje przybliżeniem po wykryciu aktywności w danym obszarze, a następnie oddala ujęcie po zaprogramowanym czasie. AXIS P5534 ma także specjalny tryb nocny, zapewniający wysoką jakość obrazu przy słabym oświetleniu.

Obsługa standardu High Power over Ethernet znacznie upraszcza instalację kamery, ponieważ jeden kabel służy jako przewód do zasilania, przesyłu sygnału wideo oraz sterowania ruchem i przybliżeniem kamery. AXIS P5534 ma wbudowany system detekcji dźwięku, przesyła również sygnał audio w dwóch kierunkach. Urządzenie jest wyposażone w cztery konfigurowalne wejścia/wyjścia do podłączenia zewnętrznych urządzeń, np. czujników bądź przekaźników. Wbudowane gniazdo pamięci SD/SDHC pozwala na lokalne przechowywanie nagrań. Kamera jest odporna na kurz i wilgoć dzięki szczelnej obudowie zgodnej z klasą szczelności IP51.

AXIS P5534 oferuje najbardziej zaawansowany na rynku zestaw funkcji zabezpieczających i służących do zarządzania sieciowego. Produkt jest obsługiwany przez oprogramowanie AXIS Camera Station, a także przez najszerszą w branży gamę aplikacji stworzonych w ramach programu Axis Application Development Partner.

Kamera sieciowa AXIS P5534 jest dostępna na rynku od listopada 2009 r.

Bezpośr. inf. Kamila Wierzbicka
Mmd Corporate
Public Affairs & Public Relations Consultants Poland

Nagroda dla **Martina Grena** z Axis Communications

Martin Gren, jeden z założycieli **Axis Communications** (firma Axis Communications została założona przez Martina Grena i Mikeala Karlssona w 1984 roku w Lund w Szwecji), otrzymał nagrodę *Lifetime Achievement Award* za stworzenie dobrze prosperującego przedsiębiorstwa oraz przyczynienie się do powstania i rozwoju szybko rozwijającego się rynku systemów monitoringu wizyjnego. Fundatorem nagrody jest branżowe czasopismo *Detektor*. Dzięki wyjątkowej przedsiębiorczości Martin Gren przyczynił się do ogromnego sukcesu firmy. Jego pełna pasji praca, wiara w możliwości techniki, rozumienie potrzeb rynku oraz niezwykłe umiejętności biznesowe sprawiły, że Szwecja jest aktualnie liderem na światowym rynku kamer sieciowych, wykorzystywanych głównie do budowy systemów nadzoru wizyjnego.

W tym roku Firma Axis Communications otrzymała wiele nagród w dziedzinie biznesu, a Martin Gren będzie reprezentował Szwecję w światowym finale konkursu **„Przedsiębiorca Roku”**, organizowanego przez Ernst&Young.

Redakcja
Opracowano na podstawie materiałów Ratata Communication

Nowa klawiatura DCZ

pozwala na zarządzanie aplikacjami CCTV za pośrednictwem komputera, poprzez USB

Klawiaturę z joystickiem, 38 podświetlanymi przyciskami i brzęczykiem można łatwo połączyć z systemami sterującymi, stosując podstawowe techniki programowe bez SDK. Jej funkcje zależą wyłącznie od zastosowanej aplikacji.

Klawiaturę DCZ można użyć do sterowania aplikacjami już występującymi na rynku, emulując czterokierunkowy joystick HID za pomocą 24 przycisków. Można ją również połączyć z urządzeniami peryferyjnymi PC, takimi jak klawiatury, myszki, joysticki i in. Jest zasilana poprzez kabel USB i do działania wymaga tylko jednego kabla.

Użycie klawiatury może być jeszcze bardziej intuicyjne dzięki personalizacji zespołów na panelu klawiatury. W tym celu użytkownik może łatwo personalizować i zadrukowywać arkusze dostarczane wraz z wyrobem. Warstwa ochronnego plastiku chroni klawiaturę przed zużyciem.

Klawiaturę można tak zmodyfikować, że zarówno prawa, jak i lewa strona mogą służyć do łatwego wykorzystania wszystkich funkcji.

Ta prosta, przyjazna dla użytkownika i w pełni implementowalna klawiatura pozwala na łatwe i wygodne zarządzanie wszystkimi aplikacjami CCTV za pośrednictwem komputera PC.

Bezpośr. inf. Martina Panighel
Videotec
Tłumaczenie: Redakcja

ULISSE COMPACT z oświetlaczem IR LED

Szybki, wydajny i elastyczny system pozycjonujący

Nowy **pozycjoner ULISSE COMPACT** jest niezawodnym rozwiązaniem przeznaczonym do stosowania w zewnętrznych systemach telewizji dozorowej.

Dzięki zaawansowanej technologii możliwe jest szybkie i dokładne pozycjonowanie głowicy. Ponadto system cechuje się prostotą obsługi i konfiguracji oraz wysoką odpornością na warunki zewnętrzne.

ULISSE COMPACT gwarantuje wysoką jakość obrazu nawet w warunkach niskiego natężenia oświetlenia (również w nocy). Istnieje możliwość fabrycznego zintegrowania systemu z promiennikami podczerwieni.

System ULISSE COMPACT oferuje wybór modułów kamerowych SONY o krotności zoomu 36×, 18× lub 10× oraz o różnorodnym zasilaniu (230 V_{AC}, 24 V_{AC} lub 120 V_{AC}), pracujących w systemie PAL lub NTSC. Dostępne są wersje z wbudowaną wycieraczką i oświetlaczem.

Obecnie wszystkie modele są dostępne w sprzedaży.

Bezpośr. inf. Martina Panighel
Videotec
Tłumaczenie: Redakcja

HID Global rozszerza ofertę

wysyłek 48-godzinnych Priority Plus na Europę

HID Global ogłosił rozszerzenie dostępności usługi Priority Plus Credential Service o wysyłki do Europy. Usługa gwarantuje wysłanie w ciągu 48 godzin standardowych zestawów HID Indala Prox i iCLASS w liczbie od 100 do 500 kart, a także obejmuje zaprogramowanie oraz nadruk numerów na kartach.

Usługa ta jest dostępna w przypadku wszystkich produktów zamówionych po 27 października 2009 roku dla klientów w Unii Europejskiej. Każde zamówienie zostanie zrealizowane w ciągu dwóch dni roboczych po otrzymaniu zamówienia, pełnej informacji o kartach i potwierdzeniu zamówienia przez

HID Global. Zakwalifikowane zamówienia zostaną automatycznie objęte bezpłatną usługą Priority Plus z wyłączeniem możliwości odwołania zamówienia w ciągu 24 godzin.

Bezpośr. inf. Paula Tienza
HID Global
Tłumaczenie: Redakcja

Szybkoobrotowe kamery kopułowe Samsung SPU
o szerokim zakresie funkcjonalnym

Firma **Samsung Techwin** wprowadziła na rynek nową serię prostych w montażu, odpornych na warunki pogodowe szybkoobrotowych kamer kopułowych o szerokim zakresie funkcjonalnym.

Wszystkie **modele serii SPU** są fabrycznie montowane w solidnej obudowie, która jest odporna na warunki pogodowe i spełnia wymagania IP66. Dzięki połączeniu zatrzaskowemu (*twist-lock*) można ją łatwo zintegrować z dostarczaną w zestawie skrzynką połączeniową.

Seria SPU została zaprojektowana z myślą o zapewnieniu dużego zakresu funkcji przy zachowaniu łatwego montażu. W ofercie znajdują się przetworniki z zoomem 27×, 33× i 37×, w tym wersje z automatycznym śledzeniem i funkcją *Wide Dynamic Range* (szeroki zakres dynamiki). W standardzie jest prędkość uchyłu/obrotu rzędu 500 stopni na sekundę, funkcja HLC (korekcja silnego światła padającego na przetwornik), cyfrowa stabilizacja obrazu, maskowanie stref prywatności, zintegrowany filtr odcinający promienie podczerwone oraz szereg możliwości programowania położeń i ruchów kamery.

– *Serię kamer SPU można określić jako przyjazną dla instalatora* – mówi Peter Ainsworth, menedżer produktu w dziale profesjonalnego monitoringu firmy Samsung Techwin. – *Odpowiadając na sugestie naszych klientów, zintegrowaliśmy moduł kamerowy z obudową, umożliwiając jego użycie natychmiast po rozpakowaniu, a także dołączyliśmy niezwykle łatwą do podłączenia skrzynkę połączeniową z wysuwanym panelem umożliwiającym dostęp do złącz wizyjnych, zasilających i alarmowych. W ofercie mamy również bogaty asortyment uchwytów, m.in. wysięgników ściennych i mocowań na parapet. Zapewniamy także możliwość sterowania kamerami za pośrednictwem kabla koncentrycznego. Wszystko to pozwala na skrócenie zarówno czasu instalacji, jak i kosztów związanych z okablowaniem.*

Bezpośr. inf. David Solomons
DRS Marketing
Tłumaczenie: Redakcja

Samsung Techwin wprowadza do swojej oferty kamer
nowe modele megapikselowe

Pierwszy model nowej generacji **kamer IP** o nazwie **SNC-1300** został wyposażony w wiele cech i funkcji, które umożliwiają użytkownikom czerpanie korzyści z najnowszych osiągnięć w dziedzinie monitoringu IP.

Obrazy zarejestrowane przez kamery megapixelowe zawierają większą liczbę szczegółów w porównaniu do obrazów ze standardowych kamer przemysłowych. Dla przykładu: obraz ze standardowej kamery 540 TVL zawiera typowo 473 820 pikseli, natomiast obraz z kamery SNC-1300 zawiera 1,3 miliona pikseli.

Model SNC-1300 został wyposażony w technologię jednoczesnej obsługi kodeków MPEG-4/JPEG, umożliwia generację obrazów oraz wysoce skompresowanych strumieni obrazu w czasie rzeczywistym z prędkością do 20 obr./s w rozdzielczości 1280×960 bądź do 25 obr./s w rozdzielczości 1280×720.

Dzięki obsłudze wielu protokołów oraz funkcjom prywatności i wykrywania ruchu kamera SNC-1300 z wbudowanym filtrem podczerwieni jest przeznaczona zarówno do pracy w dzień i w nocy. Jeśli kamera zostanie odpowiednio zaprogramowana, w przypadku wykrycia ruchu lub aktywacji alarmu SNC-1300 natychmiast prześle przechwycony obraz na adres e-mail użytkownika.

Instalowane w gnieździe karty SD ułatwiają przechowywanie i tworzenie kopii zapasowych plików. Urządzenie zawiera standardowo kartę pamięci o pojemności 2 GB. Dwukierunkowa transmisja dźwięku umożliwia odsłuchiwanie rozmów prowadzonych w monitorowanych pomieszczeniach. Zapewnia jednocześnie możliwość przesyłania komunikatów ostrzegawczych i poleceń do tych pomieszczeń bezpośrednio z centrum sterowania.

Model SNC-1300 generuje obrazy w rozdzielczości do 1280×960 punktów z wykorzystaniem technologii skanowania progresywnego. Skanowanie progresywne to metoda analizy, przechowywania i przesyłania ruchomych obrazów, która polega na wyświetlaniu kolejnych linii każdego obrazu . Tradycyjne kamery przemysłowe wykorzystują technologię przeplotu, tj. analizy na zmianę parzystych i nieparzystych linii obrazu. Skanowanie progresywne umożliwia wyeliminowanie problemów związanych z przeplotem, tj. zakłóceń (artefaktów) obrazu i niskiej rozdzielczości pionowej.

Wbudowany serwer WWW umożliwia monitorowanie obrazu z kamery pięciu użytkownikom jednocześnie. Oprogramowanie do centralnego zarządzania (CMS) SVM-S1, dołączane do kamery SNC-1300, umożliwia stworzenie wydajnego systemu zarządzania przez sieć, a także wygodnego interfejsu do wizualnego monitorowania obszaru, w tym wyświetlania różnorodnych zdarzeń oraz map.

Bezpośr. inf. David Solomons
DRS Marketing
Tłumaczenie: Redakcja

MAXXESS wprowadza
wersję 2.0 platformy eFusion

W związku z wydaniem drugiej generacji **platformy programowej eFusion MAXXESS Systems** oczekuje wzrostu swojego udziału w rynku aplikacji zarządzających systemami bezpieczeństwa.

Wersja 2.0 platformy eFusion składa się z dziesięciu niezależnych modułów oprogramowania, które są przeznaczone do konkretnych systemów bezpieczeństwa. W przypadku równoczesnej pracy stają się zawansowaną, globalną i zintegrowaną platformą zarządzania.

– Platforma eFusion generuje korzyści, ponieważ pozwala szybko reagować na wydarzenia, podejmować bardziej świadomie decyzje i lepiej wykorzystywać zasoby ludzkie i wymianę informacji w organizacji przy znacznej redukcji kosztów bezpieczeństwa – powiedział Lee Copland, dyrektor zarządzający MAXXESS Systems EMEA.

Platforma eFusion została zaprojektowana w sposób przejrzysty i dostosowany do indywidualnych, zmieniających się wymagań użytkownika. Wśród modułów eFusion znaleźć można ViewPoint, który pozwala na wyświetlanie sygnałów wizji z wielu źródeł na jednym głównym wyświetlaczu, niezależnie od marki urządzeń CCTV. Axis, Bosch, Cieffe/March, Cisco, Dedicated Micros, Geutebruck, Pelco, Samsung Techwin, Sony i Vicon to tylko niektórzy z wielu producentów, których protokoły zostały zintegrowane z modułem ViewPoint. Szczególnie przydatnym modułem jest Integrator, który pozwala integratorom systemów na łatwe programowanie i integrację innych systemów bezpieczeństwa.

– Jedną z głównych zalet eFusion jest to, że pozwala integratorom na redukcję kosztów obsługi klientów oraz pełne wykorzystanie możliwości integrowanych systemów. Zapewnia również bezproblemową migrację do nowych technologii – stwierdził Lee Copland. *– eFusion zapewni rosnącej sieci naszych autoryzowanych dealerów przewagę konkurencyjną i możliwość realizacji wartości dodanej dla klientów w czasie, gdy budżety na bezpieczeństwo mogą zostać zredukowane.*

MAXXESS Systems działa w branży zabezpieczeń. Od dziesięcioleci firma jest liderem w produkcji systemów kontroli dostępu. Od pięciu lat ze szczególnym powodzeniem integruje rozwiązania sprzętowe i oprogramowanie. Integracja ta zapewnia wysoki poziom zarządzania bezpieczeństwem przedsiębiorstwom i administracji publicznej. Systemy MAXXESS są instalowane na całym świecie, zarówno w systemach małych (od dwojga drzwi) i dużych (obejmujących np. kampusy uniwersyteckie składające się z wielu budynków, setek kontrolowanych przejść i tysięcy kart kontroli dostępu).

Bezpośr. inf. David Solomons
DRS Marketing
Tłumaczenie: Redakcja

Cisco i Pelco zawierają strategiczne porozumienie technologiczne

Pelco i **Cisco** zawarły strategiczne porozumienie technologiczne w celu wspólnego opracowania nowych kamer sieciowych o wysokiej rozdzielczości HD na bazie platformy technologicznej Sarix firmy Pelco.

Nowe kamery pod wspólną marką połączą obróbkę obrazu firmy Pelco z doświadczeniem Cisco w dziedzinie połączeń sieciowych, dając nową generację kamer. Kamery te będą sprzedawane na świecie przez autoryzowanych przedstawicieli Cisco. Ich dostępność jest zaplanowana na koniec 2009 roku.

– Połączenie doświadczeń firmy Cisco w zakresie transmisji sieciowej IP z doświadczeniem Pelco w zakresie generacji i obróbki sygnału wizji jest wielką szansą dla klientów. Po starannej ocenie dostępnych technologii stwierdziliśmy, że Pelco opracowało jeden z najbardziej zaawansowanych systemów generacji i obróbki sygnału wizji wysokiej rozdzielczości HD w technice IP na światowym rynku zabezpieczeń – wyjaśnia Bill Stuntz, dyrektor generalny i wiceprezes oddziału Cisco Physical Security.

– Pelco i Cisco są naturalnymi partnerami wspomagającymi rozwój następnej generacji systemów bezpieczeństwa. Cieszymy się na ścisłą współpracę z Cisco. Chcemy połączyć ich olbrzymią wiedzę o sieciach IP z zaawansowaną technologią Sarix i zapoczątkować opracowanie najnowszych kamer HD IP kierowanych na rynek światowy. Nasze wspólne zaangażowanie na rzecz klientów i osiągnięte już sukcesy we współpracy pozwolą nam zapewnić nowe możliwości i korzyści, które spełnią dzisiejsze wymagania specjalistów w zakresie bezpieczeństwa – mówi Dean Meyer, dyrektor i prezes Pelco.

Pelco dostarczy Cisco kompletną linię technologii generacji i obróbki sygnału HD, która zostanie wykorzystana do rozszerzenia istniejącej linii kamer Cisco i sieciowych systemów wizyjnych.

Kamery pod wspólną marką Cisco i Pelco wykorzystają znakomitą funkcjonalność technologii Sarix, w tym rozdzielczość D1, kompresję H.264, wysoką czułość, wbudowaną analitykę, auto focus i przyjazną instalację.

Źródło: www.securityworldhotel.com
Tłumaczenie: Redakcja

Firma Bosch wprowadza nową wersję oprogramowania układowego do sieciowych produktów wizyjnych

Pełna obsługa kompresji H.264 i nowy standard Open Network Video Interface Forum

Firma **Bosch Security Systems** wprowadza ważną aktualizację oprogramowania układowego do swoich sieciowych platform wizyjnych. Nowa wersja oprogramowania układowego 4.0 jest dostępna dla kamer Dinion IP, FlexiDome IP, kamer serii Extreme IP i AutoDome IP, jak również nadajników serii VideoJet X oraz wielokanałowych nadajników i odbiorników VIP X1600. Aby zaktualizować wszystkie posiadane sieciowe produkty wizyjne, wystarczy pobrać jedną wersję oprogramowania układowego.

Nowa wersja oprogramowania układowego zawiera wiele nowych funkcji oraz zmian strukturalnych w mechanizmach zapisu. Dzięki oprogramowaniu układowemu w wersji 4.0 kamery sieciowe i nadajniki firmy Bosch mogą teraz obsługiwać standard kompresji (kodowania) H.264, dostarczając wysokiej jakości obraz przy mniejszym zapotrzebowaniu na pasmo sieciowe i przestrzeń zapisu. Zmniejsza to koszty przestrzeni zapisu nawet o 30% w porównaniu z systemami opartymi na dotychczasowej kompresji MPEG-4.

Obraz z kamer i nadajników H.264 firmy Bosch można przeglądać, używając oprogramowania VIDOS v4.0 lub hybrydowego rejestratora wizyjnego Bosch Divar XF, a także zapisywać w hybrydowym rejestratorze wizyjnym Bosch Divar XF, lokalnie w nadajniku lub bezpośrednio w macierzy iSCSI RAID firmy Bosch, umieszczonej w dowolnym miejscu sieci IP. Nowe oprogramowanie układowe oferuje również dotychczasowe tryby kompresji MPEG-4 i JPEG w celu zapewnienia kompatybilności z systemami, które nie obsługują standardu H.264.

Kamery sieciowe Bosch z nową wersją oprogramowania są gotowe do pracy z ostatnio wprowadzonym standardem Open Network Video Interface Forum (ONVIF), który definiuje wspólny protokół przeznaczony dla sieciowych urządzeń wizyjnych, standaryzujący wymianę informacji w rodzaju obrazu bieżącego czy metadanych. Standaryzacja daje możliwość współpracy z innymi zgodnymi ze standardem ONVIF sieciowymi produktami dozorowymi, niezależnie od producenta. Standard ONVIF zapewnia klientom większą elastyczność w zakresie przyszłych aktualizacji i rozbudowy sieciowych systemów wizyjnych.

Oprogramowanie układowe w wersji 4.0 umożliwia również bieżącą kontrolę obrazu za pomocą samej klawiatury IntuiKey i odbiornika, bez potrzeby korzystania z komputera PC czy oprogramowania komputerowego. Wnosi także więcej inteligencji do sieciowych produktów wizyjnych firmy Bosch, umożliwiając w ten sposób tworzenie wirtualnej krosownicy do podglądu obrazu i sterowania maks. 32 kamerami na 10 monitorach bez potrzeby stosowania wizyjnego oprogramowania zarządzającego. Pozwala to użytkownikom końcowym na indywidualne dostosowanie systemu do swoich potrzeb oraz zapewnia dalszą redukcję kosztów.

Użytkownicy już zainstalowanych sieciowych produktów wizyjnych Bosch mogą pobrać oprogramowanie układowe w wersji 4.0 ze strony internetowej firmy Bosch, natomiast nowi użytkownicy kamer i nadajników Bosch otrzymają produkty już obsługujące standard H.264 oraz dodatkowe funkcje zawarte w oprogramowaniu układowym 4.0.

Bezpośr. inf. Bosch Security Systems

Najlepsze produkty z branży zabezpieczeń

nagrodzone w Sztokholmie

Nagrody **Detektor International 2009** są już rozdane. Ponad 350 gości uczestniczyło w ceremonii wręczenia nagród podczas uroczystej kolacji zorganizowanej z okazji Detektor International Awards podczas otwarcia Sectech w Sztokholmie w dniu 20 października.

Lennart Alexandrie, redaktor naczelny Detektor International i prezes wydawnictwa AR Media International, przedstawił jedenastu finalistów.

– *Najlepsze wyroby w swojej klasie wybrano na podstawie innowacyjności i zorientowania na klientów. Wyroby zwycięskie muszą być zarówno eleganckie, jak i użyteczne* – stwierdził Lennart Alexandrie.

Trzy kategorie nagradzanych wyrobów to *kontrola dostępu, alarm i detekcja* oraz *telewizja dozorowa.*

Kategoria kontrola dostępu

Nagroda za najlepszy wyrób w kategorii *kontrola dostępu* przypadła firmie Suprema (Korea Płd.) za **zewnętrzny czytnik odcisków palców BioLite Net**. Uzasadnienie jury: „Czytnik zewnętrzny BioLite Net nie tylko oferuje natychmiastową identyfikację dla potrzeb kontroli dostępu i rejestracji obecności, ale działa nawet w trudnych warunkach pogodowych, co sprawia że odpowiada oczekiwaniom rynku".

Nagroda za wyrób rekomendowany przypadła **klamce kodowej 8810** firmy ASSA OEM (Szwecja).

Nagroda za innowacyjne osiągnięcie w kategorii *kontrola dostępu* przypadła w tym roku produktowi **HID on the Desktop**, rozwiązaniu firmy HID Global (USA), które przekształca fizyczną i logiczną kontrolę dostępu w pojedynczy, zintegrowany system.

Kategoria alarm i detekcja

Nagroda za najlepszy wyrób w kategorii *alarm i detekcja* przypadła wyrobowi **Skygd Panic Alarm**, oprogramowaniu alarmowemu firmy Skygd (Szwecja) przeznaczonemu do standardowych telefonów komórkowych.

Nagroda za wyrób rekomendowany w kategorii *alarm i detekcja* przypadła **RLS-3060**, detektorowi laserowemu firmy Optex (Japonia), który może określić rozmiar, prędkość i odległości wykrywanych obiektów.

Nagroda za innowacyjne osiągnięcie w kategorii *alarm i detekcja* przypadła **AdvanceGuard 350-X**, czujnikowi radarowemu firmy Navtech Radar (UK) przeznaczonemu do ochrony obwodowej.

Nagroda za innowacyjne osiągnięcie w kategorii *alarm i detekcja* przypadła **DD669 AM**, detektorowi dualnemu firmy GE Security (USA), który ma zasięg 360 stopni.

Kategoria CCTV

Nagroda za najlepszy wyrób w kategorii CCTV przypadła **OPAX VCA with Saab Stereo Technology**, wzmocnionemu rozwiązaniu VCA firmy OPAX (Norwegia), które jest oparte na technologii stereo.

Nagroda za wyrób rekomendowany w kategorii CCTV przypadła kamerze **SNC-RH124P**, pierwszej kamerze PTZ HD firmy Sony (Japonia).

Nagroda za innowacyjne osiągnięcie w kategorii CCTV przypadła kamerze **AXIS P3344**, stałej kamerze kopułkowej HD firmy Axis Communications (Szwecja).

Nagroda za innowacyjne osiągnięcie w kategorii CCTV przypadła kamerze **NBC-255-P**, kompletnemu sieciowemu systemowi obserwacyjnemu firmy Bosch Security Systems (Niemcy).

W każdej kategorii wyrobów przyznawano nagrody za najlepszy wyrób (pierwsze miejsce), za wyrób rekomendowany (drugie miejsce) oraz za innowacyjne osiągnięcie (trzecie i czwarte miejsce).

Jury składało się z dziewięciu członków z sześciu różnych krajów, z których wszyscy są w zarządzie pisma DETEKTOR.

Następne wręczenie nagród Detektor International odbędzie się na Sectech w Kopenhadze w listopadzie 2010 r.

Bezpośr. inf. Marika Thelenius
Ratata Communication
Tłumaczenie: Readakcja

HID on the Desktop nagrodzony

HID Global informuje, że pakiet o nazwie *HID on the Desktop* (HID na pulpicie) został wyróżniony nagrodą jako innowacyjne osiągnięcie w dziedzinie kontroli dostępu podczas wręczania nagród Detektor International Awards 2009 w Sztokholmie.

Dziesiąta doroczna ceremonia wręczania nagród Detektor International odbyła się na terenie Sectech Expo równocześnie z otwarciem wystawy szwedzkiej, jednej z ważniejszych w Europie i w rejonie nordyckim.

Kryteriami wyróżnień były zarówno innowacyjność, jak i zorientowanie na klienta. W swoim werdykcie jury podkreśliło, że „HID raz jeszcze przyczynił się do zwiększenia bezpieczeństwa zarówno w sektorze komercyjnym, jak i w sektorze organizacji publicznych".

Bezpośr. inf. Paula Tienza
HID Global
Tłumaczenie: Redakcja

Kompletny system dozorowy w niewielkiej kamerze

Bosch wprowadził do oferty nową kamerę sieciową serii 200

Bosch Security Systems wprowadził do sprzedaży nową **kompaktową kamerę sieciową serii 200**, która już zyskała uznanie na rynku systemów zabezpieczeń. Wyrazem tego jest nagroda **Detektor International Award 2009** w kategorii „innowacyjne osiągnięcie".

Kamera sieciowa serii 200 to całkowicie samodzielny system dozorowy. Kamery tej serii stanowią ekonomiczne rozwiązanie umożliwiające małym firmom efektywną ochronę i monitorowanie mienia. Nowa kamera jest gotowa do pracy od momentu jej wyjęcia z opakowania, działa bez potrzeby dołączania cyfrowego rejestratora wizyjnego czy komputera PC. Kamera rozpoczyna rejestrację obrazów zaraz po włączeniu zasilania, jedyne, co należy zrobić, to podłączyć kamerę do sieci. Możliwe jest także przechowywanie kilkudniowych nagrań na wewnętrznej karcie pamięci SD.

Kamera wykorzystuje najnowszy standard kompresji obrazu H.264, dzięki czemu wymagania dotyczące przestrzeni pamięciowej maleją nawet o 30% w porównaniu z zapisem obrazu w standardzie MPEG-4, obniżając tym samym koszty archiwizacji.

Nowa, łatwa w instalacji kamera znajduje szerokie zastosowanie między innymi w małych biurach, sklepach i szkołach. Aby z niej korzystać, nie jest potrzebna specjalistyczna wiedza. Należy jedynie podłączyć kamerę do sieci i włożyć kartę SD. Jeśli dostępny jest przełącznik sieciowy dostarczający zasilanie metodą PoE (ang. *Power over Ethernet*), pojedynczy kabel sieciowy posłuży do doprowadzenia zasilania, podglądu na żywo i zapisu obrazu.

System jest dostarczany z obiektywem zmiennoogniskowym. Jako że kamera jest wyposażona w standardowe mocowanie typu CS, na żądanie mogą być dołączane również inne obiektywy.

System zawiera również dedykowane oprogramowanie dozorowe zapewniające zdalny podgląd na komputerze PC. Umożliwia to odtwarzanie zapisanego obrazu z maks. 16 kamer na ekranie monitora komputerowego. Dzięki temu oprogramowaniu można także łatwo archiwizować obraz w celu jego późniejszego wykorzystania. Funkcja inteligentnego wyszukiwania zapewnia śledzenie wybranych zdarzeń oraz przeszukiwanie zapisu pod kątem występowania ruchu.

Kamera zawiera dodatkowo funkcje wykrywania ruchu, sabotażu oraz dźwięku, które mogą posłużyć do uruchomienia alarmu lub podwyższenia jakości zapisywanego obrazu w celu uchwycenia większej liczby detali w scenie. Dostępna jest również funkcja dwukierunkowego przesyłania dźwięku, umożliwiająca komunikację operatora z gośćmi lub pracownikami za pośrednictwem kamery.

Przyznając firmie Bosch Security Systems nagrodę Detektor International 2009 w kategorii „innowacyjne osiągnięcie", jury doceniło połączenie wysokiej jakości i gotowości kamery do pracy zaraz po wyjęciu z opakowania. Zdaniem jury kamera sieciowa serii 200 stanowi innowacyjne rozwiązanie dozorowe dla szerokiego kręgu użytkowników.

Firma Bosch Security Systems już po raz trzeci została wyróżniona przez niezależnych, międzynarodowych ekspertów przyznających nagrody Detektor International. Nagrodę Best Alarm & Detection Product Award otrzymał głośnik wszechkierunkowy, natomiast Highly Commended Award przyznano Inteligentnej Analizie Obrazu (IVA – *Intelligent Video Analysis*). Nagrody przyznawane są corocznie przez międzynarodowy magazyn *Detektor International*. Do głównych kryteriów oceny należy wyróżniająca się innowacyjność oraz wkład w rozwój branży systemów zabezpieczeń.

Bezpośr. inf. Bosch Security Systems

Czytniki inteligentnych kart HID

pracują z nowym systemem operacyjnym **Windows 7**

Firma **HID Global** ogłosiła, że czytniki inteligentnych kart HID z łączem do komputera serii OMNIKEY uzyskały certyfikat zgodności z nowym systemem Microsoft Windows 7. Czytniki kontaktowe i zbliżeniowe OMNIKEY, które zdobyły uznanie dzięki łatwości instalacji i stabilności sterownika, zostały przebadane i są kompatybilne z nowym systemem operacyjnym.

Na początku roku, oczekując na nową platformę programową Windows, inżynierowie produktu HID Global zaczęli opracowywać, testować i wdrażać oprogramowanie. Pierwsze czytniki certyfikowano w kwietniu 2009 r. Zapewniają one współpracę poprzez łącze USB. Użytkownicy komputerów PC, którzy wykorzystują czytniki OMNIKEY do identyfikacji lub innych zastosowań, mają pewność, że będą one działać po przejściu na nowy system operacyjny.

Certyfikat WHQL uzyskały sterowniki do następujących rodzin czytników OMNIKEY:

- **czytniki bezkontaktowe (zbliżeniowe) lub w technologii dualnej**: 5321, 5125, 5325, 6321,
- **czytniki kontaktowe**: 3021, 3121, 3621, 3821, 3921, 1021, 4040, 4321, 7121.

Sterowniki do czytników OMNIKEY wraz ze sterownikiem Windows 7 można pobrać pod adresem: *http://www.hidglobal.com/driverDownloads.php?techCat=19*.

Bezpośr. inf. Paula Tienza
HID Global
Tłumaczenie: Redakcja

Warsztaty Boscha:

Projektowanie systemów bezpieczeństwa w budynkach

– podsumowanie

Firma **Bosch** przykłada szczególną wagę do wsparcia technicznego udzielanego projektantom systemów zabezpieczeń, dlatego regularnie przeprowadza specjalne szkolenie poświęcone projektowaniu systemów bezpieczeństwa w budynkach. W tym roku warsztaty odbyły się 5 listopada w hotelu Polonia Palace w Warszawie. Warsztaty przeprowadzono w czterech blokach tematycznych, zaś uczestnicy zostali podzieleni na mniejsze grupy, umożliwiające swobodną interakcję z prelegentami. Podczas spotkania projektanci mieli okazję zapoznać się z zasadami projektowania, jak również z narzędziami wspomagającymi projektowanie, a nawet przetestować urządzania prezentowane podczas szkolenia. Projektanci docenili organizację i tematykę warsztatów.

Pierwszy blok dotyczył projektowania systemów telewizji dozorowej w technologii IP. Obok korzyści z zastosowania systemów IP przedstawiono budowę sieci komputerowej dedykowanej systemowi CCTV IP i podkreślono rolę okablowania strukturalnego. Poruszono temat systemów zarządzania sygnałem wizyjnym w systemach IP i nowoczesnych technologii – Inteligentnej Analizy Obrazu (IVA) oraz inteligentnego wyszukiwania nagrań – które wspomagają działanie tych systemów. Prowadzący przedstawili również przykładową konfigurację urządzeń składających się na system CCTV IP.

W bloku poświęconym nagłośnieniu położono nacisk na narzędzia wspomagające projektowanie, dźwiękowe systemy ostrzegawcze (DSO) oraz systemy kongresowe. Firma Bosch zaprezentowała wiele przydatnych aplikacji, które znacznie upraszczają proces konfiguracji systemów nagłośnieniowych i DSO, m.in. narzędzie doboru głośników, które pomaga prawidłowo rozmieścić głośniki w wybranym obiekcie, program EASE Address do symulacji warunków akustycznych w budynkach, jak również konfigurator systemu nagłośnieniowego Plena. Wiele uwagi poświęcono również konfiguracji systemu Praesideo w oparciu o rozwiązania MCI/BAM oraz nagłośnieniu IP Audio. Na spotkaniu dla projektantów po raz pierwszy zaprezentowano systemy kongresowe firmy Bosch. Zdobyta przez uczestników wiedza z zakresu systemów konferencyjnych może okazać się szczególnie przydatna w momencie objęcia przez Polskę przewodnictwa w Radzie Unii Europejskiej. Projektowanie systemów kongresowych zaprezentowano na przykładzie rozwiązań Integrus oraz DCN.

Dużą popularnością cieszył się blok poświęcony projektowaniu systemów sygnalizacji pożarowej. Do ważnych punktów spotkania należało przedstawienie zasad projektowania SAP na przykładzie wymagań VdS, a także zastosowanie narzędzi wspomagających projektowanie – Fire System Designer firmy Bosch.

Kolejna sesja dotyczyła projektowania zintegrowanych systemów zabezpieczeń obiektów wykorzystujących systemy kontroli dostępu firmy Bosch. Przedstawiono tu Access Professional Edition z funkcją wideoweryfikacji oraz zastosowanie systemu zarządzania budynkowego Building Integration System.

W tym bloku położono nacisk na rozwiązania stosowane w projektowaniu nowoczesnych systemów sygnalizacji włamania i napadu (SSWiN). Poruszono kwestię norm europejskich dotyczących systemów alarmowych. Zaprezentowane zostało narzędzie wspierające prace projektowe – program doboru czujek. Obecni na szkoleniu projektanci jako pierwsi poznali nową centralę alarmową Modular Alarm Panel. Uczestnicy zgodnie potwierdzili, iż jest to całkowicie nowatorskie podejście do sposobu zabezpieczania obiektów przed włamaniem.

Specjalne aplikacje, pomocne podczas konfiguracji systemów zabezpieczeń, są dostępne na stronie internetowej Bosch Security Systems (*www.boschsecurity.pl*).

Bezpośr. Inf. Bosch Security Systems

Współpraca CMA z LKW WALTER Internationale Transportorganisation

Zakończył się proces integracji oferowanego przez **CMA** Satelitarnego Systemu Monitorowania Pojazdów z systemami wykorzystywanymi przez **LKW WALTER**.

Firma LKW WALTER Internationale Transportorganisation – potentat na rynku spedycji międzynarodowej w Europie – rekomenduje Automonitoring GPS współpracującym z nią firmom przewozowym.

Automonitoring podlega nieustannemu rozwojowi, integruje się z innymi firmami i wzbogaca się o możliwość wykonywania zdjęć systemowych przez miniaturową kamerę VGA. Transmisja obrazu jest realizowana w postaci stop-klatek – zdjęć, które poddane są kompresji JPEG. Poprzez pozycjoner C1 zdjęcia są przesyłane do systemu Automonitoring. Gdy żądane jest wykonanie zdjęcia, możliwe jest określenie jego rozmiaru (320×240 lub 640×480). Kamerka jest przeznaczona do zastosowania wewnątrz kabiny kierowcy, wewnątrz przestrzeni ładunkowej, a także na zewnątrz pojazdu (po zastosowaniu specjalnej obudowy).

Zastosowanie:

– wykonywanie zdjęć wnętrza kabiny pojazdu, przestrzeni ładunkowej lub otoczenia pojazdu (droga przed lub za pojazdem),
– weryfikacja obecności osób w kabinie kierowcy lub przestrzeni ładunkowej pojazdu,
– bankowozy,
– autobusy komunikacji miejskiej,
– busy,
– monitoring pracy pojazdów specjalistycznych, takich jak wozy asenizacyjne przedsiębiorstw wodociągowych, pługi, solarko-piaskarki, zamiatarki itp.

Bezpośr. inf. Magdalena Kalinowska
CMA

Targi INTELECTRICA 2009
– podsumowanie

24 września, w Białymstoku, odbyły się pierwsze targi **INTELECTRICA 2009** zorganizowane przez Zakład Technicznej Ochrony Mienia **CORAL** (projektowanie i kompleksowa realizacja instalacji elektrycznych i teletechnicznych oraz automatyki budynków) oraz Wyższą Szkołę Administracji Publicznej im. Stanisława Staszica.

Na targach zaprezentowano nowoczesne technologie z zakresu elektronicznych systemów ochrony mienia, telekomunikacji i łączności, automatyki budynków, instalacji elektrycznych i systemów grzewczych. Intencją organizatorów targów było przybliżenie mieszkańcom koncepcji inteligentnego budynku.

Była to pierwsza tego typu impreza na Podlasiu. Ofertę targową skierowano do firm instalacyjnych branży elektrycznej i *security*, architektów i projektantów systemów zabezpieczeń, przedstawicieli administracji państwowej, dyrektorów szkół, spółdzielni mieszkaniowych, przedstawicieli banków i firm ubezpieczeniowych oraz wiodących przedsiębiorstw z regionu północno-wschodniej Polski. Goście odwiedzający targi mieli wyjątkową okazję do rozmowy z ekspertami na interesujące ich tematy.

Wystawcy pierwszych targów INTELECTRICA 2009 to: ADI Ultrak, Altram i systemy IP Sony, Bosch, C&C Partners, DEVI/Danfoss, Elkond z ofertą partnerów handlowych Philips, OBO Betermann i ZPAS, Eltcrac, Felix i systemy grzewcze LG, agencja ochrony G4S, GE Security, MoelleR, Intratel, Pulsar, Ropam, Siemens.

Podczas targów prowadzone były wykłady tematyczne:

– Bosch: *Zaawansowana analiza obrazu IVA*;
– Philips/Elkond: *Ekonomiczne i techniczne aspekty modernizacji oświetlenia szkół. Przykłady rozwiązań w oparciu o oprawy i źródła światła Philips*;
– WSAP: *Dotacje dla małych i średnich przedsiębiorstw z funduszy Unii Europejskiej*;
– Siemens: *Obniżenie kosztów funkcjonowania przedsiębiorstw i uczelni w czasach kryzysu a zawansowane rozwiązania transmisji głosu i wideo oparte na protokole IP*;
– Sony: *IPELA, czyli telewizja przemysłowa w technologii sieciowej, systemy multimedialne Sony – ekrany, projektory, systemy zarządzające.*

Atrakcją targów INTELECTRICA 2009 były pokazy Białostockiego Klubu Karate.

Bezpośr. inf. Coral

Systemy monitoringu wideo na stadionach
– podsumowanie konferencji

Realizacja ustawy z zachowaniem zdrowego rozsądku

W dniu 28 października 2009 roku, z inicjatywy **spółki PL.2012** (spółka ma za zadanie koordynować przygotowania do piłkarskich mistrzostw EURO 2012), w Centrum Olimpijskim w Warszawie odbyła się konferencja *Systemy monitoringu wideo na stadionach*. W konferencji udział wzięli przedstawiciele spółki PL.2012, inwestorów, MSWiA i policji, klubów piłkarskich, producentów urządzeń i systemów monitoringu oraz instalatorzy tych systemów. Aby konferencja miała wysoki poziom merytoryczny, do dyskusji w panelu bloków tematycznych zaproszeni zostali liczni eksperci z branży zabezpieczeń, na co dzień zajmujący się najnowszymi rozwiązaniami z zakresu monitoringu wizyjnego.

W czasie konferencji wygłoszono kilka referatów. Sympozjum otworzył Rafał Kapler – członek zarządu PL.2012 ds. organizacji. Podczas swojego wystąpienia powiedział zebranym, że EURO 2012 to szansa na przyspieszenie cywilizacyjne dla Polski, a dzięki nowym inwestycjom mamy szansę pokazać Europie, że jesteśmy solidnym partnerem w dużych przedsięwzięciach i że zależy nam nie tylko na zbudowaniu nowoczesnego centrum monitoringu, ale również na zapewnieniu kibicom i sportowcom dobrej, sportowej atmosfery podczas imprez sportowych. W swoim wystąpieniu przekazał informacje o stanie przygotowań do EURO 2012 w odniesieniu do sześciu stadionów, budowy dróg, komunikacji kolejowej i lotniczej, a także innych aspektów związanych z organizacją tej imprezy.

– Planuje się zamontowanie na Stadionie Narodowym 900 kamer, które będą monitorowały trybuny i inne miejsca należące do obiektu. W Poznaniu mają być 673 kamery, we Wrocławiu 553, a w Gdańsku 500. Dla porównania podczas EURO 2008 na wiedeńskim stadionie było zainstalowanych 40 kamer, natomiast na stadionie Allianz Arena w Monachium jest ich ponad 90 – powiedział Rafał Kapler.

Generalnie przesłanie Rafała Kaplera było następujące: czy monitoring wizyjny musi być aż tak rozbudowany?

Zaraz po nim wystąpił Michał Błażewicz ze spółki PL.2012, odpowiedzialny za projekty związane z telekomunikacją i systemami teleinformatycznymi na potrzeby organizacji EURO2012. W swej prezentacji odniósł się, naszym zdaniem bardzo merytorycznie, do wymagań technicznych przedstawionych w projekcie nowego (projekt z 30 września 2009 r.) rozporządzenia MSWiA „w sprawie sposobu utrwalania przebiegu imprezy masowej, minimalnych wymagań technicznych dla urządzeń rejestrujących obraz i dźwięk oraz sposobu przechowywania materiałów". Pokazał, że można złagodzić wymogi związane z jakością nagrania (liczba pikseli w stosunku do wielkości obrazu) bez większego uszczerbku dla ich jakości.

Interesujące było wystąpienie inspektora Marka Pękały (z-cy dyrektora Centralnego Laboratorium Kryminalistycznego), który omówił możliwości procesowego wykorzystania nagrań z monitoringu. Podał on przykłady z życia wzięte i omówił problematykę jakości nagrań, która musi być odpowiednia, by można było wykorzystać nagrania jako dowód procesowy. Według niego obecne systemy rejestracji wideo na stadionach pełnią prawie wyłącznie prewencyjną funkcję. Nie pomagają w identyfikacji osób. Kamery nie rejestrują dostatecznej liczby stopklatek podczas ekspresyjnych zachowań kibiców, co bardzo utrudnia ich kontrolę podczas imprezy. – *Monitorowanie trybun i obiektów musi być rejestrowane w wysokiej rozdzielczości, w przeciwnym razie można zapomnieć o możliwości identyfikacji nagranych osób, które zachowywały się agresywnie i wobec których powinniśmy zastosować konsekwencje karne* – powiedział inspektor.

Prezentacje firm podzielone były na cztery bloki tematyczne:
– blok I – *Kompleksowe podejście przy tworzeniu systemu monitoringu wideo*,

– blok II – *Rejestrowanie, przechowywanie i kodowanie obrazu*,
– blok III – *Właściwy dobór kamer w zależności od miejsca montażu*,
– blok IV – *Ilościowa i jakościowa optymalizacja systemu monitoringu wideo*.

W poszczególnych blokach tematycznych swoje rozwiązania prezentowali przedstawiciele producentów urządzeń do monitoringu wizyjnego: Sony, Bosch Security Systems, Axis Communications, ISM EuroCenter, Pelco, Mobotix.

Byliśmy świadkami kilku prezentacji i ożywionych dyskusji na temat możliwych rozwiązań, a także podejścia projektantów do zagadnienia stosownej do rozporządzenia liczby kamer i faktycznej praktyki realizowania systemów monitoringu – w praktyce liczba zainstalowanych kamer jest znacznie mniejsza od liczby podanej w projekcie.

Przedstawiciele klubów sportowych i inwestorów, a nawet producentów sprzętu, pytali o powód tak restrykcyjnych wymagań odnośnie liczby kamer i jakości obrazu. Zastanawiali się, czy potrzebny jest stały monitoring ciągów komunikacyjnych, ogrodzenia i parkingów. W toku dyskusji padały argumenty przemawiające za zmniejszeniem liczby kamer. Za przykład podawano doświadczenia innych krajów europejskich, które uporały się z problemem bezpieczeństwa na stadionach, a ich sprawdzone już rozwiązania moglibyśmy przenieść na nasz polski grunt.

