CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 1(83)/2012

ZABEZPIECZENIA

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

W NUMERZE:

Maksymalna szybkość i precyzja nadzoru o znaczeniu strategicznym? **To proste.**

Zarządzanie bezpieczeństwem obiektów o znaczeniu strategicznym to zadanie skomplikowane i poważne. Kamery muszą poradzić sobie ze wszystkim. Bez żadnych niedociągnięć.

Kamery Axis z linii Q z funkcjami obrót/pochylenie/zbliżenie stanowią najbardziej zaawansowane na rynku sieciowe rozwiązanie nadzoru wizyjnego o intuicyjnej instalacji i niezawodnym działaniu. W rzeczywistości kamery z zasilaniem przez sieć Ethernet i gotowe do działania na zewnątrz zaraz po wyjęciu z pudełka oszczędzają czas, pieniądze i eliminują problemy.

Materiał wizyjny o jakości HDTV, wysokiej klasy obrót/pochylenie/zbliżenie i inteligentne technologie – takie jak automatyczne śledzenie, zaawansowana funkcja strażnika, rejestracja tras strażnika oraz wykrywanie dźwięku – zapewniają świetną kontrolę, szybkość i efektywność. Nic nie umknie Państwa uwadze.

Zero zamieszania. Pełna kontrola. Łatwy wybór.

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

Kopułkowa kamera sieciowa PTZ AXIS z serii Q60 • Jakość materiału wizyjnego do poziomu HDTV 1080p • WDR • Szybki obrót i pochylenie • Zoom optyczny do 35x • Zasilanie High PoE • Funkcja Arctic Temperature Control • Ochrona klasy IP

AXIS COMMUNICATIONS

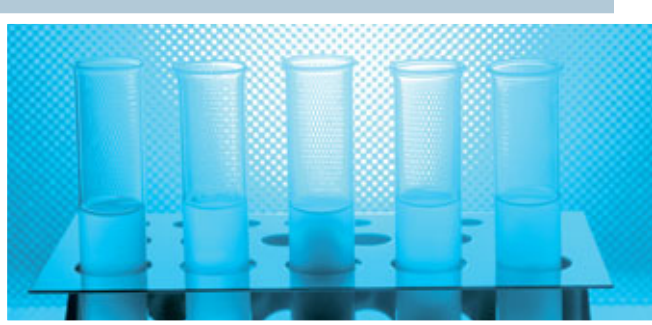
Spis treści

CZASOPISMO ZABEZPIECZENIA 1/2012

Cień GPS
– podąża za obiektem jak cień **22**

Rewolucja sektora nadzoru wizyjnego **24**

Sieciowe systemy wizyjne
– nowe możliwości biznesowe
dla instalatorów i integratorów **28**



DNA w walce z przestępczością **56**

POLALARM i MTP zapraszają na konferencję

Serdecznie zapraszamy do udziału w **II Konferencji Zarządzania Bezpieczeństwem Obiektów i Informacji** „Najnowsze kierunki zastosowania zarządzania bezpieczeństwem w praktyce", która odbędzie się **24 kwietnia 2012 r.** (w drugi dzień Międzynarodowej Wystawy Zabezpieczeń SECUREX 2012) na terenie Międzynarodowych Targów Poznańskich (MTP).

Konferencję organizuje Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „**POLALARM**" oraz **MTP**.

Będzie to już druga konferencja z cyklu poświęconego zarządzaniu bezpieczeństwem w praktyce. Pragniemy zwrócić uwagę szerokiego grona przedsiębiorców na możliwość diametralnej poprawy bezpieczeństwa przy minimalnych nakładach – w myśl zasady „tak wiele za tak niewiele". Stanowi to przykład doskonałej inwestycji we własną wiedzę, mającej na celu poprawę bezpieczeństwa własnej firmy. Uznając tę tematykę za niezwykle istotną dla poprawy bezpieczeństwa, planujemy kontynuację tego cyklu w przyszłości.

Proponowany program konferencji:

Wprowadzenie: O konieczności rozpowszechniania w Polsce wiedzy o zarządzaniu bezpieczeństwem;

1) Dlaczego świat uznaje zarządzanie bezpieczeństwem za najważniejszy czynnik ochrony;
2) Szczególne znaczenie zarządzania bezpieczeństwem w sytuacjach kryzysowych;
3) Zarządzanie bezpieczeństwem inteligentnych obiektów jako nowa forma bezinwestycyjnego podnoszenia poziomu bezpieczeństwa;
4) Zastosowanie koncepcji zarządzania bezpieczeństwem do projektowania osiedli oraz zespołów budynków mieszkalnych i wyposażania ich w różne systemy zabezpieczeń;
5) Zarządzanie bezpieczeństwem powodziowym przez rozbudowę systemu monitoringu alarmowego w Polsce;
6) Znaczenie wprowadzenia zarządzania bezpieczeństwem dla poprawy zabezpieczenia informacji i danych osobowych w Polsce;
7) Kompleksowe zarządzanie bezpieczeństwem w Polsce z wykorzystaniem Krajowego Systemu Informatycznego;
8) Rola zarządzania bezpieczeństwem w projektowanej zmianie przepisów budowlanych w Polsce;
9) Rola normalizacji europejskiej i międzynarodowej w kreowaniu zarządzania bezpieczeństwem;
10) Uwzględnianie w normach branżowych zarządzania bezpieczeństwem w różnych dziedzinach, jako ważna kwestia wynikająca z rozwoju cywilizacyjnego świata;
11) Wykorzystanie metod zarządzania bezpieczeństwem informacji niejawnych w zarządzaniu bezpieczeństwem informacji jawnych w ekstremalnie trudnych warunkach;
12) Usprawnienie zarządzania bezpieczeństwem obiektów i informacji przez wprowadzenie oceny stanu bezpieczeństwa w oparciu o międzynarodowe przepisy dotyczące audytów;
13) Zarządzanie bezpieczeństwem z zastosowaniem systemów wykrywania ulotów informacji oraz metody ochrony przed ulotami;
14) Zarządzanie bezpieczeństwem obiektów podstawą prowadzenia działalności przez przedsiębiorców – analiza ryzyk, eliminowanie błędów, właściwy dobór zabezpieczeń;
15) Specyfika usług kształtowania inteligentnych obiektów oraz zarządzania ich bezpieczeństwem jako nowy kierunek usług technicznych w Polsce;
16) Dyskusja i podsumowanie II konferencji.