Reasumując, uważamy, że nowe rozporządzenie powinno być jeszcze raz skonfrontowane z rzeczywistymi potrzebami i realnymi technicznymi możliwościami realizacji systemów monitoringu wizyjnego na stadionach – ale nie tylko tam, gdyż rozporządzenie odnosi się do wszystkich imprez masowych zgodnie z ich definicją.

Piotr Czernoch
Teresa Karczmarzyk

Zapraszamy do obejrzenia fotoreportażu na stronie *www.zabezpieczenia.com.pl*.

Prezentacja systemu **Kronos** 750 m n.p.m.

17.10. br. w Ośrodku Konferencyjno-Wypoczynkowym „Kocierz", położonym w malowniczej scenerii Parku Krajobrazowego Beskidu Małego, firma Next! z Bielska-Białej zorganizowała pokaz swojego autorskiego, nowatorskiego nawet na skalę międzynarodową, systemu Kronos NET v. 2.0 Revolution.

Sam ośrodek, jak sądzę nieprzypadkowo wybrany na miejsce pracy i wypoczynku przez przedstawicieli firmy Next!, jest usytuowany na szczycie Przełęczy Kocierskiej i został wyróżniony na liście rankingowej „Dziesięć NAJ" Katalogu Obiektów i Usług Konferencyjnych „konferencje w Polsce" na rok 2009 w kategorii „TOP 10 Obiekty Incentive". Nie pisałabym o tym, ale sam ośrodek i jego otoczenie zasługują na rekomendację. Kompleks posiada typowe cechy efektownej góralskiej architektury drewnianej i jednocześnie uwzględnia współczesne potrzeby przyjezdnych, co nie jest dla nas, mieszczuchów, całkiem bez znaczenia. Oryginalne, utrzymane w góralskim stylu wnętrza, dyskretna i życzliwa pomoc pracowników oraz doskonała kuchnia sprawiają, że chce się tam wracać i polecać ośrodek innym. Zadziwił mnie ogrom ośrodka, a także wielość i różnorodność imprez odbywających się jednocześnie, bez uszczerbku dla którejkolwiek.

Powracam do wątku głównego mojego sprawozdania, czyli zaktualizowanej i poprawionej wersji systemu Kronos. Robię to z wielką przyjemnością, bo zawsze twierdziłam (i podtrzymuję swoją opinię), że mamy w kraju bardzo zdolnych inżynierów, którzy już nie raz udowodnili, że potrafią wykorzystać swoją wiedzę i zastosować ją w praktyce, w tym konkretnym przypadku tworząc oprogramowanie dla rynku ochrony, z którego wywodzą się właściciele firmy, ale nie tylko. Dzięki elastyczności i wszechstronności produktów klientami Nexta są, oprócz agencji ochrony i stacji monitorowania, między innymi: koncerny energetyczne, wojsko, korporacje, lotniska, policja i straż pożarna. Należy zwrócić uwagę na to, że firma ma wdrożony System Zarządzania Jakością ISO 9001:2000 a produkty mają zapewnioną ochronę ubezpieczeniową TU Allianz.

Podczas pobytu w siedzibie firmy oraz w czasie prezentacji systemu w Kocierzy zauważyłam, że właściciele Nexta mają bardzo dobry kontakt z pracownikami. Razem tworzą zgrany, energiczny i sympatyczny zespół. Gołym okiem widać, że szefowie zarazili swoim zapałem i pasją młodsze koleżanki i kolegów. Wszystko to powoduje, że opinie o samej firmie i o stylu jej działania są pozytywne – wyczuwa się w niej olbrzymi potencjał intelektualny. Elastyczność działania i kreatywność to tylko niektóre cechy, które wyróżniają ją spośród innych tego typu firm. W przypadku zakupu oprogramowania istotna dla odbiorców jest gotowość sprzedawcy do jego aktualizacji. Tak samo ważne jest wczesne eliminowanie wszelkich ewentualnych, wynikłych podczas prac programistycznych, usterek. Serwisanci utrzymują stały kontakt z klientem i służą pomocą w sytuacjach, gdy wsparcie programistów jest niezbędne. Tak właśnie jest w przypadku firmy Next!.

Ponadto programy są pisane tak, aby można je było łatwo dostosować do specyfiki różnych branż czy firm w ramach ceny oprogramowania.

Aby dobrze przygotować nasze niedotlenione, przepracowane umysły do wysiłku, czyli do pełniejszego zrozumienia i przyswojenia zerojedynkowego świata programistów (a konkretnie – aby przygotować zaproszonych gości do prezentacji systemu Kronos), gospodarze imprezy zaprosili na wyprawę na quadach lub – jak kto woli – wszędołazach (to określenie bardziej mi się podoba). Nadmienię, że pogoda spłatała nam psikusa i, zamiast jesiennej, przywitała nas typowa zimowa aura. Oczywiście, jak skomentowali nasi trenerzy sportów ekstremalnych, uchroniło to nas, ale tylko częściowo, od kąpieli błotnej. Jazda na wszędołazach w terenie górzystym, po zaśnieżonych, leśnych bezdrożach, była nie lada wyzwaniem, ale urok miejsca i wysoki poziom adrenaliny spowodowały, że z eskapady wróciliśmy przemoczeni i zmęczeni, ale za to doskonale zregenerowani i naładowani energią nie tylko na czas prezentacji systemu – wystarczyło mi jej również na kilka kolejnych, pracowitych dni w redakcji.

Nie będę opisywać Kronosa, gdyż po pierwsze moja wiedza na jego temat jest, delikatnie mówiąc, niewystarczająca, a po drugie mogę zacytować Sławomira Pielę, który pięknie opowiedział mi o systemie. Sławomir Piela i Bartłomiej Dryja są pomysłodawcami i współtwórcami Kronosa.

– Nasza praca z Kronosem, pośród radości, sukcesów i nieuniknionych porażek, to z jednej strony reagowanie na nowe pomysły klientów dostrzegających elastyczność i potencjał tej platformy (czasem uginamy się pod ich liczbą, co i cieszy, i martwi), a z drugiej sprawdzanie, jak nowe, oryginalnie przez nas stworzone rozwiązania, ubrane w realny kształt funkcjonalności systemu, spełniają oczekiwania użytkowników. Część pomysłów, jak na przykład praca grupowa czy nowy interfejs, jest unikatowa, wedle naszej wiedzy na skalę światową. Warto przy okazji wspomnieć, że nasze pomysły doceniane są także poza granicami Polski. Pomijając wdrożenia w wielu krajach, mamy swoich dystrybutorów w Czechach, Rosji, Słowacji, Ameryce, na Węgrzech. Obecni jesteśmy między innymi na rynku ochrony w Republice Południowej Afryki, Ugandzie. Tworzenie interfejsów w języku chińskim czy hebrajskim było jednym z ciekawszych doświadczeń. Efekty splatania się tych dwu dróg mieliśmy okazję niedawno zaprezentować. Szczególny nacisk kładliśmy na nowe, nietypowe rozwiązania, nie tylko pozwalające pracować efektywniej, ale dające możliwość zmiany sposobu myślenia o tym, w jaki sposób można prowadzić usługi ochrony. Podstawą budowy wspomnianych rozwiązań jest unikatowy silnik systemu – wydajny, uniwersalny, zapewniający szyfrowanie i bezpieczeństwo dzięki trójwarstwowej architekturze systemu monitoringu, którą wprowadziliśmy jako pierwsi w Polsce i prawdopodobnie na świecie. Wszystko to zostało zrealizowane w sposób nie wymagający ogromnych inwestycji w drogi sprzęt. Znający choć trochę kulisy pracy programistów wiedzą, że świadczy to o nieprzeciętnej jakości wykonania. Na tej bazie oparta jest możliwość pracy w grupie, polegająca na łączeniu się systemów Kronos i dynamicznej wymianie informacji pomiędzy zleceniodawcami i podwykonawcami. Automatyczny przepływ informacji o zdarzeniach oraz przepływ dokumentów pomiędzy firmami diametralnie zmienia jakość i skuteczność kooperacji.

Aby przybliżyć zakres działalności firmy Next!, przedstawię główne produkty wraz z ich krótką charakterystyką:

Kronos NET 2.0 – system zarządzania i integracji dużych stacji monitorowania (jest nie tylko programem do monitoringu, ale także wsparciem dla działów rozliczeń i serwisu). Połączenie w jednej platformie monitoringu budynków, pojazdów, osób, środowiska i telewizji dozorowej z kontrolą wykonywania serwisów, konserwacji, montaży i demontaży systemów alarmowych, a także z automatycznym wystawianiem faktur uwzględniających złożone kalendarze promocji, daje kompleksowe rozwiązanie informatyczne dla nowoczesnej stacji monitorowania. System będzie nadal rozwijany.

Kronos LT – jednostanowiskowy program integrujący dla małej i średniej stacji monitorowania. Powstał z myślą o klientach, którzy nie są informatykami i nie chcą zatrudniać specjalistycznej kadry. Jest łatwy do zainstalowania i natychmiast gotowy do użycia.

Kronos Guard – jednostanowiskowy program do aktywnej kontroli niewielkiej liczby strażników. Jest standardowym rozwiązaniem dostarczanym wraz z systemem aktywnej kontroli strażników ActiveGuard. W przeciwieństwie do tradycyjnych systemów pozwala na bieżąco kontrolować cykliczność dokonywania obchodów i natychmiast informuje o wszelkich spóźnieniach lub nieobecnościach.

Testowaliśmy nasz system w zakresie wydajności. Obsługa 50 tysięcy (słownie: pięćdziesięciu tysięcy) alarmów na jednym stanowisku bez opóźnień przy ich przejmowaniu to niby niepraktyczna ciekawostka, świadcząca jednak o potężnej nadmiarowości systemu i skuteczności mechanizmu synchronizacji rozsyłania zmian. Absolutnie praktycznym zastosowaniem tego mechanizmu jest pobieranie raportów, które, niezależnie od swej wielkości, nie blokują i nie zatrzymują pracy systemu. Co więcej – można je w dowolnej chwili zatrzymać.

Najnowszym elementem systemu jest nowy dotykowy interfejs. Swoją premierę będzie miał na targach Securex – już dziś zapraszamy na nasze stoisko, aby tym razem DOSŁOWNIE dotknąć czegoś, czego nikt nigdy i nigdzie wcześniej nie zrobił.

Prawda, że warto było zacytować całą wypowiedź Sławomira Pieli?

Teresa Karczmarzyk

Jubileuszowa edycja
targów Alarm już za nami

4 i 5 listopada 2009 r. w Kielcach odbyła się **IX Międzynarodowa Konferencja „Bezpieczny Stadion 2009”** i **Wystawa Wyposażenia i Budowy Obiektów Sportowych „SPORT-OBIEKT”**, a także jubileuszowa **X Ogólnopolska Konferencja „Bezpieczne miasto – monitoring wizyjny miast”** i **Wystawa Monitoringu Wizyjnego „ALARM”.**

Patronat honorowy nad konferencjami objęli: Minister Spraw Wewnętrznych i Administracji, Minister Sportu i Turystyki, Komendant Główny Policji oraz Prezes Polskiego Komitetu Olimpijskiego.

Konferencja Bezpieczny Stadion 2009 została zorganizowana we współpracy z Polskim Związkiem Piłki Nożnej. Wiceprezes zarządu Targów Kielce Bożena Staniak powitała wszystkich gości i uczestników, a uroczystego otwarcia konferencji i wystawy dokonał prezes PZPN Grzegorz Lato. W swoim wystąpieniu wyraził nadzieję, że spotkanie przyczyni się do wymiany doświadczeń związanych m.in. z bezpieczeństwem w ramach organizacji piłkarskich mistrzostw Euro 2012, które odbędą się na terenie Polski i Ukrainy. Następnie Andrzej Bińkowski, przewodniczący Wydziału Bezpieczeństwa PZPN, podsumował sezon piłkarski 2008/2009. Podkreślił, że przez ostatnie lata stan bezpieczeństwa na polskich stadionach ulegał poprawie i jest coraz lepszy. Kluby inwestują w infrastrukturę stadionową. W związku ze zbliżającymi się mistrzostwami piłkarskimi powstają cztery nowe stadiony (w Warszawie, Wrocławiu, Gdańsku i Poznaniu), a pozostałe są modernizowane.

W konferencji wzięli udział także przedstawiciele Ministerstwa Spraw Wewnętrznych, którzy przedstawili ustawę o bezpieczeństwie imprez masowych oraz zadania Rady Bezpieczeństwa Imprez Masowych, która jest organem pomocniczym Prezesa Rady Ministrów. Rada zajmuje się m.in. opracowywaniem i oceną realizacji programów, których celem jest poprawa bezpieczeństwa imprez sportowych.

Kolejnym gościem konferencji był podinspektor Dariusz Dymiński, naczelnik Wydziału Operacyjnego Komendy Głównej Policji. W swoim wystąpieniu przedstawił wdrażaną obecnie w Policji filozofię 3T (troska, tolerancja, tłumienie). Filozofia 3T sprawdziła się w krajach, które organizowały duże imprezy piłkarskie. Wszelkiego rodzaju działania policji będą prowadzone w trosce o kibiców. Musimy nauczyć się również większej tolerancji dla tych, których zachowanie może odbiegać od ogólnie przyjętych norm społecznych. Tłumienie oznacza interwencję małych jednostek policji w przypadku zaistnienia sytuacji zakłócających porządek lub zagrażających bezpieczeństwu pozostałych kibiców. Ważną rolę podczas mistrzostw w 2012 r. mają odegrać spottersi, którzy współpracują z prawdziwymi fanami piłki nożnej. Ich zadaniem jest przenikanie w struktury kibiców i prowadzenie działań prewencyjnych. Dotychczas w szeregach policji jest 50 odpowiednio przeszkolonych funkcjonariuszy. Ich liczba na pewno wzrośnie do 2012 roku. Podinspektor Dariusz Dymiński powiedział, że „należy zdecydowanie oddzielić kibiców od chuliganów, ponieważ ci drudzy to stadionowi przestępcy”.

Po wystąpieniu przedstawiciela KG Policji zabrał głos Marcin Stefański, dyrektor Departamentu Logistyki Rozgrywek Ekstraklasa. Uczestnicy konferencji mieli okazję zapoznać się z celami i misją Systemu Identyfikacji Osób uczestniczących w imprezach piłkarskich.

Stan przygotowań do mistrzostw w 2012 r. podsumował Adam Olkowicz, dyrektor turnieju UEFA Euro 2012. 18 kwietnia 2007 r. Michel Platini ogłosił, że Polska i Ukraina będą gospodarzami piłkarskich mistrzostw Europy w 2012 r., ale to w 2003 r. zarządy PZPN-u i FFU (ang. *Football Federation of Ukraine*) podjęły wspólną uchwałę w sprawie starań o Euro 2012. Oprócz budowy i modernizacji stadionów potrzebujemy olbrzymiej bazy hotelowej i odpowiedniego poziomu transportu i komunikacji. Zorganizowanie mistrzostw Europy to duże przedsięwzięcie, ale jesteśmy na dobrej drodze, żeby wszystko zakończyło się pomyślnie.

Gośćmi specjalnymi konferencji Bezpieczny Stadion 2009 byli Marc Timmer, dyrektor Departamentu Bezpieczeństwa Stadionowego UEFA, i Kenneth Scott, doradca UEFA ds. Bezpieczeństwa. W swoim wystąpieniu reprezentanci UEFA przedstawili problemy pojawiające się podczas organizacji mistrzostw piłki nożnej, w tym Euro 2012. UEFA stawia wysokie wymagania organizatorom mistrzostw, ale chętnie dzieli się swoim doświadczeniem. Najważniejsze jest bezpieczeństwo. – *Jeżeli turniej nie jest bezpieczny, to ponieśliśmy porażkę* – powiedział Marc Timmer.

Kenneth Scott podkreślił, że standardy bezpieczeństwa UEFA muszą być spełnione. Aby tak się stało, potrzebna jest wymiana informacji i doświadczenia. W swoim wystąpieniu przypomniał o tragedii w Bradford z 11 kwietnia 1985 r., gdzie zginęło 56 osób, i tragedii w Sheffield z 15 kwietnia 1989 r. – wówczas na stadionie Hillsborough zginęło 96 osób. Po tak dramatycznych wydarzeniach na stadionie Hillsborough władze nakazały zdjęcie wszelkiego rodzaju ogrodzenia (siatek, płotów) i utworzenie wyłącznie miejsc siedzących. Ważne jest również szkolenie ludzi zajmujących się ochroną stadionów. Poza zapewnieniem bezpieczeństwa bardzo ważna jest odpowiednia atmosfera mistrzostw. W krajach europejskich, które organizowały już mistrzostwa, zamiast dużej liczby policjantów, którzy wzbudzają w kibicach różne emocje, na stadionach obecni są spottersi.

Wystąpienie przedstawicieli UEFA zakończyło IX Międzynarodową Konferencję „Bezpieczny Stadion 2009", po której wszyscy goście udali się na uroczystą GALĘ FAIR PLAY, podczas której rozdano nagrody i wyróżnienia.

Nagrody i wyróżnienia przyznane w kategorii SPORT-OBIEKT (branża *security*)

Medale Targów Kielce

– za TCS-B5 z czytnikiem TCS-UCS4 dla firmy **Transcom System** z Krakowa

Wyróżnienia Targów Kielce

– za wysoką, podwójną bramkę stadionową BR3-2SK dla firmy **Gastop** z Zabierzowa

Nagrody i wyróżnienia przyznane w kategorii ALARM

Medale Targów Kielce

– za wysokiej rozdzielczości system nadzoru wideo AVIGILON dla **ISM EuroCenter** z Warszawy

– za inteligentny system analizy ruchu oraz monitoringu CCTV TATTILE dla **Fortuna Communication** z Wrocławia

– za grupę urządzeń do bezprzewodowej transmisji danych ULTIAIR dla firmy **Dipol** z Krakowa

Wyróżnienia Targów Kielce

– za IP-PRO 362/POE dla **Miwi-urmet** z Łodzi

Puchar Polskiego Związku Piłki Nożnej

– za inteligentny system analizy ruchu oraz monitoringu CCTV TATTILE dla firmy **Fortuna Communication** z Wrocławia

Drugiego dnia odbyła się X jubileuszowa konferencja „Bezpieczne miasto – monitoring wizyjny miast", którą oficjalnie otworzył Dariusz Michalak, dyrektor Wydziału Targów. Pierwszym prelegentem był Jerzy Bukała, główny specjalista w Wydziale Zarządzania Kryzysowego i Bezpieczeństwa Urzędu Miasta Kielce. Wygłosił referat pt. „Założenia funkcjonalno-użytkowe modernizowanego systemu monitoringu wizyjnego miasta Kielce". Rozbudowa i modernizacja już istniejącego systemu monitoringu ma na celu stworzenie systemu elastycznego i skalowanego. W planie jest również budowa sieci światłowodowej. Powstaną nowe stanowiska operatorskie.

Kolejnymi prelegentami byli Jarosław Kateusz, prezes zarządu Przedsiębiorstwa Komunikacji Miejskiej w Starachowicach, i Teresa Prokop, prokurent, którzy omówili wykorzystanie systemu monitoringu w środkach komunikacji miejskiej. Głównymi problemami związanymi z naruszeniem bezpieczeństwa w komunikacji miejskiej w Starachowicach są: dewastacja mienia w środkach komunikacji miejskiej, dewastacja wiat przystankowych, kradzież mienia, agresywne zachowanie pasażerów. W celu poprawy bezpieczeństwa Miejskie Zakłady Komunikacyjne zakupiły sześć nowych autobusów wyposażonych w system monitoringu, podpisały umowę z agencją ochrony, systematycznie szkolą swoich pracowników, rozpoczęły współpracę z kibicami klubu sportowego Star i uczestniczą w programie „Bezpieczna podróż". Miejskie Zakłady Komunikacyjne w Starachowicach pozyskały również środki finansowe z programu „Razem bezpieczniej". Od momentu pojawienia się monitoringu w środkach komunikacji miejskiej zmniejszyła się liczba aktów wandalizmu i aspołecznych zachowań.

W dalszej części konferencji firmy Dipol, Microsystem, S.P.S. Trading, ISM Eurocenter oraz Miwi-Urmet zaprezentowały swoje produkty przeznaczone do wykorzystania w systemach monitoringu.

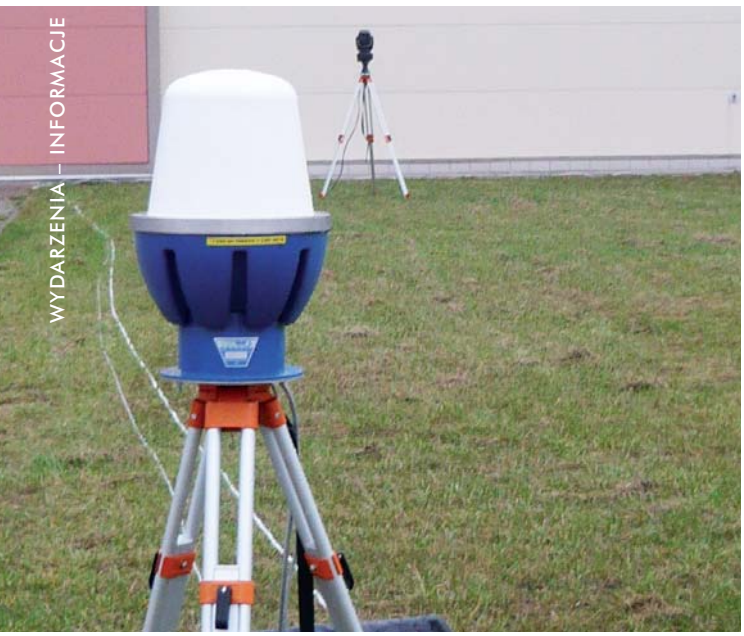
Ponadto w konferencji udział wzięli Bogusław Dyduch – ekspert PISA w zakresie bezpieczeństwa, Kazimierz Mądzik – dyrektor Zespołu Szkół Informatycznych w Kielcach, Jacek Balicki – sekretarz Urzędu Gminy w Wiślicy i ks. Paweł Tkaczyk – konserwator diecezjalny w Kielcach.

Z okazji jubileuszu w imieniu redakcji *Zabezpieczeń* składam na ręce Grzegorza Figarskiego, dyrektora projektu Ogólnopolskiej Konferencji „Bezpieczne miasto – monitoring wizyjny miast" i Wystawy Monitoringu Wizyjnego „ALARM", najserdeczniejsze gratulacje i wyrazy uznania za dotychczasowy wkład pracy, a także życzę kolejnych udanych konferencji i wystaw.

Ela Końka

Nowe trendy bezpieczeństwa na lotniskach w Polsce

– relacja z międzynarodowej konferencji w Izbicku



W dniach 12–13 września w Pałacu Izbicko (woj. opolskie), na zorganizowanej przez firmę **KABE Systemy Alarmowe** konferencji, spotkali się przedstawiciele polskich portów lotniczych oraz innych instytucji związanych z branżą lotniczą. Celem konferencji było przedstawienie zagrożeń, na jakie narażone są polskie lotniska, i zaprezentowanie najnowszych rozwiązań, które takim zagrożeniom mogą zapobiegać. Omawiane zagadnienia dotyczyły w szczególności bezpieczeństwa na terenach otwartych, wymagających równie dokładnego nadzoru, jak budynki terminali.

Niestety, obecnie zaobserwować można znaczną rozbieżność w poziomie ochrony na niekorzyść terenów otwartych. Co więcej, tereny otwarte traktuje się, często niesłusznie, jako drugorzędne w analizie zagrożeń i podczas projektowania systemów ochrony. Ponadto teren otwarty lotniska bardzo utrudnia patrolom Służby Ochrony Lotniska należyty nadzór ze względu na swoją wielkość i ciągły ruch samolotów.

Swoje propozycje rozwiązania tych problemów zaprezentowały na konferencji zarówno firmy polskie (KABE Systemy Alarmowe, CBC Poland, ADI Global Distribution), jak i światowi liderzy w tej branży (ICx Technologies, Fiber SenSys, Navtech Radar, TELESTE).

Spośród proponowanych rozwiązań szczególną uwagę słuchaczy zwróciły:

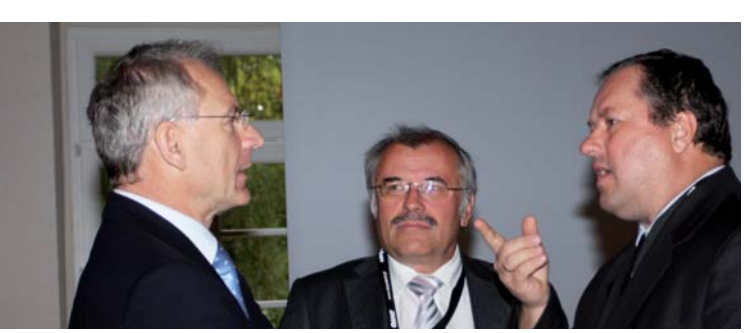
– radary mikrofalowe i kamery termowizyjne dalekiego zasięgu służące do detekcji, weryfikacji i śledzenia intruza na obszarze płyty lotniska w każdych warunkach pogodowych i świetlnych,
– system detekcji intruza do ochrony obwodowej, oparty na światłowodowym kablu sensorycznym montowanym na ogrodzeniu,
– rozwiązania integrujące powyższe systemy przy wykorzystaniu programów zarządzających oraz z użyciem technologii wideo 3D,
– ręczne urządzenie służące do wykrywania materiałów wybuchowych oraz innych niebezpiecznych substancji.

Dodatkowym atutem konferencji okazała się prezentacja działania wyżej wymienionych urządzeń i rozwiązań w warunkach terenowych na pobliskim lotnisku w Kamieniu Śląskim.

Przed Polską chyba najważniejsza w historii kraju impreza sportowa – EURO 2012. Zarządy polskich lotnisk chcą jak najlepiej wykorzystać pozostały czas na inwestowanie w rozbudowę i modernizację infrastruktury swoich portów lotniczych. Z uwagi na jakże realne w tych czasach zagrożenia terrorystyczne nie można zapomnieć także o rozszerzeniu i unowocześnieniu systemów potrafiących skutecznie tym zagrożeniom przeciwdziałać. Zapewnienie pasażerom odpowiedniego poziomu bezpieczeństwa urasta do rangi najważniejszego wyzwania dla służb ochrony lotnisk. Prezentowane podczas konferencji rozwiązania potrafią w znacznym stopniu pomóc sprostać tym wyzwaniom.

Pragniemy podziękować wszystkim uczestnikom oraz firmom, dzięki którym organizacja tej konferencji była możliwa. Opinie zaproszonych gości na jej temat były bardzo pozytywne, co utwierdza nas w przekonaniu, że tego typu inicjatywy są potrzebne. Podobna konferencja z pewnością zostanie przez nas zorganizowana w przyszłym roku. Już teraz zapraszamy do regularnych odwiedzin naszej strony internetowej *www.kabe.pl*, na której będziemy zamieszczać bieżące informacje na ten temat.

Bezpośr. inf. Kabe



Bezpiecznych Świąt!

Spokój w rodzinnym gronie
zapewniają urządzenia do systemów alarmowych Satel.

Z okazji zbliżających się Świąt Bożego Narodzenia
pragniemy życzyć Państwu dużo spokoju,
rodzinnej atmosfery oraz
wielu sukcesów...

Satel®

ul. Franciszka Schuberta 79, 80-172 Gdańsk, tel.: (0 58) 320 94 00, fax: (0 58) 320 94 01
e-mail: satel@satel.pl, www.satel.pl

Co nowego na targach SECUREX?

Nowa lokalizacja, nowy system rejestracji zwiedzających, nowy szef projektu to tylko niektóre zmiany, które czekają na uczestników 17-tej już edycji Międzynarodowej Wystawy Zabezpieczeń SECUREX

Międzynarodowa Wystawa Zabezpieczeń SECUREX odbędzie się w dniach od 26 do 29 kwietnia 2010 roku w Poznaniu. Dyrektorem targów została Joanna Jasińska, która już w przyszłym roku planuje wdrożenie innowacyjnych pomysłów.

– *Jesteśmy dumni z faktu, że z roku na rok liczba uczestników oraz profesjonalistów wzrasta, a targi SECUREX zdobyły pozycję największego i najbardziej prestiżowego wydarzenia branży zabezpieczeń w Polsce i w Europie Środkowej. Jestem przekonana o tym, że przyszłoroczna edycja będzie wyjątkowa* – mówi nowy dyrektor targów.

Przyszłoroczna edycja po raz pierwszy zostanie zlokalizowana w „czteropaku" – nowoczesnym kompleksie pawilonów 7, 7A, 8, 8A. Dzięki nowej lokalizacji wszystkich wystawców targów SECUREX będzie można znaleźć w jednym miejscu, a zwiedzający dotrą do nich bez konieczności wychodzenia na zewnątrz. Profesjonalistom z branży zabezpieczeń z pewnością ułatwi to rozeznanie się w bogatej ofercie wystawców i odnalezienie w krótkim czasie interesujących ich produktów czy rozwiązań. Ale to nie koniec nowości. We wrześniu 2009 roku Międzynarodowe Targi Poznańskie wdrożyły nowoczesny system rejestracji zwiedzających, dzięki któremu można uzyskać pełną wiedzę na temat profilu i zainteresowań gości. Dodatkowo podczas nowej edycji zwiedzający będą mieli możliwość zakupu biletów on-line, co znacznie ułatwi zwiedzającym zaplanowanie wizyty w Poznaniu.

Mnóstwo nowości

Rozwój branży zabezpieczeń jest nierozerwalnie związany z postępem technologicznym oraz wdrażaniem innowacji. Targi SECUREX odbywają się w cyklu dwuletnim, dlatego zwiedzający z pewnością docenią fakt, iż w jednym miejscu i czasie będą mogli zapoznać się nie tylko z premierami targowymi, ale także z absolutnymi nowościami na rynku.

– *Liczymy na to, że wzorem ostatniej edycji, podczas której zaprezentowano ponad 180 nowości, również w przyszłym roku firmy zaskoczą gości imponującą liczbą nowinek technologicznych – produktów debiutujących w ofercie lub po raz pierwszy*

prezentowanych na targach. Wspólnie z Państwem chcemy zainteresować nimi profesjonalistów. W tym celu wydamy specjalny przewodnik dla zwiedzających (zawierający opis nowości, które będzie można zobaczyć na targach SECUREX), który będzie wysłany do gości targowych na miesiąc przed targami – mówi Joanna Jasińska.

Podobnie jak w roku 2008, w ramach przyszłorocznej edycji prezentowane będą najnowsze rozwiązania z dziedziny systemów wykrywania i zwalczania przestępczości, mechanicznych i elektronicznych systemów zabezpieczeń, systemów wizyjnego nadzoru (CCTV) i ochrony mienia. Międzynarodowa Wystawa Zabezpieczeń daje możliwość zaprezentowania swojej oferty wśród przedstawicieli branży zabezpieczeń. Na targach SECUREX można z powodzeniem kreować wizerunek firmy, umacniać markę produktów, promować debiutujące produkty, weryfikować konkurencyjność i innowacyjność swojej oferty, a także nawiązać cenne kontakty biznesowe z przedstawicielami rynku polskiego i partnerami zagranicznymi. Do odwiedzenia Międzynarodowej Wystawy Zabezpieczeń i zaprezentowania oferty podczas targów zachęca hasło przewodnie: „SECUREX – zabezpiecz swój sukces".

Program wydarzeń – istota targów

Program wydarzeń Międzynarodowej Wystawy Zabezpieczeń jest bardzo interesujący – nie zabraknie konferencji, seminariów, wykładów i pokazów zorganizowanych z udziałem stowarzyszeń branżowych, ośrodków naukowych lub pod patronatem wystawców dla wszystkich poszukujących najnowszej wiedzy praktycznej z dziedziny zabezpieczeń.

Istotnym elementem programu targów SECUREX będą konkursy promujące innowacyjność, jakość produktów oraz profesjonalizm w zakresie instalowania systemów alarmowych.

Pierwszego dnia targów odbędzie się uroczystość wręczenia nagród w XIII edycji konkursu Polski Mistrz Techniki Alarmowej, organizowanego przez Stowarzyszenie POLALARM, w którym udział wezmą polscy i zagraniczni producenci i dystrybutorzy elektronicznych i elektromechanicznych urządzeń oraz systemów przeznaczonych do ochrony osób i mienia.

Instalatorów z pewnością zainteresują II Mistrzostwa Polski Instalatorów Systemów Alarmowych organizowane wraz z Polską Izbą Systemów Alarmowych.

Ponadto odbędą się liczne konferencje dedykowane poszczególnym grupom zwiedzających, przede wszystkim projektantom, instalatorom i wykonawcom, a także inwestorom, w tym przedstawicielom samorządów, instytucji, branży bankowej i sieci handlowych.

Organizatorzy – Międzynarodowe Targi Poznańskie oraz ich partnerzy – dokładają wszelkich starań, by wiedza o bogatym programie targów na czas dotarła do zainteresowanych osób, a także aby strona merytoryczna SECUREXU stanowiła dodatkowy powód zachęcający gości do przyjazdu na targi do Poznania. Międzynarodowa Wystawa Zabezpieczeń jest dużym wydarzeniem medialnym. Świadczy o tym obecność czołowych pism branżowych oraz mediów ogólnopolskich.

Duże zainteresowanie wystawców i zwiedzających

Targi SECUREX cieszą się niesłabnącym zainteresowaniem. Ostatnia edycja targów w 2008 roku zgromadziła blisko 220 wystawców z 18 krajów, min. z Austrii, Danii, Holandii, Niemiec, Szwecji, Wielkiej Brytanii i Korei Płd. W Poznaniu obecni byli przedstawiciele niemal wszystkich najważniejszych polskich firm z branży zabezpieczeń (w tym wielu firm działających na rynku globalnym), a także wielu małych i średnich przedsiębiorstw. Na podkreślenie zasługuje rekordowa w historii frekwencja profesjonalistów z branży zabezpieczeń. Tymczasem na kolejną edycję targów, drugą od momentu wprowadzenia cyklu dwuletniego, zgłosiło się zdecydowanie więcej wystawców niż w roku 2008.

Równocześnie z Międzynarodową Wystawą Zabezpieczeń SECUREX odbywają się Międzynarodowe Targi Instalacyjne INSTALACJE oraz Międzynarodowe Targi Ochrony Pracy, Pożarnictwa i Ratownictwa SAWO. Jest to zatem doskonała propozycja dla wszystkich zainteresowanych kompleksową ofertą dotyczącą najnowszych systemów zabezpieczeń, rozwiązań w zakresie ochrony pracy i ratownictwa oraz systemów instalacyjnych.

Więcej informacji: *www.securex.pl*

Międzynarodowa Wystawa Zabezpieczeń SECUREX

Ochrona żeglugi i portów morskich

część 1

Poruszając tematykę ochrony żeglugi i portów morskich, należy wrócić do wydarzeń, jakie miały miejsce w Nowym Jorku 11 września 2001 r. Wtedy po raz pierwszy na taką skalę użyto środka transportu, nie tylko jako celu zamachu, ale również jako środka do jego wykonania. W związku z tymi wydarzeniami natychmiast zmieniony został sposób, a także zakres ochrony i kontroli na lotniskach i w samolotach. Na tym jednak nie poprzestano. Po przeprowadzeniu oceny ryzyka wykryta została inna gałąź transportu, która w związku z ilością, wartością oraz rodzajem przewożonego ładunku oraz pasażerów, przy jednoczesnym niskim ówcześnie stopniu zabezpieczenia, może stanowić przyszły cel ataków terrorystycznych lub stanowić środek takiego ataku. Mowa tu oczywiście o transporcie morskim, przy którego wykorzystaniu odbywa się ponad 90% międzykontynentalnych przewozów ładunku. Jednocześnie ocena wykazała, że większość portów stanowi część miast portowych i są to z reguły tereny całkowicie otwarte dla ruchu publicznego. Atak na statek pasażerski przewożący ponad 4000 osób lub użycie statku, który służy do przewozu skroplonego gazu i może pomieścić na pokładzie nawet do 200 000 metrów sześciennych gazu pod ciśnieniem, jako środka ataku terrorystycznego na niechroniony, znajdujący się na terenie miasta port morski musi działać na wyobraźnię każdego człowieka, nawet nie posiadającego szczegółowej wiedzy morskiej

W związku z powyższym Międzynarodowa Organizacja Morska (IMO[1]) podjęła prace mające na celu wzmocnienie ochrony żeglugi i obiektów portowych jako potencjalnie narażonych na akty terroru. W efekcie na Konferencji Dyplomatycznej w dniach 9–13 grudnia 2002 r. uchwalono poprawki do „Międzynarodowej konwencji o bezpieczeństwie życia na morzu, 1974 (SOLAS)", które wprowadziły nowy rozdział XI-2 przedmiotowej konwencji, odnoszący się wyłącznie do ochrony żeglugi, oraz „Międzynarodowy kodeks ochrony dla statków i obiektów portowych" (kodeks ISPS), jako załącznik do ww. konwencji, a także nałożono obowiązek ich wdrożenia do dnia 1 lipca 2004 r.[2]

Zapisy rozdziału XI-2 konwencji SOLAS przewidują, że rozdział oraz kodeks mają zastosowanie do wszystkich statków pasażerskich w żegludze międzynarodowej oraz statków towarowych i ruchomych platform wiertniczych o pojemności brutto powyżej 500[3] w żegludze międzynarodowej oraz wszelkich obiektów portowych obsługujących ww. statki. Zdefiniowany został również poziom ochrony jako prawdopodobieństwo stopnia ryzyka zajścia zdarzenia naruszającego ochronę lub próby jego wywołania. Aby zróżnicować stopień ryzyka, a tym samym zróżnicować środki zapobiegawcze w celu zmniejszenia prawdopodobieństwa zajścia zdarzenia, które wpłynęłoby na ochronę obiektów portowych, określono trzy poziomy ochrony.

W rozdziale XI-2 opisane zostały również ogólne obowiązki administracji państwa oraz statku i obiektu portowego, które następnie szczegółowo opisano w kodeksie ISPS. Przewidziano również powstanie tzw. „uznanych organizacji ochrony" (RSO – *Recognized Security Organization*), którymi mogą zostać organizacje posiadające odpowiednią wiedzę specjalistyczną dotyczącą ochrony i odpowiednią wiedzę na temat eksploatacji statków i portów. Będą one upoważnione przez administrację do prowadzenia działalności w zakresie ochrony żeglugi i portów.

1) Agenda ONZ ds. morskich.

2) W związku z szerokim zakresem regulacji dotyczących w równie szerokim stopniu statków i obiektów portowych, na potrzeby niniejszego artykułu oraz w związku z faktem, że problematyką ochrony statku zajmują się głównie przedsiębiorstwa armatorskie, instytucje klasyfikacyjne oraz administracja morska, omówione zostaną jedynie wymagania odnośnie obiektów portowych.

3) Pomiaru pojemności dokonuje się zgodnie z międzynarodową konwencją o pomierzaniu statków – TONNAGE 69.

Jak wspomniano powyżej, kodeks ISPS stanowi uszczegółowienie zapisów i wymagań konwencji SOLAS. Wstępnie został on podzielony na dwie części – A i B. Wymagania części A są obowiązkowe dla wszystkich państw stron konwencji, natomiast zapisy części B stanowią wytyczne dotyczące zakresu wykonania zobowiązań wynikających z części A, które mogą, ale nie muszą być stosowane – decyzję pozostawiono administracjom państw. Jako kluczowe wymagania kodeksu ISPS należy wskazać:

a) obowiązek stosowania trzech poziomów ochrony (poziom pierwszy obowiązuje podczas normalnego, codziennego funkcjonowania obiektu portowego, poziom drugi – gdy istnieje nieokreślone zagrożenie dla ochrony obiektu portowego, a poziom trzeci – gdy zagrożenie ochrony jest bezpośrednie),
b) przeprowadzenie ocen stanu ochrony obiektów portowych (PFSA – *Port Facility Security Assesment*), będących ocenami ryzyka i zagrożeń dla ochrony obiektu oraz ciągłości prowadzonej w nim działalności, która będzie zawierała:
   – identyfikację i ocenę ważnych składników majątku i infrastruktury, których ochrona ma ważne znaczenie,
   – identyfikację możliwych zagrożeń dla majątku i infrastruktury oraz określenie prawdopodobieństwa ich zajścia w celu ustalenia środków ochrony (zapobiegawczych),
   – identyfikację, wybór i ustalenie kolejności środków przeciwdziałania i zmian w procedurach oraz poziomu ich skuteczności w ograniczaniu podatności na zagrożenia,
   – identyfikację słabych punktów (w tym czynnika ludzkiego) w infrastrukturze, polityce i procedurach,
c) stworzenie planów ochrony obiektów portowych (PFSP – *Port Facility Security Plan*) – na podstawie ocen stanu ochrony – które będą zawierać postanowienia i wyznaczać różne środki ochrony (przeciwdziałania) dla każdego z trzech poziomów ochrony,
d) wyznaczenie odpowiednio wyszkolonej (zgodnie ze standardami IMO) osoby odpowiedzialnej za opracowanie i realizację postanowień PFSP – tzw. oficera ochrony obiektu portowego (PFSO – *Port Facility Security Officer*),
e) przeprowadzanie regularnych szkoleń i ćwiczeń związanych z ochroną obiektu portowego.

W praktyce przepisy kodeksu oznaczają zamknięcie dotychczas otwartych terenów portowych poprzez wprowadzenie środków ochrony fizycznej (kontroli dostępu) i zabezpieczenia technicznego (ogrodzeń, barier, systemów alarmowych) na podstawie przeprowadzonej oceny stanu ochrony obiektów portowych oraz postanowień ich planów ochrony. Przepisy kodeksu mają zapobiegać naruszeniom terenu obiektów portowych i statków, a także określać działania prewencyjne. W przypadku naruszenia zastosowanie powinny mieć środki, procedury i przepisy wynikające z odpowiednich regulacji krajowych, które określają postępowanie w sytuacji wystąpienia kryzysu lub zagrożenia obronności państwa.

W ślad za działaniami Międzynarodowej Organizacji Morskiej Unia Europejska podjęła inicjatywę w tej sprawie i dnia 31 marca 2004 r. Parlament Europejski i Rada przyjęły rozporządzenie w sprawie wzmocnienia ochrony statków i obiektów portowych (nr 725/2004). W zakresie ochrony obiektów portowych przepisy rozporządzenia zasadniczo stanowią powtórzenie przepisów kodeksu ISPS, wprowadzając dodatkowo jako obowiązkowe w państwach członkowskich UE ponad 30 punktów dotychczas zalecanej części B kodeksu. Tym samym zostały określone minimalne obowiązkowe wymagania w zakresie:

a) przeprowadzania ocen stanu ochrony obiektów portowych i planów ich ochrony,
b) minimalnych kryteriów, jakie musi spełniać uznana organizacja ochrony,
c) maksymalnego zakresu upoważnienia uznanej organizacji ochrony.

Rozporządzenie wprowadziło również system nadzoru nad państwami członkowskimi Unii Europejskiej w zakresie wykonywania obowiązków wynikających z kodeksu ISPS. W ramach nadzoru Komisja Europejska będzie wykonywać inspekcje w państwach członkowskich, aby ustalić, czy stosują się one do postanowień kodeksu i rozporządzenia WE 725/2004. Nieprawidłowe wdrożenie będzie podlegało sankcjom przewidzianym dla państw UE, które nie respektują postanowień Traktatu o Unii Europejskiej.

Przedstawiając projekt ww. rozporządzenia, Komisja Europejska wskazała wzmocnienie ochrony portów jako kolejny niezbędny krok, który powinien zostać wykonany w celu zapewnienia należytego zabezpieczenia zarówno portu, jak i miejsca styku portu z jego zapleczem. Z tego względu Komisja przedłożyła projekt stosownej dyrektywy. Przyjęta dnia 26 października 2005 r. dyrektywa 2005/65/WE w sprawie wzmocnienia ochrony portów wskazała ramy rozwoju polityki w zakresie ochrony portów, na obszarze których znajdują się wcześniej opisane obiekty portowe. Jako główny wymóg dyrektywy należy wskazać konieczność opracowania ocen stanu ochrony portów (PSA – *Port Security Assesment*) oraz planów ochrony portów (PSP – *Port Security Plan*) jako dokumentów integrujących wcześniej powstałe oceny stanu ochrony oraz plany ochrony obiektów portowych, ale także obejmujących w ocenie ryzyka tereny nie znajdujące się w granicach portów i obiektów portowych, które, znajdując się w pobliżu, mogą jednak stanowić zagrożenie dla ochrony portu lub stanowią infrastrukturę kluczową ze względu na bezpieczeństwo ekonomiczne państwa lub obronność. Dyrektywa określa również kryteria i wytyczne, którymi należy się posługiwać przy opracowywaniu ww. dokumentów ochrony portu.

O ile przepisy ratyfikowanej przez Polskę konwencji SOLAS oraz kodeksu ISPS jako przepisy międzynarodowe, a także przepisy rozporządzenia WE 725/2004, mogą być stosowane wprost, o tyle przepisy wspomnianej dyrektywy należy odpowiednio wdrożyć do prawa krajowego. W momencie publikacji ww. dyrektywy jedynym przepisem wymagającym ochrony portów morskich była ustawa o ochronie osób i mienia, która jednak wprowadzała tak szeroki zakres regulacji, że nie było możliwe wprowadzenie do niej szczegółowych i specjalistycznych wymagań z zakresu gospodarki morskiej. W związku z tym rozpoczęto prace nad projektem nowej ustawy, której celem jest stworzenie systemu ochrony żeglugi i portów morskich, w szczególności ochrony życia i zdrowia ludzi oraz ochrony portów, obiektów portowych i statków, na wypadek zagrożeń wynikających z ataków kryminalnych, w tym ataków terrorystycznych, które wymagają podjęcia szczególnych działań ze strony organów administracji rządowej i organów samorządu terytorialnego. W systemie uczestniczyć będą przede wszystkim organy administracji morskiej, armatorzy oraz podmioty zarządzające portami i obiektami portowymi, a także inne służby publiczne (policja, Straż Graniczna, Służba Celna) oraz służby ochrony prowadzące działalność na terenie portów i obiektów portowych. Powyższe założenia zostały wykonane – w dniu 4 września 2008 r. uchwalona została ustawa o ochronie żeglugi i portów morskich (Dz. U. Nr 171, poz. 1055) określająca założenia systemu ochrony żeglugi i portów morskich, wdrażająca przepisy dyrektywy 2005/65/WE oraz porządkująca i doprecyzowująca obowiązujące wymagania międzynarodowe i europejskie, określone w rozdziale XI-2 konwencji SOLAS, kodeksie ISPS oraz rozporządzeniu WE 725/2004.

mgr inż. Wojciech Zdanowicz

Bibliografia:

1. Międzynarodowa konwencja o bezpieczeństwie życia na morzu (konwencja SOLAS).
2. Międzynarodowy kodeks dla ochrony statków i obiektów portowych (kodeks ISPS).
3. Rozporządzenie (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie wzmocnienia ochrony statków i obiektów portowych.
4. Dyrektywa 2005/65/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie wzmocnienia ochrony portów.


Smart MD
600TVL
Multi Language OSD
D&N
DIS
SAMSUNG TECHWIN
KOREA
W-5 0751
SSNR3-2K7V1
5CD-BCCM
NOP88SA2
SSNRIII
HLC
0.05Lux
SAMSUNG
SVR-1670
COPY REC HDD EVENT PLAY NETWORK
MULTI MENU
AUTO SEARCH
PTZ COPY
MONITOR FUNC
ESC
PAUSE
REW PLAY ENTER FWD
STOP
NAJNOWSZE TECHNOLOGIE
SAMSUNG TECHWIN
SAMSUNG
Dostępne w największej sieci dystrybucyjnej w Polsce
ALPOL
ALPOL Sp. z o.o.
ul. H. Krahelskiej 7
40-285 Katowice
tel.: 0 801 77 77 90
www: www.samsung.e-alpol.com.pl
www.e-alpol.com.pl
ProfiCCTV
ProfiCCTV Sp z o.o.
ul. Obornicka 276
60-693 Poznań
e-mail: samsung@cctvsamsung.pl
www: www.cctvsamsung.pl

Nowa rodzina central alarmowych **SmartLiving** firmy INIM

We wrześniu br. firma Vidicon wprowadziła na polski rynek nową centralę alarmową SmartLiving włoskiej firmy INIM o bardzo zaawansowanej i pomysłowej funkcjonalności oraz nowatorskich technologicznie rozwiązaniach. Centrala jest łatwa w programowaniu i przyjazna dla użytkownika. Zapewnia wysoki poziom zabezpieczenia w połączeniu z łatwością użytkowania, jej elementy są wykonane z materiałów wysokiej jakości, a jej stylistyka jest zgodna z najnowszymi trendami. Produkt w pełni wykorzystuje najnowszą technologię mikroprocesorową, architekturę magistrali BUS oraz środki komunikacji

Technologie

Zastosowane przy projektowaniu nowej rodziny central technologie i rozwiązania zostały opatentowane przez firmę INIM. Są to:

Easy4U – technologia i prostota

Nowa rodzina central jest oparta na dźwiękowych i wizualnych technologiach, które stanowią podstawę wielu niespotykanych rozwiązań. Możliwa jest komunikacja głosowa pomiędzy klawiaturami. W centralach zastosowano duży wyświetlacz tekstowo-graficzny, na którym są ikony graficzne zwane skrótami. Skróty są przypisane do przycisków funkcyjnych, które służą do najczęściej wykonywanych operacji – dla użytkownika wykonanie operacji sprowadza się do naciśnięcia tylko jednego przycisku. Możliwe jest również skorzystanie z przewodnika głosowego, który ułatwia użytkownikowi wykonywanie operacji. Kolejną innowacyjną właściwością central jest funkcja *text-to-speech*, która umożliwia wpisanie tekstu na klawiaturze i stworzenie z niego komunikatu głosowego. Zaawansowana technologia powala na zautomatyzowaną parametryzację linii centrali, co umożliwia systemowi samoistne zrównoważenie, zgodne z jego parametryzacją. Jest to rozwiązanie polecane zwłaszcza w przypadku wymiany systemu dotychczasowego na SmartLiving – instalator nie musi podejść do każdego czujnika, aby go rozkręcić i sprawdzić, w jaki sposób został sparametryzowany.

VoIB – technologia i komunikacja

Architektura systemu może wykorzystać szynę komunikacji pomiędzy płytą główną centrali a klawiaturą do transmisji głosowej (*Voice over I-BUS*), co pozwala na korzystanie z funkcji interkomowych pomiędzy klawiaturami, podsłuch, korzystanie z opisanego wcześniej komunikatora głosowego.

FlexIO – technologia i elastyczność

Opatentowana technologia FlexIO znosi podział na wejścia i wyjścia w systemie. W rzeczywistości terminale korzystające z tej technologii można zaprogramować jako wejścia, wyjścia lub oba jednocześnie. Oznacza to, że wyłącznie instalator określa, czy dany terminal ma być wejściem czy wyjściem w systemie.

Janus – technologia i spójność

Niezwykle pożyteczna technologia Janus, zastosowana w opcjonalnej karcie SmartLAN, pozwala na połączenie centrali alarmowej z komputerem poprzez sieć LAN. SmartLAN daje możliwość dostępu do centrali poprzez Internet, wysyłania e-maili z powiadomieniem o zdarzeniach, sprawdzenia aktualnego stanu centrali (możliwość wyboru dowolnej wirtualnej klawiatury w systemie), dokonania zmian w oprogramowaniu centrali. Do programowania central stworzono oprogramowanie SmartLeague, które w łatwy sposób umożliwia komunikację z centralą i jej wszystkimi peryferiami. To samo oprogramowanie jest przeznaczone również dla innej gamy produktów firmy INIM – dla central pożarowych.

System

INIM oferuje pięć modeli central alarmowych SmartLiving: SmartLiving 515 (możliwość obsługi do 30 czujek, pięciu klawiatur i pięciu partycji), SmartLiving 1050, SmartLiving 1050L (możliwość obsługi do 100 czujek, 10 klawiatur i 10 partycji), SmartLiving 10100 oraz SmartLiving 10100L (możliwość obsługi do 200 czujek, 15 klawiatur i 15 partycji). Dodatkowymi elementami systemu są ekspandery wykorzystujące technologię FlexIO (dowolnie programowalne wejścia lub wyjścia w systemie), klawiatury, czytniki zbliżeniowe i karty umożliwiające pracę urządzeń bezprzewodowych.

Wszystkie te urządzenia są połączone ze sobą magistralą I-BUS. Jest to stworzony przez firmę INIM rdzeń systemu umożliwiający typ komunikacji nowej generacji. Magistrala I-BUS pozwala na bardzo szybką komunikację pomiędzy elementami systemu a płytą główną centrali, a także zapewnia dodatkowo transmisję głosową pomiędzy klawiaturami na zasadzie interkomu z wykorzystaniem technologii VoIB. Dzięki temu nie ma konieczności ułożenia dodatkowego okablowania pomiędzy klawiaturami, służącego do komunikacji pomiędzy nimi.

Do centrali można podłączyć również czytniki zbliżeniowe oraz zaprogramować karty lub breloki spełniające rolę kluczy cyfrowych. Mogą one funkcjonować identycznie jak kody użytkowników i powodować wykonywanie różnorodnych funkcji przez centralę. Podłączone do centrali klawiatury typu JOY/MAX mają wbudowane czytniki zbliżeniowe. W obudowie klawiatury znajduje się również czujnik termiczny, a informacja o aktualnej temperaturze pomieszczenia, w którym klawiatura została zainstalowana, podawana jest na wyświetlaczu na zmianę z aktualnym czasem.

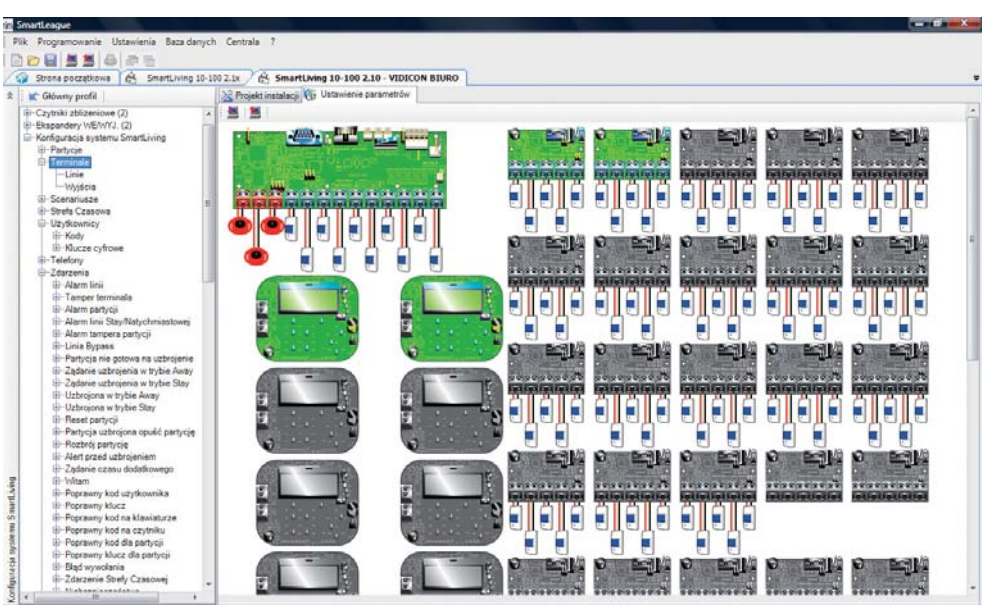
Pod wyświetlaczem obu typów znajdują się cztery przyciski funkcyjne F1–F4. Nad nimi, na wyświetlaczu, pojawiają się graficzne ikony, które czytelnie odzwierciedlają skróty danych funkcji (np. załączenie w dozór / wyłączenie z dozoru / kasowanie pamięci zdarzeń / sterowanie wyjściami itp.) Możliwych jest ponad czterdzieści różnych ikon skrótów, które użytkownik może dowolnie przypisać do każdego z przycisków funkcyjnych. W każdej klawiaturze można zaprogramować do 12 skrótów skojarzonych z czterema przyciskami funkcyjnymi.

W klawiaturach JOY/GR oraz JOY/MAX znajdują się także po dwa terminale, które można skonfigurować jako wejście lub wyjście. Klawiatury JOY/MAX są dodatkowo wyposażone w mikrofon i głośnik, które służą do wykonywania funkcji głosowych. Instalację można wyposażyć dodatkowo w moduł SmartLogos30. Pozwala to na wykorzystanie całej gamy zaawansowanych funkcji głosowych i nagranie komunikatów głosowych (nawet do 500 różnych komunikatów o łącznym czasie trwania do 30 minut).

Za pomocą transceivera (urządzenia nadawczo-odbiorczego) o nazwie Air2 do centrali SmartLiving można przyłączyć urządzenia bezprzewodowe. Na uwagę zasługują piloty bezprzewodowe oznaczone symbolem KF100. W innych dostępnych systemach alarmowych piloty służą jedynie do wysłania do centrali sygnału, który spowoduje wykonanie dowolnej czynności. W centrali firmy INIM komunikacja jest dwukierunkowa – otrzymujemy informację zwrotną o powodzeniu lub niepowodzeniu danej operacji. Odbierane przez pilota informacje są sygnalizowane przez diodę, która w zależności od sygnalizowanego stanu może mieć kolor zielony lub czerwony. Pilot posiada również brzęczyk sygnalizujący informacje zwrotne. Do każdego z czterech przycisków pilota można przypisać dowolny skrót. W systemie można zaprogramować do 100 pilotów.

Pozostałe urządzenia bezprzewodowe, takie jak czujnik PIR oznaczony IR100 lub kontaktron o symbolu MC100, również mają zapewnioną dwukierunkowa łączność. Ich łączna liczba to maksymalnie 50.

Centrala ma również możliwość komunikacji przez sieć LAN. W czasach coraz powszechniejszego korzystania z Internetu możliwość zdalnego sprawdzenia lub przeprogramowania centrali sprawia, że z każdego zakątka świata można sprawdzić, co działo się w systemie podczas naszej nieobecności. W przypadku alarmu urządzenie jest w stanie wysłać odpowiedniego e-maila z powiadomieniem o zdarzeniu. Moduł SmartLAN/G jest wyposażony w serwer WWW.



Innym modułem, który można dołączyć do centrali, jest SmartLink. Standardowo centralę SmartLiving można podłączyć pod telefoniczną linię miejską. W przypadku jej braku lub uszkodzenia nadajnik GSM lub SmartLink może zapewnić niezbędną łączność.

Urządzenie SmartLink ma wiele użytecznych funkcji, takich jak wybór głosowy lub cyfrowy, dialer SMS, zarządzanie centralą poprzez SMS-y lub przez kody DTMF. Moduł umożliwia także identyfikację dzwoniącego. Płyta SmartLink zawiera dodatkowo pięć terminali z możliwością dowolnej konfiguracji.

Do programowania modułu SmartLink używa się tego samego oprogramowania co w przypadku centrali alarmowej (SmartLeague).

Programowanie

Centrale SmartLiving można zaprogramować na kilka sposobów.

Każda klawiatura w systemie może służyć do zaprogramowania lub przeprogramowania danych w centrali. Proste, całkowicie spolszczone menu pozwoli nawet nieznającemu systemu instalatorowi na intuicyjne i łatwe zaprogramowanie wszystkich potrzebnych funkcji w centrali. Osobne menu posiada użytkownik. Po wpisaniu swojego hasła może on zarządzać alarmami, aktywować/dezaktywować wyjścia, ustawić datę/czas, przeglądać dzienniki (logi) zdarzeń itp.

Używając portu RS232, można zaprogramować centrale lokalnie (dołączywszy kabel z komputera bezpośrednio do centrali) lub zdalnie (za pomocą modemu podłączonego do portu RS232 i linii telefonicznej).

Centrale SmartLiving można zaprogramować także przez sieć LAN, korzystając z interfejsu sieciowego SmartLAN.

W dwóch ostatnich przypadkach (RS232 i LAN) do programowania można użyć dołączonego do centrali oprogramowania SmartLeague. Jest ono łatwe w obsłudze i dostępne w języku polskim. Przedstawia graficzny obraz podłączonych urządzeń i umożliwia szybki wybór wybranych parametrów.

Podsumowanie

Dzięki zainstalowaniu centrali SmartLiving użytkownik ma zapewnioną nie tylko znakomitą ochronę, ale również narzędzie do sterowania wieloma urządzeniami znajdującymi się w domu. Łatwość obsługi powoduje, że każda osoba jest w stanie w bardzo krótkim czasie przyswoić sobie niezbędną wiedzę dotyczącą tego urządzenia. Charakteryzuje się ono wieloma nietypowymi i niedostępnymi w innych centralach, lecz niezbędnymi funkcjami takimi jak: przewodnik głosowy, interkom, rozbudowane opcje funkcji głosowych, potwierdzanie operacji wykonywanych za pomocą pilotów bezprzewodowych itp.

Każdy z elementów systemu określony jest mianem *smart*. W języku angielskim słowo to znaczy «sprytny, bystry, zręczny, zgrabny, energiczny, zdolny», ale również «elegancki» i «szykowny». I właśnie taka jest opisana powyżej centrala.

Więcej informacji na temat centrali znajduje się na stronie internetowej *www.vidicon.pl*.

Wojciech Pawlica
Vidicon

Świat IP coraz bliżej.

SONY

Najnowsze oprogramowanie Real Shot Manager Advanced dostaniesz w prezencie przy zakupie dowolnych 4 kamer IP. Jest to autorskie oprogramowanie Sony stworzone do monitoringu. W połączeniu z kamerami IP Sony dostajecie Państwo gwarancje, serwis oraz Prime Support*. Ponadto łącząc inteligentną analizę wideo, alarmy na żądanie i wiele innych funkcjonalności, Real Shot Manager Advanced zapewnia bezpieczeństwo na najwyższym poziomie oraz daje możliwość wprowadzenia klienta w świat IP.

*Prime Support coś więcej niż gwarancja, zamiana uszkodzonego sprzętu na sprawny w ciągu trzech dni!!!

Chcesz wiedzieć więcej, skontaktuj się z nami:
www.sonybiz.pl

IPELA

Wąskie gardła w IP

Budowa profesjonalnego systemu CCTV IP z uwzględnieniem opisów liczenia przepustowości sieci, wąskich gardeł, wykorzystania strumieni unicastowych i multicastowych oraz trybów dwustrumieniowych

Przykład budowy takiej sieci opartej na przełącznikach gigabitowych oraz szkielecie światłowodowym

Czym się różni sieć monitoringu IP od klasycznej sieci komputerowej?

Próbując zastanowić się nad budową i działaniem sieci IP wykorzystywanych w systemach monitoringu telewizyjnego, należy zwrócić uwagę na cechy odróżniające te sieci od klasycznych instalacji komputerowych. Pomimo tego, że w obu przypadkach mamy do czynienia z podobną strukturą okablowania oraz podobnym sprzętem sieciowym, jest jednak jeden czynnik stanowiący zdecydowaną różnicę. Tym czynnikiem jest ciągły, praktycznie nieprzerwany przepływ informacji w sieciach monitoringu wizyjnego, na dodatek odznaczający się dużą intensywnością[1].

W klasycznych sieciach komputerowych także możemy mieć do czynienia z transmisją znacznych ilości informacji, jednakże generowany w ten sposób ruch ma charakter okresowy, co pozwala stosować powszechnie znane techniki podziału pakietów na mniej lub bardziej ważne, ustawiania tych pakietów w kolejki zgodnie z hierarchią ważności i sukcesywnej wysyłki w tempie, na jakie pozwalają łącza transmisyjne. Jak widać, czynnik przepływności tych łącz ma tu znaczenie istotne, ale nie decydujące. Cóż złego stanie się na skutek dostarczenia poczty elektronicznej o minutę później, czy na skutek skopiowania pliku z najnowszym teledyskiem w trzy razy wolniejszym tempie? Jedyna sensowna odpowiedź brzmi: nic się nie stanie.

1) Przed przystąpieniem do rozważań na temat budowy sieci IP, która umożliwia obsługę rozległego systemu monitoringu telewizyjnego, należy zaznaczyć, że wszystkie zawarte tu stwierdzenia mają jedynie charakter instruktażowy i przykładowy. Faktyczna budowa takiej sieci, odpowiedni dobór mediów transmisyjnych i sprzętu sieciowego oraz sposób zaprogramowania poszczególnych urządzeń muszą być przedmiotem szczegółowej analizy, opartej na danych dotyczących konkretnego obiektu.

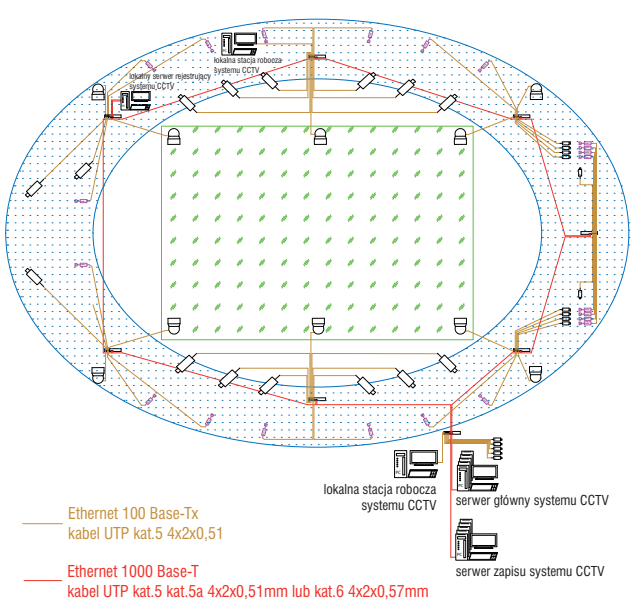
rozdzielczość / kompresja	JPEG	MPEG4	H.264
4CIF	2,8 Mb/s	700 kb/s	350 kb/s
4xVGA (1,3 Mpix)	12 Mb/s	4 Mbit/s	2 Mbit/s

Tab. 1. Przykładowe wartości strumieni danych generowanych przez kamery

W przypadku sieci wykorzystywanych w monitoringu wizyjnym przyjęcie takiej koncepcji byłoby poważnym błędem. Biorąc pod uwagę fakt, że od działania systemu zależy bezpieczeństwo ludzi lub dóbr materialnych, nie można zakładać, że jakaś informacja dotrze do odbiorcy z dużym opóźnieniem. W wielu przypadkach względy użytkowe lub formalne wymuszają konieczność podglądu obrazów z wielu kamer w trybie „live", czyli w czasie rzeczywistym. To z kolei oznacza nieprzerwany przepływ znacznej ilości danych.

Z jak dużymi strumieniami danych będziemy mieć do czynienia?

Zastanówmy się, jak szybka powinna być sieć IP, by mogła sprostać tego typu wymaganiom. Nasze rozważania zacznijmy od źródła danych, czyli od kamer telewizyjnych. Te, w zależności od poklatkowości, czyli liczby obrazów telewizyjnych wytwarzanych w ciągu sekundy, od rozdzielczości tych obrazów oraz od przyjętej metody kompresji, generują strumień danych o określonej intensywności. Nie wdając się w rozważania na temat budowy kamer i skuteczności metod kompresji, przyjmijmy przykładowe dane liczbowe, dotyczące wielkości strumieni danych, zawarte w tabeli 1, zakładając, że od systemu wymaga się wyświetlania obrazów w czasie rzeczywistym, co oznacza konieczność transmisji dwudziestu pięciu obrazów na sekundę z każdej z kamer. Ograniczmy się do kamer o rozdzielczości nie przekraczającej 1,3 Mpix, gdyż takie są najczęściej stosowane w systemach monitoringu. Rozważania nad zastosowaniem kamer o znacznie większych rozdzielczościach wykraczają poza ramy tej publikacji.



Rys. 1. Uproszczony schemat sieci IP o topologii pierścienia

Co prawda tak przyjęte przykładowe założenia nie są do końca precyzyjne, gdyż faktyczne wielkości strumieni danych generowanych przez kamery zależą od wielu czynników, ale pamiętajmy, że celem tego artykułu jest wyjaśnienie pewnych zasad, a nie zaprojektowanie konkretnego systemu. Ponadto pod znakiem zapytania należy postawić możliwość generacji dwudziestu pięciu obrazów na sekundę z rozdzielczością 1,3 Mpix i z kompresją H.264, ale podkreślmy to jeszcze raz – to jest tylko przykład hipotetycznego systemu, jakieś wartości trzeba przyjąć do dalszych rozważań.

Przyjmijmy teraz kolejne założenie, dotyczące liczby i rozmieszczenia kamer. Rozważania na temat budowy sieci szkieletowej mają sens tylko w odniesieniu do rozbudowanych instalacji, dlatego dla przykładu przyjmijmy, że mamy do czynienia z obiektem sportowym, na którym ma znajdować się około czterystu kamer. Osobie niezorientowanej w temacie mogłoby się wydawać, że jest to bardzo duża liczba, jednakże wymuszają to wymogi wynikające z „Rozporządzenia w sprawie sposobu utrwalania przebiegu imprez masowych oraz minimalnych wymagań technicznych dla urządzeń rejestrujących obraz i dźwięk" z dnia 28 października 2004 r. Kamery muszą być rozmieszczone na terenie całego obiektu, nierzadko w znacznych odległościach od pomieszczenia, z którego system będzie obsługiwany. Ponadto istnieje wymóg stworzenia dodatkowych stanowisk dozorowych, pozwalających na szybką emisję materiałów operacyjnych oraz archiwizację tworzonych nagrań.

Dodatkowym czynnikiem komplikującym budowę systemu jest konieczność spełnienia ustawowych wymagań dotyczących rejestracji dźwięku z obszarów obserwowanych przez kamery, co zmusza do rozmieszczenia w obiekcie znacznej liczby mikrofonów, cyfrowych koderów dźwięku i odpowiednich kabli transmisyjnych. Na potrzeby dalszych rozważań przyjmijmy konieczność zainstalowania około stu mikrofonów IP.

Na koniec załóżmy, że budujemy prawdziwy, nowoczesny system IP, to znaczy taki, w którego żadnym fragmencie, nawet lokalnie nie są wytwarzane i transmitowane żadne sygnały analogowe. Wszystkie obrazy z kamer, wszystkie strumienie niosące informację o dźwięku oraz wszystkie informacje o charakterze pomocniczym, takie jak dane niezbędne do sterowania ruchem kamer, są na całej swojej trasie przekazywane w formie cyfrowej, w pakietowej sieci IP.

Przechodząc do rozważań na temat budowy sieci IP, która mogłaby być zastosowana do obsługi tak dużego systemu, w pierwszym przybliżeniu zastanówmy się nad topologią gwiazdy. W zasadzie nic nie stoi na przeszkodzie, by taką sieć zbudować. Suma wszystkich strumieni danych występujących w całym systemie nie przekroczy 500 Mbit/s, więc można by pozwolić sobie na doprowadzenie wszystkich pakietów do jednego miejsca, ale w praktyce taki pomysł okazuje się karkołomny. Duże odległości, o których wspomniano we wcześniejszej części artykułu, wykluczają możliwość zastosowania popularnych kabli miedzianych, gdyż technologia Ethernet, w dowolnej swojej „miedzianej" odmianie, nie przewiduje możliwości transmisji danych na odległość rzędu kilkuset metrów, a z kolei stosowanie światłowodów w stosunku do pojedynczych kamer jest kłopotliwe i kosztowne.

Rys. 2. Przykładowy przełącznik sieciowy

Ze względu na przyjętą, hipotetyczną specyfikę naszego obiektu sportowego znacznie lepsza okazuje się topologia mieszana, to znaczy przewidująca zastosowanie pierścienia światłowodowego z punktami węzłowymi i lokalnych odgałęzień od tych punktów, w topologii gwiazdy, w miarę możliwości realizowanych na kablach miedzianych. Bardzo uproszczony przykład tego typu sieci wraz ze szkicem monitorowanego obiektu jest przedstawiony na rys. 1. Rysunek „nie trzyma skali" i nie uwzględnia przyjętej przez nas liczby kamer i mikrofonów, jednakże dobrze ilustruje opisywaną topologię mieszaną sieci IP.

Podstawową zaletą takiego rozwiązania jest pewna nadmiarowość w części szkieletowej, gdyż pierścień z natury rzeczy jest tworem zamkniętym i jego przerwanie w jednym miejscu nie powoduje utraty połączeń między poszczególnymi składnikami. Ponadto kable światłowodowe mają to do siebie, że są produkowane w postaci wielowłóknowej i, budując jeden pierścień światłowodowy, bardzo łatwo jest go zdublować. Tego typu rozwiązanie pozwala na poprawę parametrów transmisyjnych sieci.

W punktach węzłowych sieci mogą być zastosowane różne urządzenia, na przykład lokalne serwery lub – częściej – zarządzalne przełączniki sieciowe (tak zwane przełączniki trzeciej warstwy[2]). Przełączniki takie są wyposażone w kilka rodzajów interfejsów sieciowych, które w warstwie pierwszej sieci[3] wykorzystują różne media transmisyjne. Przeważnie są one wyposażone w dwa interfejsy światłowodowe i pewną liczbę interfejsów Fast Ethernet, przystosowanych do kabli miedzianych. Przykład takiego przełącznika jest przedstawiony na rys. 2.

Jak widać, przedstawiony na rysunku przykładowy przełącznik sieciowy zawiera zarówno interfejsy dostosowane do kabli miedzianych, jak i światłowodowych. I tu dochodzimy do pierwszego wąskiego gardła sieci IP – kumulacji strumieni danych w przełącznikach. W klasycznych sieciach komputerowych nie ma to większego znaczenia, gdyż, jak wspomniano wcześniej, ruch sieciowy nie ma charakteru ciągłego, lecz okresowy. Duże strumienie danych są transmitowane w zależności od konkretnych potrzeb, na przykład w sytuacji, gdy któryś z użytkowników sieci rozpoczyna ściąganie plików o dużej objętości. Trudno wyobrazić sobie sytuację, w której wszystkie komputery zainstalowane w dużym biurowcu jednocześnie powodują wysokie obciążenie sieci, dlatego wymagania dotyczące przepływności przełączników sieciowych mogą być mniejsze. Inaczej przedstawia się sprawa w systemach monitoringu IP, gdzie jednocześnie i nieprzerwanie wszystkie aktywne w danej chwili kamery wysyłają swoje strumienie danych. Strumienie te wpływają do przełączników sieciowych kilkunastoma interfejsami, ale są przekazywane do części szkieletowej już tylko za pomocą dwóch interfejsów. Poprawność działania tego segmentu sieci zależy od konstrukcji przełączników, które powinny być przystosowane do takiej kumulacji danych.

W innej koncepcji sieci szkieletowej o topologii pierścienia zamiast przełączników sieciowych w punktach węzłowych zastosowane są lokalne serwery. W pewnym stopniu zmniejsza to obciążenie sieci, gdyż serwery pełnią funkcję lokalnych rejestratorów danych, co uwalnia od konieczności transmisji wszystkich pakietów do serwerowni głównej. Ponadto ogólna niezawodność systemu wzrasta, gdyż nawet całkowity brak połączenia z głównym pierścieniem światłowodowym nie powoduje przerwy w rejestracji obrazów z kamer, a jedynie uniemożliwia ich wyświetlenie na stacjach roboczych.

Kolejnym elementem sieci są serwery, czyli jednostki centralne zarządzające całym systemem. W zależności od zastosowanego oprogramowania serwery powodują mniejsze lub większe obciążenie sieci szkieletowej. Przykładowo, w przypadku systemu monitoringu bazującego na oprogramowaniu ExacqVision pakiety danych niemal w ogóle nie są przetwarzane przez serwer główny, lecz są od razu kierowane do miejsc przeznaczenia, to znaczy do stacji roboczych dokonujących obróbki i filtracji danych lub do jednostek pamięci masowej (macierzy dyskowych). Odwrotnie jest w przypadku programu Sony Real Shot Manager, w którym wszystkie pakiety podlegają intensywnemu przetwarzaniu przez serwer główny, zaś do stacji roboczych wysyłane są wstępnie obrobione dane. Oba te rozwiązania mają swoje wady i zalety, jednakże z punktu widzenia topologii sieci niewiele się zmienia, gdyż i tak w jakimś jej punkcie muszą się skumulować strumienie danych ze wszystkich kamer. Na całe szczęście w przypadku naprawdę rozległych instalacji serwer główny składa się z kilku lub nawet kilkunastu maszyn, tym samym ruch sieciowy ulega rozproszeniu i dla każdej z maszyn jest proporcjonalnie mniejszy.

System wydzielony czy sprzężony z innymi?

W naszym konkretnym przykładzie zastosowanie około czterystu kamer, wśród których większość ma rozdzielczość 4CIF, a kilkanaście procent to kamery megapikselowe o rozdzielczości 1,3 Mpix, spowoduje, że sumaryczny, skumulowany w jednym punkcie strumień danych nie przekroczy 500 Mbit/s. Jak widać, zastosowanie sieci o maksymalnej przepływności 1 Gbit/s i rozsądne gospodarowanie przepływnością w poszczególnych jej fragmentach okaże się wystarczające do poprawnej pracy całego systemu.

Nie są to wygórowane wymagania. Wspomniana sieć szkieletowa dysponuje pewnym zapasem przepływności. W zasadzie nie ma formalnego wymogu, który zabraniałby użycia takiej sieci do różnych celów, nie tylko do obsługi systemu monitoringu wizyjnego. Jak twierdzą osoby biegłe w sztuce projektowania sieci szkieletowych, zastosowanie nowoczesnych urządzeń sieciowych, na przykład zarządzalnych przełączników warstwy

2) Określenie „przełącznik trzeciej warstwy" odnosi się do warstwowego modelu sieci OSI, w którym klasyczne przełączniki operują w warstwie drugiej, nie uwzględniającej adresów IP urządzeń sieciowych, zaś przełączniki zarządzalne operują także w warstwie trzeciej, uwzględniającej adresy IP, czym w pewnym sensie upodabniają się do prostych ruterów sieciowych. Decyzje rutingowe podejmowane są na podstawie danych z trzeciej warstwy.

3) Jest to kolejne odniesienie do modelu sieci OSI. Warstwa pierwsza jest warstwą fizyczną, w której następuje faktyczna transmisja danych z użyciem kodowania, modulacji etc., ale bez jakiejkolwiek zmiany ich treści.

trzeciej i warstw wyższych oferowanych przez firmę Cisco oraz nowoczesnych kabli światłowodowych, pozwoliłoby obsłużyć cały obiekt wielkości stadionu sportowego, włącznie z telefonami, biurowością i księgowością, sterowaniem automatyką obiektu, systemem monitoringu etc., i byłoby to rozwiązanie uzasadnione ekonomicznie. Jednakże w rozsądnie pojmowanym interesie bezpieczeństwa publicznego nie praktykuje się takich połączeń. Dobrym przykładem może być system sygnalizacji pożarowej, który z natury rzeczy nie wchodzi w skład żadnego innego systemu bezpieczeństwa, a co najwyżej jest z nim sprzężony peryferyjnie. Podobnie należy traktować projektowanie systemów monitoringu telewizyjnego i wydzielać te sieci jako osobne instalacje.

Unicasting i multicasting

Znakomita większość współczesnych kamer IP przeznaczonych do pracy w systemach monitoringu telewizyjnego może obsłużyć od kilku do kilkudziesięciu klientów sieciowych[4], co w praktyce oznacza konieczność jednoczesnego wysyłania wielu pakietów niosących identyczną treść, a różniących się jedynie adresacją. Taki sposób transmisji jest określany jako unicastingowy i z punktu widzenia przepływności sieci można go uznać za mało efektywny. Unicasting w sposób oczywisty zwiększa ruch sieciowy i można zadać sobie pytanie, po co wielokrotnie wysyłać te same przesyłki do różnych odbiorców, skoro można wysłać tylko jedną taką przesyłkę i dostarczyć jej kopie wszystkim zainteresowanym? Z kolei ten sposób transmisji jest określany jako multicastingowy i stwarza możliwości ograniczenia ruchu sieciowego w sytuacji, w której wielu odbiorców chce korzystać z tych samych strumieni danych.

Innym zagadnieniem jest wielostrumieniowość transmisji. Jak już wspomniano, znakomita większość współczesnych kamer IP przeznaczonych do pracy w systemach monitoringu telewizyjnego może generować kilka rodzajów strumieni danych, różniących się parametrami obrazu, to znaczy metodą kompresji, rozdzielczością, poklatkowością (liczbą obrazów na sekundę). Stwarza to możliwość wysyłania różnym klientom różnych informacji, niosących zasadniczo tę samą treść, ciągle bowiem jest to ten sam obraz, tyle że inaczej przetworzony i inaczej podany. Przykładowym zastosowaniem wielostrumieniowości może być rejestracja wysokiej jakości obrazów z mało wydajną kompresją, taką jak JPEG, z jednoczesną transmisją tych samych obrazów do zdalnego odbiorcy, za pośrednictwem łącz o ograniczonej przepływności, co zmusza do zastosowania innej, wydajniejszej, ale bardziej inwazyjnej metody kompresji, jaką jest na przykład MPEG4. Należy pamiętać, że wielostrumieniowość nie ma nic wspólnego z multicastingiem. Są to dwa zupełnie różne pojęcia.

Multicasting polega na wysyłaniu tych samych pakietów danych do różnych klientów, mających identyczne multicastingowe adresy sieciowe. To brzmi jak herezja – jak to możliwe, że różne urządzenia mają ten sam adres sieciowy? Nie wdając się w zbędne rozważania, należy stwierdzić, że szeroko pojmowane adresy sieciowe można podzielić na kilka klas.

4) Z punktu widzenia sieci kamera jest serwerem, to znaczy urządzeniem wysyłającym pakiety danych na wyraźne życzenie innych hostów, czyli klientów sieciowych. Klientem może być dowolne urządzenie zgłaszające zapotrzebowanie na pakiety, na przykład jednostka pamięci masowej lub stacja robocza.

Podział ten miał zasadnicze znaczenie w pierwszych latach rozwoju sieci IP. Obecnie większość sieci traktuje się bezklasowo, jednakże pewne elementy starego sposobu myślenia nadal obowiązują. Wśród wszystkich dostępnych adresów wydzielono pewną grupę, nazwano ją Klasą D i przeznaczono ją do transmisji multicastingowej. Adres multicastingowy jest unikatowym adresem w sieci, kierującym jednakowe pakiety danych do wszystkich odbiorców należących do predefiniowanej grupy adresów IP. Adresy klasy D muszą zawierać się w zakresie od 224.0.0.0 do 239.255.255.254.

Z sieciowego punktu widzenia pakiety unicastingowe są traktowane jak pojedyncze, indywidualne przesyłki, dostarczane konkretnemu odbiorcy przez konkretnego nadawcę. Kolejne rutery sieciowe przekierowują te pakiety na odpowiednie trasy tak, żeby w efekcie dotarły do punktu przeznaczenia, ale ani ich liczba, ani treść nie ulega zmianie.

W przypadku multicastingu kolejne rutery kopiują te same pakiety danych i przekierowują kolejne ich kopie na trasy prowadzące do wielu odbiorców. Czynność ta wymaga specjalnej obsługi i nie wszystkie rutery potrafią ją wykonać. Innymi słowy transmisja multicastingowa jest możliwa tylko w sieciach, które są do tego przystosowane.

Realizacja transmisji multicastingowej nabiera znaczenia dopiero w przypadku sieci rozległych WAN oraz dużych grup użytkowników korzystających z tych samych pakietów danych. Przykładem może być duże osiedle mieszkaniowe, w którym pewna grupa mieszkańców zgłosiła chęć oglądania tego samego programu telewizyjnego, zaś dostawca usług telewizji sieciowej wysyła do nich te same pakiety danych. Niestety w praktyce jest to dużo bardziej skomplikowane. W odróżnieniu od transmisji unicastingowej, w przypadku multicastingu nie mamy jasno określonej listy odbiorców. Konieczne jest uruchomienie specjalnych protokołów w sieci, pozwalających wychwycić nowych klientów dołączających do danej grupy adresowej oraz tych, którym znudziło się oglądanie akurat tego filmu i właśnie wyłączyli swój odbiornik. Ten bardzo uproszczony opis ma zilustrować mnogość problemów związanych z transmisją multicastingową.

W codziennej praktyce projektowej i instalacyjnej związanej z systemami monitoringu telewizyjnego transmisja multicastingowa jest stosowana sporadycznie, a właściwie niemal wcale nie jest stosowana. Jest to związane z jej specyfiką. Rzadko zachodzi potrzeba oglądania tego samego obrazu przez dużą grupę odbiorców. Tak więc multicasting jest domeną telewizji domowej, o charakterze abonenckim. Fakt, że kamery przemysłowe także dysponują opcją multicastingu nie powinien dziwić, gdyż jej realizacja nie wpływa w zasadniczy sposób ani na budowę samej kamery, ani na oprogramowanie zawartego w niej serwera. Ostatecznie fakt nadania jakimś pakietom jakiegoś konkretnego, wspólnego dla dużej grupy odbiorców adresu sieciowego nie komplikuje ani oprogramowania, ani konstrukcji sprzętu. Ciężar przesuwa się w stronę infrastruktury sieciowej, zaś w sieciach LAN, dominujących w instalacjach monitoringu telewizyjnego, multicasting nie ma istotnego znaczenia praktycznego. Według opinii renomowanych producentów kamer wprowadzenie tej opcji raczej nie wiąże się z jej znaczeniem praktycznym, natomiast może mieć wpływ na rozstrzygnięcia podczas przetargów publicznych, aczkolwiek trudno kogokolwiek zmusić do publicznego wygłoszenia takiej opinii.

Z nielicznymi próbami wykorzystania transmisji multicastingowej można spotkać się w systemach monitoringu miejskiego w miejscach, w których lokalna rozgłośnia telewizyjna chce sporadycznie wykorzystywać obrazy pochodzące z kamer ulicznych. Innym zastosowaniem multicastingu mogą być próby przesyłania obrazów z wielu kamer przez łącze o małej przepływności, na przykład z jednej dzielnicy miasta do drugiej, z zamysłem wykorzystania tych obrazów na różnych posterunkach policyjnych, są to jednak dość skrajne przykłady. Prostszym i tańszym sposobem wydaje się budowa wydajniejszych łącz oraz lepsze wykorzystanie sprzętu sieciowego w taki sposób, by nie dopuszczać do kumulacji strumieni danych. Takie zadania potrafią realizować przełączniki warstwy trzeciej, relatywnie tanie w stosunku do urządzeń zdolnych do realizacji transmisji multicastingowej. Podobnie przedstawia się sprawa z nakładem pracy programistów podczas konfiguracji systemów.

Tak więc aby zbudować rozległy, sieciowy system monitoringu wizyjnego, najprościej jest wykorzystać wielostrumieniową transmisję unicastingową i sieć o topologii pierścienia światłowodowego z punktami węzłowymi w postaci lokalnych serwerów lub przełączników warstwy trzeciej. Technologię multicastingu wraz ze wszystkimi problemami związanymi z rutingiem pakietów multicastingowych należy pozostawić sieciom WAN i masowym usługom abonenckim.

Andrzej Walczyk
Altram

GO MEGA

Przedstawiamy nową rodzinę megapikselowych kamer Sony

ZAPROJEKTOWANE Z MYŚLĄ O BEZPIECZEŃSTWIE

SONY

IPELA

Inteligentna analiza obrazu... bezpieczeństwo dla Ciebie

ALTRAM

ALTRAM tel. +48 22 847 55 05
altram@altram.com.pl www.altram.com.pl

www.sonybiz.pl

Zupełnie nowe oblicze monitoringu wizyjnego CCTV

Nieustające przywiązanie wyspiarzy do CCTV

Londyńskie służby policyjne Metropolitan Police Service zyskały nowe narzędzie do walki z przestępczością – pierwszy pojazd do mobilnego monitoringu o nazwie *Mobile Surveillance Vehicle* (MSV). Reporter Brian Sims rozmawiał ze wszystkimi osobami, które przyczyniły się do realizacji tego projektu

Standardowy model vana marki Mercedes został wyposażony w najnowocześniejsze kamery CCTV, sprzęt nagrywający i monitory LCD w ramach wspólnego projektu *First Security* znanej agencji ochrony, Sony, władz dzielnicy Covent Garden oraz policji w dzielnicy Westminster, który ma związek ze staraniami na rzecz skutecznego monitoringu ulic i zwalczania przestępczości.

Całkowity koszt wyposażenia wyniósł 150 000 funtów. Pierwsza mobilna jednostka CCTV policji w Westminster jest gotowa do akcji 24 godziny na dobę przez siedem dni w tygodniu wszędzie tam, gdzie zagrożone jest bezpieczeństwo i porządek publiczny. Możliwość wysłania pojazdu na miejsce zdarzenia niezwłocznie po otrzymaniu zgłoszenia daje nieocenioną możliwość dokonania bezpośredniej oceny wydarzeń oraz szybkiej identyfikacji osób zarówno bezpośrednio zaangażowanych, jak i postronnych.

Na miejscu zdarzenia van może również służyć jako prowizoryczne centrum dowodzenia, miejsce koordynacji działań policji.

Dodatkowy czynnik odstraszający

Samochód można również zaparkować i pozostawić bez załogi jako dodatkowy, widoczny czynnik odstraszający potencjalnych przestępców oraz widoczny znak, dzięki któremu zwykli obywatele poczują się bezpieczniej.

W rozmowie z redaktorem *SMT Online*, Brianem Simsem, Simon Bray, dowódca oddziału policji w dzielnicy Westminster, wyjaśnia: – *Pojazd ten jest dla nas niezwykle cennym nabytkiem. Pomaga nam ścigać przestępców i osoby naruszające porządek publiczny na West End. Westminster jest nadal jedną z najbezpieczniejszych dzielnic w Londynie. Oczekujemy, iż inicjatywa ta zapewni jeszcze wyższy poziom bezpieczeństwa wszystkich gości, mieszkańców i osób pracujących w naszej dzielnicy.*

Bogate wyposażenie

Firma First Security pokryła koszty zakupu vana marki Mercedes oraz unikatowego numeru rejestracyjnego pojazdu – P999 SEE, natomiast władze dzielnicy Covent Garden (Londyn) pokryły koszty dostosowania pojazdu do celów operacyjnych. Zadaniem firmy Sony było dostarczenie niezbędnego sprzętu do monitoringu i nagrywania.