Szczegółowy program konferencji oraz karta zgłoszenia uczestnictwa będą dostępne od marca 2012 r. na stronie Stowarzyszenia „POLALARM" – www.polalarm.org. Osoby, które zgłoszą chęć udziału w konferencji do Biura Zarządu Stowarzyszenia „POLALARM" – *polalarm@polalarm.com.pl*, tel. 22 626 90 31, 22 625 57 43, otrzymają zaproszenie, program oraz kartę zgłoszenia uczestnictwa na swój adres e-mail.

Bezpośr. inf. POLALARM

Nowy interfejs komunikacyjny TCP/IP do systemu RACS4 firmy ROGER

Firma **ROGER**, wiodący dostawca urządzeń do systemów kontroli dostępu, poszerza swoją ofertę o nowy **interfejs komunikacyjny TCP/IP**, o nazwie **UT-4DR**. Interfejs ten jest następcą popularnego modułu UT-4 i będzie oferowany w znacznie niższej cenie niż jego poprzednik.

UT-4DR umożliwia komunikację z systemem kontroli dostępu RACS4 za pośrednictwem sieci komputerowej LAN/WAN 10/100 BaseT Ethernet. Może on pracować zarówno ze stałym, jak i dynamicznym adresem IP, a jego konfiguracja odbywa się z poziomu przeglądarki internetowej.

Zastosowanie modułu UT-4DR pozwala budować rozproszone systemy kontroli dostępu, co ma szczególne znaczenie w przypadku firm i instytucji posiadających oddziały w różnych, oddalonych od siebie lokalizacjach.

Oprócz pełnienia swej podstawowej funkcji – interfejsu komunikacyjnego – urządzenie udostępnia cztery linie zewnętrzne, które w zależności od potrzeb konkretnej aplikacji mogą być skonfigurowane jako dwustanowe wejścia lub wyjścia. Sterowanie liniami wyjściowymi oraz odczyt stanu linii wejściowych mogą być realizowane za pośrednictwem przeglądarki internetowej lub z użyciem komend protokołu Telnet. Właściwość ta stwarza warunki do wykorzystania modułu poza systemem kontroli dostępu RACS jako zdalnego portu WE-WY sterowanego za pośrednictwem sieci komputerowej.

Układ elektroniczny modułu bazuje na nowoczesnym 32-bitowym procesorze o architekturze ARM.

Urządzenie jest oferowane w obudowie z tworzywa sztucznego przeznaczonej do montażu na szynie DIN 35 mm.

Bezpośr. inf. ROGER

W kwietniu spotykamy się w Poznaniu

securex 2012 POLAND
Międzynarodowe Targi Zabezpieczeń

Międzynarodowe Targi Zabezpieczeń SECUREX to największe i najbardziej prestiżowe targi branży zabezpieczeń w Polsce i w Europie Środkowej. Kolejna odsłona już od **23 do 26 kwietnia w Poznaniu.**

Co dwa lata Poznań zmienia się w międzynarodową arenę prezentacji najnowszych rozwiązań i technologii w zakresie zabezpieczeń. Targi SECUREX kierują swoją ofertę do wszystkich zainteresowanych usługami ochrony mienia i informacji, systemami wykrywania i zwalczania przestępczości lub systemami wizyjnego nadzoru (CCTV). Kwietniowa wystawa zostanie zlokalizowana w czterech pawilonach – 7, 7A, 8 i 8A na terenie Międzynarodowych Targów Poznańskich (MTP). Przejrzysty podział ekspozycji na sektory tematyczne z pewnością ułatwi zwiedzającym znalezienie interesujących ich firm. W jednym z pawilonów zaprezentowana zostanie oferta związana z mechanicznymi systemami zabezpieczeń, takimi jak sejfy, system ochrony zewnętrznej, ochrona bezpośrednia. W kolejnym pawilonie znajdą się instalacje służące do dozoru wizyjnego (CCTV); w innym – systemy sygnalizacji pożarowej. W tym roku po raz pierwszy pokazana będzie również ekspozycja związana z bezpieczeństwem IT.