Simon Nash (Senior European Marketing Manager, Video Security) – odpowiedzialny za wizyjne systemy bezpieczeństwa w Sony Professional Solutions w Europie – chętnie wyjaśnił przyczyny zaangażowania firmy Sony oraz opisał zastosowane wyposażenie.

– *Rozwiązanie Sony Professional zostało opracowane z myślą o nagrywaniu, monitorowaniu i zarządzaniu wszelkimi działaniami, które mają miejsce w pobliżu pojazdu* – wyjaśnia Simon. – *Dwie różne kamery monitorujące (pierwsza z nich to kopułkowa kamera megapikselowa typu SNC-DM160, druga to kamera szybkoobrotowa w obudowie zewnętrznej typu SNC-RX570P/outdoor) umożliwiają operatorom monitorowanie zdarzeń i przybliżanie wybranych obrazów.*

Pojazd został wyposażony także w monitory Sony Bravia, które wyświetlają obrazy rejestrowane przez kamery, a oprogramowanie RealShot Manager uzupełnia cały proces monitoringu poprzez aktywne zarządzanie wszystkimi zarejestrowanymi obrazami.

Zainstalowane wyposażenie zapewnia pełny obraz w zasięgu 360°, rejestrowany przez zainstalowane kamery i synchronizowany przez dodatkowe urządzenia, który stanowi nieoceniony materiał dowodowy w prowadzonych śledztwach i procesach sądowych. System może każdorazowo nagrywać obrazy rejestrowane przez okres do 12 h, które można natychmiast skopiować z dedykowanego twardego dysku.

Simon Nash z nieskrywaną dumą opowiada o osiągnięciu Sony: – *Od wstępnego śledzenia po analizę i zarządzanie danymi – owo niezwykłe połączenie różnych technologii umożliwi policji w Westminster prowadzenie pełnego procesu nadzoru wideo za pośrednictwem jednej mobilnej jednostki. Jestem przekonany, że van znacznie wzmocni siły policyjne w dzielnicy Westminster.*

Policja i agencje ochrony łączą siły

Mike Crump, dyrektor zarządzający, reprezentujący firmę First Security, przyznał, że rynek usług ochrony stanowił nie lada wyzwanie przez ostatnie 18 miesięcy i z dużym uznaniem wyrażał się o pracy policjantów. – *Ten pojazd to kolejny przykład doskonałych stosunków między branżą ochrony oraz różnymi oddziałami policji, w szczególności Metropolitan Police, British Transport Police oraz City of London Police* – deklaruje Mike Crump. – *W ostatnim okresie zorganizowaliśmy wiele spotkań z naszymi nowymi klientami, na których policjanci z City of London Police prezentowali cenne informacje. Bariery, które istniały między policją a agencjami ochrony, powoli zaczynają znikać.*

John Purnell – dyrektor w Interserve Group – były szef ds. ochrony i zapobiegania stratom w Tesco oraz jeden z głównych decydentów w Worshipful Company of Security Professionals – również podzielił się swoją opinią. – *Pracownicy Interserve bardzo mi imponują. Kadra zarządzająca ma wiele pomysłów i skupia się na klientach. Chodzi o całościowe, pełne rozwiązanie dla użytkownika, a nie tylko standardowe usługi ochrony fizycznej. Jestem pewny, że czeka nas jeszcze wiele sukcesów.* Purnell wypowiedział się też na temat swojej nowej roli w Interserve Group. – *Jest to szeroko zakrojona operacja zarządzania nieruchomościami, która zapewnia szerokie pole działania i możliwości dla firmy First Security.*

First Security jest naturalnie jedną z wiodących agencji ochrony w Londynie. Firma powstała w roku 1987, otrzymała licencję Security Industry Authority, zatrudnia około 2000 osób i zyskała sobie opinię wiarygodnego dostawcy wysokiej jakości usług ochrony fizycznej zgodnych z najwyższymi standardami.

Bezpieczeństwo w Covent Garden

W ramach inicjatywy tworzenia mobilnej jednostki CCTV Westminster w roli klienta występują władze dzielnicy Covent Garden w Londynie, a szef marketingu, Ros Barclay, zgodził się opowiedzieć nam o nowym projekcie. – *Ogromnie cieszymy się, że możemy wesprzeć policję w Westminster* – wyjaśnia Ros Barclay. – *Covent Garden to miejsce o dogodnym położeniu, z rynkiem zamkniętym dla ruchu pojazdów oraz bogatą ofertą sklepów i restauracji. Nowy system CCTV z pewnością poprawi atrakcyjność tej dzielnicy.*

Corocznie Covent Garden odwiedza ponad 40 milionów ludzi, a współpracownicy Rosa Barclaya są w pełni zaangażowani w zapewnienie pełnego bezpieczeństwa wszystkim odwiedzającym (jak również mieszkańcom i osobom tu pracującym). – *Dzięki wielu projektom, w tym zaawansowanej sieci monitoringu ulicznego CCTV w Market Building i Piazza, jak również dedykowanej Security Team pracującej na miejscu przez 24 h na dobę oraz ścisłej współpracy z policją w Westminster i lokalną społecznością Covent Garden może pochwalić się jednym z najniższych wskaźników przestępczości na West End. Jesteśmy z tego naprawdę dumni* – przekonuje Ros Barclay.

Po rozmowie z nadinspektorem Colinem Morganem spotkałem się również z inspektorem Johnem Dalem (kluczową osobą zajmującą się tym projektem, nad którym prace rozpoczęły się jeszcze przed Bożym Narodzeniem w 2006 r.). – *To właśnie wtedy odbyła się wstępna rozmowa z Peterem Simpsonem z First Security* – wyjaśnia John Dale. – *Rozmawiałem z Simonem Nashem w styczniu, a władze Covent Garden (Londyn) włączyły się do przygotowań w październiku 2007 roku. Projekt obejmował ogromne koszty przebudowy pojazdu, które pokryły władze samorządowe.*

Jak długo van będzie w użytku?

Główny inspektor John Dale chce korzystać z vana przez kolejne siedem lat. Pojazd ma być wysyłany do miejsc najbardziej zagrożonych przestępczością, jak również wszędzie tam, gdzie dochodzi do niepokojących zdarzeń. – *Pojazd będzie miał również kluczowe znaczenie w zarządzaniu i planowaniu działań policji* – wyjaśnia John Dale.

John Dale pracuje obecnie dla Territorial Support Group 5 w Metropolitan Police Service, gdzie zajmuje się ochroną i bezpieczeństwem imprez masowych. Rozmawialiśmy o ochronie policyjnej meczów piłki nożnej, kiedy przypomniałem spotkanie West Ham United – Millwall, rozegrane na stadionie The New Den w marcu 2004 roku.

W tamtym czasie byłem szczęśliwym posiadaczem karnetu biletowego na mecze na stadionie Upton Park, a The New Den niegdyś nie był najbardziej przyjaznym miejscem dla wszystkich kibiców drużyny, której znakiem rozpoznawczym są niebiesko-czerwone barwy. Ale policja tego dnia spisała się na medal. Wysłałem nawet w tej sprawie list do dowódcy policji w Lewisham, Archibalda Torrance'a. W odpowiedzi przesłał mi wyrazy podziękowania za moje słowa uznania. – *Zawsze miło jest usłyszeć taką pochwałę* – wyjaśnia John Dale.

Brian Sims
dla Security Management Today Online

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Rozwiązanie dla dużych obiektów

krosownica wizyjna NV-MTX328

- 32 przelotowe wejścia kamerowe, 8 wyjść monitorowych z funkcją OSD
- możliwość rozbudowy systemu do 512 wejść kamerowych i 128 wyjść monitorowych w trybie równoległym
- możliwość rozbudowy systemu do 128 wejść kamerowych i 8 wyjść monitorowych w trybie MASTER-SLAVE
- możliwość równoczesnego sterowania krosownicami, kamerami obrotowymi i rejestratorami z klawiatury NV-KBD70
- możliwość podłączenia do 8 klawiatur NV-KBD70
- zawansowane funkcje automatyzacji zarządzania systemem: 80 sekwencji, 80 grup, 80 funkcji makro, wywoływanych zgodnie z harmonogramem

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

Krosowniczy system CCTV marki NOVUS dla dużych obiektów

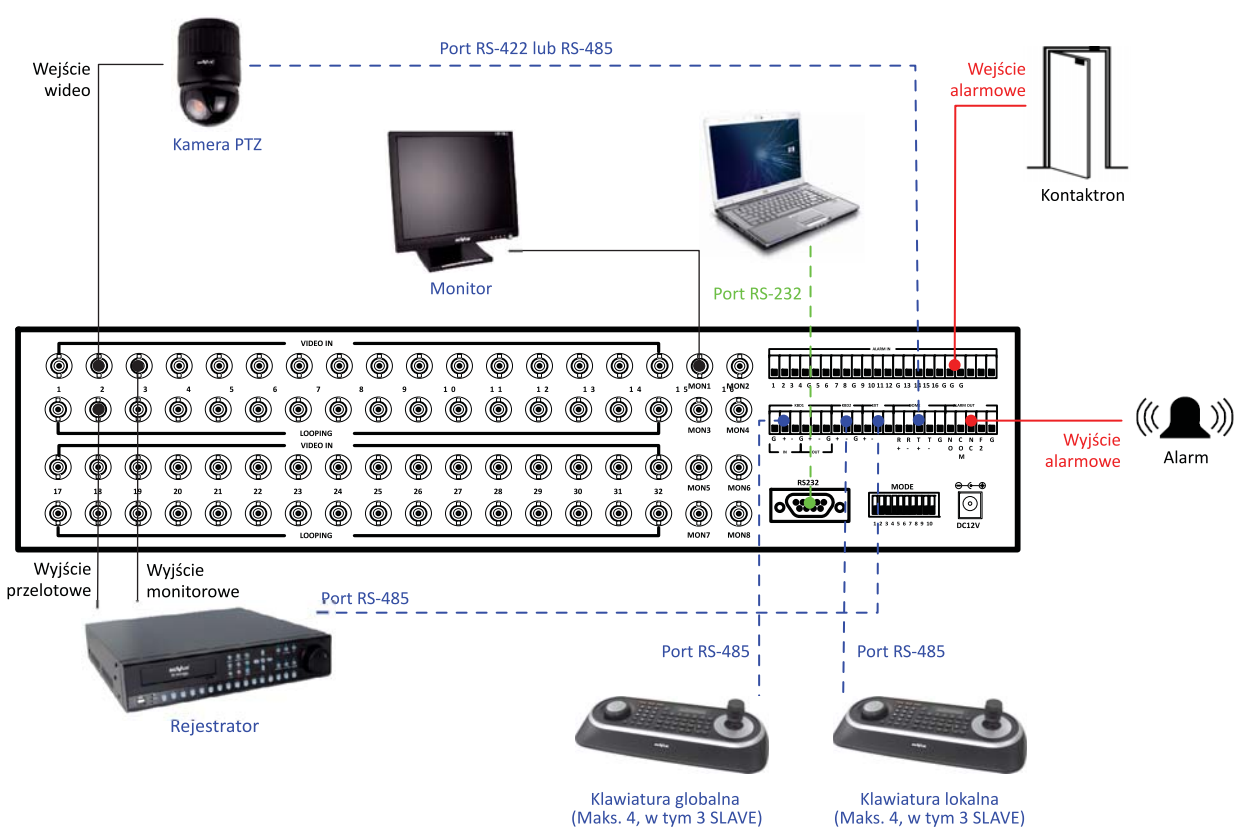
Efektywne zarządzanie systemem telewizji dozorowej w obiekcie z wieloma punktami nadzoru i dużą liczbą kamer nie może ograniczać się tylko do instalacji rejestratorów. W takiej konfiguracji trudno bowiem umożliwić poszczególnym użytkownikom pełny dostęp do zasobów systemu, tj. podglądu, odtwarzania, sterowania kamerami obrotowymi czy konfiguracji poszczególnych elementów. Na tak sformułowane założenia dotyczące systemu nadzoru wizyjnego odpowiedzią może być sieciowe oprogramowanie do zdalnego monitoringu i zarządzania rozproszoną grupą rejestratorów, np. RASplus dla rejestratorów serii 5000, system monitoringu IP (np. oprogramowanie NMS) lub zaawansowane systemy krosownicze. Dwa pierwsze rozwiązania zostały już przedstawione w poprzednich numerach magazynu *Zabezpieczenia*. Niniejszy artykuł poświęcony jest systemowi krosownic

Dla wielu obiektów z ciągłym nadzorem operatorskim, w tym szczególnie dla systemów monitoringu miejskiego, w których mamy do czynienia z ręcznym sterowaniem kamerami obrotowymi, szczególnie ważny jest wymóg pracy w czasie rzeczywistym, bez opóźnień. Wymóg ten w najwyższym stopniu spełniają systemy analogowe. Jest to jedna z niewielu przewag systemów analogowych nad cyfrowymi. Aby umożliwić efektywne zarządzanie monitoringiem, system krosowniczy musi zapewnić sprawną komunikację pomiędzy poszczególnymi jego elementami: krosownicami, rejestratorami, kamerami obrotowymi i klawiaturami. Dlatego, przedstawiając system krosowniczy, należy odnieść się do wszystkich wymienionych elementów i kompatybilności między nimi.

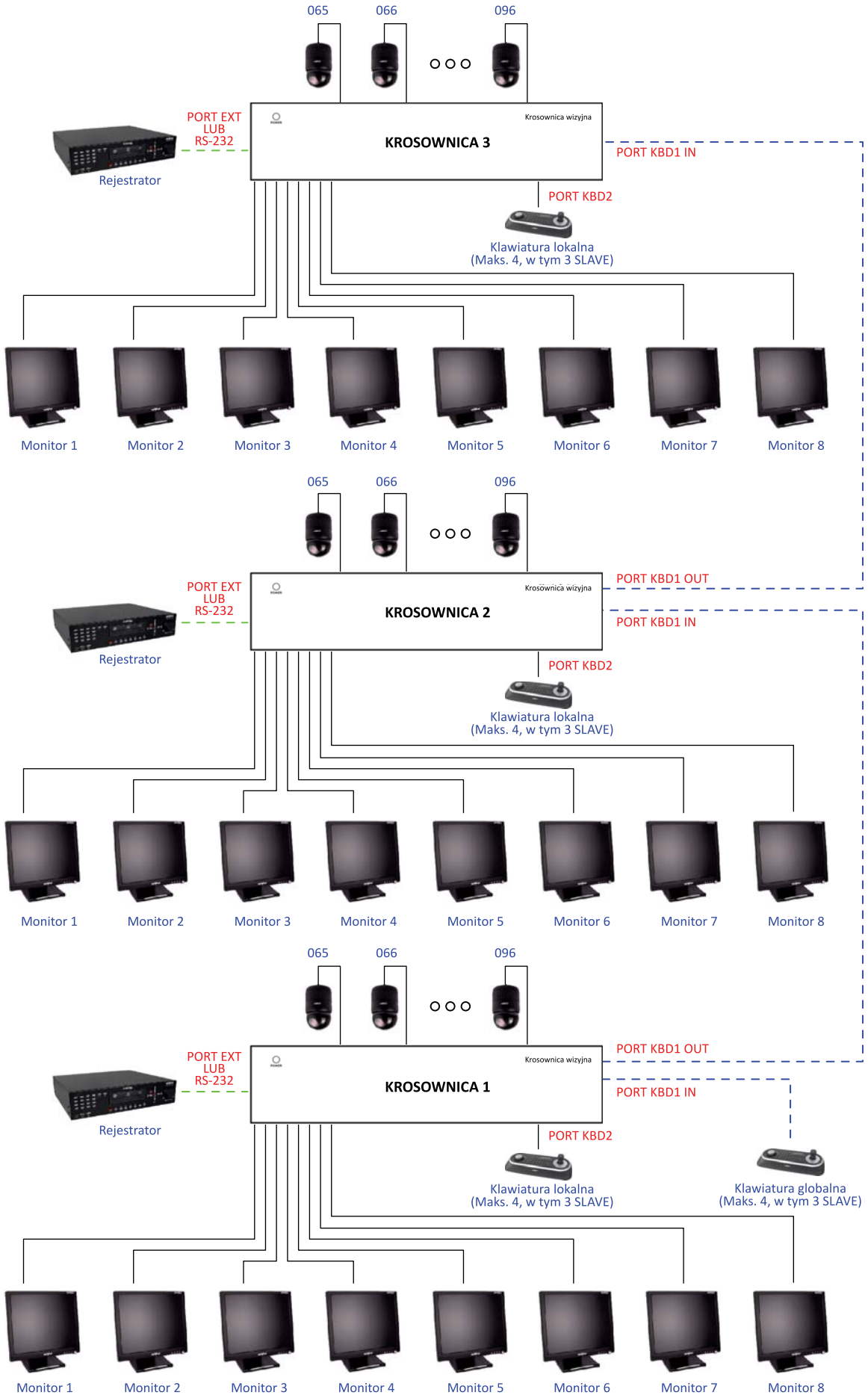
System krosowniczy marki NOVUS, wykorzystujący krosownicę NV-MTX328 z 32 wejściami wideo i ośmioma wyjściami monitorowymi, ma strukturę modułową. Tym samym pozwala zarządzać 512 lub 128 kamerami, w zależności od sposobu konfiguracji: równoległej lub typu *master/slave*. Niniejsze omówienie podstawowych funkcji krosownicy wykorzystuje schemat przedstawiający autonomiczną pracę pojedynczej krosownicy (Rys.1).

Zarządzanie krosownicą jest realizowane za pomocą klawiatury NV-KBD70 oraz menu ekranowego. Do krosownicy można podłączyć do ośmiu klawiatur poprzez dwa porty RS485. Klawiaturom tym można przyporządkować odpowiednie priorytety, to znaczy jedną z klawiatur podłączoną do portu można zdefiniować jako nadrzędną. Warto podkreślić fakt, że wszyscy operatorzy klawiatur mogą sterować nimi równocześnie. Rozwiązany został problem blokowania klawiatur przez pojedynczego operatora. Krosownice mają zaimplementowany protokół N-Control. Ten sam protokół jest wykorzystany do sterowania kamerami obrotowymi (port DOME) oraz rejestratorami (port EXT). W celu zapewnienia kompatybilności z już eksploatowanymi systemami w krosownicy zostały również zaimplementowane protokoły Novus-C, Novus-C1 oraz Pelco-D i Pelco-P. Ponadto krosownica posiada port RS232, który może być wykorzystany do celów diagnostyki lub aktualizacji *firmware* urządzenia z poziomu PC.

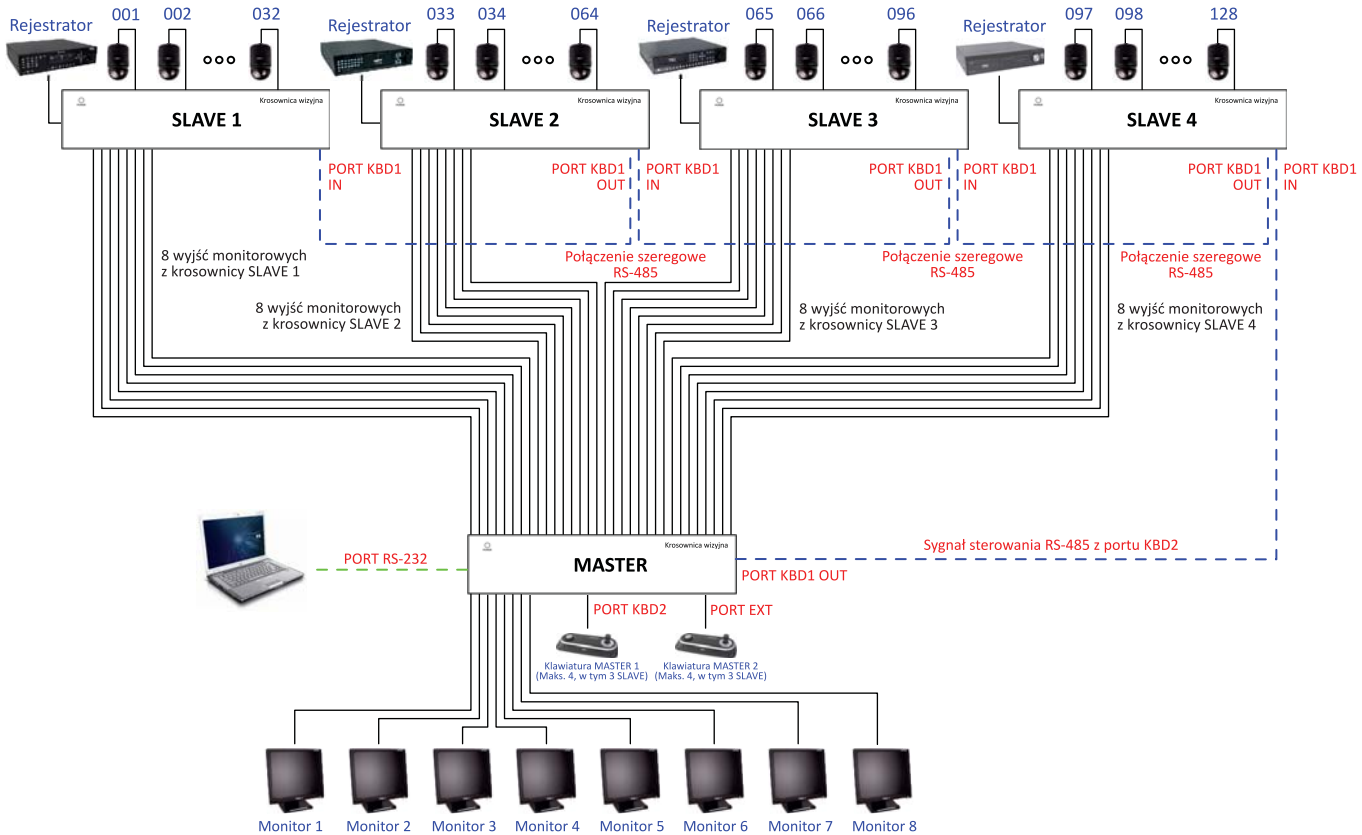
Niezależnie od liczby krosownic, kamer i rejestratorów zastosowanych w systemie dostęp do poszczególnych urządzeń można uzyskać za pomocą jednej komendy. Taki tryb pracy, bardzo efektywny i przejrzysty dla operatorów, należy zdefiniować w menu krosownicy. Krosownica ma szereg programowalnych funkcji, które ułatwiają obsługę systemu: 80 sekwencji, 80 grup, 80 funkcji makro, 80 zaprogramowanych funkcji wywoływanych zgodnie z ustalonym harmonogramem. Funkcja grupy pozwala na równoczesne wyświetlenie zaprogramowanych kombinacji kamer na wszystkich ośmiu monitorach. Pozwala to na szybki dozór wybranych stref. Dla poszczególnych monitorów można również zdefiniować pełnoekranową sekwencję z różnym czasem przełączania dla poszczególnych kamer. Wykorzystując zaprogramowane poprzednio grupy, można również zdefiniować dla nich funkcję sekwencji. Powiązanie z kamerami obrotowymi zapewnia funkcja makro, umożliwiająca równoczesne wywołanie ośmiu funkcji w kamerach obrotowych (presety, patrole, trasy obserwacji) i wyświetlenie obrazów z tych kamer na ośmiu monitorach. Za pomocą harmonogramu można zautomatyzować wykonywanie wymienionych funkcji w zależności od czasu (np. inne trasy patrolowania dla kamer w godzinach pracy i poza godzinami pracy obiektu).



Rys.1. Schemat konfiguracji pojedynczej krosownicy



Rys. 2. Konfiguracja równoległa pracy krosownic



Rys. 3. Konfiguracja master/slave pracy krosownic

Krosownica wizyjna ma 16 wejść alarmowych i dwa wyjścia alarmowe oraz rozbudowane menu definiowania alarmów na wypadek utraty sygnału wizji, komunikacji z daną kamerą lub aktywacji alarmu w krosownicy *slave*. Dostęp do ustawień menu jest zabezpieczony 6-znakowym hasłem. Ustawienia krosownicy, w tym hasło oraz wbudowany zegar systemowy, są podtrzymywane bateryjnie. W związku z tym chwilowy brak zasilania nie powoduje utraty ustawień. Menu krosownicy jest dostępne między innymi w języku polskim.

W konfiguracji równoległej operator może kontrolować do 16 krosownic i 512 kamer obrotowych równocześnie. W tej konfiguracji wszystkie krosownice są niezależne (autonomiczne) i dodatkowo mogą być sterowane jednocześnie klawiaturami lokalnymi oraz maksymalnie czterema klawiaturami określanymi mianem globalnych.

Szczególnie interesującym trybem pracy jest konfiguracja *master/slave*. Konfiguracja ta pozwala na podłączenie do 128 kamer wideo (cztery krosownice *slave*). Wyjścia monitorowe z tych krosownic podłączone są do wejść kamerowych krosownicy *master*. W ten sposób obraz z dowolnej kamery w systemie można wyświetlić na dowolnym monitorze krosownicy *master*. W przypadku pracy z mniejszą liczbą krosownic *slave* pozostałe wejścia kamerowe krosownicy *master* mogą zostać wykorzystane do bezpośredniego podłączenia sygnałów wideo z kamer. Wszystkie elementy systemu, również rejestratory podłączone do wyjść przelotowych krosownicy *slave*, sterowane są z poziomu klawiatur podłączonych tylko do krosownicy *master*.

Wszystkie elementy łączy klawiatura systemowa NV-KBD70 do zdalnego sterowania rejestratorami, kamerami i krosownicami. Obsługuje ona następujące serie rejestratorów marki NOVUS: NV-DVR1200, NV-DVR4600, NV-DVR5000 oraz NDR-H.

Kamerami obrotowymi steruje się, wykorzystując protokoły Pelco-D, Pelco-P, Novus-C, Novus-C1 oraz N-Control. Tak duży wybór protokołów sterowania zapewnia kompatybilność z wieloma typami kamer obrotowych i zestawami typu kamera – motor-zoom. Dwa poziomy haseł – *ADMINISTRATOR* i *USER* – umożliwiają operatorom systemu ograniczenie dostępu do konfiguracji klawiatury. Szczególnie ważną funkcją dla systemów z dużą liczbą kamer jest ściąganie i zapisywanie ustawień z kamer obrotowych (*data bank*). Opcja ta pozwala na zgranie lub wgranie ustawień wybranej kamery. Klawiatura ma dwa banki pamięci, w których można przechowywać konfigurację kamer. Funkcja ta jest dostępna w przypadku sterowania poprzez protokoły Novus-C i Novus-C1. Przejrzysty podział 48 przycisków wielofunkcyjnych na sekcje krosownic, rejestratorów i kamer oraz 32-znakowy wyświetlacz LED umożliwiają sprawne zarządzanie złożonymi systemami.

Zastosowanie urządzeń analogowych jest jedną z możliwości w przypadku realizacji dużych systemów monitoringu wizyjnego. Obecnie w wielu obiektach systemy bazujące na krosownicach są zastępowane przez systemy cyfrowe IP. Niemniej, ze względu na brak opóźnień w dystrybucji sygnału, co jest istotnym wymaganiem, zwłaszcza przy sterowaniu kamerami obrotowymi, znajdują one uznanie wielu projektantów i instalatorów systemów monitoringu wizyjnego.

Patryk Gańko
NOVUS Security

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

NOWA wielofunkcyjna klawiatura

klawiatura systemowa NV-KBD70

- zdalne sterowanie rejestratorami cyfrowymi NOVUS®, krosownicą NV-MTX328 oraz kamerami z interfejsem RS-485
- protokoły do sterowania rejestratorami: Novus-D2, N-Control
- protokoły do sterowania kamerami: Novus-C, Novus-C1, N-Control, Pelco-D, Pelco-P
- 3-osiowy dżojstik z funkcją zoom w pokrętle, 48 przycisków wielofunkcyjnych
- możliwość podłączenia do 3 klawiatur SLAVE do klawiatury MASTER
- 2 poziomy uprawnień: administrator (dostęp zabezpieczony hasłem) i operator
- bateryjne podtrzymanie zegara systemowego

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

Czy przekonałeś się już, jak cenna była zawartość twojego laptopa

Co łączy menedżerów, przedstawicieli handlowych i dziennikarzy? Każda z tych grup zawodowych musi być gotowa do mobilnej pracy, niezależnie od pory dnia lub tygodnia. Telefon komórkowy, samochód służbowy i laptop to nieodłączne atrybuty przedstawicieli tych grup. Dziś posiadanie tych dóbr nie jest już oznaką wysokiego statusu społecznego użytkownika. Dla wielu z nas są one po prostu podstawowymi narzędziami pracy, bez których nie bylibyśmy w stanie poradzić sobie z bezlitosną walką z konkurencją

Rozwój systemów telekomunikacyjnych umożliwia szybkie przesyłanie informacji pomiędzy siedzibą firmy, mobilnym pracownikiem i kontrahentem. Wymagający klienci cenią sobie wysoki poziom obsługi, skuteczność działania partnera biznesowego oraz zaufanie i bezpieczeństwo współpracy. Każda ze stron stara się dbać o własną reputację, chroniąc jedno z najcenniejszych dóbr niematerialnych, jakim jest informacja. Poziom zaufania niejednokrotnie stanowi o „być albo nie być" wielu instytucji. Ma bardzo istotne znaczenie w przypadku operowania na danych osobowych oraz newralgicznych informacjach, których nieuprawnione ujawnienie mogłoby doprowadzić do zakończenia działalności firmy.

Sposobów na zabezpieczenie się przed niekontrolowanym wyciekiem informacji jest wiele. Jedne są bardziej skuteczne, inne mniej, ale, zamiast stosować każde z nich z osobna, warto rozważyć wdrożenie kompleksowych rozwiązań. Takie podejście gwarantuje największą skuteczność i osiągnięcie najwyższego poziomu bezpieczeństwa.

Dostępność rozwiązań umożliwiających korzystanie z Internetu sprawia, iż możemy czerpać korzyści z tego dobrodziejstwa niemalże w każdym miejscu. O ile możemy czuć się w miarę spokojni o bezpieczeństwo danych przesyłanych przez nas za pośrednictwem modemu podłączonego bezpośrednio do laptopa wyposażonego w kartę SIM operatora telekomunikacyjnego, o tyle ryzyko pozyskania informacji przez osoby nieuprawnione wzrasta lawinowo wtedy, gdy korzystamy z darmowych punktów dostępowych, które często nie umożliwiają szyfrowania transmisji[1].

Możliwość bezpiecznego przesyłania danych to tylko jeden z elementów profilaktyki. Innym problemem jest konieczność zapewnienia bezpieczeństwa danych zapisywanych na lokalnym dysku twardym laptopa. W przypadku zagubienia czy kradzieży niezabezpieczonego laptopa możemy nie tylko bezpowrotnie stracić dane, ale również narazić na szwank reputację swoją, naszego pracodawcy oraz klientów. Jak się przed tym chronić? Czy istnieje możliwość bezpiecznej pracy z daleka od nafaszerowanego systemami bezpieczeństwa budynku firmy?

Sposobów na minimalizację ryzyka jest kilka, niektóre z nich postaram się pokrótce opisać.

1) Więcej informacji na temat zagrożeń związanych z korzystaniem z bezprzewodowych punktów dostępowych można znaleźć w artykułach „Phishing – polowanie na łatwowiernych" publikowanych na łamach Zabezpieczeń w numerach 63 i 64 (5/2008 i 6/2008).

Zanim zabierzemy się za uzbrajanie swojego sprzętu w zabezpieczenia uniemożliwiające potencjalnemu przestępcy dostęp do naszych danych, wykonajmy najprostsze działanie. Naklejmy na komputer niewielką kartkę z informacją o właścicielu urządzenia i jego numerem telefonu. Wiele laptopów ma na spodniej stronie specjalnie przeznaczone do tego celu miejsce. Jeśli go nie ma, można zastosować karteczkę samoprzylepną. Warto również zastanowić się nad dodaniem informacji o nagrodzie za zwrot urządzenia – nawet niewielka nagroda może usatysfakcjonować znalazcę, a na pewno będzie dodatkowym bodźcem do rozważenia zwrotu komputera.

Kolejnym krokiem jest uaktywnienie opcji w BIOS, która wymusi konieczność podania hasła umożliwiającego start systemu operacyjnego komputera. W przypadku większości laptopów obejście tego zabezpieczenia nie jest proste, a niejednokrotnie możliwe wyłącznie w autoryzowanym punkcie serwisowym. Zastosowanie takiego rozwiązania nie uchroni nas przed utratą danych (w szczególności wówczas, gdy nie są dodatkowo szyfrowane) – znalazca laptopa może po prostu wymontować twardy dysk i podłączyć go do innego komputera, dzięki czemu uzyska dostęp do naszych danych – może jednak skutecznie zniechęcić znalazcę do zatrzymania komputera i skłonić do zwrócenia go właścicielowi. Przy stosowaniu hasła BIOS należy pamiętać o przechowaniu kopii hasła w bezpiecznym miejscu, gdyż w przypadku jego zagubienia możemy wpaść w zastawioną przez siebie pułapkę i narazić się na koszty związane z wizytą w serwisie.

Następnym elementem zabezpieczenia komputera jest uaktywnienie opcji wymuszenia wprowadzenia hasła logowania do systemu operacyjnego. Należy przy tym pamiętać o zasadzie, że im bardziej skomplikowane jest hasło (zawierające małe i wielkie litery, cyfry oraz znaki specjalne), tym trudniejsze jest jego przełamanie. Nie jest jednak tajemnicą, iż o ile zabezpieczenie to bardzo skutecznie chroni przed mało doświadczonymi włamywaczami, o tyle wprawny informatyk potrafi sobie z nim poradzić w stosunkowo niedługim czasie. Podobnie jak w przypadku hasła w BIOS, zabezpieczenie to utrudni dostęp do systemu operacyjnego, natomiast nie uchroni nas przed nieuprawnionym dostępem do danych zgromadzonych na dysku. Prócz możliwości zamontowania naszego dysku w innym komputerze – co umożliwi dostęp do naszych plików – istnieje możliwość wystartowania komputera z tzw. bootowalnego nośnika zewnętrznego (np. CD, DVD, dysku USB), umożliwiającego uruchomienie na naszym laptopie drugiego systemu operacyjnego z dostępem do danych zawartych na lokalnym dysku twardym. W przypadku zastosowania hasła w BIOS zmiana sposobu uruchamiania komputera (np. z nośników zewnętrznych) nie jest możliwa – jest to kolejny argument przemawiający za słusznością korzystania z tego rozwiązania.

Skutecznym zabezpieczeniem jest również zastosowanie dodatkowo sprzętowych kluczy systemowych (np. w postaci nośników USB lub kart z chipem), zawierających certyfikat umożliwiający zalogowanie do systemu – oczywiście o ile nie są one przechowywane w tej samej torbie co laptop. Bez takiego klucza uruchomienie systemu operacyjnego jest bardzo utrudnione. Zaawansowane systemy wykorzystujące klucze sprzętowe bardzo często połączone są z rozwiązaniami umożliwiającymi szyfrowanie danych, przy czym systemy szyfrowania danych mogą być również rozwiązaniami wyłącznie aplikacyjnymi. Do szyfrowania danych można wykorzystywać różnego rodzaju oprogramowanie – programy kompresujące typu RAR i ZIP, które umożliwiają tworzenie archiwów zabezpieczonych hasłami, dedykowane rozwiązania do szyfrowania pojedynczych plików, kompleksowe systemy umożliwiające szyfrowanie całej zawartości dysku. Im wyższy stopień zaawansowania rozwiązania, tym wyższa jego cena, więc przed podjęciem decyzji o wyborze systemu warto oszacować ryzyko pozyskania danych przez nieuprawnione osoby. Niektóre z wyrafinowanych systemów bezpieczeństwa występują w kilku wersjach, w których część funkcji jest dostępna nieodpłatnie, a część aktywowana po wniesieniu opłaty za licencję (przykładem może być oprogramowanie PGP Desktop, które w wersji podstawowej – służącej m.in. do szyfrowania plików i kasowania zbędnych plików w sposób uniemożliwiający odtworzenie skasowanych danych – jest oprogramowaniem darmowym do zastosowań niekomercyjnych, a po wniesieniu opłaty dostępnych jest więcej funkcji – m.in. szyfrowanie dysków i tworzenie wirtualnych, szyfrowanych wolumenów). Stosowanie tego typu rozwiązań należy do najbezpieczniejszych, gdyż nawet w przypadku wymontowania lokalnego dysku twardego i podłączenia go do innego komputera dostęp do naszych danych będzie niemożliwy.

Dodatkowymi środkami ostrożności (przeznaczonymi dla pracodawców chcących uchronić się przed niekontrolowanym wypływem danych spowodowanym przez pracowników) są systemy monitorowania gromadzące informacje o rodzaju danych kopiowanych na nośniki zewnętrzne lub wysyłanych za pośrednictwem poczty elektronicznej.

Alternatywą dla wcześniej wymienionych sposobów zabezpieczeń – aczkolwiek niekoniecznie je eliminującą – jest praca na zdalnym, firmowym zasobie, dzięki której dostęp do newralgicznych danych jest znacznie bardziej utrudniony. Jak to wygląda w praktyce? Wykorzystując system operacyjny i odpowiednią aplikację zainstalowaną na laptopie, za pośrednictwem łącza internetowego użytkownik loguje się do sieci wewnętrznej swojej firmy. Udostępnione użytkownikowi zasoby firmowe mogą być widoczne jako dodatkowy folder lub np. portal z dokumentami służbowymi. Wykorzystywanie takich zasobów podczas pracy sprawia, iż laptop jest jedynie terminalem umożliwiającym wykorzystanie dysków twardych zdalnie, a dokumenty, które wykorzystujemy podczas pracy, wcale nie muszą być kopiowane na lokalny dysk twardy. W przypadku utraty laptopa możemy zatem być spokojni o bezpieczeństwo danych. Zastosowanie tego rodzaju rozwiązania wymaga odpowiedniego zabezpieczenia połączenia firmy z Internetem – minimalizującego ryzyko włamania do zasobów wewnętrznych podmiotu – oraz zabezpieczenia laptopa przed włamaniem z zewnątrz. W tym przypadku wymagane jest kierowanie się podstawowymi zasadami bezpieczeństwa, zgodnie z którymi konieczne jest posiadanie legalnego, na bieżąco aktualizowanego systemu operacyjnego, aktualnej wersji firewalla oraz oprogramowania antywirusowego.

Nie należy jednak zapominać, iż żadne – nawet najbardziej wyrafinowane – rozwiązanie nie uchroni w stu procentach przed zagrożeniem ze strony celowego działania pracownika. Warto więc dbać o dobrą atmosferę w pracy, gdyż zadowolony pracownik to dobry pracownik.

Krzysztof Białek

Czujki LC - gwarancja optymalnej ochrony

DSC

Zewnętrzne czujki dualne LC-151 i LC-171, z funkcją odporności na zwierzęta, wykorzystują technologię detekcji podczerwieni i detekcji mikrofalowej. Specjalnie zaprojektowane do zastosowań w trudnych warunkach zewnętrznych, zapewniają precyzyjne wykrycie intruza, redukując do minimum możliwość występowania fałszywych alarmów. Pole detekcji każdej z czujek oraz czułość czujnika PIR regulowane są za pomocą przełączników, dzięki czemu działanie urządzeń można dostosować do warunków środowiskowych panujących w obszarze detekcji czujnika. LC-151 i LC-171 doskonale sprawdzają się do zewnętrznej ochrony dużych powierzchni, a w zależności od miejsca instalacji mogą być montowane na ścianach lub słupkach.

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

iProtect oraz DIVA

Inteligentne rozwiązania, inteligentny system bezpieczeństwa

Standardy obowiązujące obecnie w systemach bezpieczeństwa są efektem wyraźnej ewolucji, która dokonała się w ciągu ostatnich kilku lat. Korzystamy już nie tylko z kontroli dostępu, monitoringu CCTV czy centrali alarmowej. O bezpieczeństwo dbają potężne systemy zapewniające podgląd stanu obiektu w dowolnym miejscu i chwili. W dobie globalizacji i Internetu coraz bardziej doceniane i potrzebne stają się systemy zintegrowane. Właśnie taką integrację oferuje pakiet iProtect oraz DIVA holenderskich firm należących do holdingu THK. Współdziałanie tych rozwiązań daje idealne narzędzie do zarządzania bezpieczeństwem dzięki integracji wielu różnych modułów, z których każdy stanowił dotychczas niezależny podsystem. Platforma SMS (*Security Management System*) pozwala na obniżkę kosztów związanych z ochroną fizyczną, a dodatkowo zwiększa funkcjonalność indywidualnych zazwyczaj systemów

Fot. 1. Stanowisko dowodzenia w przeglądarce internetowej

Stanowisko dowodzenia w przeglądarce internetowej

iProtect to pierwszy system sieciowy, który oferuje wiele zaawansowanych funkcji i skupia w sobie moduł kontroli dostępu, system sygnalizacji włamania, rejestrację czasu pracy, system telewizji dozorowej, pakiet zarządzania parkingiem i współpracujący z systemami komunikacji Commend lub Astrisk.

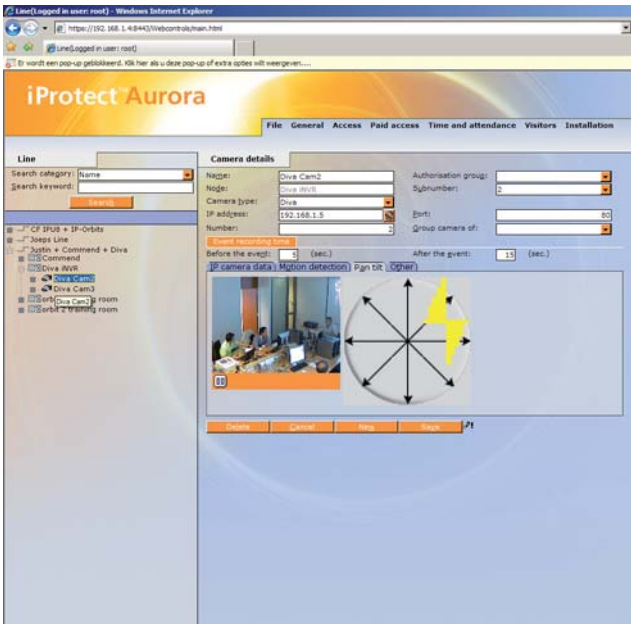
Oprócz możliwości sporządzania wielu raportów system może także wizualizować stan urządzeń. Interaktywne mapy ułatwiają kontrolę stref oraz przypisanych im elementów (czytników, czujek, kamer, interkomów, telefonów IP, osób). Po wskazaniu myszką odpowiedniej ikony możliwy jest odczyt ostatnich zdarzeń lub zmiana statusu urządzenia (wraz ze zmianą statusu ikony). W systemie dostępny jest moduł zarządzania alarmami, który pozwala na przygotowanie scenariusza zdarzeń dla operatora. Moduł potrafi inteligentnie kierować zdarzenia (raporty) do zalogowanych użytkowników, zgodnie z ustalonymi wcześniej definicjami zdarzeń alarmowych. Raporty mogą być z łatwością drukowane, przesyłane i archiwizowane. Podstawowym narzędziem do konfigurowania systemu, wprowadzania w nim zmian i odczytu parametrów jest komputer PC z zainstalowaną przeglądarką internetową Internet Explorer 6 lub Mozilla Firefox 3 (lub nowszą). Aplikacja jest wyświetlana w oknie przeglądarki jako strona HTML, dlatego nie wymaga instalacji dodatkowego oprogramowania na komputerze roboczym. Dzięki zastosowaniu technologii IP możliwe jest zarządzanie i nadzór nad odległym budynkiem z dowolnego miejsca na świecie. Komunikacja między serwerem Sun Fire z iProtect a terminalem roboczym wykorzystuje kodowanie SSL.

Różni klienci – różne potrzeby

Niewątpliwą zaletą systemu jest skalowalność. Nie należy obawiać się, że raz zakupiony sprzęt w przyszłości nie będzie spełniał wymogów związanych z rozbudową systemu. Początkowo inwestor może korzystać z małego systemu, a z czasem uzupełniać go o kolejne elementy tak, by sprostać oczekiwaniom klienta końcowego. Dodanie modułów czy też urządzeń wiąże się z kupnem dodatkowej licencji.

Obserwacja za pośrednictwem telewizji dozorowej jest od lat jednym z najbardziej popularnych sposobów ochrony obiektów. Kilkanaście kamer oraz nieostry obraz na wysłużonym monitorze to już, na szczęście, przeszłość. Obecnie systemy IP, współdziałające z programami zarządzającymi, takimi jak iProtect, dają zdecydowanie więcej. Współpraca kamer z iProtect pozwala między innymi na dokonywanie identyfikacji tablic rejestracyjnych i obiektów, przypisywanie kamery do czytnika, strefy oraz interkomu, automatyczne przerzucanie obrazu, zapisywanie pojedynczych klatek itd.

Podstawowym modułem w iProtect jest jednak moduł kontroli dostępu. Oferowany system obsługuje wszelkie popularne standardy i zaawansowane funkcje, takie jak śluza, APB, rejestracja obecności pracowników i gości. Wykorzystanie kart dostępowych i systemu kamer obserwacyjnych umożliwia także nadzór nad parkingiem firmowym, natomiast wszędzie tam, gdzie potrzebna jest komunikacja głosowa, wykorzystywany jest system interkomowy Commend.



Fot. 2. Konfiguracja modułu wideo – wybór kamery w iProtect

Kolejnym chętnie stosowanym sposobem ochrony obiektów jest sygnalizacja włamania. Wykorzystanie sieciowej centrali alarmowej CCS128, komunikującej się za pośrednictwem protokołu TCP/IP, umożliwia zastosowanie w systemie do 128 czujek, stworzenie 16 stref i obsłużenie ośmiu manipulatorów. Oczywiście możliwe jest dodanie kolejnej centrali i kolejnych koncentratorów linii w celu zwiększenia obszaru ochrony o nowe strefy i manipulatory.

W dużych przedsiębiorstwach przydaje się także rejestracja czasu pracy. Innowacją w rozwiązaniu RCP firmy Keyprocessor jest terminal INFOBOX, umożliwiający przeglądanie statystyk przez przeglądarkę internetową i ingerowanie w nie.

Współpraca iProtect i DIVA

W niniejszym artykule opisany zostanie moduł wideo w systemie iProtect. Aby, oprócz rejestrowania wideo, system mógł reagować na odpowiednie zdarzenia, potrzebny jest dodatkowy serwer z oprogramowaniem. Platforma DIVA rozszerza systemy monitorowania o wiele funkcji analizy obrazu. Największą zaletą systemu jest połączenie techniki kompresji danych przesyłanych z kamer IP oraz analizy obrazu. W celu uniknięcia przesyłania dużej ilości danych w systemie DIVA zastosowane zostały kamery i kodery mające funkcje analizy obrazu, dlatego funkcje te wykonywane są na obrazie najwyższej jakości i bez obciążenia sieci. Oprócz analizowania obrazu platforma DIVA współpracuje z systemem kontroli dostępu i autoryzacji iProtect. Integracja systemu iProtect z Diva fizycznie polega na wpięciu serwera oraz kamer do jednej sieci IP. W oprogramowaniu iProtect dokonuje się wyboru odpowiednich kamer i przypisuje się je np. do czytnika czy strefy SSWiN. Ideą integracji jest powiązanie zdarzenia w jednym z systemów (np. w popularnym systemie KD) z odpowiednią, krótką sekwencją obrazów z pobliskiej kamery, co pozwala na jednoznaczny opis zaistniałej sytuacji. Algorytmy detekcji obiektu, wykrywania zmian w tle sceny, rozpoznawania tablic rejestracyjnych oraz rozpoznawania

Fot. 3. Serwer DIVA

twarzy, wykonywane już w kamerze lub koderze, pozwalają rozszerzyć funkcjonalność systemu o kolejne elementy.

Koncepcja platformy DIVA jest oparta na strukturze zdarzeń, reguł, makr i profili definiowanych przez użytkownika. Każdy inteligentny komponent z zaprogramowanymi regułami generuje zdarzenie, uaktywniając zdefiniowane wcześniej macro, np. otwarcie drzwi w systemie kontroli dostępu. Kombinacja makr powiązanych z ustawieniem kamer nazywana jest profilem. Taka architektura pozwala na elastyczną współpracę z innymi systemami, dając nieograniczone możliwości w systemach wirtualnych.

System współpracuje z różnymi kamerami IP, od 1-megapikselowych po 8-megapikselowe, z serwerami o pojemności nawet do 24 TB, a także z zaawansowaną aplikacją zarządzająca całym systemem.

Aplikacja zarządzająca systemu DIVA od wersji 1.5 posiada wbudowany moduł obsługi map i wizualizacji. Naniesione w systemie mapy można wzbogacić o ikony reprezentujące kamery, dowolnie je przenosić i łączyć ze sobą (np. łączyć mapy pięter budynku w podkatalogi).

Opcjonalnie serwer sieciowy DIVA umożliwia dodanie połączenia XML i komunikację z systemem iProtect, dzięki czemu serwer wysyła i odbiera informacje. Obsługa odbywa się za pomocą okna przeglądarki.

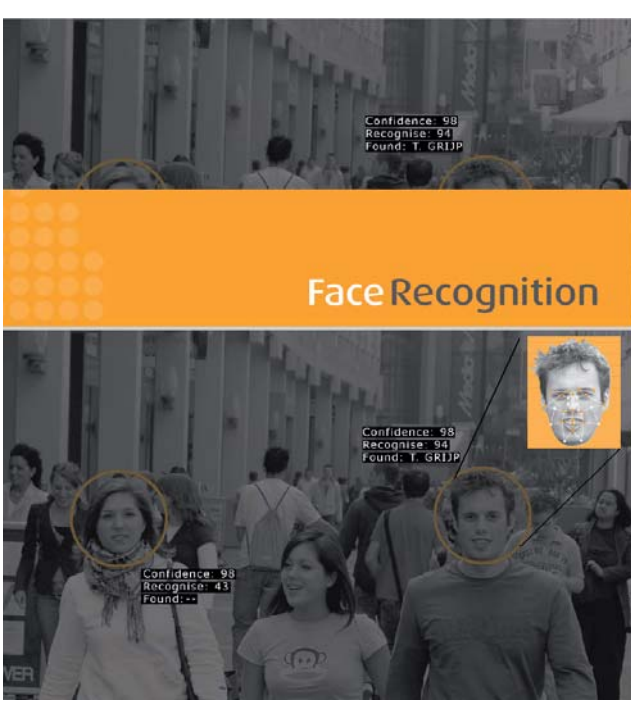
System wirtualnej krosownicy bazuje na programowym tworzeniu profili użytkownika, skryptów oraz makr, które można powielać i przenosić na inne stanowiska obsługi. Daje to możliwość kreowania podglądu dla potrzeb danego użytkownika lub obiektu i zwiększa funkcjonalność systemu. W zależności od potrzeb użytkownika platforma DIVA może zostać wyposażona w dodatkowe moduły funkcjonalne, takie jak FaceR, ObjectR, SceneR, CarR.

Moduł FaceR to aplikacja do rozpoznawania twarzy. Umożliwia ona rejestrowanie i weryfikację twarzy na podstawie wizerunku umieszczonego we wcześniej utworzonej bazie danych. Taka weryfikacja może być wykorzystana w systemie kontroli dostępu iProtect firmy Keyprocessor. System ten, w odróżnieniu od innych biometrycznych systemów kontroli dostępu, jest w niewielkim stopniu inwazyjny i umożliwia weryfikację osoby na podstawie obrazu jej twarzy (2D) zarejestrowanego z pewnej odległości, nie sygnalizując zaistnienia procesu weryfikacji i nie zmuszając badanej osoby do wykonania jakiejkolwiek czynności (np. do skanowania linii papilarnych czy siatkówki oka). System automatycznie lokalizuje i identyfikuje 17 punktów na twarzy obserwowanej osoby (wokół oczu, nosa i ust) i porównuje wynik z wzorcem z bazy danych.

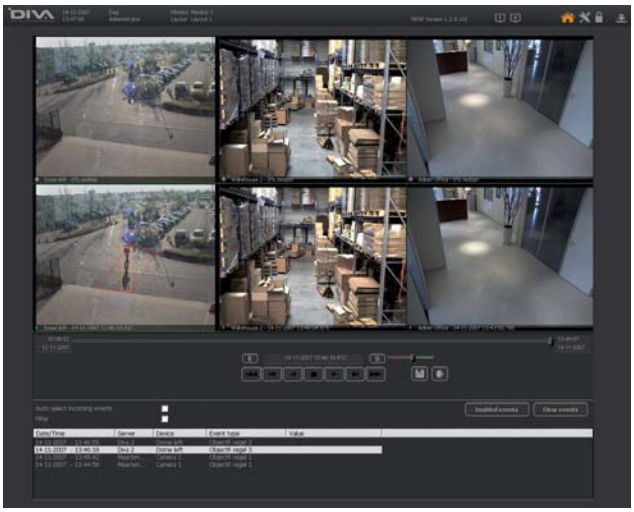
Moduł ObjectR to aplikacja do rozpoznawania obiektów. Umożliwia ona zliczanie osób/obiektów, określa czas przebywania osób na wyznaczonym obszarze lub pozwala na detekcję kolejki. Moduł wykrywa pojawienie się obiektów na obrazie (np. graffiti, śmieci itd.) lub zniknięcie obiektów (np. dzieł sztuki na wystawach). Umożliwia również tworzenie wirtualnej ochrony obwodowej, wybór obiektów widocznych na obrazie i ich selekcję, detekcję aktów wandalizmu, detekcję źle zaparkowanych aut, ustalanie reguł zachowania się wyselekcjonowanych obiektów. Dzięki temu możliwe jest tworzenie kryterium powstania alarmu w polu widzenia kamery.

Moduł SceneR umożliwia detekcję sceny i wykrywa wszelkie zmiany położenia kamery. Dzięki temu w momencie, gdy intruz obróci kamerę, aby uniemożliwić obserwację danej sceny, system zaalarmuje o tym zdarzeniu. Eliminuje to próby sabotażu systemu monitoringu.

Moduł CarR służy do rozpoznawania tablic rejestracyjnych. Idealnie współpracuje on z aplikacją parkingową w systemie iProtect. Dzięki niemu możliwe jest tworzenie białych i czarnych list (*black/white lists*) służących do weryfikacji pojazdów. W połączeniu z systemem kontroli dostępu i systemem szlabanów możliwy jest odczyt tablic każdego z aut i zweryfikowanie, czy dany pojazd może wjechać na teren obiektu, czy nie. System odczytuje numery tablic za pomocą specjalnie rozlokowanych kamer oraz klasyfikuje je w bazie danych. Klasyfikacja odbywa się na podstawie kraju, numeru tablicy, godziny detekcji oraz daty. Informacje są przesyłane do klienta i mogą być odczytane w intuicyjnym i przejrzystym panelu, za pomocą przeglądarki lub dedykowanego oprogramowania.



Fot. 4. Moduł rozpoznawania twarzy FaceR



Fot. 5. Interfejs DIVA

Platforma DIVA umożliwia również integrację systemu z innymi interfejsami, takimi jak LENEL lub TOKHEIM. Dodatkowym atutem jest możliwość współpracy popularnych kamer IP, np. VIVOTEK, MOBOTIX, AXIS, ARECONT, z serwerem DIVA.

Oferowana przez C&C Partners platforma zarządzania bezpieczeństwem ma następujące cechy użytkowe:

– jest aplikacją sieciową, obsługiwaną przez przeglądarkę,
– umożliwia komunikację z urządzeniami za pomocą standardowego protokołu IP,
– umożliwia dołączenie analogowych kamer CCTV,
– integruje czytniki kontroli dostępu zewnętrznych dostawców,
– umożliwia nadzór oddalonych od siebie obiektów,
– umożliwia tworzenie systemów o nieograniczonej wielkości,
– umożliwia obsługę interaktywnych map,
– umożliwia dopasowanie systemu do bieżących potrzeb i możliwości klienta oraz łatwą rozbudowę systemu w przyszłości,
– umożliwia użycie modułu zawierającego wbudowane elementy analityki wideo.

Tylko cztery firmy (w tym Keyprocessor) oferują system bezpieczeństwa *End-to-End*, czyli kodowanie połączenia od czytnika do samego serwera. Protokół zabezpieczający to AES256.

W przeciwieństwie do systemów konkurencyjnych rozwiązanie firmy Keyprocessor jest zainstalowane na serwerze Sun Fire, dedykowanym aplikacjom pracującym nieprzerwanie przez wiele lat.

Niektóre rozwiązania konkurencyjne potrafią integrować kilka podsystemów, jednak oprócz wizualizacji nie dają niczego więcej. iProtect umożliwia predefiniowanie zdarzeń, dzięki czemu jeden z systemów może reagować na sygnał z innego. Ponadto podczas przeglądu historii zdarzeń w jednym z modułów użytkownik znajdzie jednoznaczne odniesienia do aktywności innego modułu.

Marek Katarzyński
Michał Wilkoński
C&C Partners Telecom

ZSJZ

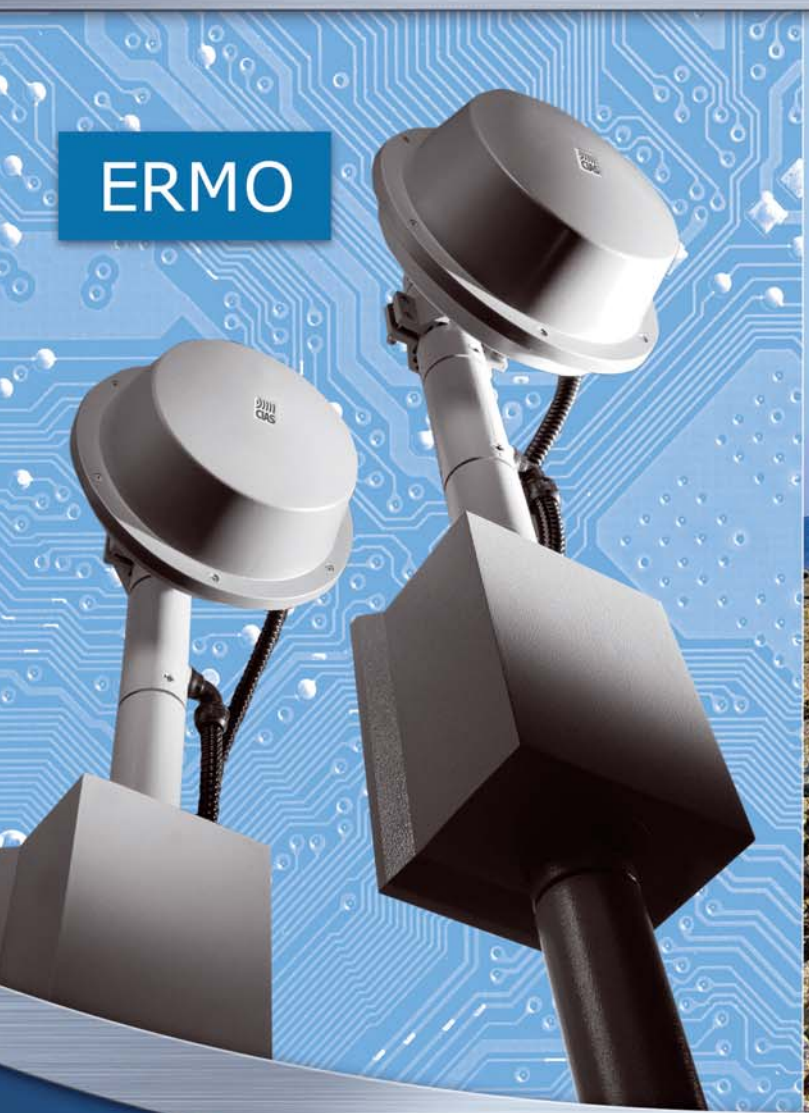
AQAP 2110:2006

Certyfikowany na zgodność z: PN - EN ISO 9001 : 2001

firma **ATLine®**

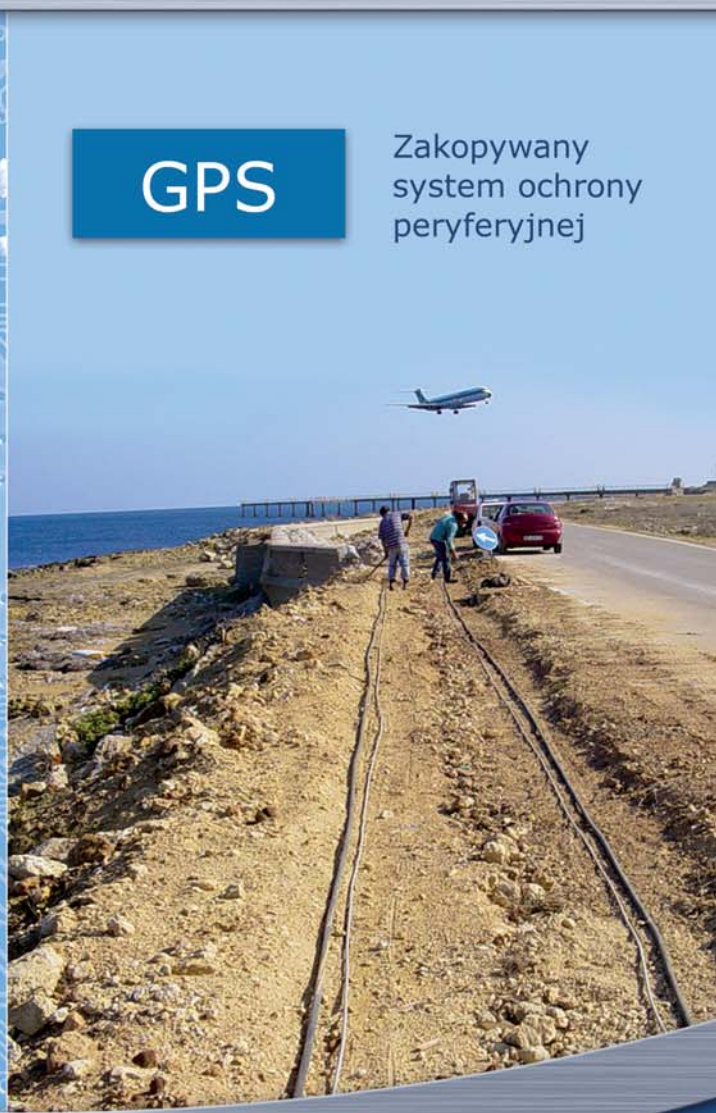
kompleksowe zabezpieczanie obiektów

ERMO



GPS

Zakopywany system ochrony peryferyjnej



16 LAT DOŚWIADCZENIA

16 lat doświadczenia, profesjonalizm i wysoka jakość oferowanych przez nas usług, gwarantują Państwu pełną satysfakcję.
Oferujemy Państwu atrakcyjne ceny, bezpłatne szkolenia i wsparcie fachowców w ramach zakupu.
Zapraszamy na naszą stronę www.atline.pl
Wszelkie wyceny i propozycje zabezpieczeń przeprowadzamy bezpłatnie.

Firma ATLine sp.j. K. Cichulski S. Pruski, 91-845 Łódź, ul. Franciszkańska 125
tel. +48 042 657 30 80, fax +48 042 655 20 99, e-mail: info@atline.pl, handel@atline.pl

Czas

jako kryterium skuteczności przebiegu procesu neutralizacji zagrożeń w systemach nadzorujących stan chronionego obiektu

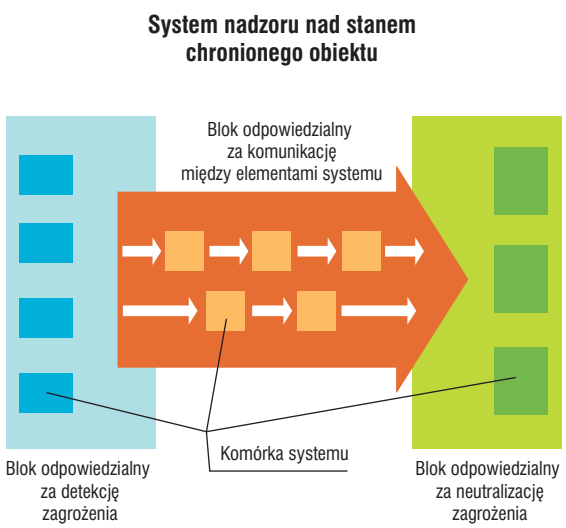
Nieustanny rozwój technologii teleinformatycznych daje użytkownikowi coraz to bardziej wyrafinowane środki techniczne umożliwiające nadzór i kontrolę nad chronionym obiektem. Wykorzystanie nowych technologii ma następujący cel: skrócić czas potrzebny na neutralizację zaistniałego w obiekcie zagrożenia. W artykule przedstawiona została analiza czynników wpływających na przebieg procesu przekazywania informacji oraz na czas neutralizacji zagrożenia. Artykuł ten stanowi wstęp do przedstawienia możliwości zastosowania elementów współpracujących z siecią telefonii mobilnej i Internetem w systemach nadzoru nad stanem chronionego obiektu

Wstęp

Od systemów zabezpieczających i nadzorujących stan chronionego obiektu wymaga się nie tylko skutecznych rozwiązań umożliwiających wykrycie różnych możliwych zagrożeń. Ważne jest również szybkie i precyzyjne skierowanie informacji o wykrytym zagrożeniu do odpowiednich komórek organizacyjnych i grup użytkowników systemu. Przez użytkowników systemu należy rozumieć zarówno osoby bezpośrednio odpowiedzialne za nadzór nad chronionym obiektem (właściciel obiektu, ochrona obiektu), jak i odpowiednie służby zewnętrze (policja, straż pożarna). Wynika z tego, że każdy system nadzoru musi posiadać bloki funkcyjne skupiające elementy odpowiedzialne za:

– detekcję zagrożenia,
– komunikację między komórkami organizacyjnymi i użytkownikami systemu,
– fizyczną neutralizację zagrożeń.

Schemat funkcyjny systemu nadzoru nad stanem chronionego obiektu został przedstawiony na rys. 1.



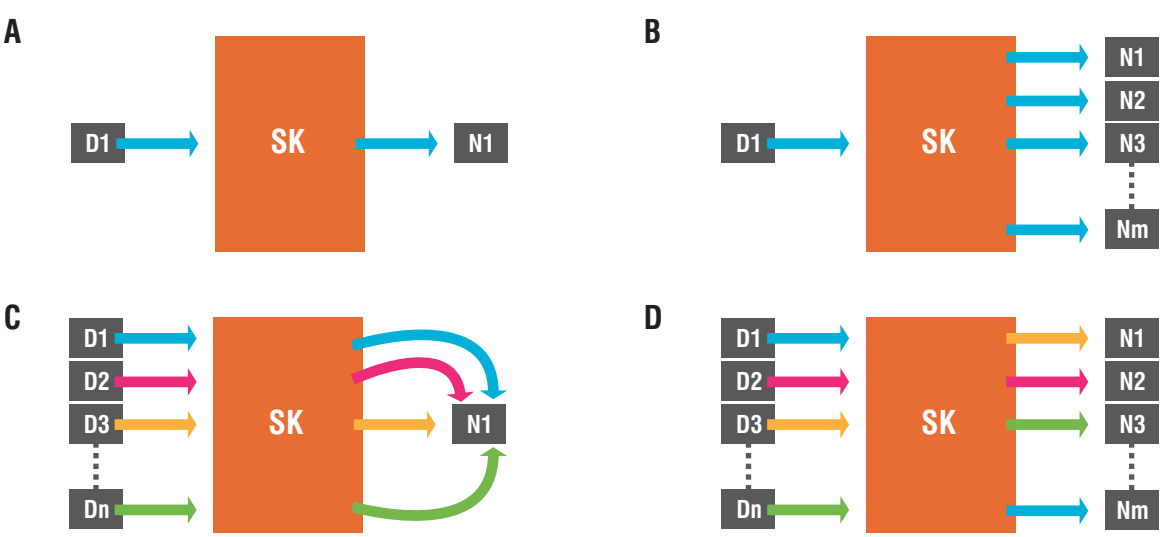
Rys. 1. Schemat funkcyjny systemu nadzoru nad stanem chronionego obiektu

Skuteczność systemu i podjętych przez niego działań jest zatem ściśle związana z czasem przebiegu sygnału informacyjnego od detektora do służb odpowiedzialnych za neutralizację zagrożenia. Im krótszy jest czas pomiędzy chwilą wykrycia zagrożenia a reakcją użytkownika systemu na dane zagrożenie, tym większa jest szansa na ograniczenie szkód wywołanych tym zagrożeniem. Ze względu na liczbę elementów w blokach odpowiedzialnych za detekcję i fizyczną neutralizację zagrożenia wyróżnić można następujące warianty systemów nadzoru nad stanem chronionego obiektu (rys. 2):

– system 1:1 (jeden detektor – jedna komórka organizacyjna systemu odpowiedzialna za neutralizację),
– system 1:M (jeden detektor – M komórek systemu odpowiedzialnych za neutralizację),
– system N:1 (N detektorów – jedna komórka systemu odpowiedzialna za neutralizację),
– system N:M (N detektorów – M komórek systemu odpowiedzialnych za neutralizację).

Pomimo tego, że we wszystkich tych modelach rola elementów odpowiedzialnych za przekazywanie informacji jest taka sama (powiadomienie konkretnej komórki systemu w przypadku zadziałania danego detektora), wraz ze wzrostem liczby detektorów i służb algorytm przesyłu sygnału informacyjnego komplikuje się. Ponadto na skomplikowanie procedury komunikacyjnej wpływa liczba ogniw pośredniczących w przekazywaniu informacji (rys. 3). Przeważnie podczas wzrostu liczby ogniw pośredniczących w procesie przekazywania informacji rośnie liczba rodzajów mediów wykorzystywanych w tym procesie. Podczas realizacji zadań powierzonych poszczególnym blokom funkcyjnym mogą być wykorzystane komórki systemowe z udziałem ludzi lub techniczne (sprzętowe). Przewaga czynnika ludzkiego nad czynnikiem sprzętowym wynika między innymi z wpływu inteligencji i doświadczenia człowieka. Natomiast czynnik sprzętowy przewyższa czynnik ludzki precyzyjnością i powtarzalnością pomiaru.

Istotne staje się zatem wyposażenie systemów nadzoru w środki techniczne, dzięki którym proces przekazywania informacji o stanie obiektu na drodze system – użytkownik



Rys. 2. Warianty systemów nadzoru ze względu na liczbę elementów odpowiedzialnych za detekcję zagrożenia (D) i neutralizację zagrożenia (N): a) system 1:1, b) system 1:M, c) system N:1, system N:M, SPI – system przekazywania informacji

odbywa się automatycznie, według pewnego ustalonego wcześniej algorytmu działania, najlepiej z wyeliminowaniem zbędnych ogniw pośredniczących i ograniczoną rolą czynnika ludzkiego. Ponadto ważne jest, aby aktualna informacja o stanie obiektu, zarówno w stanie normalnej pracy jak i w stanie wykrycia zagrożenia, była dostępna na każde żądanie użytkownika w trybie pracy *on-line*, aby nie była ograniczona do pewnego obszaru oraz była przeznaczona i skierowana tylko do wybranej grupy odbiorców.

Z przedstawionych wymagań najwięcej kontrowersji budzi ograniczenie roli człowieka w procedurze przekazywania informacji. O ile od strony technicznej jest to jak najbardziej wykonalne, trudno zrealizować to od strony formalno-prawnej, szczególnie w zakresie związanym z odpowiedzialnością karną za nieuzasadnione wezwanie służb i organów państwowych. W przypadkach, gdy konieczne jest wezwanie służb zewnętrznych, rola człowieka jest nieodzowna.

Czynniki wpływające na czas trwania procedury neutralizacji zagrożenia

W procesie przekazywania i interpretowania strumienia informacji w systemie nadzorującym najistotniejszym parametrem, za pomocą którego można dokonać oceny skuteczności działania takiego procesu, jest czas, jaki upłynie od momentu zaistnienia zagrożenia do momentu jego zneutralizowania. Jest to czas związany z realizacją trzech następujących procesów (rys. 4):

– procesu wykrycia zagrożenia przez system nadzorujący,
– procesu przekazywania informacji użytkownikowi systemu o wykryciu zagrożenia,
– procesu działania odpowiednich komórek odpowiedzialnych za neutralizację zagrożenia.

Proces wykrycia zagrożenia ma związek z możliwościami zastosowanych w systemie nadzorującym elementów detekcyjnych. Podczas projektowania systemu dąży się do realizacji następujących zasadniczych celów:

– wykrywania jak największej liczby zagrożeń,
– minimalizowania czasu reakcji systemu na wystąpienie zagrożenia.

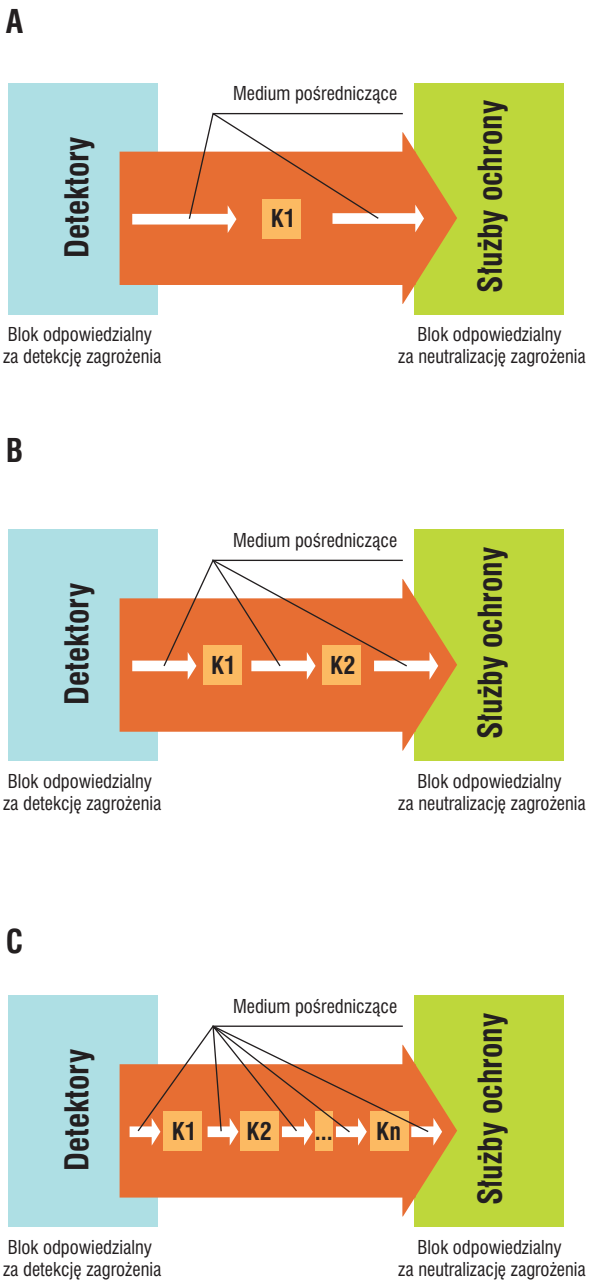
Ze względu na założony arbitralnie przez projektanta poziom prawdopodobieństwa wystąpienia w chronionym obiekcie danego typu zdarzeń proces wykrywania zagrożenia jest charakteryzowany przez skończoną liczbę zagrożeń, na które system reaguje. Liczba wykrywanych zdarzeń jest zatem ściśle związana z liczbą elementów detekcyjnych w systemie, która z kolei ma związek z kosztem instalacji systemu. Na realizację drugiego celu, polegającego na zminimalizowaniu czasu reakcji systemu na wystąpienie zagrożenia, mają wpływ zarówno parametry techniczne elementu detekcyjnego, jak i miejsce, w którym dany element został zamontowany.

Przedział czasowy, który określa prawidłowo przebiegający proces wykrywania zagrożenia, może zatem zostać opisany zależnościami:

$$t_r \in (t_1, t_2) \,, (1)$$

$$t_r \geq t_0 = 0 \,, (2)$$

$$t_1 \rightarrow 0 \,, (3)$$



Rys. 3. Warianty systemów nadzoru ze względu na liczbę ogniw pośredniczących w przekazywaniu informacji o wystąpieniu zagrożenia: a) system jednoetapowy, b) system dwuetapowy, c) system n-etapowy

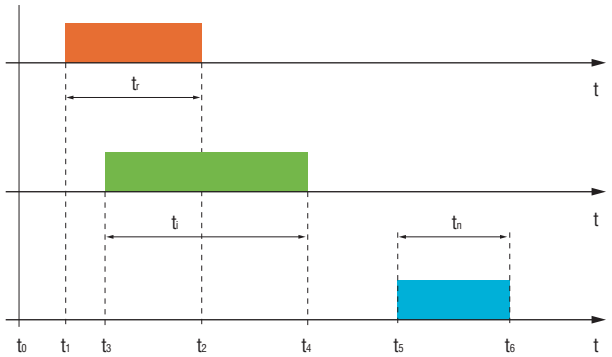
gdzie:

t_0 – moment wystąpienia zagrożenia w chronionym obiekcie,

t_1 – minimalny czas reakcji systemu związany z najmniej czasochłonną procedurą identyfikacji przewidzianego zagrożenia,

t_2 – maksymalny czas reakcji systemu związany z najbardziej czasochłonną procedurą identyfikacji przewidzianego zagrożenia.

W procesie identyfikacji występujących w obiekcie zaburzeń (rozumianych jako stany nieprawidłowe lub nadzwyczajne) mogą zaistnieć trzy sytuacje związane z nieprawidłowym przebiegiem procesu wykrywania zagrożenia. Pierwsza taka sytuacja



Rys. 4. Proces procedury neutralizacji zagrożenia:
t_r – czas związany z wykryciem zagrożenia,
t_i – czas związany z przekazywaniem informacji o zagrożeniu, t_n – czas związany z fizyczną neutralizacją zagrożenia przez odpowiednie komórki systemu

występuje w przypadku urzeczywistnienia się zagrożenia, na którego identyfikację system nie został przygotowany. Wtedy:

$$t_r \to +\infty \,. \quad (4)$$

Druga jest związana z pierwszą i ma miejsce w przypadku, gdy wystąpiło zagrożenie, na które system jest niewrażliwy, ale przez eskalację tego zagrożenia w obiekcie wystąpi zagrożenie, które jest już rejestrowane. Taka sytuacja może mieć miejsce wtedy, gdy w obiekcie wystąpi pożar, a z powodu braku systemu sygnalizacji pożarowej informacja o wszczęciu alarmu może być podjęta przez czujkę służącą do regulacji temperatury w pomieszczeniu po znacznym przekroczeniu jej górnej wartości progowej. Wtedy:

$$t_r \in (t_2, +\infty) \,. \quad (5)$$

Trzecia sytuacja nieprawidłowego przebiegu procesu wykrywania zagrożenia ma miejsce w przypadku wykrycia przez system zagrożenia, które nie nastąpiło. Wtedy:

$$t_r \le 0 \,. \quad (6)$$

Najistotniejszy z punktu widzenia sprawności przebiegu procesu neutralizacji zidentyfikowanego zagrożenia jest proces polegający na jak najszybszym przekazywaniu informacji o wystąpieniu zagrożenia do odpowiednich służb odpowiedzialnych za likwidację konkretnego rodzaju zagrożenia. Na czas trwania tego procesu ma wpływ wiele czynników. Najważniejsze z nich to:

a) związane z zastosowanym algorytmem powiadamiania:
- skomplikowanie algorytmu powiadamiania,
- stopień zindywidualizowania procedur dla poszczególnych zagrożeń,
- wykorzystanie wielowątkowych i alternatywnych dróg przesyłu informacji,
- wykorzystanie scentralizowanego lub rozproszonego systemu podejmowania decyzji,
- liczba kroków (etapów) związanych z realizacją procesu przekazywania informacji,

– dostosowanie algorytmu działania do występującej w otoczeniu obiektu sytuacji,
– konieczność autoryzacji i wzajemnego uwierzytelniania podjętych działań;

b) związane ze sposobem przekazywania informacji:
– rodzaj medium przesyłu informacji,
– zakres przekazywania informacji,
– przepustowość kanału przesyłu informacji;

c) związane z wpływem czynnika ludzkiego:
– doświadczenie użytkowników systemu,
– aktualny stan psychofizyczny osoby związanej z procesem przekazywania informacji,
– poziom zaangażowania i chęci do współpracy ludzi uczestniczących w procesie przekazywania informacji,
– poziom wzajemnego zaufania osób biorących udział w procesie przekazywania i uwierzytelniania informacji.

Przedział czasowy określający prawidłowo przebiegający proces przekazywania informacji o wykryciu zagrożenia przez system detekcyjny do momentu powiadomienia odpowiedniej komórki odpowiedzialnej za neutralizację konkretnego typu zagrożenia opisuje zależność:

$$t_i \in (t_3, t_4) , (7)$$

$$t_i \geq 0 , (8)$$

gdzie:

t_3 – czas rozpoczęcia procedury powiadamiania odpowiednich służb,

t_4 – maksymalny czas powiadamiania odpowiednich służb o wykrytym przez system detekcyjny zagrożeniu. Można przyjąć, że:

$$t_1 \leq t_3 \leq t_2 , (9)$$

ponieważ procedura wysyłania informacji przez część detekcyjną systemu powinna rozpocząć się bezzwłoczne po wykryciu zagrożenia, nie szybciej niż wynosi minimalny czas reakcji systemu związany z najmniej czasochłonną procedurą identyfikacji przewidzianego zagrożenia i nie wolniej niż wynosi maksymalny czas reakcji systemu związany z najbardziej czasochłonną procedurą identyfikacji przewidzianego zagrożenia.

Występujące w procesie przekazywania informacji anomalie to przypadki związane z nieprawidłowym działaniem elementów odpowiedzialnych za przekazywanie informacji. W odróżnieniu od pozostałych procedur (związanych z procesem detekcji zagrożenia i procesem działania odpowiednich służb) tych anomalii może być dużo i są związane w zasadzie z każdym z wymienionych czynników wpływających na przebieg procesu przekazywania informacji. Najistotniejsze przypadki to:
– brak lub zanik medium odpowiedzialnego za przekazywanie informacji,
– nieprawidłowa interpretacja stanu normalnego,
– brak reakcji na dochodzące sygnały o zaistniałym zagrożeniu,
– zapętlenie się procedury przekazywania informacji,
– nieprawidłowe przekazywanie informacji między elementami systemu powiadamiania,
– brak uzyskania autoryzacji i uwierzytelnień (ich uzyskanie jest konieczne do podjęcia dalszego działania).

Wiele przypadków nieprawidłowego przebiegu procesu przekazywania informacji odnosi się do sytuacji, w których kluczowe jest zachowanie i postępowanie człowieka. Zachowanie to często bywa irracjonalne, niejednokrotnie wręcz niemożliwe do przewidzenia, a przez to trudne do określenia w ramach sztywnych procedur. Dlatego, o ile jest to możliwe i pozwalają na to środku techniczne i prawne, dąży się do wyeliminowania czynnika ludzkiego z tego procesu.

Czas związany z fizyczną realizacją procesu neutralizacji zagrożenia to czas reakcji odpowiednich komórek organizacyjnych systemu, odpowiedzialnych za wykonanie powierzonego zadania (służb ochrony, policji, straży pożarnej, sąsiadów) od momentu otrzymania informacji o zagrożeniu do momentu jego neutralizacji. Czas procesu neutralizacji zagrożenia można określić przedziałem czasowym:

$$t_n \in (t_5, t_6) , (10)$$

$$t_n \geq 0 , (11)$$

gdzie:

t_5 – minimalny czas potrzebny do rozpoczęcia fizycznej neutralizacji zagrożenia,

t_6 – maksymalny czas potrzebny do zakończenia fizycznej neutralizacji zagrożenia.

Również w przypadku określania czasu związanego z procesem neutralizacji możemy wyróżnić trzy anomalie. Jednak w odróżnieniu od sytuacji występującej w procesie wykrywania zagrożenia przez system, w której wszystkie anomalie są niekorzystne dla użytkownika, w tym przypadku jedna sytuacja jest korzystna. Występuje ona w przypadku opisanym następującym warunkiem:

$$0 \leq t_n \leq t_5 . (12)$$

Taka sytuacja może wystąpić, gdy służby mające zneutralizować dane zagrożenie podejmą akcję przed upływem przewidzianego minimalnego czasu potrzebnego do rozpoczęcia fizycznej neutralizacji zagrożenia (np. patrol policji był świadkiem wtargnięcia intruza do chronionego obiektu i zareagował, zanim otrzymał formalne zgłoszenie wynikające z procedury działania systemu). Może zaistnieć również sytuacja, w której służby podejmą próbę neutralizacji zagrożenia pomimo tego, że faktycznie zagrożenia nie było. Wtedy:

$$t_n \leq t_0 = 0 . (13)$$

Trzecia sytuacja nieprawidłowego przebiegu procesu fizycznej neutralizacji zagrożenia występuje w przypadku braku reakcji odpowiednich służb na zgłoszenie o wystąpieniu zagrożenia. Wtedy:

$$t_n \to +\infty . (14)$$

Podsumowanie

Głównym zadaniem systemu nadzoru nad stanem chronionego obiektu jest skuteczne przeprowadzenie procesu neutralizacji zagrożenia. W tym celu dąży się do ograniczenia do minimum czasu, jaki upłynie od momentu wykrycia zagrożenia do momentu jego opanowania lub zlikwidowania. To czas reakcji systemu nadzorującego na zaistniałe zagrożenie ma największy wpływ na rozmiar szkód powstałych w obiekcie.

Przeprowadzenie szybkiego procesu neutralizacji zagrożenia oparte jest na zoptymalizowaniu trzech procesów – procesu detekcji zagrożenia, procesu fizycznej neutralizacji zagrożenia przez odpowiednie komórki systemu oraz łączącego te dwa etapy procesu przekazywania informacji między komórkami systemu. W procesie detekcji zagrożenia dąży się do wyposażenia systemu w czujniki umożliwiające wykrycie różnych możliwych zdarzeń. Proces przekazywania informacji powinien charakteryzować się czytelnym algorytmem powiadamiania – takim, w którym informacja o danym zagrożeniu przekazywana jest w sposób prawidłowy i niezawodny do odpowiednich komórek systemu. Na skuteczność procesu fizycznej neutralizacji zagrożenia ma wpływ dobór odpowiednich środków (ilościowych i jakościowych), jakie są przewidziane do likwidacji zagrożenia.

Ograniczenie ogniw pośredniczących w procesie przekazywania informacji nie tylko ma wpływ na przejrzystość algorytmu powiadamiania, ale także skraca czas niezbędny do powiadomienia odpowiednich komórek systemu. Od systemów komunikacyjnych wymaga się szybkiego i jak najpełniejszego przekazu informacyjnego, który dociera do użytkownika. Dzięki temu użytkownik wie, co dzieje się w chronionym obiekcie. Ponadto ważne jest, aby proces ten był niezależny od czynników zewnętrznych, a czas powiadamiania był powtarzalny. Dąży się do wykorzystania takich nośników informacji, które eliminują ogniwa uzależnione od czynnika ludzkiego, ponieważ zachowanie czynnika ludzkiego w systemie nadzoru jest najbardziej nieprzewidywalne.

dr inż. Marcin Buczaj
Politechnika Lubelska
Katedra Inżynierii Komputerowej i Elektrycznej

Bibliografia

1. Nawrocki W., *Komputerowe systemy pomiarowe*, WKiŁ, Warszawa 2006.
2. Szulc W., Rosiński A., *Systemy sygnalizacji włamania, część I*, w: Zabezpieczenia nr 2/2009.
3. Kargul D., *Tendencje rozwoju współczesnych technik zabezpieczenia mienia stosowanych w budownictwie*, praca dyplomowa, Politechnika Lubelska, Lublin 2009.
4. Daniluk M., *Tendencje rozwoju nowoczesnych technik zabezpieczenia mienia w motoryzacji*, praca dyplomowa, Politechnika Lubelska, Lublin 2007.
5. Ożga B., *Wykorzystanie systemów GSM i GPS do monitorowania położenia obiektu*, praca dyplomowa, Politechnika Lubelska, Lublin 2007.
6. *www.wikipedia.org*

Nagłaśnianie stref

na przykładzie głośników pożarowych serii UNISPEAKER

Projektując Dźwiękowy System Ostrzegawczy (DSO) dla obiektu coraz trudniej jest sprostać rosnącym wymaganiom stawianym przez inwestorów. Poza oczywistym aspektem wymagań technicznych oraz dotyczących estetyki głośników, coraz częściej bierze się pod uwagę także racjonalizację kosztów. Wydaje się, że rozwiązaniem odpowiadającym wszystkim tym wymaganiom, przy zachowaniu zdolności przekazywania komunikatów o wysokiej jakości akustycznej, jest zastosowanie głośników UNISPEAKER

Wiele obiektów, na które nałożony został obowiązek instalacji DSO, wynikający z rozporządzenia MSWiA w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów z dnia 21 kwietnia 2006 r., nie było projektowanych pod kątem tego typu systemów. Dotyczy to oczywiście głównie obiektów powstałych w latach wcześniejszych. Niektóre z nich były wyposażane w systemy rozgłoszeniowe (tzw. *Public Address* – PA), które miały służyć do przekazywania informacji muzyczno-reklamowych bądź krótkich komunikatów informacyjnych, ale technologicznie nie nadają się do zastosowań związanych z ewakuacją przy zapewnieniu niezawodnego działania w warunkach pożaru.

Obecnie przystępując do budowy każdego budynku, w którym obowiązkowo należy zainstalować DSO, już na etapie projektu architektonicznego powinno się uwzględnić rodzaj i jakość materiałów wykończeniowych, które mają kolosalny wpływ na jakość warunków akustycznych panujących w pomieszczeniach. Ma to z kolei wpływ na dobór odpowiednich typów i mocy głośników, co w efekcie przekłada się na wartość wskaźnika zrozumiałości mowy.