Po wiedzę na targi

Targi SECUREX są platformą dla ważnych dyskusji merytorycznych. Bogaty program warsztatów i konferencji z udziałem specjalistów z branży pozwalają na przeprowadzenie debat na najwyższym poziomie. W ramach tegorocznego spotkania odbędą się po raz kolejny Mistrzostwa Polski Instalatorów Systemów Alarmowych i finał konkursu Polski Mistrz Techniki Alarmowej. Ponadto we współpracy z Urzędem Wojewódzkim planowana jest konferencja na temat bezpieczeństwa imprez masowych. Bezpieczeństwo bankowości oraz bezpieczeństwo muzeów i budowli sakralnych to tematy wykładów organizowanych przez Komendę Wojewódzką Policji i MTP. Nowością w programie jest rozszerzenie tematyki o seminaria poświęcone bezpieczeństwu IT. Poznańskie Centrum Superkomputerowo-Sieciowe wraz z Targami Poznańskimi przygotują seminarium dla kadry zarządzającej i warsztaty dla informatyków. Bardzo ciekawie zapowiada się również debata na temat prawnej regulacji zasad nadzoru wizyjnego w Polsce pod tytułem „Prawo dla monitoringu wizyjnego?". Dyskusja organizowana przez Polską Izbę Systemów Alarmowych (PISA) i MTP ma na celu uregulowanie możliwości przetwarzania i ochrony wizerunku osób oraz określenie minimalnych standardów funkcjonalności systemów telewizji dozorowej.

Premiery rynkowe w Poznaniu

Rozwój branży zabezpieczeń jest nierozerwalnie związany z postępem technologicznym oraz wdrażaniem innowacji. Odbywające się w cyklu dwuletnim targi są doskonałą okazją do zaprezentowania premier targowych oraz absolutnych nowości na rynku zabezpieczeń. – *Wzorem lat ubiegłych spodziewamy się bardzo dużej liczby zgłoszeń* – mówi **Joanna Jasińska**, dyrektor projektu.

Duże zainteresowanie wystawców

– *Targi od wielu lat cieszą się niesłabnącym zainteresowaniem. Ostatnia ich edycja dwa lata temu zgromadziła blisko 260 wystawców z 14 krajów. W porównaniu z analogicznym okresem 2010 roku o 35% wzrośnie zarówno powierzchnia wystawiennicza, jak i liczba wystawców* – dodaje Joanna Jasińska. Wszelkie niezbędne informacje można pobrać ze strony internetowej organizatora z zakładki „Informacje dla wystawców".

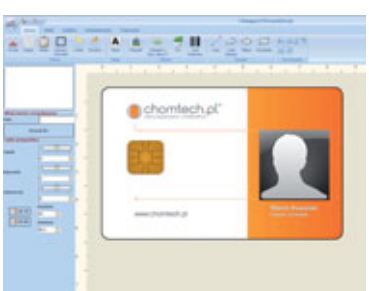
Złoty Medal w nowej odsłonie

Począwszy od stycznia, na MTP obowiązywać będzie nowa formuła Konkursu o Złoty Medal MTP. Wiąże się ona nie tylko z odświeżonym wizerunkiem medalu, ale przede wszystkim z całym pakietem unikatowych korzyści, na które liczyć mogą laureaci konkursu. Podstawową innowacją jest znacznie wcześniejszy termin wyłaniania laureatów. Lista produktów nagrodzonych złotym medalem będzie znana już na kilka tygodni przed rozpoczęciem targów. Wyniki Sądu Konkursowego na targach SECUREX zostaną ogłoszone w połowie lutego. Laureat Złotego Medalu otrzyma *Pakiet medalisty* – komplet materiałów promocyjnych, których wystawca będzie mógł użyć w kampanii promocyjnej. Gwarantem jakości nagrodzonych produktów będzie renomowane jury, w skład którego wchodzić będą eksperci z branży *security*. Przewodniczącym Sądu Konkursowego na targach SECUREX będzie prof. dr hab. inż. Bogdan Branowski z Politechniki Poznańskiej.

Bezpośr. inf. Katarzyna Jardanowska
Zespół PR i Promocji Produktów

Chomguard Personalizacja

Nowoczesna aplikacja do drukarek kart plastikowych: FARGO, EVOLIS



Firma **chomtech.pl** wprowadziła na rynek nową aplikację przeznaczoną do tworzenia barwnych i monochromatycznych projektów kart plastikowych (ze szczególnym uwzględnieniem nanoszenia na nie grafiki wektorowej oraz plików rastrowych, np. zdjęć, w wybranych formatach). Program umożliwia umieszczenie na karcie indywidualnych informacji o użytkowniku, np. danych personalnych lub zdjęcia. Chomguard Personalizacja ma wbudowaną bazę danych do seryjnego wydruku kart. Współpracuje z zewnętrznymi bazami danych (MS Access, MS Excel itp.) oraz programami graficznymi, jak CorelDRAW i Adobe Photoshop.

Aplikacja jest dostępna w kilku wersjach językowych.