Jak wiadomo, podczas procedury odbioru technicznego budynku jednym z elementów jest weryfikacja protokołu z pomiarów zrozumiałości mowy w obiekcie (czasami pomiary przeprowadzane są w trakcie procesu odbioru) i to od wyników tych pomiarów zależy, czy system będzie uznany jako działający prawidłowo (zgodnie z PN-EN 60849:2001), czy nie. Efektem takiej weryfikacji może być np. konieczność dokonania modyfikacji systemu w zakresie doboru rodzaju, mocy i rozmieszczenia głośników pożarowych.

Należy pamiętać, że na jakość komunikatu głosowego emitowanego do danej strefy nagłośnieniowej ma wpływ nie tylko akustyka wnętrza, ale także cały proces na drodze „nadawca – odbiorca". Jej początek ma miejsce w studiu nagrań, gdzie komunikat zostaje nagrany (zgodnie z wytycznymi projektu nagłośnienia obiektu), a koniec w nagłaśnianym pomieszczeniu, w którym dociera do odbiorcy.

Nazwa pomieszczenia	Czas min. [s]	Czas maks. [s]
Studio telewizyjne	0,3	0,7
Studio nagraniowe	0,3	1,0
Sala audytoryjna	0,7	0,9
Kino	0,6	1,3
Hala sportowa	1,0	1,5
Sklep	1,0	1,6
Opera	1,0	2,0
Teatr	1,0	2,0
Sala koncertowa	1,4	2,8
Kościół	2,0	4,5

Tab. 1. Przykładowe czasy pogłosu dla danych typów pomieszczeń

Dobierając głośniki, należy wziąć pod uwagę parę ważnych zagadnień z zakresu akustyki, które powinny być uwzględniane we wstępnej fazie projektu nagłośnienia.

Już na etapie projektu architektonicznego projektant powinien wiedzieć, jakie przeznaczenie będzie miał budynek, i na tej podstawie kształtować przestrzeń w pomieszczeniach oraz dobierać materiały wykończeniowe, od których zależy, jakie warunki akustyczne będą w nich panować.

Podstawowymi parametrami decydującymi o jakości odbieranych później komunikatów głosowych, np. ostrzegawczych, alarmowych i ewakuacyjnych, są: pogłos, poziom szumu tła akustycznego i zniekształcenia.

Pogłos jest to zjawisko fizyczne wynikające z wielokrotnego odbicia się fal dźwiękowych, uprzednio wygenerowanych przez źródło dźwięku, od powierzchni ograniczających (ścian, sufitów, podłóg oraz elementów wyposażenia danego pomieszczenia). Po wyłączeniu źródła dźwięku nie następuje od razu całkowity zanik sygnału (cisza), moment ten zależy od liczby odbić i czasu, po jakim zaniknie wygenerowana energia fali dźwiękowej. Liczba odbić i czas ich zanikania ściśle zależy od rodzaju zastosowanych materiałów wykończeniowych (wełna, cegła, glazura, szkło itp.) oraz kubatury pomieszczenia. Czas pogłosu jest tym dłuższy, im większa jest kubatura pomieszczenia oraz im twardsze i gładsze materiały wykończeniowe zostały w nim zastosowane.

Czas pogłosu jest to czas, po którym natężenie dźwięku w pomieszczeniu zamkniętym zmaleje po wyłączeniu źródła dźwięku o 60 dB.

Do obliczenia czasu pogłosu RT_{60} możemy posłużyć się następującymi wzorami: **Sabine'a** – w przypadku dużych pomieszczeń o w miarę równomiernej chłonności akustycznej ($\alpha_{śr} < 0{,}2$):

$$RT_{60} = \frac{0{,}161 \cdot V}{A} \quad [s]$$

gdzie:
V– objętość pomieszczenia
A – chłonność akustyczna, wyznaczana wzorem:

$$A = \sum_i S_i \cdot \alpha_i$$

gdzie:
S_i – powierzchnia i-tej płaszczyzny ograniczającej wnętrze
α_i – współczynnik pochłaniania i-tej płaszczyzny

W przypadku pomieszczeń o większej chłonności akustycznej ($\alpha_{śr} > 0{,}2$) powinniśmy posługiwać się wzorem **Eyring'a**:

$$RT_{60} = \frac{0{,}161 \cdot V}{-S \cdot \ln(1 - \overline{\alpha})} \quad [s]$$

gdzie:
V – objętość pomieszczenia
S – powierzchnia płaszczyzny ograniczającej wnętrze
$\overline{\alpha}$ – średni współczynnik pochłaniania obliczany według wzoru:

$$\overline{\alpha} = \frac{\alpha_1 S_1 + \alpha_2 S_2 + \ldots + \alpha_n S_n}{S_1 + S_2 + \ldots + S_n}$$

gdzie:
S – powierzchnia płaszczyzny ograniczającej wnętrze
α – współczynnik pochłaniania dla danej powierzchni

Ciśnienie akustyczne [Pa]	Poziom ciśnienia akustycznego SPL [dB_{SPL}]	Miejsce odniesienia
$2x10^{-5}$	0	Próg słyszenia
$1,1x10^{-4}$	15	Poziom tła w studiu nagrań
$6,3x10^{-3}$	50	Rozmowa
$6,3x10^{-2}$	70	Odkurzacz
$6,3x10^{-1}$	90	Ciężki transport
2	100	Młot pneumatyczny, dyskoteka
6,3	110	Koncert zespołu rockowego
20	120	Próg bólu
200	140	Start odrzutowca (Jumbo Jet w odległości ok. 50 m)

Tab. 2. Przykładowe wartości ciśnienia akustycznego SPL dla danych typów pomieszczeń

Wraz z rozwojem nauki powstało jeszcze kilka modyfikacji wzoru Sabine'a, uwzględniających dodatkowo np. warunki atmosferyczne panujące w pomieszczeniu.

Poziom szumu tła akustycznego jest odstępem sygnału od szumu S/N – to nic innego, jak szum generowany przez otoczenie o pewnym poziomie ciśnienia akustycznego, który w przypadku dużych wartości SPL może spowodować zamaskowanie sygnału/komunikatu głosowego dystrybuowanego przez zainstalowany w pomieszczeniu głośnik. Dlatego też wymagania normy PN-EN 60849:2001 mówią o minimalnym odstępie sygnału od szumu, który musi wynosić 6dBA, gdzie A odpowiada krzywej ważonej, skorygowanej do charakterystyki ucha ludzkiego.

W tab. 2 przedstawiono przykładowe wartości poziomu tła akustycznego w zależności od typów obiektów.

Zniekształcenia są spowodowane przez różnego typu czynniki (przesterowany sygnał, uszkodzony głośnik, uszkodzony wzmacniacz, źle zmontowane połączenie, źle nagrany komunikat itp.), które powodują, że emitowany sygnał jest zniekształcony, mało klarowny, co w efekcie pogarsza wskaźnik zrozumiałości mowy.

Kolejnymi czynnikami wpływającymi na zrozumiałość mowy są parametry akustyczne pomieszczenia wynikające z zastosowanych materiałów wykończeniowych.

Wartości współczynników pochłaniania są ściśle zależne od gęstości, a także porowatości materiału. Im twardsze są materiały (beton, stal), tym mniejszy jest współczynnik pochłaniania energii akustycznej. Z kolei im bardziej miękki jest materiał (wełna, gąbka), tym większy jest współczynnik pochłaniania.

Biorąc to wszystko pod uwagę, można przystąpić do doboru głośników. Warto jednak wspomnieć jeszcze o kilku zasadach obowiązujących w akustyce.

Szczególnie przy doborze głośnika musimy mieć podstawowe informacje dotyczące:

– poziomu tła akustycznego panującego lub przewidywanego w danym pomieszczeniu,
– wartości poziomu SPL (1W / 1m) dla danego głośnika,
– kąta rozproszenia/zasięgu głośnika dla poszczególnych częstotliwości oktawowych,
– odległości płaszczyzny odsłuchu od źródła dźwięku,
– wielkości powierzchni nagłaśnianego pomieszczenia.

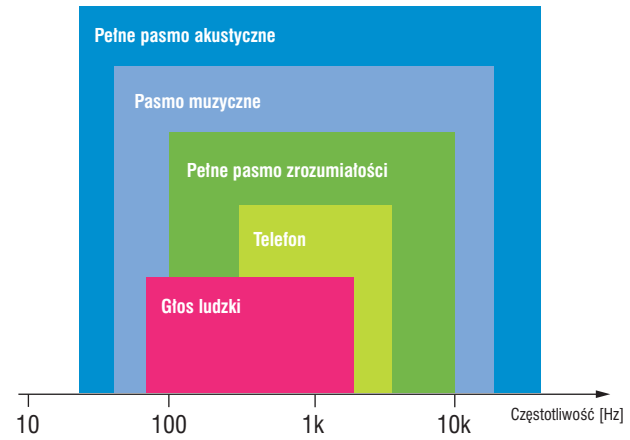
Mając te dane, należy pamiętać, że:

1) Z każdym podwojeniem odległości odbiorcy od źródła dźwięku (głośnika) poziom SPL spada o 6 dB, co przedstawia rys.1.
2) Z każdym podwojeniem mocy (np. na odczepie transformatora) wartość SPL wzrasta już tylko o 3 dB, co powoduje, że w przypadku konieczności zapewnienia poziomu dźwięku rzędu np. 88 dB w odległości od tego źródła np. 4 m, znając wartość SPL głośnika (1 W / 1 m), np. 94 dB, to wartość SPL w określonej odległości (4 m) będzie wynosiła 82 dB. Aby zapewnić żądany poziom należy więc zwiększyć moc czterokrotnie (4 W zamiast 1 W).

Rys. 1. Spadek poziomu SPL w funkcji odległości słuchacza od źródła

Materiał	Wartości pogłosowego współczynnika pochłaniania w danym paśmie					
	125 Hz	250 Hz	500 Hz	1 kHz	2 kHz	4 kHz
Beton	0,01	0,012	0,016	0,019	0,023	0,035
Ściana ceglana	0,03	0,03	0,03	0,04	0,05	0,07
Dywan o grubości 5 mm	0,02	0,03	0,05	0,10	0,30	0,50
Wełna mineralna o grubości 25 mm	0,18	0,24	0,68	0,85	0,99	0,99

Tab. 3. Przykładowe wartości współczynników pochłaniania dla wybranych materiałów



Rys. 2. Zakresy częstotliwości w paśmie akustycznym

3) Wraz ze wzrostem częstotliwości kąt rozpraszania głośnika zmniejsza się, choć nie jest to regułą, czego dobrym przykładem są głośniki UNISPEAKER.

Zaleca się dobieranie i rozmieszczanie głośników z uwzględnieniem kąta zasięgu 2–4 kHz, co znacznie zwiększy prawdopodobieństwo, że odległości między głośnikami nie będą zbyt duże i nie spowodują zbyt dużych spadków poziomu SPL w przestrzeni pomiędzy tymi głośnikami. Wynika to też z pasma mowy (ok. 100 Hz–3,5 kHz), które dla celów ewakuacji ma największe znaczenie (inaczej niż w przypadku systemów PA, w których, ze względu na emitowanie muzyki, ważny jest przede wszystkim sygnał w szerokim paśmie akustycznym, w systemach DSO jest to tylko drugorzędna funkcja).

W przypadku pomieszczeń, w których znajduje się sufit podwieszany, można zastosować głośniki sufitowe serii **USP-540** lub **USP 640** (głośniki do zastosowań wewnątrz budynków, rodzaj środowiska pracy A).

Głośniki sufitowe serii USP-540 oraz USP-640 są urządzeniami wysokiej jakości. Potwierdzają to certyfikat zgodności CNBOP nr 2690/2009 i świadectwo dopuszczenia CNBOP nr 0556/2009. Cechą szczególną tych głośników są bardzo dobre parametry akustyczne, dzięki czemu można stosować je wszędzie tam, gdzie mamy do czynienia z sufitem podwieszanym. Warto również zwrócić uwagę na rozwiązania konstrukcyjne, które stwarzają poczucie bezpieczeństwa dzięki pewnemu przytwierdzeniu obudowy głośnika do sufitu podwieszanego, a także eliminują powstawanie różnego typu przydźwięków powstałych w wyniku drgań oraz zbyt słabego przymocowania głośnika do tej obudowy, co w efekcie może mieć wpływ na obniżenie zrozumiałości mowy.

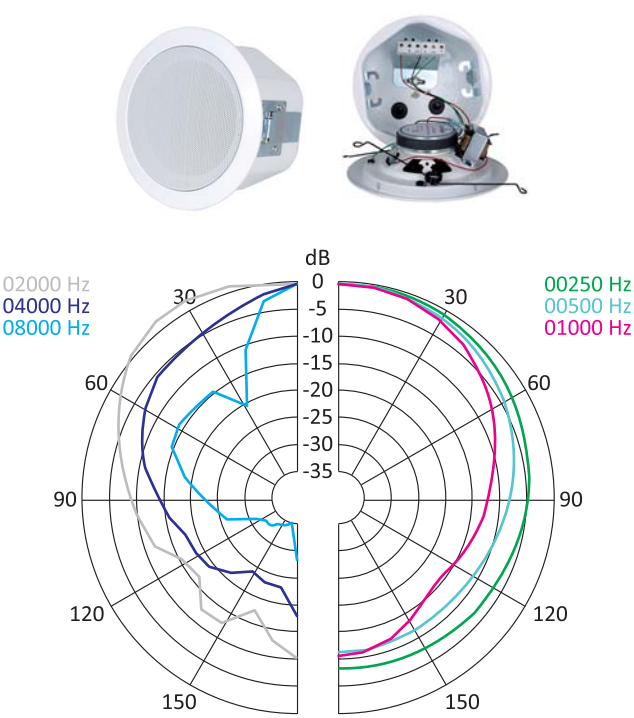
Głośnik USP-640 jest przeznaczony do zastosowania w miejscach, w których sufit podwieszany jest zlokalizowany wysoko, co często wymusza zastosowanie głośnika o większej mocy akustycznej.

Mając powyższe informacje i znając wszystkie wytyczne, można obliczyć, jaka liczba głośników będzie potrzebna do nagłośnienia danej powierzchni/pomieszczenia, korzystając ze wzoru:

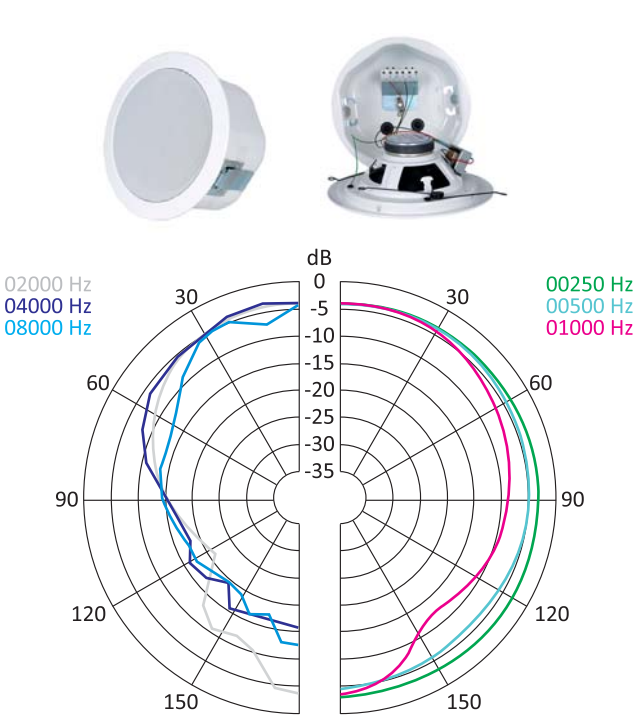
$$O = 2 \cdot H \cdot \tan(\alpha / 2)$$

$$LG = \frac{P}{O} \cdot 2$$

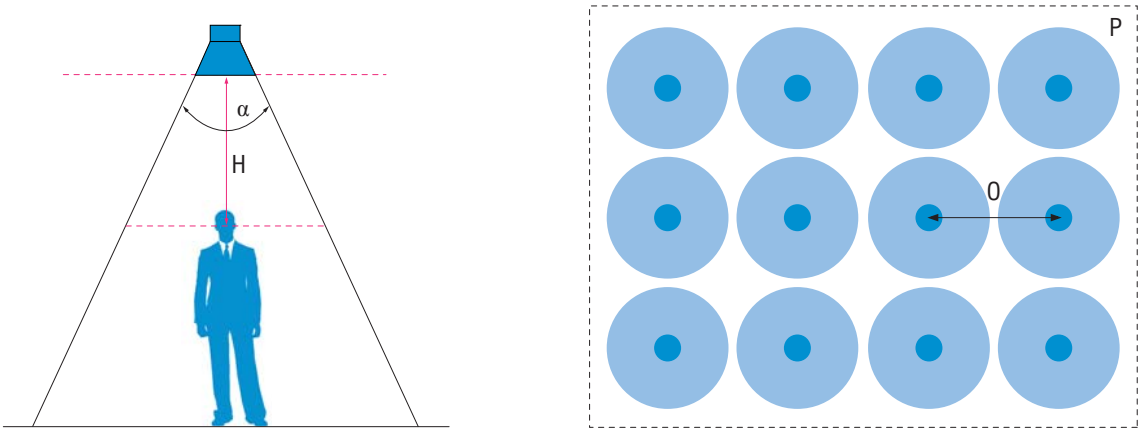
gdzie:
O – odległość między głośnikami
H – odległość płaszczyzny odsłuchu od czoła głośnika
α – kąt rozpraszania dla danej częstotliwości oktawowej
LG – liczba głośników
P – nagłaśniana powierzchnia



Rys. 3. Charakterystyki kierunkowe (kąty rozpraszania) dla głośnika USP-540



Rys. 4. Charakterystyki kierunkowe (kąty rozpraszania) dla głośnika USP-640



Rys. 5. Przykład doboru liczby głośników sufitowych do nagłaśnianej powierzchni

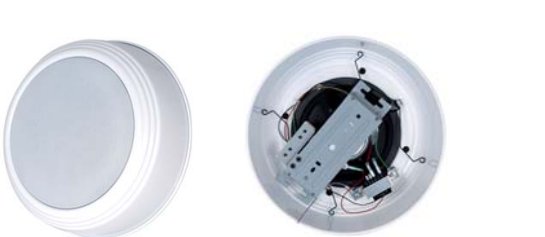
Kolejnymi głośnikami z rodziny UNISPEAKER są głośniki ścienno-sufitowe typu **USP-601**, które ze względu na swoje walory techniczne mogą być stosowane wszędzie tam, gdzie wymagana jest odporność na zwiększoną wilgotność otoczenia. Głośniki USP-601 mogą pracować w dwóch środowiskach klimatycznych, A i C, co pozwala na szerszy zakres zastosowań. Zastosowane rozwiązanie konstrukcyjne umożliwia zainstalowanie tych głośników zarówno na ścianie, jak i bezpośrednio na stropie właściwym, co potwierdzają certyfikat zgodności CNBOP nr 2691/2009 i świadectwo dopuszczenia CNBOP nr 0557/2009.

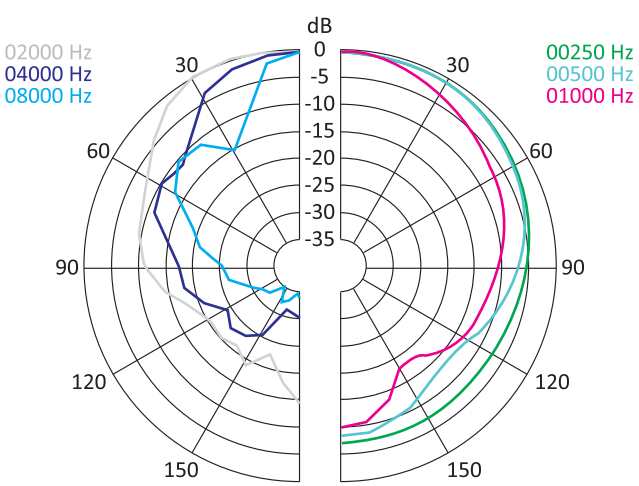
Ostatnimi z prezentowanych głośników serii UNISPEAKER są **stalowe** projektory dźwięku **USP-53**. Ich podstawową zaletą i zarazem cechą szczególną, na którą warto zwrócić uwagę, jest materiał obudowy – stal, która zdecydowanie podwyższa ich odporność na działanie czynników zewnętrznych, np. na wysoką temperaturę, uderzenia. Drugą cechą wyróżniającą projektory USP-53 jest możliwość instalacji głośnika na zewnątrz budynku (rodzaj środowiska pracy **B**), która została potwierdzona certyfikatem zgodności CNBOP nr 2689/2009 oraz świadectwem dopuszczenia CNBOP nr 0555/2009.

Konstrukcja głośników USP-53 umożliwiająca montaż zarówno na ścianie, jak i bezpośrednio na stropie ułatwia zainstalowanie ich np. na parkingach (zarówno zamkniętych, jak i otwartych), w salach gimnastycznych itd.

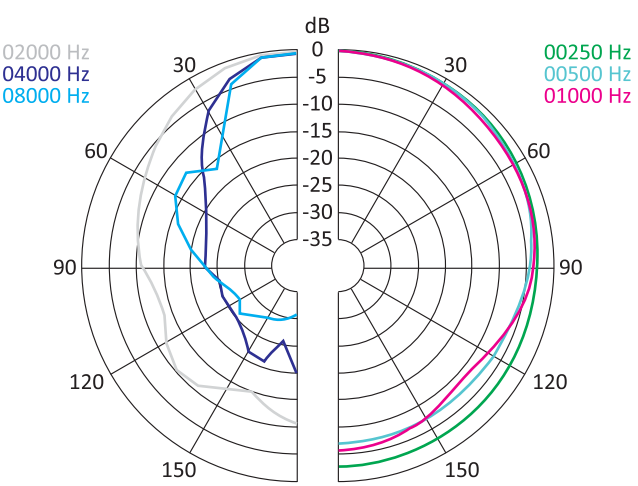
Mając niezbędną wiedzę o projektowaniu systemów DSO i doborze głośników, a także certyfikowane głośniki UNISPEAKER, można śmiało stawiać czoła wymaganiom stawianym przez inwestorów. Dodatkową korzyścią, wynikającą z ceny tych urządzeń, będzie (szczególnie w przypadku dużych obiektów) znaczne obniżenie kosztów inwestycji.

Rafał Kowal
AAT Holding





Rys. 6. Charakterystyki kierunkowe (kąty rozpraszania) dla głośnika USP-601



Rys. 7. Charakterystyki kierunkowe (kąty rozpraszania) dla głośnika USP-53

Nowa jakość dźwięku!

UNISPEAKER

Podstawowym zadaniem Dźwiękowych Systemów Ostrzegawczych (DSO) jest rozgłaszanie komunikatów głosowych w sytuacji zagrożenia, gdy szybkie i czytelne przekazanie informacji (np. o ewakuacji) staje się jednym z kluczowych elementów. Głośniki UNIspeaker, zapewniając najwyższą jakość rozgłaszanego dźwięku, stanowią niezawodny element każdego systemu DSO. Charakteryzują się estetycznym wyglądem, bardzo dobrymi parametrami technicznymi i wysoką jakością wykonania. Ich dodatkowym atutem jest konkurencyjna cena.

Głośniki UNIspeaker posiadają odpowiednie Certyfikaty i Świadectwa Dopuszczenia CNBOP.

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

Elektroniczny system sygnalizacji pożarowej

dla wagonów pasażerskich, autobusów szynowych i autobusów miejskich

Elektroniczne systemy sygnalizacji pożarowej dla wagonów pasażerskich oraz autobusów szynowych zostały opisane w *Zabezpieczeniach* w numerach 6(40)/2004 (część 1) oraz 1(41)/2005 (część 2). Przedstawiona koncepcja dotyczyła elektronicznego systemu sygnalizacji pożarowej (SSP) dla wagonów pasażerskich. Podstawowa propozycja powstała w wyniku analizy zagrożeń, jakie istnieją zarówno na trasie jazdy pociągu, jak i w wagonowniach. Autorzy przedstawili ogólną konfigurację Automatycznego Urządzenia Sygnalizacji Pożarowej (AUSP), aby dokonać wyboru SSP do zastosowania w wagonach kolejowych. Przedstawiona została propozycja algorytmu pracy centrali SSP i koncepcja SSP w składzie pociągu. Podano ogólne założenia techniczne dotyczące SSP dla wagonów lub ich składów z uwzględnieniem wymagań i zaleceń specjalnych przepisów i norm. W latach 2008/2009 powstał realny projekt elektronicznego systemu sygnalizacji pożarowej. Po otrzymaniu pozytywnych wyników pomiarowych, wynikających z badań pełnych, w maju 2009 r. rozpoczęto produkcję urządzeń pod nazwą CSP1. Niezmiernie istotnymi danymi są również informacje dotyczące założeń szczegółowych przy projektowaniu systemu sygnalizacji pożarowej dla potrzeb transportowych. Zostały one precyzyjnie opisane w *Zabezpieczeniach*. Istotne założenia podano w kolejnym rozdziale niniejszego artykułu

Założenia szczegółowe

Istotne założenia, niezbędne do zaprojektowania SSP dla składów wagonowych, autobusów szynowych oraz autobusów miejskich:

– założenia dotyczące specyfikacji sprzętowej,
– założenia dotyczące detektorów (właściwy dobór czujek),
– założenia dotyczące central i modułów do SSP (terminal typu CSP1T oraz koncentrator czujek typu CSP1C),
– założenia dotyczące instalacji elektrycznej SSP (przebudowana instalacja wagonowa, instalacja w autobusie szynowym i w autobusach miejskich),
– założenia dotyczące sposobu adresowania w systemie SSP (informacje z czujek przekazywane do koncentratora i dalej – do terminala CSP1T),
– założenia dotyczące automatycznego systemu gaszącego (przekazywanie informacji o zagrożeniu),
– założenia dotyczące monitorowania (terminal CSP1T).

Założenia dotyczące specyfikacji sprzętowej dla SSP typu CSP1

Ze względu na rozmiary specyfikacji sprzętowej zostaną przytoczone tylko te parametry, w których wprowadzono pewne uzupełnienia. Sprzęt wykrywający zagrożenie pożarowe (czujki) powinien spełniać szczególne wymagania pod względem odporności mechanicznej i elektrycznej, co wynika ze specyfiki miejsca, w którym ma być zamontowany system.

Podstawowymi zagrożeniami dla systemów sygnalizacji pożaru w środkach transportowych są:

– poziome i pionowe wibracje, które mogą zakłócać pracę systemu, a także powodować szybkie niszczenie się sprzętu,
– zakłócenia elektromagnetyczne (kompatybilność elektromagnetyczna), które mogą wywoływać powstawanie fałszywych alarmów na skutek przepięcia i przebicia (co w przypadku pojazdów transportowych nie powinno nikogo dziwić),
– praca w środowisku o bardzo szerokim przedziale zmian temperatur,
– duża wilgotność (także zmienna), przeciągi,
– fluktuacja napięcia zasilającego (pokładowego) – np. w przypadku wagonów pasażerskich może ono wahać się od 16 V do 33 V przy napięciu znamionowym U_{ZN}=24 V (problem ten jest trochę lepiej przestrzegany w autobusach miejskich),
– wandalizm – jest to szczególnie ważny problem, ponieważ zniszczenie przez wandali pewnego elementu (np. kradzież czujki) może spowodować niewykrycie pożaru we wczesnej fazie, w wyniku czego mogą zginąć ludzie.

Klasyczne systemy sygnalizacji pożarowej są przewidziane do stosowania w budynkach i budowlach. Aby zastosować taki system w wagonowych systemach wykrywania pożaru, należy dostosować go do wymagań stawianych przez kolej oraz władze komunikacji miejskiej.

Do wymogów takich należą między innymi:

– zmiana obudowy czujek w celu łatwiejszego ukrycia ich w strukturze wagonu lub autobusu szynowego i zabezpieczenia ich w ten sposób przed zainteresowaniem się nimi przez osoby niepowołane (rozwiązania przedstawione na rysunkach niniejszego artykułu nie spełniają jeszcze tego warunku),
– montowanie czujek w obudowach i na podstawach absorbujących uderzenia, wstrząsy i wibracje (będące poważnym problemem w ruchomych środkach transportu),
– zastosowanie ekranu w czujkach w celu ochrony przed zakłóceniami elektromagnetycznymi (np. iskrzeniem pochodzącym od trakcji lub przetwornic znajdujących się w wagonie),
– zastosowanie ekranów na wagonowe urządzenia elektryczne w celu wyeliminowania wpływu zakłóceń EM na pracę czujek.

Centrale typu CSP1 i panele sterowania (koncentratory CSP1C) muszą być montowane na elementach absorbujących wstrząsy, a poszczególne moduły należy połączyć ze sobą w sposób trwały, uniemożliwiający przypadkowe rozłączenie (w wagonach montuje się je w specjalnych szafach sterowniczych). Przykład rozwiązania pokazano na rys. 6.

Przeznaczenie centrali sygnalizacji pożarowej typu CSP1

Centrala sygnalizacji pożarowej typu CSP1 jest przeznaczona do sygnalizowania wystąpienia zagrożenia pożarowego w wagonach zespołu trakcyjnego, w wagonach osobowych (szczególnie w wagonach sypialnych z pokładową siecią prądu stałego o napięciu U_{ZN}=24 V), w innych dowolnych pojazdach szynowych oraz w autobusach komunikacji miejskiej.

Opis centrali sygnalizacji pożarowej typu CSP1

Centrala typu CSP1 składa się z dwóch urządzeń: terminala CSP1T i koncentratora czujek CSP1C. Do jednego terminala można podłączyć maksymalnie 16 koncentratorów czujek, do każdego z koncentratorów można podłączyć do sześciu czujek.

W przypadku braku napięcia głównego centrala przełącza się na zasilanie rezerwowe z bezobsługowych akumulatorów ołowiowo-żelowych o pojemności 7 Ah / 12 V. Akumulatory są podłączone do aktywnego terminala CSP1T. Układ jest wyposażony w system buforowego ładowania akumulatorów w czasie pracy.

Terminal generuje informację dźwiękową i optyczną o zadziałaniu czujki, wskazując jej numer na wyświetlaczu ciekłokrystalicznym. Centrala współpracuje z czujkami dymu rozmieszczonymi w wielu punktach pojazdu. Czujki umożliwiają wykrycie dymu pochodzącego ze spalania lub żarzenia się drewna, chemikaliów, tworzyw sztucznych, tkanin itp. w początkowej fazie powstawania pożaru. Ze względu na specyfikę miejsca zainstalowania (narażenia na udary mechaniczne i wibracje, zagrożenie działaniem ludzi) nie stosuje się czujek jonizacyjnych. W zależności od wykonania, do koncentratora CSP1C można przyłączyć czujkę płomienia lub czujkę nadmiarowo-różnicową ciepła. Wyświetlacz LCD i diody LED na panelu czołowym terminala CSP1T informują o pracy centrali i działaniu nadzorowania systemu przeciwpożarowego.

Centrala CSP1 posiada wyjście, z którego sygnał pozwala uruchomić np. rejestrację sygnału z kamery CCTV lub funkcję obserwacji w kamerach obrotowych. Centrala jest przystosowana do pracy w sieci CANOpen.

Przygotowanie SSP do pracy (terminal – koncentrator)

Aby zapewnić poprawną pracę systemu detekcji pożaru, należy ustawić adresy na obrotowym koderze, zarówno na pulpicie terminala centrali, jak i na koncentratorach czujek.

Adresy terminala centrali i koncentratorów są traktowane oddzielnie i mogą się pokrywać – w systemie może istnieć zarówno koncentrator o numerze 7 i terminal o numerze 7, ponieważ są one inaczej rozpoznawane. Wszystkie nieużywane w koncentratorze wejścia czujek („SABOTAŻ”) powinny być zwarte do plusa napięcia ich zasilania, a wejścia („ALARM”) do minusa ich zasilania, by nie powodować niepotrzebnego alarmu.

Obsługa koncentratora typu CSP1C

Koncentrator przedstawiony na rys. 3 nie wymaga żadnych dodatkowych czynności obsługowych.

Informacje dotyczące komunikacji koncentratora z terminalem centrali sygnalizowane są za pośrednictwem diody znajdującej się na obudowie koncentratora. Miganie diody oznacza poprawną pracę procesora.

Stan braku komunikacji z terminalem można odróżnić od stanu normalnej komunikacji w następujący sposób:
– jeśli komunikacja przebiega normalnie, to dioda miga raz na sekundę, świecąc się przez 100 ms,
– jeśli koncentrator nie ma komunikacji z terminalem centrali przez przynajmniej 10 sekund, to dioda zmienia stan w interwale migania wynoszącym jedną sekundę.

Obsługa eksploatacyjna terminala centrali

Na ścianie czołowej terminala centrali (rys. 1 i 2) umieszczono przycisk „ON/OFF”, służący do przełączania urządzenia ze stanu aktywnego w nieaktywny i odwrotnie. Załączenie terminala centrali następuje przez naciśnięcie przycisku „ON/OFF” przez trzy sekundy. Na wyświetlaczu pojawia się napis „CZEKAJ”. Po kilku sekundach napis zmienia się („AKTYWNY”), jednocześnie wyświetlana jest data i godzina, a także zapala się dioda zielona oraz miga żółta, która sygnalizuje komunikację z koncentratorami. Wyłączenie terminala centrali realizuje się przez ponowne naciśnięcie przycisku „ON/OFF” – wyświetla się napis „TAK/NIE” (należy wybrać przyciskami „ ▲▼ ” opcję „TAK” i nacisnąć przycisk „MENU” – na wyświetlaczu pojawi się napis „NIEAKTYWNY”).

Na rys. 1 przedstawiono terminal centrali w wersji kasetowej.

W stanie aktywnym terminal centrali zasila wewnętrzną magistralę transmisyjną i „pyta” koncentratory o stan czujek alarmowych. „Odpytywane” są zawsze wszystkie adresy od 0 do 15. Przysłanie informacji o wystąpieniu stanu sabotażu lub alarmu w którejkolwiek czujce powoduje automatycznie przejście pulpitu w stan alarmowy, który sygnalizowany jest miganiem czerwonej diody „ALARM” lub A oraz 45- sekundowym sygnałem dźwiękowym. Po upływie tego czasu sygnał akustyczny zanika, lecz czerwona dioda miga do momentu skasowania alarmu[1].

Na rys. 2 przedstawiono terminal centrali w tzw. aparatowej wersji.

Komunikat o rodzaju alarmu jest wyświetlany na wyświetlaczu („ALARM”, „SABOTAŻ”, „BŁĄD ADRESU”) w kolejności: adres (numer) koncentratora, numer czujki lub błąd adresu („POL”).

Kasowanie alarmu następuje po naciśnięciu przycisku „MENU”, wybraniu przyciskami „▲▼” opcji „KASOWANIE ALARMU” i naciśnięciu przycisku „MENU”.

System sygnalizuje trzy możliwe rodzaje alarmu:
– alarm pożarowy,
– alarm sabotażowy,
– alarm informujący o braku komunikacji z modułem określonym w konfiguracji jako aktywny.

Na ekranie ciekłokrystalicznego wskaźnika każdej przyczynie alarmu przypisany jest jeden wiersz, pierwszy z oznaczeniem „ALM”, drugi – „SAB”, a trzeci – „POL”. W jednym wierszu wyświetlane są adresy koncentratorów, które zgłosiły problem. Jeśli na przykład koncentrator o adresie 7 zgłosił alarm, to w wierszu ALM na pozycji 7 będzie świecić się cyfra 7. Jeśli zgłosił problem z sabotażem, w wierszu SAB na pozycji 7 zaświeci się cyfra 7. W przypadku sabotażu i alarmu jednocześnie świecą się obie cyfry.

1) Stan nazwany tu „stanem sabotażu” jest w istocie stanem uszkodzenia i w myśl PN-EN-54-1 powinien być sygnalizowany odmiennie niż stan alarmu pożarowego (przyp. red.).

Rys. 1. Terminal centrali pożarowej typu CSP1TK (wersja kasetowa)

Rys. 2. Terminal centrali (wesja aparatowa)

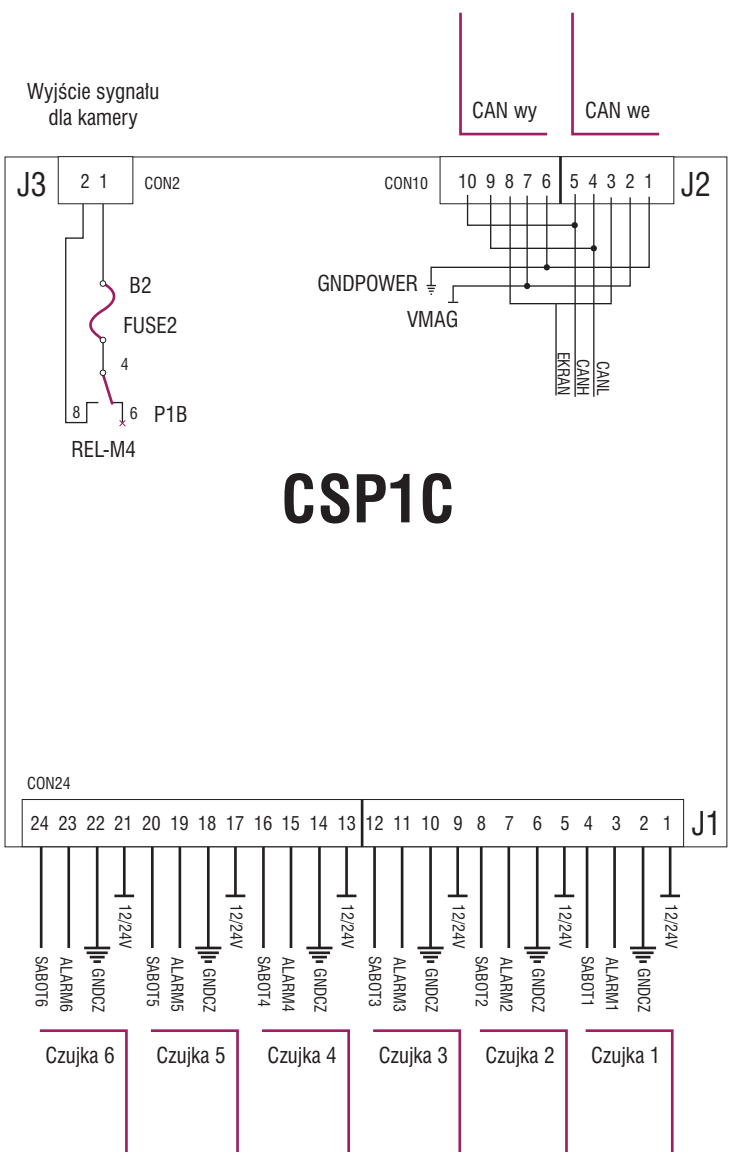
Rys. 3. Koncentrator typu CSP1C, do którego dołączane są czujki dymu lub płomienia

Podczas kasowania następuje chwilowe odłączenie napięcia na magistrali, a następnie sprawdzenie, czy wszystkie moduły przestały odpowiadać na zapytania (potwierdzenie wyłączenia napięcia), i ponowne załączenie napięcia na magistrali.

Jeśli odłączenie napięcia na magistrali nie powiodło się, pulpit zgłosi błąd i przejdzie w tryb alarmowy. W przypadku kasowania alarmu dane o alarmie zostaną zapisane w pamięci EEPROM terminala i będzie można je podglądać, wybierając opcję „PRZEGLĄD ZDARZEŃ”.

Na rys. 3 przedstawiono koncentrator typu CSP1C, do którego dołączane są czujki dymu lub płomienia (często z uwzględnieniem czujnika temperatury).

Rys. 4. Stanowisko do badań SSP: terminal centralki pożarowej typu CSP1TA oraz dwa koncentratory



Rys. 5. Uproszczony układ koncentratora typu CSP1C, do którego można dołączyć sześć czujek ppoż.

Rys. 6. Widok koncentratora typu CSP1C zainstalowanego w wagonie pasażerskim

Rys. 7. Widok terminala centrali (szafa sterownicza wagonu)

Rys. 8. Przykładowa lokalizacja czujki dymu typu OSD23 w przedziale wagonu pasażerskiego (lokalizacja przejściowa)

Niezmiernie ważnym i zarazem trudnym problemem jest dobór właściwych czujek dymu i płomienia. Do badań zastosowano (wstępnie) czujki dymu typu OSD 23. Wybór wynikał z dopuszczenia szerokiego zakresu napięcia zasilającego dla tych czujek. W przypadku braku wagonowego zasilania pokładowego, które wynosi U_{ZAS}= 24 $V^{16V\ do\ 33V}$, badany system przechodzi automatycznie na zasilanie rezerwowe, które wynosi 12 V (akumulator żelowy). Bardzo uproszczony układ takiego mikroprocesorowego koncentratora typu CSP1C przedstawiono na rys. 5. Obwody CAN_{WE} i CAN_{WY} są dołączone do terminala centrali. Jest również wyjście do kamer CCTV. Koncentrator posiada sześć wejść czteroprzewodowych dla dołączenia sześciu czujek dymu lub płomieni. Na rys. 5 przedstawiono tylko jeden koncentrator. Maksymalnie może być ich 16, a więc maksymalna liczba czujek ppoż. może wynieść 96. Taka liczba wystarcza do zapewnienia ochrony ppoż. pełnego składu pociągu.

Na rys. 6 przedstawiono koncentrator typu CSP1C zainstalowany w specjalnej szafie sterowniczej w wagonie pasażerskim (w przedsionku wagonu). Warto również nadmienić, że polski producent wagonów musiał dostosować całą instalację kablową do potrzeb zaprojektowanego i wdrożonego systemu ppoż. Podobnie instalacje musi dostosować również producent autobusów miejskich.

Na rys. 7 przedstawiono fotografię terminala centrali, który również został zlokalizowany w szafie sterowniczej wagonu pasażerskiego nowej generacji(w przedsionku). Nieco inaczej rozwiązuje się problem w wagonach bezprzedziałowych.

Na rys. 8 przedstawiono przykład lokalizacji czujki ppoż. zamontowanej w suficie przedziału wagonu pasażerskiego. Jest to lokalizacja przejściowa, podobnie jak typ czujki (OSD23).

Zakończenie i wnioski

Pierwsze uzgodnienia dotyczące budowy centrali przeciwpożarowej (wówczas o nazwie CPP) pochodzą z marca 2004 r. Powstały w Zakładzie Pojazdów Szynowych CNTK (Centrum Naukowo-Techniczne Kolejnictwa). Jak już wspomniano, autorzy sygnalizowali już ten problem w Zabezpieczeniach w 2004 i 2005 r. Były to pierwsze w Polsce próby podjęcia trudnego wyzwania zaprojektowania i budowy systemu ppoż. dla potrzeb transportu szynowego. Bardzo trudne warunki eksploatacyjne systemu wykorzystywanego w transporcie szynowym wymagały dużej wiedzy normatywnej. Należało spełnić wszystkie wymagania dotyczące wyposażeń elektronicznych stosowanych w taborze, badań środowiskowych, wytrzymałości mechanicznej, kompatybilności elektromagnetycznej (w tym: UIC-564-2, UIC-642-2, UIC-849). Ponadto należało zachować zgodność z zasadami projektowania elektronicznych systemów ppoż., które zostały szczegółowo przedstawione przez Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej (CNBOP). Należało brać pod uwagę również sam przyszły proces eksploatacyjny zarówno taboru szynowego, jak i autobusów miejskich. Powyższe uzgodnienia stały się kanwą do opracowania mikroprocesorowego systemu ppoż. składającego się z terminala centrali pożarowej typu CSP1TA (różne wersje) i koncentratorów typu CSP1C. Dodatkową trudnością był dobór czujek pożarowych (dymu i płomienia). Problem czujek jest nadal otwarty ze względu na miejsce ich lokalizacji oraz pracę w warunkach wibracji i drgań. Problemem

jest również (niestety) wandalizm, a więc kradzieże lub dewastacja sprzętu. Wyżej opisany elektroniczny system sygnalizacji pożaru wszedł do eksploatacji w składach pociągów ekspresowych, Intercity i w autobusach szynowych w 2009 r. W najbliższej przyszłości pojawi się w autobusach miejskich (z czujkami umieszczonymi również w komorach silnikowych). Wszystkie te działania mają na celu bezpieczeństwo pasażerów oraz ochronę taboru. Po wdrożeniu systemu przeciwpożarowego nadal prowadzone będą badania eksploatacyjno-niezawodnościowe.

Bibliografia

1. Haykin S., *Systemy telekomunikacyjne*, t. I i II, WKiŁ, Warszawa 2004.
2. Horowitz P., Hill W., *Sztuka elektroniki*, t. I i II, WKiŁ, Warszawa 2006.
3. Ciszewski J., *Podstawowe zasady projektowania systemów sygnalizacji pożarowej*, CNBOP, Józefów 2004.
4. Kula S., *Systemy teletransmisyjne*, WKiŁ, Warszawa 2004.
5. Nawrocki W., *Komputerowe systemy pomiarowe*, WKiŁ, Warszawa 2006.
6. Norma PN-EN 50155:2007 *Zastosowania kolejowe. Wyposażenie elektroniczne stosowane w taborze.*
7. Szulc W., *Opracowanie koncepcji Elektronicznego Systemu Przeciwpożarowego dla potrzeb nowej generacji wagonów*, prace własne, Politechnika Warszawska, Wydział Transportu, Zakład Telekomunikacji w Transporcie, Warszawa 2006.
8. Szulc W., Rosiński A., P*roblemy eksploatacyjno-niezawodnościowe rozproszonego systemu bezpieczeństwa*, Zabezpieczenia nr 1 (47)/2006.
9. Szulc W., Rosiński A., *Wybrane zagadnienia z miernictwa i elektroniki dla informatyków* (cz. 1 – analogowa), Oficyna Wydawnicza WSM, Warszawa 2008.
10. Szulc W., *Koncepcja elektronicznego systemu przeciwpożarowego dla wagonów pasażerskich* (cz. 1), *Koncepcja elektronicznego systemu przeciwpożarowego dla wagonów pasażerskich i autobusów szynowych* (cz. 2) , w: *Zabezpieczenia* nr 6 (40)/2004 i 1 (41)/2005.
11. *Warunki techniczne wykonania i odbioru. Centrala przywoławcza typu CP*, - opracowanie firmy Eltronik, Poznań 2004.
12. Nowak J., *Dokumentacja techniczno-ruchowa. Centrala sygnalizacji pożarowej typu CSP1*, Poznań 2009.

doc. dr inż. Waldemar Szulc
WSM w Warszawie
Wydział Informatyki Stosowanej
Zakład Bezpieczeństwa Obiektów i Informacji
współpracownik WAT
Wydział Elektroniki

dr inż. Adam Rosiński
WSM w Warszawie
Wydział Informatyki Stosowanej
Zakład Bezpieczeństwa Obiektów i Informacji
Politechnika Warszawska
Wydział Transportu
Zakład Telekomunikacji w Transporcie
współpracownik WAT
Wydział Elektroniki

Bosch zabezpiecza stocznię jachtową Delphia Yachts

Ochrona przeciwpożarowa stanowi w obecnych czasach niezwykle istotny element bezpieczeństwa. Coraz więcej obiektów, nawet niewymagających systemu ochrony w świetle przepisów prawnych dotyczących systemów sygnalizacji pożarowej, jest zabezpieczanych w trosce o życie ludzkie. Przykładem takiego obiektu jest stocznia jachtowa Delphia Yachts. Potrzeba zastosowania w niej odpowiednich zabezpieczeń przeciwpożarowych została zgłoszona przez inwestora ze względu na zagrożenia związane z procesem technologicznym, bezpieczeństwo zatrudnionej załogi i dużą wartość mienia zakładowego

Zakład Delphia Yachts to jedna z największych w Polsce stoczni jachtowych. Produkowane w niej jachty żaglowe i łodzie motorowe różnej klasy sprzedawane są z sukcesem na rynkach całego świata – od Rosji poprzez Francję, Niemcy, USA aż po Australię. Delphia Yachts od wielu lat jest stabilnym miejscem pracy dla większości mieszkańców Olecka i okolic.

Stocznia składa się z trzech hal produkcyjnych, budynku magazynowego połączonego z częścią biurową oraz portierni. Dużym wyzwaniem, zarówno na etapie projektu, jak i instalacji, były trudne i bardzo zróżnicowane warunki środowiskowe panujące w zabezpieczanym zakładzie. W pomieszczeniach, w których odbywa się obróbka laminatów, występuje duże zapylenie, które uniemożliwia zastosowanie tradycyjnych punktowych czujek optycznych. Powodem jest zbyt szybkie ich brudzenie się oraz duże ryzyko potencjalnych fałszywych alarmów. Nie było również możliwości zastosowania czujek liniowych z uwagi na pracujące w zakładzie suwnice, które mogłyby zakłócać pracę czujek. Szczególne trudności pojawiły się również przy zabezpieczaniu pomieszczeń w halach, w których metodą natryskową na wcześniej utwardzone skorupy nakładane są żelkoty. Proces ten wiąże się z dużym zapyleniem, pył osadza się na wszystkich elementach pomieszczenia, co również wyklucza użycie czujek tradycyjnych. Duże zagrożenie fałszywymi alarmami stwarzał również proces wymiarowania, trasowania i docinania skorupy jachtów ze zbędnych resztek. W wyniku tego procesu wydzielane są ogromne ilości pyłu. Tego rodzaju zapylenia występują w każdej z hal w różnych ich częściach.

Nietypowe warunki panujące w zakładzie wymusiły przeprowadzenie szczegółowych analiz zmierzających do wytypowania właściwego rodzaju czujek i rozmieszczenia ich w różnych halach. Przeprowadzono analizę ewentualnych przyczyn i okoliczności powstania pożaru oraz jego przebiegu (dynamiki rozwoju) oraz analizę zjawisk występujących w procesie produkcyjnym, umożliwiających powstanie fałszywych alarmów pożarowych.

Na podstawie wyników analiz wykluczono możliwość zabezpieczenia niektórych przestrzeni obiektu środkami technicznymi sygnalizacji pożarowej w postaci czujek punktowych. Analizy stanowiły także podstawę doboru właściwego rodzaju czujek, które sprawdzają się w tak ciężkich warunkach, jak również miały wpływ na sposób ich rozmieszczenia. W oparciu o wyniki tych analiz zaprogramowano również system, określono ściśle warunki jego obsługi, a także właściwy sposób postępowania w przypadku wykrycia i ustalenia miejsca pożaru.

Najbardziej optymalnym rozwiązaniem, zapewniającym bezpieczeństwo w tak trudnych i nietypowych warunkach, okazał się system sygnalizacji pożarowej marki Bosch wykorzystujący centrale sygnalizacji pożarowej FPA5000.

W przypadku wykorzystania pojedynczej centrali system ten może mieć przyłączone 32 pętle dozorowe i obsłużyć do 4096 elementów, a długość pętli, jaką można osiągnąć, to 3000 m przy obciążeniu do 1,5 A. Pracując w sieci, można połączyć ze sobą 32 centrale lub klawiatury wyniesione, co pozwala na obsługę 32512 punktów. Centrala jest wyposażona w kontroler z ekranem dotykowym i intuicyjnym menu, co sprawia, że jej obsługa jest łatwa. Jest to centrala charakteryzująca się dużą

Fot. 1. (z lewej) Budowa czujki płaskiej serii FAP 520
Fot. 2. (z prawej) Centrala sygnalizacji pożarowej FPA5000

elastycznością, która została osiągnięta dzięki zastosowaniu wielu funkcjonalnych modułów instalowanych w dowolnych slotach centrali, a także dzięki możliwości doboru obudów w zależności od wielkości obiektu. Ponadto zabudowana elektronika modułów i możliwość ich wymiany w trakcie pracy systemu sprawia, że system pracuje bezawaryjnie nawet w trudnych warunkach.

Do centrali FPA 5000, oprócz modułów funkcjonalnych instalowanych wewnątrz obudowy, można również podłączyć różne moduły sterująco-monitorujące, instalowane na pętlach dozorowych. Na różnorodność tych modułów wpływa zarówno zróżnicowanie w sposobie ich instalacji (instalacja w obudowach naściennych, w szafach montażowych na szynach DIN), jak również różne możliwości konfiguracji ich wejść i wyjść.

Zasadniczą rolę w przypadku Delphia Yachts odegrały jednak czujki. Oprócz klasycznych czujek punktowych – optycznych, termicznych, optyczno-termicznych czy nawet optyczno-termiczno-chemicznych – firma Bosch posiada w swojej ofercie także czujki płaskie serii 520. Dzięki swojej konstrukcji czujki serii 520 stanowią doskonałe rozwiązanie do zabezpieczania obiektów o dużym zapyleniu, w których zastosowanie klasycznych czujek punktowych czy liniowych może być bardzo trudne lub nieefektywne.

Parametry techniczne i konstrukcja czujki płaskiej znacznie odbiegają od typowych rozwiązań dostępnych na rynku. W przeciwieństwie do tradycyjnych punktowych czujek dymu urządzenia serii 520 nie są wyposażone w komorę optyczną. Rozwiązanie opiera się na dwóch parach diod LED i fotodiod pracujących jako nadajnik i odbiornik. Diody są zainstalowane na zewnętrznej powierzchni czujki. Jeśli w wolnej przestrzeni pod czujką nie znajduje się dym, promieniowanie emitowane przez diody LED nie dociera do fotodiod. Pojawienie się dymu w wolnej przestrzeni pod czujką skutkuje załamaniem światła na cząsteczkach dymu i w rezultacie promieniowanie emitowane przez diody LED dociera do fotodiod. Takie rozwiązanie pozwala na monitorowanie przestrzeni pod czujką bez wykorzystania komory optycznej.

Brak komory optycznej i wykorzystanie zjawiska załamania światła w wolnej przestrzeni pod czujką umożliwiło stworzenie zupełnie płaskiej powierzchni detekcyjnej urządzenia. Ponadto w przypadku czujek serii 520 całe zabrudzenie sprowadza się do osadu zbierającego się na zewnętrznej, płaskiej powierzchni czujki. Czyszczenie urządzenia jest bardzo prostą czynnością polegającą na przetarciu powierzchni czujki za pomocą miękkiej szmatki.

Zainstalowane w stoczni jachtowej czujki płaskie w wersji wielodetektorowej (FAP-OC-520) wyposażone są w dodatkowy sensor chemiczny. Pozwala on na monitorowanie koncentracji tlenku węgla (gazowego produktu spalania), co przyspiesza zadziałanie czujki i eliminuje fałszywe alarmy. Zwiększa to zdolność czujek do odróżniania zapylenia (związanego z procesem technologicznym) od zadymienia, jakie miałoby miejsce w przypadku ewentualnego pożaru.

Udane wdrożenie nowego systemu sygnalizacji pożarowej w stoczni Delphia Yachts to doskonały dowód na to, że możliwe jest zapewnienie bezpieczeństwa ludzi i mienia w obiektach o wyjątkowo wysokich wymaganiach. System zbudowany z centrali FPA5000 i czujek płaskich serii FAP 520 stanowi doskonałe zabezpieczenie obiektów, w których klasyczne czujki nie mogą być stosowane.

Monika Kołodziejczyk
Bosch Security Systems

W niniejszym artykule wykorzystano opracowania na temat projektu SAP dla Delphia Yachts autorstwa Romana Pawłowskiego.

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

ŻYWIOŁY
POD KONTROLĄ

„POLON-ALFA" Zakład Urządzeń Dozymetrycznych sp. z o.o.

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

PATROL II LCD – rejestracja pracy wartowników

PATROL II LCD jest uniwersalnym, przenośnym czytnikiem transponderów zbliżeniowych UNIQUE, przeznaczonym do rejestracji obecności wartownika w wyznaczonych miejscach i o określonych porach.

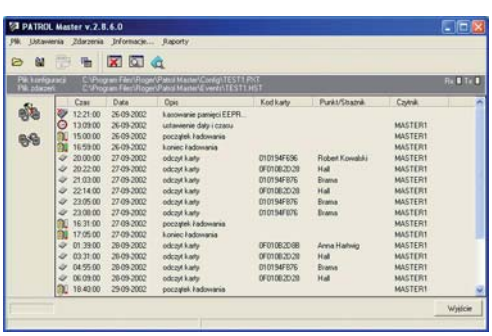
Urządzenie przeznaczone jest do weryfikacji rzetelności pracy wartowników, niemniej może znaleźć zastosowanie wszędzie tam, gdzie zachodzi potrzeba kontroli przemieszczania się ludzi pod względem miejsca i czasu.

Instalacja systemu polega na rozmieszczeniu w wybranych miejscach obiektu punktów kontrolnych oraz skonfigurowaniu czytnika. Każdemu punktowi kontrolnemu oraz identyfikatorowi użytkownika przypisuje się etykiety, co umożliwia później łatwą interpretację historii zarejestrowanych zdarzeń.

Charakterystyka:

- Odczyt zbliżeniowych punktów kontrolnych standardu EM 125 kHz
- Wyświetlacz LCD z podświetleniem
- Nieulotna pamięć 32 tys. zdarzeń
- Rejestracja zdarzeń alarmowych i serwisowych
- Odtwarzanie zdarzeń archiwalnych i celowo skasowanych
- Wyświetlanie nazw odczytanych punktów kontrolnych
- Wyświetlanie nazw identyfikatorów strażników
- Wyświetlanie podpowiedzi z zaplanowanej trasy obchodu
- Ładowanie baterii w gniazda USB lub zewnętrznej ładowarki
- Zasilanie z dwóch baterii lub akumulatorków typu LR6 (AA)
- Zabezpieczenie przed wilgocią i kondensacją pary
- Prosta i intuicyjna obsługa za pomocą jednego klawisza
- Do 8 tys. cykli odczytów na jednym zestawie baterii (*)
- Odporność na upadki z wys. do 1.5 m (*)
- Obsługa przez port USB
- Możliwość aktualizacji oprogramowania czytnika z poziomu PC
- Darmowy program zarządzający pod Windows
- Możliwość dopasowania funkcjonalności urządzenia do wymogów klienta

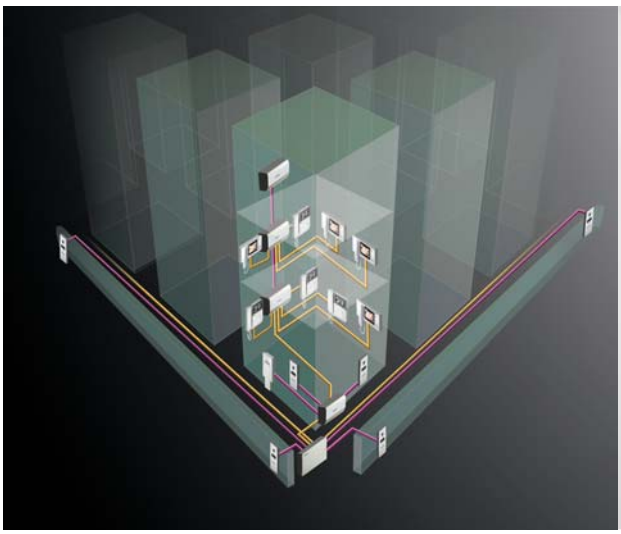
* Parametry oznaczone gwiazdką zostały podane przy założeniu spełnienia pewnych warunków dodatkowych, które zostały określone szczegółowo w instrukcji urządzenia



Patrol Master

roger®
Roger Sp. j.
Gościszewo 59
82-416 Gościszewo, woj. Pomorskie
tel. (55) 272 0132, faks (55) 272 0133
e-mail: roger@roger.pl
http://www.roger.pl

System wieloabonentowy serii 2400



Elementy systemu:

Monitory / Unifony

CAV-51M

APV-4PM

CAV-51AM

AP-5HM

1 przewód . . . . . wiele możliwości

Stacje bramowe

DRC-MSC/MSB
DRC-OSC/OSB

DRC-nSC/nSB

DR-nSB

DR-nMS

Dystrybutory

CCU-OS

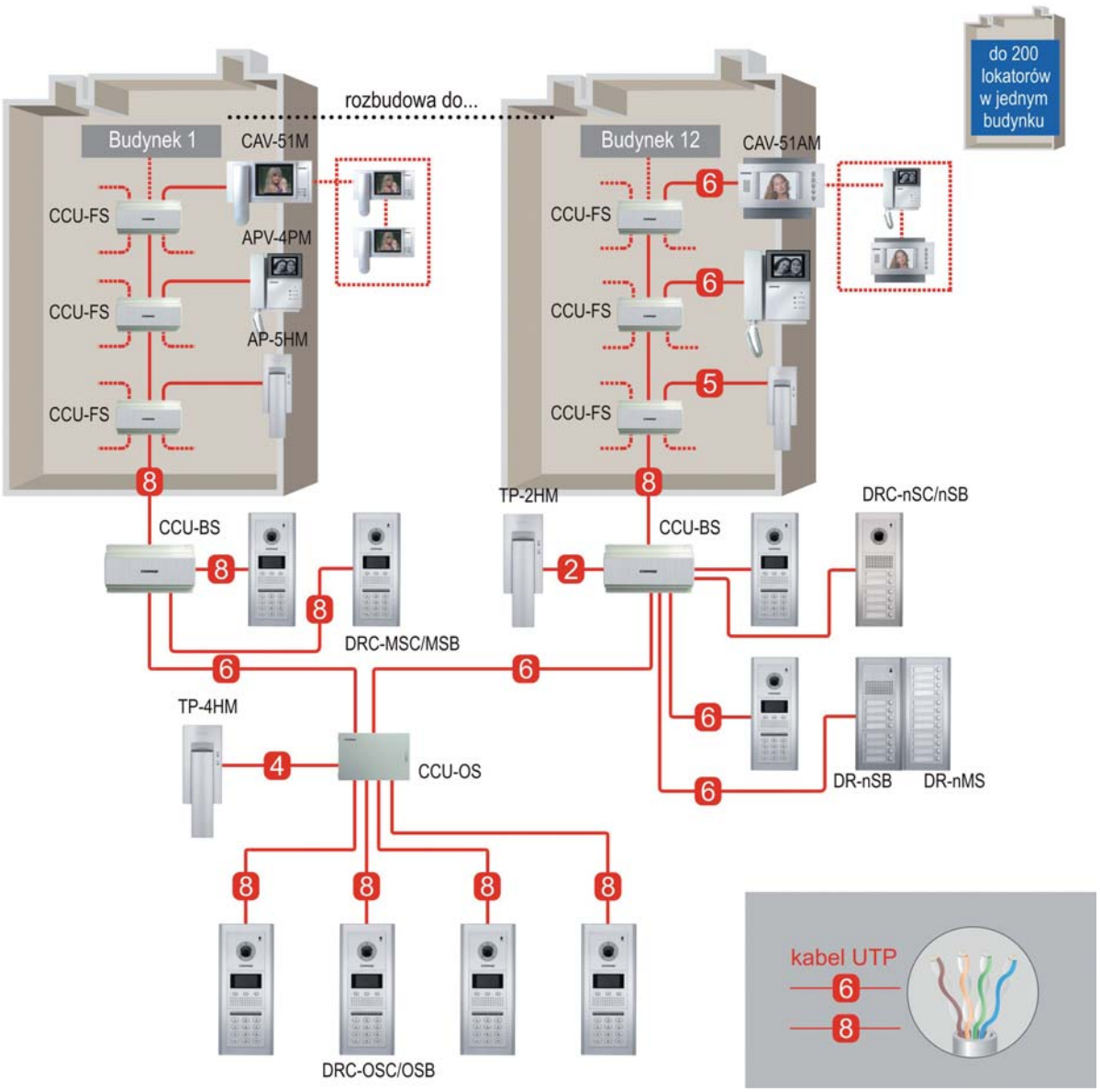
CCU-BS
CCU-FS

GDE POLSKA
Global Distributor of Electronics

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

System wieloabonentowy serii 2400



System wieloabonentowy serii 2400 przeznaczony jest do instalacji zarówno w prostych, jak i w bardzo rozbudowanych aplikacjach - maksymalna liczba obsługiwanych przez system abonentów wynosi 2400. U każdego lokatora może być zainstalowane do 3 urządzeń (jedno urządzenie typu Master i dwa urządzenia typu Slave).

Lokator może mieć zainstalowany prosty unifon, umożliwiający kontakt głosowy z osobą odwiedzającą, jak i monitor (czarno-biały lub kolorowy), pozwalający także na obserwację wizualną osoby odwiedzającej.

System umożliwia zastosowanie zarówno paneli zewnętrznych audio, jak wideo - wyposażonych w moduł kamery (czarno-biały lub kolorowy). Panele zewnętrzne występują w wersji przyciskowej lub z klawiaturą numeryczną (umożliwiającą dodatkowo wybór lokatora za pomocą spisu lokatorów oraz otwieranie zamka elektrycznego przy użyciu indywidualnych kodów).

System może być wyposażony w unifon instalowany w portierni, przez co lokatorzy mogą mieć kontakt z osobą dozorującą (portierem). Dzięki dużej elastyczności możliwe jest skonfigurowanie systemu dla małych, pojedynczych bloków, jak i całych osiedli zamkniętych, gdzie ogrodzonych może być klikanaście budynków, a całość jest nadzorowana przez kilku portierów.

GDE POLSKA
Global Distributor of Electronics
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

Inteligentny tester akumulatorów GOLD-IBT

GOLD-IBT

inteligentny tester akumulatorów

Producenci akumulatorów zalecają wymianę akumulatora, jeżeli jego współczynnik pojemności spada poniżej 65%. Typowym miernikiem można zmierzyć tylko napięcie akumulatora.

Jak zmierzyć jego pojemność?

Inteligentny Tester Akumulatorów GOLD-IBT w kilka sekund dokonuje symulacji pełnego rozładowania akumulatora.

Automatycznie wyświetla temperaturę otoczenia, napięcie akumulatora i aktualną pojemność.

- Testuje w ciągu kilku sekund akumulatory wykonane w technologii AGM (elektrolit uwięziony w separatorach z włókna szklanego) – powszechnie używane w systemach alarmowych i UPS.
- Automatycznie wyświetla temperaturę otoczenia, napięcie akumulatora i aktualną pojemność.
- Cyfrowo zaprogramowany do pomiaru szczelnych akumulatorów (SLA) 12 V oraz akumulatorów samochodowych o pojemności od 1,2 Ah do 200 Ah.
- Testuje akumulatory szybko, dokładnie i jest łatwy w użyciu.

Dane techniczne	
Model	GOLD-IBT
Zasilanie	12 V_{DC} (10-15 V_{DC})
Typ akumulatora	szczelne akumulatory (SLA) 12 V oraz akumulatory samochodowe
Pojemność akumulatora	1.2 Ah – 200 Ah
Symulowany test rozładowania akumulatora	C20 do 10,50 V_{DC} @ 25°C
Wyświetlacz	podświetlany LCD
Pomiar temperatury	0° – 100°C
Ostrzeżenie o zbyt wysokim napięciu	> 15 V_{DC}
Ostrzeżenie o zbyt niskim napięciu	< 10 V_{DC}
Ostrzeżenie o zbyt niskiej pojemności	< 0.5 Ah
Tolerancja pomiaru Ah	10% (zależy od konstrukcji i parametrów produkcyjnych akumulatora)
Zabezpieczenie temperaturowe odwrócenia polaryzacji	dioda blokująca
Zdolność wykonania kolejnych testów	do 15 następujących bezpośrednio po sobie
Ostrzeżenie przed przegrzaniem	> 55°C ± 10°
Wymiary	111 mm x 55 mm x 35 mm
Długość przewodów przyłączeniowych	40 cm
Masa w opakowaniu	400 gramów
Zawarte akcesoria	futerał, certyfikat zgodności, etykiety na akumulatory
Gwarancja	1 rok

alarmnet®

Alarmnet 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
http://www.alarmnet.com.pl

Rejestratory cyfrowe 4, 8 i 16-kanałowe 4sec serii LCD

Zintegrowane rejestratory serii 4SEC2000LCD posiadają funkcjonalność kompletnego stanowiska nadzoru CCTV. Wysokiej klasy monitory LCD przeznaczone do pracy ciągłej zapewniają doskonały obraz. Przyciski i pokrętła poniżej monitora oraz pilot pozwalają na sterowanie zapisem i podglądem z kamer, podłączenie do sieci Internet pozwala na zdalne sterowanie oraz podgląd obrazu nawet na telefonie komórkowym.

Dzięki zastosowaniu podwójnego kodowania, obraz zapisany w kompresji JPEG2000 ma doskonałą jakość, a dzięki kompresji H.264 transmisja sieciowa nie ma zbyt wygórowanych wymagań przepustowości łącza.

Dane techniczne			
Model	4SEC2004LCD10	4SEC2008LCD19	4SEC2016LCD19
Monitor TFT-LCD	10,2" WVGA	19" SXGA	19" SXGA
Ilość wejść wideo	4	8 przelotowych	16 przelotowych
Audio	4 wejścia 1 wyjście		
Kompresja	JPEG2000 – zapis i odtwarzanie / H.264 – transmisja przez sieć LAN		
Wyjścia wideo	Monitor / spot		
Dyski	1 SATA	2 SATA	
Podział ekranu	1, 4	1, 4, 6, 8, 9	1, 4, 6, 8, 9, 13, 16
Rozdzielczość zapisu	Pełny ekran – 720×288, podział – 360×288		
Prędkość zapisu (PAL)	50 fps (720×288) 100 fps (360×288)	100 fps (720×288) 200 fps (360×288)	
Prędkość podglądu	W czasie rzeczywistym dla wszystkich kanałów		
Wielozadaniowość	Triplex (Odtwarzanie / Zapis / Ethernet)		
PIP / ZOOM	Tak / Tak		
Detekcja ruchu	Strefa 16×12		
Tryby zapisu	Ciągły / Detekcja / Kalendarz / Alarm / Ręczny		
Wyszukiwanie zapisu	Procent zapisu / Data&Czas / Zdarzenia		
Zabezpieczenie	Hasła: Administratora, Managera oraz 8 użytkowników		
Wejścia alarmowe	4 (NO/NC)	8 (NO/NC)	16 (NO/NC)
Wyjścia	1 przekaźnikowe		
Archiwizacja	USB / Zdalne oprogramowanie		
Temperatura pracy	od 5°C do 40°C		
Wilgotność	< 90%		
Wymiary (SxWxG)	282×325×180 mm	418×440×230 mm	
Masa	ok. 6 kg (bez dysków)	ok. 10 kg (bez dysków)	
Zasilanie	12 V_{DC} (zasilacz w komplecie)		

JPEG2000 – najlepsza jakość zapisanego materiału, H.264 – najszybsza transmisja

Podgląd zdalny może być realizowany przez załączone oprogramowanie klienta, przeglądarkę internetową, telefon komórkowy lub w przypadku systemów wielostanowiskowych przez CMS (Centralny System Monitorowania). Dzięki zwartej obudowie rejestrator nie zajmuje więcej miejsca niż standardowy monitor LCD.

Cechy:

- Podwójny algorytm kompresji:
  - Zapis i odtwarzanie JPEG2000
  - Transmisja przez Internet H.264
- Wysoka jakość zapisanego materiału
- Tryb pracy – Duplex / Triplex
- Złącze USB do archiwizacji danych
- Sterowanie PTZ
- Wygodne wyszukiwanie i przeglądanie materiału
- Łącze USB do aktualizacji oprogramowania
- Menu w języku polskim
- Zdalne oprogramowanie
- DDNS
- Pilot
- Audio: 4 wejścia, 1 wyjście

alarmnet®

Alarmnet 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
http://www.alarmnet.com.pl

Drukarka do kart identyfikacyjnych

Pronto

MAGICARD

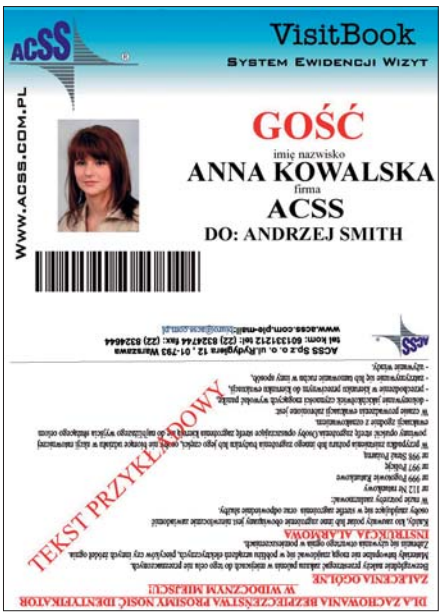
Mała, kompaktowa drukarka o nowoczesnym wyglądzie do zastosowania w każdej firmie i każdym miejscu. Do szybkiego drukowania identyfikatorów oraz wszelkiego rodzaju kart. Ręczny podajnik umożliwia łatwe drukowanie pojedynczych kart. Drukarka Pronto jest łatwa w konfiguracji i użytkowaniu, posiada instrukcję i sterowniki w języku polskim do Windows 2000, XP, Vista i zapewnia niezawodne drukowanie kart przez wiele lat. Drukarka Magicard Pronto umożliwia wykorzystanie HoloKote™ i HoloPatch™ – opatentowanych zabezpieczeń przed nieautoryzowanym kopiowaniem kart. Drukarka Pronto to wysokiej jakości kolorowe i monochromatyczne wydruki w atrakcyjnych cenach!

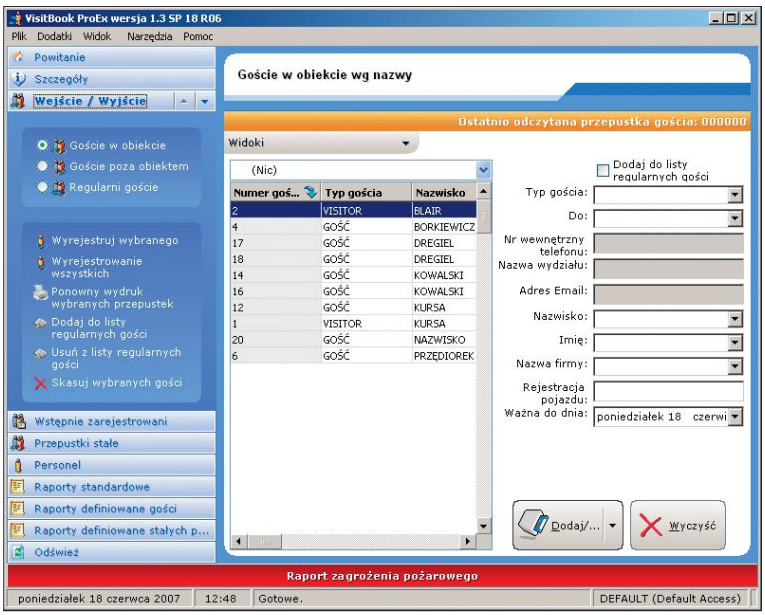
Specyfikacja techniczna	
Prędkość nadruku	Wydruk karty w kolorze od krawędzi do krawędzi w 35 sekund Monochromatyczny wydruk karty w 7 sekund
Interfejs do PC	USB rev. 1.1. (kompatybilny z USB 2.0)
Sterowniki	Windows 2000, 2003 Server user-mode, XP, Vista
Zasilanie	90-265 V / 47-63 Hz
Wymiary / Masa	270 mm × 215 mm × 233mm / 4,4 kg
Temperatura pracy	od 10°C do 30°C
Gwarancja	2 lata

Materiały eksploatacyjne	
Typy taśm	YMCKO 5 paneli nadruk 300 kart (MA300YMCKO) Monochromatyczna czarna plus overlay nadruk 600 kart (MA600KO) Monochromatyczna czarna nadruk 1000 kart (MA1000K-BLACK) Monochromatyczna czerwona nadruk 1000 kart (MA1000K-RED) Monochromatyczna biała nadruk 1000 kart (MA1000K-WHITE) Monochromatyczna niebieska nadruk 1000 kart (MA1000K-BLUE) Monochromatyczna zielona nadruk 1000 kart (MA1000K-GREEN) Monochromatyczna złota nadruk 1000 kart (MA1000K-GOLD) Monochromatyczna srebrna nadruk 1000 kart (MA1000K-SILVER)
Typy kart	Drukuje na wszystkich standardowych kartach PCV ISO CR80 i CR 79 o grubości od 0,51 mm do 1,02 mm, kartach magnetycznych, zbliżeniowych, samoprzylepnych, HoloPatch
Zestaw czyszczący	10 szt. kart czyszczących, 1 flamaster (CK1) 5 wałków czyszczących plus wymienna oś wałka

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
http://www.acss.com.pl, http://www.magicard.com.pl

System rejestracji gości VisitBook





Wybrane funkcje systemu VisitBook	wersja LITE	wersja PRO	wersja PRO EX	wersja xFR
Kontrola gości, kontrahentów, personelu	tak	tak	tak	tak
Rejestracja wstępna	–	tak	tak	tak
Lista regularnych gości	–	tak	tak	tak
Pobieranie zdjęcia	–	–	tak	tak
Czytnik kodów kreskowych	–	tak	tak	tak
Elektroniczny podpis	–	–	tak	tak
Przepustka pojazdu	–	–	tak	tak
Drukowanie na PVC	–	–	tak	tak
Format bazy danych	Access	Access	Access	MSSQL / MySQL
Dostępność w sieci	–	tak	tak	tak
Administracja konferencji/ wystaw	–	–	tak	tak
Własne wzory przepustek	–	–	tak	tak
Raport standardowy	tak	tak	tak	tak
Raporty definiowane	–	tak	tak	tak
Zabezpieczenie sprzętowe	klucz USB	klucz USB	klucz USB	klucz USB

System rejestracji gości VisitBook jest narzędziem służącym do wspomagania pracy recepcji. Zastępuje papierową księgę gości – jest jej elektronicznym odpowiednikiem. System umożliwia rejestrację danych osób odwiedzających budynek wraz z wydrukiem ich przepustek. Proces wydruku przepustki gościa oraz przechwycenia jego zdjęcia jest płynny i szybki. Rejestrację wejścia i wyjścia gościa można zautomatyzować stosując czytnik kodów kreskowych. Program VisitBook jest dostępny w czterech wersjach: Lite, Pro, ProEx i xFR.

Wersja Lite pozwala na drukowanie przepustek z podstawowymi danymi personalnymi, a rejestracji wejść i wyjść dokonuje pracownik recepcji.

Wersja Pro dodatkowo umożliwia nadruk na przepustce kodu kreskowego wykorzystywanego przy automatycznej rejestracji wejść/wyjść.

ProEx jest wersją bardziej rozbudowaną w porównaniu do wcześniejszych. Umożliwia wydruk przepustki wraz ze zdjęciem i zawiera m.in. funkcję projektowania własnych wzorów przepustek.

Podstawową zaletą różniącą czwartą wersję xFR od pozostałych jest zastosowana w niej platforma SQL zapewniająca szybkość i niezawodność obsługi dużych, ruchliwych obiektów.

Wydruk przepustek jest możliwy na standardowych drukarkach biurowych oraz drukarkach do kart PVC (tylko wersja Pro-Ex i xFR). Główną zaletą użycia systemu jest możliwość raportowania w czasie rzeczywistym, np. raport pożarowy, raport gości w obiekcie, raport ruchów gości itp. Program ponadto zawiera kilka użytecznych funkcji, takich jak: menedżer personelu, menedżer kontrahentów, obsługa konferencji.

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
http://www.acss.com.pl

MGSM 4.0+ Moduły powiadomienia i sterowania GSM
MGSM 4.0-PS+ Moduły powiadomienia i sterowania GSM z wbudowanym zasilaczem buforowym 13,8 V / 1,3 A

Nowoczesny nadajnik GSM z dwukierunkową transmisją danych. Zaprojektowany do zastosowań w systemach alarmowych, kontroli dostępu, przesyłania informacji teletechnicznych oraz M2M. Innowacyjne rozwiązania w module MGSM 4.0+, które pozwalają na przesyłanie dowolnych komunikatów: SMS, VOICE, SMS+VOICE z poszczególnych wejść modułu. Sterowanie wyjściami modułu może odbywać się poprzez SMS (o dowolnej treści) i/lub CLIP z uprawnionych numerów telefonów. Przy współpracy z FGR-4 pozwala na przesyłanie wiadomości multimedialnych MMS i E-MAIL (zdjęcia + tekst) na standardowe telefony komórkowe i adresy e-mail. Po dołączeniu czujnika temperatury TSR-1 moduł przekazuje informacje o temperaturze i/lub możliwe jest skonfigurowanie prostego termostatu temperatury.

Podstawowe właściwości

Wbudowany telefon przemysłowy
- współpraca z sieciami abonamentowymi (*post-paid*) i sprzedaży przedpłaconej (*pre-paid*)
- dwuzakresowy GSM/DCS (900/1800 MHz), GPRS

Przekazywanie informacji na numery stacjonarne, komórkowe i adresy e-mail
- współpraca ze stacjami monitoringu: SMS, CLIP
- obsługa 8 numerów telefonów do powiadomienia prywatnego: SMS, VOICE, SMS+VOICE, CLIP
- obsługa 8 numerów telefonów komórkowych oraz 4 adresów e-mail w trybie MMS

Wejścia modułu [8]
- szeroki wybór typów reakcji np. info, opóźniona, licznikowe, zał./wył. czuwanie
- programowana konfiguracja pracy: np. 2EOL/NC, NC, NO oraz czas naruszenia wejścia
- możliwość wyzwalania wejść I7/I8 poprzez „+12 V" lub „GND"

Przesyłanie informacji z systemu poprzez SMS
- dowolne komunikaty SMS z poszczególnych wejść
- niezależne informacje o naruszeniu i powrocie stanu wejścia
- komunikaty o awariach zasilania
- status systemu, stan: wejść, wyjść, zasilanie, awarii

Przesyłanie informacji głosowej VOICE
- współpraca z syntezerami mowy VSR-2 (16 komunikatów) lub VSR-1 (1 komunikat)
- dowolne komunikaty głosowe z poszczególnych wejść, w połączeniu z VSR-2
- współpraca z modułem audio AMR-1, odsłuch obiektu

Przesyłanie wiadomości multimedialnych MMS
- współpraca z modułem FGR-4, przetwarzanie sygnału wideo na klatki obrazu (zdjęcia JPG)
- przetwarzanie 4 sygnałów wideo (PAL: kolor, cz.-b.)
- regulowana jakość kompresji JPG, możliwość wysłania 4 zdjęć w jednej wiadomości MMS
- możliwość zapisu i odczytania zdjęć z lokalnej karty pamięci SD

Wyjścia modułu [8]
- wyjście O1: 1A/12 V, wyjścia O2-O8: OC 100 mA/GND
- zdalne sterowanie poprzez: SMS (dowolna treść) lub CLIP
- sterowanie poprzez stan modułu: wejścia, zdarzenie, awarie, temperaturę (termostat)
- programowany tryb i czas działania
- funkcje logiczne I/O, O/O: AND, OR, NOR, XOR
- wyjścia zasilania urządzeń dodatkowych AUX i +KB

Funkcja „centrali alarmowej"
- sterowana SMS i wejściem MGSM 4.0-PS+
- sterowana SMS, wejściem i pilotem MGSM 4.0+ i PSR-RF

Funkcja pomiaru i kontroli temperatury
- współpraca z cyfrowym czujnikiem temperatury TSR-1
- przesyłanie informacji o przekroczeniu wartości L lub H: SMS, VOICE
- wartość chwilowa temperatury w SMS „STAN"
- funkcja termostatu: sterowanie wyjściami O5 i O6

Timery [4]
- sterowanie dowolnym wyjściem, czuwaniem modułu

Funkcje ograniczenia i kontroli kosztów
- dzienny licznik SMS: powiadomienie, awarie
- sygnalizacja braku środków na koncie pre-paid

Funkcja testu łączności
- cykliczny (co 1 ... 99 godz.), według zegara lub o zadanej godzinie
- wyzwalane z wejścia, odpytanie zewnętrzne (SMS)
- programowany typ testu: SMS, CLIP, MMS (obraz z wybranych kamer)

Programowanie
- zdalne: połączenie modemowe (CSD)
- lokalne: RS232, USB
- zdalne: SMSy konfiguracyjne (wybrane funkcje)
- pamięć FLASH, aktualizacja oprogramowania (*firmware*)

Sygnalizacja pracy
- optyczna sygn. stanu modułu: praca, zasięg GSM, połączenie
- optyczna sygn. stanu wyjść

Pamięć zdarzeń
- rejestrowanie zdarzeń np. awaria, sterowanie, czuwanie
- rejestrowana data i czas zdarzenia
- rejestr 1000 zdarzeń z funkcją nadpisywania

Dwie wersje zasilania
- MGSM 4.0+: 12 V_{DC},
- MGSM 4.0-PS+: 18 V_{AC} / 24 V_{DC} z wbudowanym zasilaczem buforowym 13,8 V / 1,3 A z obsługa akumulatora 12 V SLA
- kontrola zasilania podstawowego i awaryjnego

Szeroka gama wyposażenia dodatkowego
- moduły dodatkowe np. FGR-4, VSR-2,
- obudowy: natynkowe, na szynę DIN, hermetyczne
- anteny GSM/DCS oraz przedłużacze

ROPAM elektronik

Ropam Elektronik s.c.
Os.1000-lecia 6A/1
32-400 Myślenice

tel. (12) 379 34 47, tel./faks (12) 272 39 71
e-mail: biuro@ropam.com.pl
http://www.ropam.com.pl

System kontroli dostępu VertX

Produkty VertX firmy HID, dostarczane przez firmę Katon, oferują kompletną, wyposażoną we wszystkie niezbędne cechy infrastrukturę umożliwiającą zbudowanie złożonego systemu kontroli dostępu komunikującego się poprzez standardowy protokół TCP/IP, 10/100 Mb/s Ethernet lub Internet. Podstawą kontrolerów V1000 i V2000, jest 32-bitowy procesor pracujący z systemem operacyjnym Linux. Wbudowana w kontrolerach pamięć typu flash umożliwia aktualizację oprogramowania poprzez sieć Ethernet.

Kontroler V1000 obsługuje 32 podwójne moduły drzwiowe (V100), moduły wejść alarmowych (V200) lub moduły wyjść przekaźnikowych (V300). Moduły te łączone są z kontrolerem poprzez dwa niezależne kanały sieci RS-485, z których każdy posiada dwa porty wejściowe optymalizujące topologię połączeń systemu. Architektura taka daje możliwość wykorzystania jednego adresu TCP/IP dla każdych 32 interfejsów i przesłanie danych przez sieć RS-485.

Główne cechy kontrolera V1000:

- Zapamiętanie i przechowywanie danych systemu kontroli dostępu i konfiguracji 32 kontrolerów drzwi V100 (maks. 64 czytniki) oraz 44000 użytkowników kart z możliwością rozszerzenia do 250000 użytkowników
- Połączenie z kilkoma rodzajami modułów w maksymalnych ilościach:
  - 32 moduły V100 (maks. 64 czytniki) lub
  - 32 moduły V200 (maks. 512 wejść alarmowych) lub
  - 32 moduły V300 (maks. 384 przekaźniki)
- Zarządzanie funkcjami systemu kontroli dostępu
- Raporty o stanie wejść nadzorowanych/alarmów z wykorzystaniem 255 priorytetów
- Lokalne połączenie komputera (laptopa) w celu diagnostyki i konfiguracji kontrolera
- Połączenie z hostem i innymi urządzeniami poprzez sieć TCP/IP
- Rejestracja wszystkich zdarzeń na serwerze
- Odbieranie i przetwarzanie danych z oprogramowania kontroli dostępu w czasie rzeczywistym
- Buforowanie zdarzeń off-line i przesłanie do serwera po wznowieniu połączenia
- W przypadku utraty połączenia TCP/IP możliwe jest połączenie modemowe

Kontroler V2000 pozwala na podłączenie maksymalnie dwóch czytników poprzez interfejs Wiegand lub Clock-and-Data. Można w ten sposób obsłużyć jedno lub dwa przejścia kontroli dostępu. Taka architektura systemu wykorzystuje istniejącą sieć komputerową LAN typu CAT-5.

Główne cechy kontrolera V2000:

- Pobieranie i zapamiętanie kompletnych danych systemu kontroli dostępu i konfiguracji baz danych jednych lub dwóch kontrolowanych drzwi oraz 44000 użytkowników kart z możliwością rozszerzenia do 250000 użytkowników
- Zarządzanie funkcjami systemu kontroli dostępu
- Raporty o stanie wejść nadzorowanych/alarmów z wykorzystaniem 255 priorytetów
- Lokalne połączenie komputera (laptopa) w celu diagnostyki i konfiguracji kontrolera
- Połączenie z hostem i innymi urządzeniami poprzez sieć TCP/IP
- Odbieranie i przetwarzanie danych z oprogramowania kontroli dostępu w czasie rzeczywistym
- Rejestracja wszystkich zdarzeń na serwerze
- Buforowanie zdarzeń off-line i przesłanie do serwera po wznowieniu połączenia

Z kontrolerem V1000 mogą współpracować dodatkowe moduły umożliwiające rozbudowę systemu kontroli dostępu. W zależności od konfiguracji systemu są to moduły V100, V200 lub V300 (podstawowe parametry znajdują się w poniższej tabeli).

	V1000	V2000	V100	V200	V300
Ilość obsługiwanych czytników	64 (poprzez 32 moduły V100)	2	2	brak	
Ilość obsługiwanych wejść alarmowych	512 (poprzez 32 moduły V200) + 2 konfigurowalne	3 konfigurowalne + 2 kontaktronowe	3 konfigurowalne + 2 kontaktronowe	16 + 3	2 + 3
Ilość obsługiwanych wyjść przekaźnikowych	384 (poprzez 32 moduły V300) + 2 konfigurowalne	2 (przycisk wyjścia) + 4 konfigurowalne	2 (przycisk wyjścia) + 4 konfigurowalne	2	12
Porty komunikacyjne	1x RJ45 dla TCP/IP 10 lub 100 Mb/s, 4x RS485, 2x RS232 (modem)	1x RJ45 dla TCP/IP 10 lub 100 Mb/s, 2x SIA Wiegand/Clock-and-Data	2x RS485, 2x SIA Wiegand/Clock-and-Data	2x RS485	2x RS485
Wilgotność względna pracy	5 – 95% (bez kondensacji)				
Wymiary (wys./szer./dł.)	123 mm × 147 mm × 32 mm				
Napięcie zasilania	12 – 18 V_{DC}		9 – 18 V_{DC}		
Pobór prądu	140 mA	160 mA	60 mA (bez czytników)	50 mA	60 mA

Urządzenia serii VertX do prawidłowej pracy w systemie kontroli dostępu wymagają nadrzędnego oprogramowania. Polecaną aplikacją współpracującą z urządzeniami VertX w zakresie kontroli dostępu, rejestracji czasu pracy, integracji z systemami CCTV, monitorowania alarmów, jest oprogramowanie SimpleID, dostarczane odpłatnie razem z urządzeniami VertX.