Bezpośr. inf. chomtech.pl

Specyfikacja techniczna PKN-CLC/TS 50131-7 zatwierdzona i opublikowana w języku polskim

12 sierpnia 2009 r. Polski Komitet Normalizacyjny (PKN) ustanowił w języku polskim pierwszy arkusz normy PN-EN 50131-1:2009 *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe.* Jednocześnie wycofał starą normę PN-E-08390-14:1993 jako sprzeczną z postanowieniami normy europejskiej. Dla branży, a więc projektantów, instalatorów i inwestorów, oprócz pierwszego arkusza normy ważny jest również arkusz siódmy, w którym przedstawione są wytyczne co do stosowania danego systemu zabezpieczeń.

31 października 2011 r. polska wersja specyfikacji technicznej ***PKN-CLC/TS 50131-7:2011 Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 7: Wytyczne stosowania,*** wykonana przez PKN na zamówienie Polskiej Izby Systemów Alarmowych (projekt roboczy autorstwa Komitetu Technicznego nr 52 ds. Systemów Alarmowych Włamania i Napadu), została zatwierdzona przez prezesa PKN i opublikowana w języku polskim.

W treści wprowadzającej podkreśla się, że wytyczne stosowania mają być pomocne przy projektowaniu, instalacji, obsłudze i konserwacji systemu alarmowego sygnalizacji włamania i napadu. Zaleca się korzystanie z wytycznych stosowania wraz z normą podstawową PN-EN 50131-1:2009.

Wiele zapisów zawartych w specyfikacji znajduje swoje odzwierciedlenie w wymaganiach prawnych (rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 7 września 2010 r. *w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne*). Dotyczy to m.in. poświadczenia zgodności systemu, dokumentacji i konserwacji systemów.

Kompatybilność zapisów polskich norm z serii 50131, w tym specyfikacji technicznej PKN-CLC/TS 50131-7, z treścią rozporządzenia MSWiA z 7 września 2010 r. jest dla branży zabezpieczeń technicznych dobrym przykładem na spójność wymagań polskiego prawa z zasadami sztuki opisanymi w dokumentach normatywnych.

Wytyczne są przeznaczone dla osób odpowiedzialnych za wykonanie systemów w stopniu zabezpieczenia uważanym za odpowiedni oraz dla osób odpowiedzialnych za dobór urządzeń odpowiednich do wymaganego poziomu funkcjonalności i warunków środowiskowych, w których urządzenia te będą pracować.

Wytyczne są uporządkowane w kolejności logicznej odpowiadającej czynnościom towarzyszącym projektowaniu i instalowaniu systemów sygnalizacji włamania i napadu.

W siedmiu głównych rozdziałach zostały zawarte wytyczne co do: projektowania systemu, planowania instalacji, instalowania systemu, sprawdzania funkcjonalności i uruchomienia, dokumentacji systemu, obsługi oraz konserwacji i napraw.

Branża zabezpieczeń technicznych, po samodzielnych próbach wypełnienia luki w polskich wytycznych dotyczących profesjonalnego wykonywania systemów alarmowych włamania i napadu, otrzymała dokument współczesnej europejskiej myśli technicznej zawierający zalecenia jednakowo rozumiane przez wykonawców i zamawiających usługi zabezpieczenia technicznego zarówno rynku na krajowym, jak i europejskim.

Bezpośr. inf. PISA

Rejestratory wizyjne HD serii 700 gotowe do użycia rozwiązanie HD CCTV

Bosch Security Systems wprowadził na rynek szybkie, łatwe w obsłudze i gotowe do użycia urządzenie do zapisu obrazu HD i SD oraz zarządzania zarchiwizowanymi materiałami. Łatwe w konfiguracji i konserwacji **rejestratory wizyjne serii 700** spełniają wymagania najbardziej zaawansowanych zastosowań CCTV. Rejestratory posiadają cztery twarde dyski z możliwością ich wymiany z poziomu przedniego panelu urządzenia, zabezpieczenie RAID-4 oraz zaawansowane funkcje integracyjne, dzięki czemu stanowią idealne rozwiązanie przy zastosowaniach wymagających o wysokiej jakości nagranego obrazu.

Bezpłatne oprogramowanie *Bosch Video Klient* (BVC), dostarczane wraz z rejestratorami HD serii 700, znacznie ułatwia obsługę urządzeń. Intuicyjny interfejs z wieloma opcjami w formie przejrzystego menu jest łatwy do opanowania i obsługi. Oprogramowanie umożliwia zdalne odtwarzanie aktualnie zapisywanych obrazów oraz materiałów zarchiwizowanych w rozdzielczościach HD 1080p i 720p, a także SD oraz analogowych 4CIF/D1.

Nowe rejestratory HD serii 700 powstały w związku ze wzrastającym popytem na cyfrowe systemy nadzoru w formacie HD. Rejestratory sieciowe stanowią idealne rozwiązanie w przypadku środowisk bazujących wyłącznie na transmisji sieciowej. Zintegrowany i w pełni zautomatyzowany system zarządzania kamerami sieciowymi umożliwia obsługę 32 kamer z kompresją H.264. Z kolei

modele hybrydowe stanowią idealne i przyszłościowe rozwiązanie dla rosnącej liczby zastosowań wykorzystujących równocześnie kamery analogowe i sieciowe. Mogą one obsługiwać do 8 lub 16 kamer analogowych oraz dodatkowo 8 lub 16 kanałów IP.

Rejestratory serii 700 zapisują doskonałej jakości obraz CCTV, a przy tym ograniczają do minimum wymagania w zakresie pamięci. Zoptymalizowana technologia kompresji H.264 firmy Bosch pozwala ograniczyć szerokość pasma oraz ilość wymaganej pamięci o ok. 30% w porównaniu z konwencjonalnymi systemami MPEG-4. Pamięć można w łatwy sposób rozbudować do 8 TB, stosując lokalne aktualizacje. Równie łatwo i szybko można podłączyć dodatkową zewnętrzną macierz dyskową.

Rejestratory serii 700 spełniają wymagania szerokiego zakresu zastosowań i są idealnym wyborem w przypadku średnich i dużych systemów. Można je stosować w systemach dozoru w centrach handlowych, na parkingach, w bankach, instytucjach finansowych, w centrach miast, a także do nadzoru dużych skupisk ludzkich, kasyn i kompleksów hotelowych.

Bezpośr. inf. Bosch Security Systems

C&C Partners wyłącznym partnerem Egde-Core w Polsce

Edge-Core Networks Corporation, należąca do znanej tajwańskiej firmy **Accton** – jednego z największych światowych producentów sprzętu sieciowego – wybrała w Polsce spółkę **C&C Partners** jako dystrybutora swoich systemów IT. Na mocy umowy C&C Partners, jako wiodący na krajowym rynku dostawca kompleksowych rozwiązań w dziedzinie telekomunikacji, teleinformatyki i zabezpieczeń, ma wyłączność na terenie Polski na sprzedaż i marketing pełnej gamy urządzeń i usług sieciowych Egde-Core wykorzystywanych na całym świecie przez operatorów ISP oraz przedsiębiorstwa.

Edge-Core to marka powstała w 2004 r., wprowadzona na rynek przez tajwański koncern Accton. Celem było dostarczanie klientom zintegrowanych platform sieciowych o wysokiej skalowalności i niezawodności działania. Proces tworzenia urządzeń jest traktowany przez Egde-Core kompleksowo, począwszy od projektowania i produkcji sprzętu, poprzez tworzenie własnej platformy programowej, a skończywszy na szczegółowych testach. Dzięki wieloletniemu doświadczeniu firmy Accton produkowany sprzęt dorównuje wydajnością i funkcjonalnością najlepszym urządzeniom dostępnym na świecie. Od 2010 r. Egde-Core jest niezależną spółką działającą w obrębie grupy Accton.

C&C Partners jest od blisko 20 lat dystrybutorem systemów telekomunikacyjnych i okablowania strukturalnego. Aby były one w pełni zintegrowane z innymi systemami, wymagają sprawdzonych i bezpiecznych rozwiązań do transmisji IP, takich jak te produkowane przez Edge-Core.

Firma C&C Partners już od początku roku posiadała w swojej ofercie wybrane rozwiązania sieciowe, w tym między innymi przełączniki Edge-Core, które szybko zdobyły zaufanie wielu dostawców zrzeszonych w Krajowej Izbie Komunikacji Internetowej oraz iNET Group.

– Duże zainteresowanie rozwiązaniami Egde-Core zachęciło nas do podpisania na początku grudnia 2011 r. umowy z firmą Egde-Core na dystrybucję, sprzedaż i marketing pełnej gamy urządzeń i usług sieciowych na zasadzie wyłączności – mówi **Łukasz Jankowski**, dyrektor działu marketingu C&C Partners. – *Widzimy, że produkty Edge-Core bardzo dobrze odpowiadają wymaganiom polskiego rynku i rodzimych klientów. Stanowią idealne połączenie najwyższej, profesjonalnej jakości i rozsądnej ceny. Dzięki temu będziemy w stanie sprostać rosnącym wymaganiom i dostarczać klientom zintegrowane platformy sieciowe o wysokiej skalowalności i niezawodności działania* – dodaje Łukasz Jankowski.

– Obecnie łącza wysokiej przepustowości wraz z ekonomicznymi rozwiązaniami łączności przewodowej i mobilnej pomogą spełnić

rosnące wymagania dostawców i przedsiębiorstw – powiedział **Edward Ting**, prezes Edge-Core Networks. – *Partnerstwo z firmą C&C Partners doskonale służy temu celowi i jest zgodne z naszą wizją. Jesteśmy przekonani, że obecnie klienci na polskim rynku będą mogli z powodzeniem korzystać z najnowszych technologii dostarczonych przez Edge-Core w konkurencyjnych cenach* – dodał.

Oferta firmy Edge-Core obejmuje dedykowane przełączniki (switche) dla sektorów ISP i Enteprise, takie jak przełączniki modularne, przełączniki zarządzalne warstwy 3, przełączniki zarządzalne warstwy 2, urządzenia do transmisji bezprzewodowej, oprogramowanie zarządzające, a także zasilacze redundantne do przełączników.

Jako jedne z nielicznych na rynku przełączniki (switche) agregujące oraz dostępowe dostarczane przez Edge-Core są wykonane w technologii bezwentylatorowej, a co więcej, mogą pracować w zakresie temperatur od –20°C do +65°C. Dodatkowo dualność i redundancja zasilania AC/DC w połączeniu z wyjątkowymi właściwościami łącza sprawiają, że można je wykorzystać do instalacji kontroli dostępu, dzięki czemu stają się idealnymi rozwiązaniami współpracującymi z systemami bezpieczeństwa. Rozwiązania Edge-Core są szeroko wykorzystywane w sieciach dedykowanych dla systemów zabezpieczeń, takich jak: SMS, analiza obrazu, monitoring IP, kontrola dostępu, systemy interkomowe, telefonia DECT.