KATON
ACCESS CONTROL & SECURITY SYSTEMS

Katon Sp. z o.o.
ul. Bajana 31E
01-904 Warszawa

tel. (22) 869 43 92
e-mail: biuro@katon.eu
http://www.katon.eu

Sieciowa kamera serii IXE20 Sarix

Informacje ogólne	
Matryca	1/3" (efektywnie)
Rodzaj matrycy	CMOS
Odczyt matrycy	Skanowanie progresywne
Rozdzielczość maks.	1920×1080
Stosunek sygnał/szum	50dB (automatyczna przesłona)
Typ obiektywu	Napęd DC
Zakres elekt. migawki	1~1/10 000 s
Szeroki zakres dynamiki	60 dB
Balans bieli	2 000° do 10 000°K
Czułość	przy f/1.2; 2 850°K; SNR >24dB
Kolor (33 ms)	0,50 lx
Kolor SENS (500 ms)	0,12 lx
Mono (33 ms)	0,25 lx
Mono SENS (500 ms)	0,03 lx
Informacje mechaniczne	
Mocowanie obiektywu	mocowanie CS, regulowane
Mocowanie kamery	0,25" (0,64cm) śruba UNC-20, góra i dół obudowy kamery
Właściwości fizyczne	
Wymiary	13,7 dł.× 7,9 szer.×7,6 wys. (cm)
Masa (bez obiektywu)	0,51 kg
Masa z opakow.	0,90 kg
Informacje o środowisku pracy	
Temperatura robocza	od -10° do 50°C (od 14° do 122°F)
Temperatura magazynowania	od -10° do 70°C (od 14° do 158°F)
Wilgotność	20% do 90%, bez kondensacji
Informacje elektryczne	
Port	Złącze RJ-45 dla 100 Base-TX
Auto	MDI/MDI-X
Typ okablowania	Kat.5 lub lepszy dla 100 Base-TX
Moc wejściowa	24 V_{AC} lub PoE (IEEE 802.3af klasa 3)
Pobór mocy	< 7 W
Pamięć wewnętrzna	Mini SD
Wejście alarmowe	10 V_{DC} maksymalnie, 5 mA maksymalnie
Wyjście alarmowe	0 do 15 V_{DC} maksymalnie, 75 mA maksymalnie
Złącze serwisowe	Zewnętrzne, 3 złącza, 2,5 mm
Kodowanie wideo	H.264 profil główny lub podstawowy, MJPEG
Strumienie wideo	Do 2 strumieni jednocześnie; drugi strumień zmienny, zależnie od ustawień strumienia głównego
Liczba klatek	Do 30, 25, 24, 15, 12.5, 12, 10, 8, 7. 5,6, 5, 4, 3, 2, 1 (zależnie od kodowania, rozdzielczości i konfiguracji strumienia)
Obsługiwane protokoły	TCP/IP, UDP/IP (Unicast, Multicast IGMP), UPnP, DNS, DHCP, RTP, RTSP, NTP, IPv4, SNMP, QoS, HTTP, HTTPS, LDAP (klient), SSH, SSL, SMTP, FTP, MDNS (Bonjour)
Użytkownicy	Unicast - Do 20 użytkowników jednocześnie Multicast - Nieograniczona liczba użytkowników H.264
Interfejs oprogramowania	Przeglądarka i ustawienia, do 16 kamer
Integracja z systemami	Endura 2.0 lub nowszy Digital Sentry 1.6
Otwarta integracja IP	Kamera Pelco IP API

CYFROWE KAMERY HD O ROZDZIELCZOŚCI 2,1 MEGAPIKSELA

Cechy charakterystyczne:
- Otwarta integracja IP
- Rozdzielczość do 2,1 Megapiksela (1920 x 1080)
- Do 30 obrazów na sekundę (ips) przy rozdzielczości 1280 x 720
- Funkcja ABS (Auto Back Focus)
- Kompresja H.264 oraz MJPEG
- Modele kolorowe oraz Dzień/Noc
- Wejście ustawień wideo
- Czułość do 0,03 lx
- Funkcja Power over Ethernet (IEEE 802.3af) lub zasilanie 24 V_{AC}
- Do 2 strumieni wideo jednocześnie
- Możliwość podglądu sygnału z wykorzystaniem sieci, do 16 kamer jednocześnie
- Pamięć wewnętrzna (Mini SD) w przypadku alarmu

Kamera

Serię Sarix IXE20 stanowią dwa modele o rozdzielczości 2,1 Mp: kolorowy oraz dzień/noc. Oba modele wykorzystują technologię Low Light (wykorzystywana przy słabym oświetleniu). Model dzień/noc wyposażony został w mechaniczny filtr podczerwieni (IR), mający zastosowanie w czasie pracy kamery w trybie cz.-b. Seria Sarix IXE20 obsługuje dwa strumienie wideo jednocześnie. Oba strumienie mogą zostać skompresowane do formatu MJPEG oraz H.264 o różnych rozdzielczościach. Kamera umożliwia podgląd obrazu w rozdzielczości HD w czasie rzeczywistym (30 kl./s), z wykorzystaniem kompresji H.264. Oznacza to optymalne wykorzystanie szerokości pasma oraz oszczędność miejsca na dysku HDD. Strumienie mogą być konfigurowane według liczby klatek, prędkości klatek na sekundę, oraz struktur GOP (grupy obrazów). Seria Sarix IXE20 jest łatwa w instalacji, natomiast funkcja ABS (automatyczne ustawienie ostrości) ułatwia regulację ostrości.
Pomocnicze wyjście wizyjne eliminuje potrzebę wykorzystania laptopa do podglądu obrazu w czasie instalacji kamery. Seria Sarix IXE20 posiada zintegrowany moduł Power over Ethernet (PoE) IEEE 802.3af (48 V_{DC}), alternatywnie pozostaje możliwość zasilania kamery napięciem 24 V_{AC}.

Interfejs sieci

Seria Sarix IXE20 wykorzystuje standardową przeglądarkę sieciową do administracji i programowania. W obrębie jednej sieci istnieje możliwość podglądu do 16 sygnałów kamer. Protokoły sieciowe takie jak SSL, SSH oraz QoS (priorytetu lub gwarancji przepływu danych) mogą być programowane za pomocą przeglądarki sieciowej.

Systematyzacja

Seria Sarix IXE20 może pracować z protokołem Pelco IP, systemami hybrydowymi (na przykład Endura 2.0 lub nowszy oraz Digital Sentry wersja 1.6 lub nowsza). Kamera charakteryzuje się również otwartą architekturą połączeń z oprogramowaniem firm trzecich. Pelco oferuje interfejs programowania aplikacji (ang. Application Programming Interface), co pozwala na integrację z kamerami sieciowymi Pelco.

Modele

IX20C Sieciowa kamera kolorowa Sarix 2.1 MPx
IX20DN Sieciowa kamera dzień/noc Sarix 2.1 MPx

Certyfikaty

CE, Klasa B, FCC, Klasa B Certyfikat UL/cUL, C-Tick*GOST*

Zalecane mocowania

C10-UM Uniwersalne mocowanie kamery

Zalecane obudowy

EH1512, **EH3512**, **DF8**

Zalecane obiektywy

13M2.2-6 Obiektywy megapikselowe, o zmiennej ogniskowej, 2.2~6.0 mm, f/1.3~2.0
13M2.8-8 Obiektywy megapikselowe, o zmiennej ogniskowej, 2.8~8.0 mm, f/1.2~1.9
13M2.8-12 Obiektywy megapikselowe, o zmiennej ogniskowej, 2.8~12.0 mm, f/1.4~2.7
13M15-50 Obiektywy megapikselowe, o zmiennej ogniskowej, 15.0~50.0 mm, f/1.5~2.1

Schneider Electric

Schneider Electric Buildings Polska Sp. z o.o.
ul. Rzymowskiego 53
02-697 Warszawa

tel. (22) 313 24 10, faks (22) 313 24 11
e-mail: SEPLBuildings.Poland@buildings.schneider-electric.com
http://www.schneider-electric.com/buildings

Kompaktowa obudowa serii EH 1512

KOMPAKTOWA OBUDOWA SERII EH 1512 DO ZASTOSOWAŃ WEWNĘTRZNYCH ORAZ ZEWNĘTRZNYCH

Cechy charakterystyczne:

– Kompaktowe, eleganckie i współczesne wzornictwo
– Obudowa wykonana z odlewanego ciśnieniowo aluminium
– Uszczelnione przepusty kablowe oraz otwory montażowe umieszczone u dołu obudowy
– Zaprojektowany do zastosowań wewnętrznych oraz zewnętrznych
– Spełnia normy/standardy IP66 oraz NEMA type 4X
– Prostota w instalacji i serwisowaniu
– Modele dostępne z fabrycznie zainstalowaną grzałką oraz wentylatorem o niskim poborze energii
– Uchwyt przewlekany chroniący okablowanie przed czynnikami atmosferycznymi oraz mechanicznymi
– 3-letnia gwarancja

Obudowa kamery serii EH 1512 została stworzona z myślą o wykorzystaniu jej do kamer zarówno analogowych jak i IP (seria Sarix). Mimo kompaktowych rozmiarów pozwala na pomieszczenie w jej wnętrzu kamery wraz z obiektywem oraz, w zależności od opcji, grzałki i/lub wentylatora. Dostępna jest również dedykowana osłona przeciwsłoneczna, a przewlekany uchwyt zapewni ochronę okablowania (przepusty kablowe PG9 i PG11). Kompletny uchwyt zbudowany z poszczególnych komponentów stanowi wyspecyfikowany w tabelach model tym samym znacznie ułatwiając dobór.

Całość wykonana w wyjątkowo estetycznej i nowoczesnej formie.

Szczegółowe informacje dotyczące urządzeń pod adresem **http://62.29.172.250**

Informacje ogólne	
Mocowanie kamery	Otwory montażowe na regulowanych prowadnicach
Maksymalny rozmiar kamery	Kompatybilne z kombinacjami kamer/obiektywów (wliczając złącze BNC) do 22,86×7,28×7,62 cm
Szyba przednia	3 mm grubości Lexan
Wejścia przewodów	1 x PG9, 1 x PG11 uszczelniane zaciskowo u dołu
Otwory wejściowe przewodów	Średnice: 1,91; 1,6 cm
Zaczep	Łączeniowo – blokujący nr 3
Konstrukcja	Wytłaczane aluminium odlewane kokilowo
Wykończenie	Pokrycie proszkowe szarym poliestrem
Środowisko pracy	Wewnątrz/na zewnątrz od –23° do 49°C
Zasilanie	24 V_{AC} / 230 V_{AC}
Długość bazowa/całkowita	33,99 cm / 36,55 cm
Masa (w zależności od opcji)	1,13 – 2,16 kg
Certyfikaty	Zgodne z CE Certyfikat UL/cUL Spełnia standard NEMA Type 4 Spełnia standard IP66

Schneider Electric Buildings Polska Sp. z o.o.
ul. Rzymowskiego 53
02-697 Warszawa
tel. (22) 313 24 10, faks (22) 313 24 11
e-mail: SEPLBuildings.Poland@buildings.schneider-electric.com
http://www.schneider-electric.com/buildings

3D
Wielobranżowe Przedsiębiorstwo Sp. z o.o.
ul. Kościuszki 27C
85-079 Bydgoszcz
tel. (52) 321 02 77
faks (52) 321 15 12
e-mail: biuro@3d.com.pl
www.3d.com.pl

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

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

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

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

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

ul. 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

ADT Fire and Security Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. (22) 430 83 01
faks (22) 430 83 02
e-mail: adtpoland@tycoint.com
www.adt.pl

ALARM SYSTEM
Marek Juszczyński
ul. Kolumba 59
70-035 Szczecin
tel. (91) 433 92 66
faks (91) 489 38 42
e-mail: biuro@bonelli.com.pl
www.bonelli.com.pl

ALARMNET 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

ALDOM F.U.H.
ul. Łanowa 63
30-725 Kraków
tel. (12) 411 88 88
faks (12) 294 18 88
e-mail: handel@aldom.pl
www.aldom.pl

ALPOL Sp. z o.o.
ul. H. Krahelskiej 7
40-285 Katowice
tel. (32) 790 76 56
Infolinia 0 801 77 77 90
faks (32) 790 76 61
e-mail: alpol@e-alpol.com.pl
www.e-alpol.com.pl

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

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

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

Al. Solidarności 15b, 25-323 **Kielce**
tel. (32) 720 39 82
faks (32) 790 76 94
e-mail: kielce@e-alpol.com.pl

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

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

ul. Wigury 21, 90-319 **Łódź**
tel. (32) 790 76 25
faks (32) 790 76 66
e-mail: lodz@e-alpol.com.pl

ul. Kutrzeby 16G, 61-714 **Poznań**
tel. (32) 790 76 37
faks (32) 790 76 70
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. Modzelewskiego 35/U9, 02-679 **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

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

AMBIENT SYSTEM Sp. z o.o.
ul. Sucha 25
80-531 Gdańsk
tel. (58) 345 51 95
faks (58) 344 45 95
e-mail: sekretariat@ambientsystem.pl
www.ambientsystem.pl

ANB Sp. z o.o.
ul. Ostrobramska 91
04-118 Warszawa
tel. (22) 612 16 16
faks (22) 612 29 30
e-mail: sekretariat@anb.com.pl
www.anb.com.pl

Zakład Produkcyjno-Usługowo-Handlowy ANMA s.c. Tomaszewscy
ul. Ostrowskiego 9
53-238 Wrocław
tel. (71) 363 17 53, faks wew. 7
e-mail: anma@anma-pl.eu
www.anma-pl.eu

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

ATLine Sp. J.
Krzysztof Cichulski, Sławomir Pruski
ul. Franciszkańska 125
91-845 Łódź
tel. (42) 657 30 80
faks (42) 655 20 99
e-mail: info@atline.com.pl
handel@atline.com.pl
www.atline.com.pl

Zakłady Kablowe BITNER
ul. Friedleina 3/3
30-009 Kraków
tel. (12) 389 40 24
faks (12) 380 17 00
e-mail: bitner@bitner.com.pl
www.bitner.com.pl

ROBERT BOSCH Sp. z o.o.
ul. Jutrzenki 105
02-231 Warszawa
tel. (22) 715 41 00/01
faks (22) 715 41 05
e-mail: securitysystems@pl.bosch.com
www.boschsecurity.pl

P.W.H. BRABORK Laboratorium Sp. z o.o.
ul. Postępu 2
02-676 Warszawa
tel. (22) 257 68 12
faks (22) 257 68 95
e-mail: brabork@braborklab.pl
www.braborklab.pl

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

LEGRAND POLSKA Sp. z o.o.
Tulipan House
ul. Domaniewska 50
02-672 Warszawa
tel. (22) 549 23 30
Infolinia 0 801 133 084
faks (22) 843 94 51
e-mail: info@legrand.com.pl
www.legrand.pl

C&C PARTNERS TELECOM Sp. z o.o.
ul. 17 Stycznia 119,121
64-100 Leszno
tel. (65) 525 55 55
faks (65) 525 56 66
e-mail: info@ccpartners.pl
www.ccpartners.pl

CAMSAT
ul. Garbary 5
86-050 Solec Kujawski
tel. (52) 387 36 58
tel. (52) 387 54 66, faks wew. 24
e-mail: camsat@camsat.com.pl
www.camsat.com.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: handlowy@cbcpoland.pl
www.cbcpoland.pl

CCX
ul. Ligocka 103
40-568 Katowice
tel. (32) 609 90 80
faks (32) 609 90 81
e-mail: biuro@ccx.pl
www.ccx.pl
www.zamkielektryczne.pl

Centrum Monitorowania Alarmów
ul. Puławska 359
02-801 Warszawa
tel. (22) 546 0 888
faks (22) 546 0 619
e-mail: warszawa@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 1 395
faks (12) 260 1 396

ul. Racławicka 82, 60-302 **Poznań**
tel./faks (61) 861 40 51
tel. kom. (0) 601 203 664
e-mail: poznan@cma.com.pl

Al. Niepodległości 659, 81-855 **Sopot**
tel. (58) 345 23 24
tel. kom. (0) 693 694 339
e-mail: sopot@cma.com.pl

COM-LM
ul. Ściegiennego 90
25-116 Kielce
tel. (41) 368 71 90
faks (41) 368 71 12
e-mail: biuro@com-lm.pl
www.com-lm.pl

CONTROL SYSTEM FMN Sp. z o.o.
Al. Komisji Edukacji Narodowej 96 lok. U15
02-777 Warszawa
tel. (22) 855 00 17
faks (22) 855 00 19
e-mail: biuro@cs.pl
www.cs.pl

Przedsiębiorstwo Usług Technicznych D-2 s.c.
K. Kolin, B. Czechowska
ul. Bukowa 1
40-108 Katowice
tel. (32) 253 99 10
faks (32) 253 70 85
e-mail: dravisdravis@neostrada.pl
www.dravis.pl

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

D+H Polska Sp. z o.o.
ul. Polanowicka 54
51-180 Wrocław
tel. (71) 323 52 50
faks (71) 323 52 40
e-mail: dh-polska@dh-partner.com
www.dhpolska.pl

Oddziały:
ul. Hagera 41, 41-800 **Zabrze**
tel. (32) 375 05 70
faks (32) 375 05 71

ul. Płochocińska 19 lok. 44-45, 03-191 **Warszawa**
tel. (22) 614 39 52
faks (22) 614 39 64

ul. Kielnieńska 134 A, 80-299 **Gdańsk**
tel. (58) 554 47 46
faks (58) 552 45 24

ul. Narutowicza 59, 90-130 **Łódź**
tel. (42) 678 01 32
faks (42) 678 09 20

ul. J. Bema 5A, 73-110 **Stargard Szczeciński**
tel. (91) 561 32 02
faks (91) 561 32 29

ul. Wołczyńska 18, 60-003 **Poznań**
tel. (61) 863 82 08
faks (61) 866 64 16

DANTOM s.c.
ul. Popiełuszki 6
01-501 Warszawa
tel./faks (22) 869 42 70
e-mail: biuro@dantom.com.pl
www.dantom.com.pl

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

DOM Polska Sp. z o.o.
ul. Krótka 7/9
42-200 Częstochowa
tel. (34) 360 53 64
faks (34) 360 53 67
e-mail: dom@dom-polska.pl
www.dom-polska.pl

JABLOTRON Ltd.
Generalny dystrybutor:
DPK System
ul. Piłsudskiego 41
32-020 Wieliczka
tel. (12) 288 23 75, 288 14 26, 278 18 86
faks (12) 278 48 91
e-mail: jablotron@jablotron.pl
www.jablotron.pl

Przedsiębiorstwo DYSKAM Sp. z o.o.
ul. Reymonta 22
30-059 Kraków
tel. (12) 637 80 20
faks (12) 637 80 20 wew. 23
e-mail: dyskam@dyskam.com.pl
www.dyskam.com.pl

DYSKRET Sp. z o.o.
ul. Mazowiecka 131
30-023 Kraków
tel. (12) 423 31 00
tel. kom. (0) 501 510 175
faks (12) 423 44 61
e-mail: office@dyskret.com.pl
www.dyskret.com.pl

EBS Sp. z o.o.
ul. Bronisława Czecha 59
04-555 Warszawa
tel. (22) 812 05 05
faks (22) 812 62 12
e-mail: office@ebs.pl, j.haschka@ebs.pl
www.ebs.pl

EDP Support Polska Sp. z o.o.
ul. Chłapowskiego 33
02-787 Warszawa
tel. (22) 644 53 90
faks (22) 644 35 66
e-mail: katarzyna.osiecka@edps.com.pl
www.edps.com.pl

ela-compil Sp. z o.o.
ul. Słoneczna 15 A
60-286 Poznań
tel. (61) 869 38 50
faks (61) 861 47 40
e-mail: office@ela.pl
www.ela-compil.pl

EL-MONT A. Piotrowski
ul. Wyzwolenia 15
44-200 Rybnik
tel. (32) 42 23 889
faks (32) 42 30 729
e-mail: el-mont@el-mont.com
www.el-mont.com

Przedsiębiorstwo Handlowo-Usługowe
ELPROMA Sp. z o.o.
ul. Syta 177
02-987 Warszawa
tel./faks (22) 312 06 00 ÷ 02
e-mail: elproma@elproma.pl
www.elproma.pl

ELTCRAC
Centrum Zabezpieczeń
Systemy Domofonowe
ul. Ruciana 3
30-803 Kraków
tel. (12) 292 48 60/61, 292 48 70
faks (12) 292 48 62, 292 48 65
e-mail: biuro@eltcrac.com.pl
www.eltcrac.com.pl

ELZA ELEKTROSYSTEMY
ul. Ogrodowa 13
34-400 Nowy Targ
tel. (18) 264 04 60
faks (18) 264 92 71
e-mail: elza@ceti.pl
www.elza.com.pl

EMU Sp. z o.o.
ul. Twarda 12
80-871 Gdańsk
tel. (58) 344 04 01÷03
faks (58) 344 88 77
e-mail: gdansk@emu.com.pl
www.emu.com.pl

Oddział:
ul. Jana Kazimierza 61, 01-267 **Warszawa**
tel. (22) 836 54 05, (22) 837 75 93
tel. kom. 0 602 222 516
e-mail: warszawa@emu.com.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

FACTOR SECURITY Sp. z o.o.
ul. Garbary 14B
61-867 Poznań
tel. (61) 850 08 00
faks (61) 850 08 04
e-mail: factor@factor.pl
www.factor.pl

Oddziały:
ul. Morelowa 11A, 65-434 **Zielona Góra**
tel. (68) 452 03 00
tel./faks (68) 452 03 01
e-mail: factor.zg@factor.pl

ul. Grabiszyńska 66e, 53-504 **Wrocław**
tel. (71) 78 74 741
faks (71) 78 74 742
e-mail: factor.wr@factor.pl

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

GV POLSKA Sp. z o.o.
ul. Kuropatwy 26B
02-892 Warszawa
tel. (22) 831 56 81, 636 13 73
faks (22) 831 28 52
tel. kom. 693 029 278
e-mail: warszawa@gv.com.pl
www.gv.com.pl

ul. Lwowska 74a
33-300 **Nowy Sącz**
tel. (18) 444 35 38, 444 35 39, 444 35 83
faks (18) 444 35 84
tel. kom. 695 583 424
e-mail: nowysacz@gv.com.pl

ul. Racławicka 60a
53-146 **Wrocław**
tel. (71) 361 66 02
faks (71) 361 66 23
tel. kom. 695 583 292
e-mail: wroclaw@gv.com.pl

HSA SYSTEMY ALARMOWE
Leopold Rudziński
ul. Langiewicza 1
70-263 Szczecin
tel. (91) 489 41 81
faks (91) 489 41 84
e-mail: biuro@hsa.pl
www.hsa.pl

ICS Polska
ul. Żuławskiego 4/6
02-641 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

ISM EuroCenter S.A.
ul. Wyczółki 71
02-820 Warszawa
tel. (22) 548 92 40
faks (22) 548 92 82
e-mail: ism@ismeurocenter.com
www.ismeurocenter.com

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

KABE Systemy Alarmowe Sp. z o.o.
ul. Waryńskiego 63
43-190 Mikołów
tel. (32) 324 89 46
faks (32) 324 89 01
e-mail: systemy@kabe.pl
www.kabe.pl/1

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

Systemy Alarmowe
KOLEKTOR Sp. z o.o.
ul. Gen. Hallera 2b/2
80-401 Gdańsk
tel. (58) 341 27 31, 341 47 18
faks (58) 341 44 90
e-mail: info@kolektor.com.pl
www.kolektor.com.pl

KOLEKTOR
K. Mikiciuk, R. Rutkowski Sp. J.
ul. Obrońców Westerplatte 31
80-317 Gdańsk
tel. (58) 553 67 59
faks (58) 553 48 67
e-mail: info@kolektor.pl
www.kolektor.pl

P.P.U.H. LASKOMEX
ul. Dąbrowskiego 249
93-231 Łódź
tel. (42) 671 88 00
faks (42) 671 88 88
e-mail: handel@laskomex.com.pl
www.laskomex.com.pl

MAXBAT Sp. J.
ul. Nadbrzeżna 34A
58-500 Jelenia Góra
tel. (75) 764 83 53
faks (75) 764 81 53
e-mail: info@maxbat.pl
www.maxbat.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, 642 45 35
faks (75) 642 45 25
e-mail: info@micronix.pl
www.micronix.pl

NAPCO POLSKA
ul. Pszona 2
31-462 Kraków
tel. (12) 412 13 12
faks (12) 410 05 10
e-mail: napco@napco.pl
www.napco.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

OBIS CICHOCKI ŚLĄZAK Sp. J.
ul. Rybnicka 64
52-016 Wrocław
tel. (71) 341 98 54
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. Grunwaldzka 119, 60-313 **Poznań**
tel. (61) 657 93 60
e-mail: poznan@omc.com.pl

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

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

P.P.H. PETROSIN Sp. z o.o.
ul. Rysi Stok 8/2
30-237 Kraków
tel. (12) 266 87 92
faks (12) 266 99 26
e-mail: office@petrosin.pl
www.petrosin.pl

Oddziały:
ul. Fabryczna 22, 32-540 **Trzebinia**
tel./faks (32) 618 02 00, 618 02 02

ul. Chemików 1, 32-600 **Oświęcim**
tel. (33) 847 30 83
faks (33) 847 29 52

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. Dzielna 1
00-162 Warszawa
tel. (22) 831 15 35
faks (22) 831 73 36
e-mail: biuro@polital.pl
www.polital.com.pl

POLON-ALFA
Zakład Urządzeń Dozymetrycznych Sp. z o.o.
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

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

PULSAR K. Bogusz Sp. J.
Siedlec 150
32-744 Łapczyca
tel. (14) 610 19 40
faks (14) 610 19 50
e-mail: biuro@pulsarspj.com.pl
www.pulsarspj.com.pl
www.zasilacze.pl

P.P.H. PULSON
ul. Czerniakowska 18
00-718 Warszawa
tel. (22) 851 12 20
faks (22) 851 12 30
e-mail: biuro@pulson.com.pl
www.pulson.eu

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

ROPAM Elektronik s.c.
Os. 1000-lecia 6A/1
32-400 Myślenice
tel. (12) 379 34 47
tel./faks (12) 272 39 71
e-mail: biuro@ropam.com.pl
www.ropam.com.pl

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

SATIE
ul. Łączyny 3
02-820 Warszawa
tel. (22) 462 30 86
faks (22) 314 69 50
e-mail: info@satie.pl
www.satie.pl

SAWEL Elektroniczne Systemy Zabezpieczeń
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

SCHRACK SECONET POLSKA Sp. z o.o.
ul. Wołoska 9
02-583 Warszawa
tel. (22) 33 00 620 ÷ 623
faks (22) 33 00 624
e-mail: warszawa@schrack-seconet.pl
www.schrack-seconet.pl

Oddziały:
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

P.T.H. SECURAL
ul. Gen. K. Pułaskiego 4
41-205 Sosnowiec
tel. (32) 291 86 17
tel./faks (32) 291 88 10
e-mail: info@secural.com.pl
www.secural.com.pl

S.M.A.
System Monitorowania Alarmów 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

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

SCHNEIDER ELECTRIC BUILDINGS POLSKA Sp. z o.o.
ul. Rzymowskiego 53
02-697 Warszawa
tel. (22) 313 24 10
faks (22) 313 24 11
e-mail:
SEPLBuildings.Poland@buildings.schneider-electric.com
www.schneider-electric.com/buildings

ul. Arkońska 6 bud. A2
80-387 **Gdańsk**
tel. (58) 782 00 00
faks (58) 782 00 04

ul. Rysia 1A
53-656 **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

SONY POLAND Sp. z o.o.
ul. Ogrodowa 58
00-876 Warszawa
tel. (22) 520 24 51
tel. kom. (0) 600 206 117
faks (22) 520 25 77
e-mail: marta.malecka@eu.sony.com
www.sonybiz.net/nvm

SPRINT Sp. z o.o.
ul. Jagiellończyka 26
10-062 Olsztyn
tel. (89) 522 11 00
faks (89) 522 11 25
e-mail: sprint@sprint.pl
www.sprint.pl

Oddziały:
ul. Przemysłowa 15, 85-758 **Bydgoszcz**
tel. (52) 365 01 01
faks (52) 365 01 11

ul. Budowlanych 64E, 80-298 **Gdańsk**
tel. (58) 340 77 00
faks (58) 340 77 01

ul. Heyki 27C, 70-631 **Szczecin**
tel. (91) 485 50 00
faks (91) 485 50 12

ul. Canaletta 4, 00-099 **Warszawa**
tel. (22) 826 62 77
faks (22) 827 61 21

S.P.S. Trading Sp. z o.o.
ul. Wał Miedzeszyński 630
03-994 Warszawa
tel. (22) 518 31 50
faks (22) 518 31 70
e-mail: warszawa@spstrading.pl
www.aper.com.pl

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

ul. Kościuszki 227, 40-600 **Katowice**
tel. (32) 255 64 27
faks (32) 255 64 52
e-mail: katowice@spstrading.pl

ul. Inflancka 6, 91-857 **Łódź**
tel. (42) 617 00 32
faks (42) 659 85 23
e-mail: lodz@spstrading.pl

ul. Dąbrowszczaków 2A, 10-541 **Olsztyn**
tel. (89) 527 92 72
faks (89) 527 92 30
e-mail: olsztyn@spstrading.pl

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

ul. Grudziądzka 176, 87-100 **Toruń**
tel. (56) 653 99 43
faks (56) 653 90 81
e-mail: torun@spstrading.pl

ul. Inowrocławska 39C, 53-649 **Wrocław**
tel. (71) 348 44 64
faks (71) 348 36 35
e-mail: wroclaw@spstrading.pl

STRATUS
ul. Nowy Świat 38
20-419 Lublin
tel./faks (81) 743 87 72
e-mail: stratus@stratus.lublin.pl
www.stratus.lublin.pl

SYSTEM 7
ul. Krakowska 33
43-300 Bielsko-Biała
tel. (33) 821 87 77
Infolinia 801 000 307
faks (33) 816 91 88
e-mail: biuro@s7.pl
www.system7.pl
Internetowa Hurtownia Zabezpieczeń:
www.system7.biz

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

Biuro Handlowe:
ul. Rzymowskiego 30, 02-697 **Warszawa**
tel. (22) 843 83 95
faks (22) 843 79 12
e-mail: tap5@tap.com.pl

TAYAMA POLSKA Sp. J.
ul. Słoneczna 4
40-135 Katowice
tel. (32) 258 22 89, 357 19 10, 357 19 20
faks (32) 357 19 11, 357 19 21
e-mail: biuro@tayama.com.pl
www.tayama.com.pl

TECHNOKABEL S.A.
ul. Nasielska 55
04-343 Warszawa
tel. (22) 516 97 77
Sprzedaż: (22) 516 97 97
faks (22) 516 97 87
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl

TP TELTECH Sp. z o.o.
ul. Tuwima 36
90-941 Łódź
tel. (42) 639 83 60
faks (42) 639 89 85
e-mail: teltechinfo@tpteltech.pl
www.tpteltech.pl

Oddziały:
al. Wyzwolenia 70, 71-510 **Szczecin**
tel./faks (91) 423 70 55
e-mail: witold.brzozowski@telekomunikacja.pl

ul. Rzeczypospolitej 5, 59-220 **Legnica**
tel. (76) 856 60 71
faks (76) 856 60 71
e-mail: marian.sitko@telekomunikacja.pl

ul. Nasypowa 12, 40-551 **Katowice**
tel. (32) 202 30 50
faks (32) 201 13 17
e-mail: dariusz.gawor@telekomunikacja.pl

ul. Rakowicka 51, 31-510 **Kraków**
tel. (12) 431 59 01
faks (12) 423 97 65
e-mail: marek.zembaty@telekomunikacja.pl

ul. Kosmonautów 82, 20-358 **Lublin**
tel. (81) 745 39 83
faks (81) 745 39 78
e-mail: zbigniew.chodkiewicz@telekomunikacja.pl

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

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

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
3D	TAK	TAK	–	–	TAK
AAT Holding	–	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	–
ADT Fire and Security	TAK	TAK	TAK	TAK	TAK
Alarm System	TAK	–	TAK	TAK	–
Alarmnet	–	TAK	TAK	–	TAK
Alarmtech Polska	TAK	TAK	–	–	TAK
Aldom	–	TAK	TAK	TAK	TAK
Alkam System	TAK	TAK	TAK	TAK	–
Alpol	–	–	TAK	–	TAK
Ambient System	TAK	TAK	TAK	TAK	TAK
ANB	–	TAK	TAK	TAK	–
Anma	–	TAK	–	TAK	TAK
ASSA ABLOY	–	–	TAK	–	–
Atline	–	TAK	TAK	TAK	TAK
Bitner Zakłady Kablowe	TAK	–	–	–	–
BOSCH	TAK	–	TAK	–	–
P.W.H. Brabork - Laboratorium	–	TAK	TAK	TAK	–
bt electronics	TAK	TAK	TAK	TAK	TAK
C&C Partners	–	TAK	TAK	–	TAK
CAMSAT	TAK	TAK	–	–	TAK
CBC Poland	TAK	–	TAK	–	TAK
CCX	–	TAK	TAK	TAK	TAK
CMA	TAK	TAK	TAK	TAK	–
COM-LM	TAK	TAK	TAK	TAK	–
CONTROL SYSTEM FMN	–	TAK	TAK	TAK	TAK
D-2	–	TAK	TAK	TAK	–
D-MAX	–	TAK	TAK	–	TAK
D+H Polska	–	TAK	TAK	TAK	TAK
DANTOM	TAK	–	TAK	–	–
DG Elpro	–	TAK	TAK	TAK	TAK
DOM Polska	TAK	TAK	TAK	–	–
DPK System	–	–	TAK	TAK	TAK
Dyskam	TAK	TAK	–	TAK	TAK
Dyskret	–	TAK	TAK	TAK	TAK
EBS	TAK	–	TAK	–	–
EDP Support Polska	TAK	TAK	TAK	TAK	TAK
ela-compil	TAK	–	TAK	–	TAK
El-Mont	–	TAK	–	TAK	–
Elproma	–	TAK	–	TAK	–
Eltcrac	TAK	TAK	TAK	TAK	TAK
Elza Elektrosystemy	–	TAK	–	TAK	TAK
Emu	–	–	TAK	–	–
Eureka	–	TAK	–	TAK	–
Factor Polska	–	–	TAK	–	TAK
FES	–	TAK	TAK	TAK	–
GDE Polska	–	–	TAK	–	TAK

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
GV Polska	–	–	TAK	–	TAK
HSA	–	–	TAK	–	–
ICS Polska	–	–	TAK	–	TAK
Insap	–	TAK	TAK	TAK	TAK
ISM EuroCenter	–	–	TAK	–	–
Janex International	–	–	TAK	–	–
KABE	–	TAK	TAK	TAK	TAK
KATON	–	–	TAK	–	TAK
Kolektor	–	TAK	–	TAK	–
Kolektor MR	–	TAK	TAK	TAK	–
Laskomex	TAK	TAK	TAK	–	TAK
Legrand Polska	TAK	TAK	TAK	–	TAK
MAXBAT	TAK	TAK	TAK	TAK	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	TAK	TAK	–	–
NAPCO	–	–	TAK	TAK	TAK
Nuuxe – Radioton	–	–	TAK	–	–
OBIS	–	TAK	TAK	TAK	TAK
OMC INDUSTRIAL	–	–	TAK	–	–
Petrosin	–	TAK	–	TAK	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	–	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	TAK	–	–
PPH Pulson	TAK	TAK	TAK	–	–
Ramar	TAK	–	TAK	TAK	TAK
ROPAM Elektronik	TAK	–	TAK	–	–
Satel	TAK	–	–	–	–
SATIE	TAK	–	TAK	–	TAK
Sawel	–	TAK	TAK	TAK	TAK
Schrack Seconet Polska	TAK	–	–	–	TAK
Secural	TAK	TAK	TAK	–	TAK
S.M.A.	–	TAK	–	TAK	–
Schneider Electric Buildings Polska	TAK	TAK	TAK	TAK	TAK
Sony	TAK	–	–	–	–
Sprint	–	TAK	TAK	TAK	–
S.P.S. Trading	TAK	–	TAK	–	TAK
STRATUS	–	TAK	TAK	–	TAK
SYSTEM 7	TAK	–	TAK	–	–
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Tayama	–	–	TAK	–	–
Technokabel	TAK	–	–	–	–
TP TELTECH	–	TAK	TAK	TAK	–
W2	TAK	TAK	TAK	–	–
Vision Polska	–	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
3D	–	TAK	–	–	–	–	–	–	–
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, systemy rejestracji gości, karty magnetyczne i zbliżeniowe								
ADT Fire and Security	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Alarm System	TAK	TAK	TAK	–	–	–	–	–	–
Alarmnet	TAK	TAK	TAK	–	–	TAK	–	TAK	–
Alarmtech Polska	TAK	–	–	–	–	–	–	–	–
Aldom	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Ambient System	TAK	TAK	TAK	TAK	–	–	–	–	TAK
ANB	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Anma	TAK	TAK	TAK	TAK	–	TAK	–	–	–
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
ATLine	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–
Bitner Zakłady Kablowe	kable i przewody do SSWiN, systemów telewizji dozorowej, kontroli dostępu i in.								
BOSCH	TAK	TAK	–	TAK	–	–	TAK	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
bt electronics	–	–	TAK	–	–	–	–	TAK	–
C&C Partners	TAK	TAK	TAK	–	TAK	TAK	TAK	–	–
CAMSAT	–	TAK	–	–	–	–	TAK	–	–
CBC Poland	–	TAK	–	–	–	–	–	–	–
CCX	–	–	TAK	–	–	–	–	TAK	–
CMA	TAK	–	–	–	–	–	TAK	–	–
COM-LM	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
Control System FMN	TAK	TAK	TAK	–	–	TAK	–	TAK	–
D-2	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
D-MAX	–	TAK	–	–	–	–	–	–	–
D+H Polska	–	–	–	TAK	–	–	–	TAK	TAK
DANTOM	TAK	TAK	TAK	TAK	–	–	–	TAK	–
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
DOM Polska	–	–	TAK	–	–	–	–	TAK	–
DPK System	TAK	–	–	–	–	–	–	–	–
Dyskam	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
Dyskret	TAK	TAK	TAK	TAK	–	TAK	–	TAK	TAK
EBS	TAK	–	TAK	TAK	–	TAK	TAK	–	–
EDP Support Polska	TAK	TAK	TAK	–	TAK	TAK	–	TAK	–
ela-compil	–	–	–	–	–	TAK	–	–	–
El-Mont	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Eltcrac	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–
Elza Elektrosystemy	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Emu	akumulatory bezobsługowe do zasilania awaryjnego urządzeń alarmowych								
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
Factor Polska	TAK	TAK	TAK	TAK	TAK	–	–	–	–
FES	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
GDE Polska	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
GV Polska	–	TAK	TAK	–	–	–	TAK	–	–
HSA	TAK	TAK	TAK	–	–	–	–	–	–
ICS Polska	TAK	TAK	TAK	–	–	–	–	–	–
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
ISM EuroCenter	–	TAK	TAK	–	–	TAK	TAK	–	–
Janex International	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
KATON	–	TAK	TAK	–	–	TAK	–	–	–
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Laskomex	–	TAK	TAK	–	–	–	–	TAK	–
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MAXBAT	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	TAK	–	–	–	TAK	–
NAPCO	TAK	TAK	TAK	TAK	–	–	–	–	–
Nuuxe – Radioton	–	TAK	–	–	–	TAK	–	–	–
OBIS	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	–	–	–	–	TAK	–
Petrosin	TAK	TAK	TAK	–	–	–	–	–	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	–	–	–	–	–	–	–	TAK	–
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	–	–	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
PPH Pulson	TAK	–	–	–	–	TAK	TAK	–	–
Ramar	TAK	TAK	TAK	–	TAK	–	TAK	–	–
ROPAM Elektronik	TAK	–	TAK	TAK	–	–	TAK	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
SATIE	–	–	TAK	–	–	–	–	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.M.A.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Schneider Electric Buildings Polska	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
Sony	–	TAK	–	–	–	–	TAK	–	–
Sprint	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	–	TAK	TAK	TAK	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
SYSTEM 7	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	TAK	–	TAK	–	–	–	–	–	–
Tayama	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Technokabel	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
TP TELTECH	TAK	TAK	TAK	TAK	TAK	–	TAK	–	–
W2	TAK	–	–	TAK	–	–	–	–	–
Vision Polska	–	–	–	TAK	–	–	–	–	–

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktor merytoryczny
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

Redaguje zespół
Krzysztof Białek
Marek Blim
Patryk Gańko
Norbert Góra
Ryszard Sobierski
Waldemar Szulc
Adam Wojcinowicz
Marek Życzkowski

Współpraca zagraniczna
Rafał Niedzielski

Współpraca
Marcin Buczaj
Adam Bułaciński
Piotr Czernoch
Marcin Pyclik
Adam Rosiński
Sławomir Wagner
Andrzej Wójcik

Skład i łamanie
Marek Bladoszewski

Korekta
Paweł Karczmarzyk

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

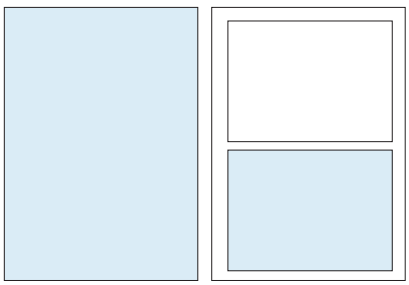
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. (22) 546 0 546
faks (22) 546 0 501

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

Cennik reklam

Reklama wewnątrz czasopisma:

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

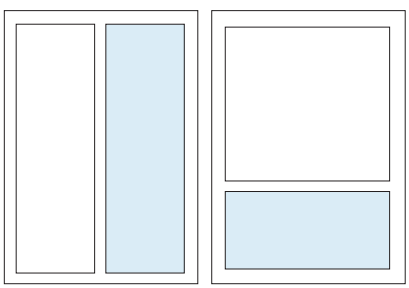


cała strona (200 x 282 mm + 3mm spad)

1/2 strony (170 x 125 mm)

Artykuł sponsorowany:

indywidualne negocjacje (forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)

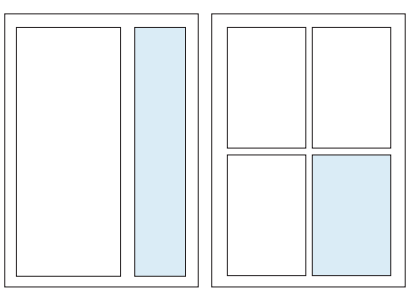


1/2 strony (83 x 260 mm)

1/3 strony (170 x 80 mm)

Reklama na okładkach:

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



1/3 strony (54 x 260 mm)

1/4 strony (83 x 125 mm)

Spis teleadresowy:

jednorazowy wpis 70 zł

Redakcja przyjmuje zamówienia na minimum 6 kolejnych emisji

W przypadku zamówienia na 12 emisji 10% rabat

Podane ceny nie uwzględniają podatku VAT (22%)

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

Spis reklam

Międzynarodowe Targi Poznańskie

spotkaj przyszłość

securex
POLAND

Międzynarodowa Wystawa Zabezpieczeń

26 – 29 kwietnia 2010

Największe targi branży zabezpieczeń w Polsce i Europie Środkowej

SECUREX – BĄDŹ O KROK PRZED ZAGROŻENIEM

www.securex.pl

Międzynarodowe Targi Poznańskie sp. z o.o.
ul. Głogowska 14; 60-734 Poznań

Potrzebuję

bezproblemowych rozwiązań dostępu, które oszczędzają pieniądze i zwiększają produktywność.

HID Global dostarcza bezpieczeństwo

w wygodnej i przyjaznej dla użytkownika formie, dzięki czemu łatwiej niż kiedykolwiek można otworzyć drzwi czy uruchomić Windows®.

Jako zaufane źródło HID Global zrewolucjonizował fizyczną kontrolę dostępu poprzez dostarczenie bezpiecznego i wygodnego sposobu dostępu do drzwi. Korzystając z doświadczeń tych samych użytkowników, HID aktualnie rewolucjonizuje dostęp logiczny. HID on the Desktop™ zapewnia użytkownikowi przyjazny i bezpieczny dostęp do Windows® oraz sieci IT poprzez użycie tej samej karty, która otwiera drzwi.

HID

Chcąc oszczędzić pieniądze i zwiększyć produktywność, odwiedź **hidglobal.com/convergencesolutions**