Do najlepiej sprzedających się produktów firmy Egde-Core na rynku polskim należą przełączniki (switche) dostępowe L2+. Zalicza się do nich takie modele jak EE-1040 (ES3528M) oraz EE-1022 (ES3510MA), które idealnie sprawdzają się w sieciach ISP, gdzie odbywa się przesył usług Triple Play. Jeśli chodzi o sektor Enterprise, rynkowymi bestsellerami okazały się przełączniki słynnej serii D: modele EE-1072 (ES4524D) i EE-1074 (ES4548D).

Bezpośr. inf. Agnieszka Stasiewicz-Swinney
Comm Start

GEKO – nowy oświetlacz LED w ofercie firmy Videotec

GEKO to **oświetlacz LED** zaprojektowany i produkowany przez firmą **Videotec**. Przeznaczony jest do współpracy z kamerami o rozdzielczości zarówno SD, jak i HD. Odznacza się wysoką niezawodnością pracy. Z wielu powodów warto go zastosować w systemie monitoringu wizyjnego.

Dobry obraz w każdych warunkach. GEKO spełnia wszystkie wymagania instalacyjne stawiane oświetlaczom. Oświetlenie całego obserwowanego obszaru jest równomierne, w warunkach nocnych wyeliminowane są lokalne prześwietlenia lub niedoświetlenia. Oświetlacze GEKO zapewniają poprawne oświetlenie obserwowanych obiektów na odległość dochodzącą do 140 m zarówno wewnątrz, jak i na zewnątrz budynków. Produkowane są modele emitujące światło o długości fali 850 nm i 940 nm, kąt promieniowania jest równy 10°, 30° lub 60°.

Wysoka sprawność energetyczna. Oświetlacze GEKO mają ośmiokrotnie wyższą sprawność energetyczną w porównaniu z tradycyjnymi źródłami światła, dlatego w normalnych warunkach eksploatacyjnych zużywają jedynie 12% energii elektrycznej, zużywanej przez tradycyjne źródła światła.

Wysoka trwałość i niezawodność. Światło emitowane przez diody LED powstaje w elemencie półprzewodnikowym, nie występuje tu żaden gaz, żadne włókna żarowe ani żadne ruchome części. By dorównać w trwałości oświetlaczowi LED, należałoby zużyć 50 żarówek lub 8 jarzeniówek. Ponadto oświetlacze GEKO mogą pracować w bardzo szerokim zakresie temperatur, poczynając od tak niskich jak –50°C, a kończąc na +60°C, i nie ma to wpływu na ich trwałość i niezawodność.

Zgodność z wymaganiami ekologicznymi. Ze względu na wysoką trwałość oświetlaczy GEKO oraz stopień zaawansowania technologii wykorzystywanych do ich wytwarzania ilość energii zużywanej podczas produkcji jest zmniejszona w stosunku do tradycyjnych rozwiązań. W związku z tym zredukowane zostaje także zanieczyszczenie środowiska. Wysoka trwałość tych oświetlaczy powoduje pięćdziesięciokrotne zmniejszenie ilości śmieci związanych z eksploatacją systemów monitoringu wizyjnego.

Oszczędność energii. Oświetlacze GEKO podczas pracy pobierają moc 6–12 W, podczas gdy konwencjonalne oświetlacze pobierają moc 50–100 W. Te liczby mówią same za siebie.

Niskie koszty eksploatacji. Pod względem kosztów eksploatacji oświetlacze GEKO są bezkonkurencyjne. Składa się na to niskie zużycie energii i bardzo znaczne zmniejszenie kosztów konserwacji. Oświetlacze te mogą bezawaryjnie pracować przez jedenaście lat (dla żarówek okres ten wynosi sześć miesięcy).

Bezpośr. inf. Martina Panighel
VIDEOTEC SpA
Tłumaczenie: Redakcja

MILES – nowoczesny system światłowodowy do ochrony rurociągów i ogrodzeń

W styczniu 2012 r. firma **GPS Standard** wprowadziła do sprzedaży najnowszy **system MILES**, którego premiera odbyła się podczas ubiegłorocznych targów Intersec w Dubaju. Jest to **system obwodowy** zaprojektowany specjalnie dla ochrony ogrodzeń, kanałów i rozległych rurociągów, wykonany w technologii światłowodowej, niewidoczny dla fal radiowych. System MILES powstał dzięki połączeniu wiedzy i doświadczenia zdobywanego w ciągu kolejnych lat przy realizacji i udoskonalaniu projektów przez firmę GPS Standard oraz oryginalnej wizji nowoczesnej ochrony w każdych warunkach. MILES doskonale spełnia wymagania związane z ochroną kanałów i ogrodzeń.

Dzięki zastosowaniu kabla światłowodowego system z jednej strony ma bardzo wysoki poziom wykrywalności alarmów, z drugiej zaś jest całkowicie odporny na zakłócenia elektromagnetyczne i zjawiska atmosferyczne takie jak deszcz, śnieg czy grad. Innowacyjność systemu polega na braku konieczności zasilania w terenie otwartym – zasilany jest wyłącznie kontroler systemu, dzięki czemu można znacznie zaoszczędzić na okablowaniu zasilającym. Światłowód, stanowiący część detekcyjną systemu, reaguje na zmiany naprężeń mechanicznych wywołane próbami sabotażu, drganiami i ruchem, zmieniając właściwości transmisyjne włókna wewnętrznego (zmiana ta jest minimalna, ale wykrywana przez analizator). Zaawansowany analizator MILES przetwarza sygnały stanowiące różnicę wysłanych i odebranych wiązek światła oraz umożliwia wprowadzanie zmian parametrów transmisji z wykorzystaniem oprogramowania monitorującego.

System umożliwia ochronę rurociągów o optymalnej długości do 50 km oraz ogrodzeń do 4 km. Miejsce dokonania sabotażu bądź próby wspięcia się na ogrodzenie jest wskazywane z dokładnością do kilku metrów przez oprogramowanie SCS. Istnieje też możliwość wizualizacji kilku systemów pracujących w sieci, na obszarze tysięcy kilometrów. Dokładność lokalizacji naruszeń generujących alarm wynosi mniej niż 0,5%, czyli przy 1 km długości światłowodu – do 5 m, przy 2 km – do 10 m itd. MILES ma ponadto bardzo niski odsetek fałszywych alarmów. Kalibruje się go po zainstalowaniu – w czasie rzeczywistym, w warunkach docelowej pracy. Kontroler MILES przetwarza sygnały zarówno w dziedzinie czasu, jak i częstotliwości. Daje możliwość stworzenia do 128 wirtualnych stref detekcji.

Mając przyjemność przebywania w siedzibie firmy GPS Standard w czasie testów gotowego systemu MILES, osobiście obserwowałam ogromne zaangażowanie inżynierów i entuzjazm wynikający z podjętego wyzwania.

Dokładniejsze informacje na temat systemu MILES i pełnej gamy oferowanych produktów można uzyskać u polskiego dystrybutora – ZBAR.

Bezpośr. inf. Karolina Zasada
ZBAR

Kamery sieciowe Axis z pamięcią masową do lokalnego przechowywania nagrań

Axis Communications wprowadza nową funkcjonalność do swoich kamer sieciowych – będą one wyposażane w **pamięć masową,** która umożliwi lokalne przechowywanie nagrań. Funkcja ta będzie ściśle zintegrowana z oprogramowaniem do zarządzania materiałem wizyjnym (VMS), oferowanym przez największych producentów, takich jak Aimetis, Genetec, Milestone, OnSSI i SeeTec, współpracujących z firmą Axis.

Choć technologia lokalnego przechowywania nagrań jest znana na rynku od kilku lat, dotychczas żadna firma nie oferowała kompleksowego rozwiązania, integrującego kamery z pamięcią masową z systemami zarządzania materiałem wizyjnym. Tymczasem funkcja ta sprawdzi się np. w sytuacji, gdy konieczne będzie zapisanie obrazu w kamerze podczas awarii zasilania rejestratora lub awarii sieci, bądź w przypadku wyłączenia systemu VMS z powodu konserwacji. Zarejestrowane materiały mogą zostać automatycznie przesłane do systemu VMS po jego uruchomieniu, dzięki czemu użytkownicy będą dysponować kompletnym zapisem wizyjnym, bez żadnych przerw. Możliwość ta jest szczególnie przydatna w instalacjach o znaczeniu strategicznym, na przykład na lotniskach lub węzłach komunikacji publicznej, gdzie pamięć masowa w kamerach monitorujących wejścia i wyjścia może stanowić kluczowy element awaryjnego planu strategicznego.

– *Wbudowana w kamery Axis pamięć masowa umożliwia korzystanie z nowatorskiej funkcji Video Trickling, którą udostępniliśmy na początku roku w oprogramowaniu Omnicast* – powiedział **Morgan Pasnon**, kierownik ds. technologii w firmie Genetec. – *Dzięki niej nasi klienci mogą optymalizować wykorzystanie pasma sieciowego, przesyłając i zapisując jedynie interesujące ich fragmenty wybrane spośród zarejestrowanego materiału. Technologia ta oferuje również zdalne rejestrowanie obrazu w dowolnej lokalizacji, bez wykorzystania serwera. Wszystkie te zintegrowane funkcje zapewniają naszym klientom większą elastyczność i niezawodność w ramach wdrożonych systemów nadzoru wizyjnego.*

– *Mamy wielu zadowolonych klientów z całego świata, korzystających z oprogramowania do zarządzania materiałem wizyjnym Milestone Xprotect oraz kamer sieciowych i enkoderów firmy Axis. Dlatego też zapewnienie zgodności operacyjnej nowych technologii to dla nas absolutnie priorytetowe zadanie* – powiedział **Christian Bohn**, wiceprezes ds. marketingu i zarządzania produktami w firmie Milestone Systems. – *Integrując technologię pamięci masowej firmy Axis z systemem XProtect, udostępniamy klientom nowe metody budowy niezawodnych systemów nadzoru wizyjnego. Kluczowym czynnikiem warunkującym wzrost popularności tego rozwiązania jest możliwość zapewnienia ciągłości nagrywania obrazu i kompletności archiwum materiałów dowodowych w przypadku awarii sieci lub serwerów.*

Lokalna pamięć masowa rozszerza także funkcjonalność systemów wykorzystujących sieć o niskiej przepustowości, w których można zapisywać obraz wprost w pamięci kamery. Po odnotowaniu incydentu użytkownik może w każdej chwili pobrać z systemu obraz o wysokiej jakości. Rozwiązanie jest też niezwykle przydatne do zarządzania procesem rejestracji w instalacjach, w których występują przerwy w dostępie do sieci, w bardzo odległych lokalizacjach lub w mobilnych systemach nadzoru, instalowanych na przykład w pociągach.

Bezpośr. inf. Kamila Wierzbicka
Grayling Poland

AXIS Q1604/-E – stacjonarne kamery sieciowe z funkcją rozszerzania zakresu dynamiki tworzonego obrazu

Firma **Axis Communications** zaprezentowała dwie nowe stacjonarne kamery sieciowe – **AXIS Q1604 i AXIS Q1604-E** – wyposażone w funkcję rozszerzania zakresu dynamiki tworzonego obrazu. Sprawdzą się one w monitoringu miejsc, w których panują skrajnie niekorzystne warunki oświetleniowe, na przykład światło przechodzi przez okno lub drzwi, tworząc jednocześnie strefy mocno i słabo oświetlone. Wówczas kamery sieciowe AXIS Q1604/-E pozwolą łatwo i jednoznacznie zidentyfikować osoby oraz obiekty widoczne zarówno w jasnych, jak i w ciemnych partiach obrazu.

Technologia *Wide Dynamic Range*, zastosowana w kamerach AXIS Q1604/-E, pozwala na utworzenie kilku obrazów przy zastosowaniu różnych czasów ekspozycji. W wyniku zaawansowanej technologicznie obróbki obrazu daje to możliwość zwiększenia przejrzystości i rozróżnialności szczegółów obrazu, na którym żaden obszar nie jest ani zbyt ciemny, ani zbyt jasny. Jest to szczególnie przydatne w miejscach, w których tło jest silnie oświetlone lub obserwowana scena ma bardzo duży kontrast. Nowe kamery sieciowe AXIS Q1604/-E idealnie nadają się do monitoringu wejść do budynków, pomieszczeń z dużymi otworami okiennymi i tuneli komunikacyjnych, na przykład na lotniskach, dworcach kolejowych i w budynkach rządowych, sprawdzą się także w systemach monitoringu miast.

Zarówno wewnętrzna kamera AXIS Q1604, jak i model AXIS Q1604-E przygotowany do montażu na zewnątrz oferują funkcję progresywnego skanowania obrazu w rozdzielczości 1 MP/HDTV 720p i mogą przesyłać wiele indywidualnie konfigurowalnych strumieni wizyjnych w formatach H.264 i Motion JPEG jednocześnie. Kamery pracują w trybie dzień/noc, są także wyposażone w obiektyw zmiennoogniskowy, zdalną regulację położenia przetwornika (*back focus*) i dwukierunkową transmisję dźwięku. Kamera AXIS Q1604-E posiada stopień ochrony IP66 (NEMA 4X) i jest dostępna razem z uchwytem ściennym oraz osłoną przeciwsłoneczną. Jej obudowa jest odporna na działanie pyłu, deszczu, śniegu i słońca. Urządzenie może pracować w temperaturach od -40°C do 50°C.

Bezpośr. inf. Kamila Wierzbicka
Grayling Poland

Samsung przedstawia nową wersję oprogramowania SAMS do systemu kontroli dostępu

Samsung zaktualizował **oprogramowanie SAMS** do zarządzania swoim systemem kontroli dostępu poprzez dodanie licznych funkcji ułatwiających pracę instalatorom.

Oprogramowanie SAMS jest dostępne bezpłatnie i bez licencji dla projektów obejmujących do 1000 użytkowników i do 40 przejść (80 czytników). Posiada obecnie funkcję raportowania Muster, którą można skonfigurować zarówno do tworzenia raportów dotyczących aktualnej obecności osób w poszczególnych strefach obiektu, jak również do automatycznego generowania listy osób w zagrożonej strefie w przypadku konieczności ewakuacji (np. alarmu pożarowego).

Najnowsza wersja SAMS pozwala również na tworzenie identyfikatorów osobistych. Oprócz wstawiania statycznego tekstu i logotypu firmy możliwe jest dodawanie dynamicznych pól bazy danych.

Oprogramowanie SAMS jest w pełni kompatybilne z rejestratorami sieciowymi SRN-3250 i SRN-6450 oraz rejestratorami DVR serii SRD firmy Samsung. Zapewnia to synchronizację czasu zapisanych w wysokiej jakości obrazów z właściwymi zdarzeniami alarmowymi kontroli dostępu. – *Na pierwszy rzut oka funkcja ta może nie wydawać się najważniejsza. Jednakże skonfundowani użytkownicy wielokrotnie zauważali, że obraz otrzymywany z rejestratora czasem przedstawiał zdarzenie wcześniejsze lub późniejsze o kilkanaście sekund bądź nawet kilka minut od tego, które rzeczywiście chcieli przejrzeć* – powiedział **David Cawley**, access control and home security products manager w Samsung Techwin Europe.

– *Wartość takiego nagrania jako materiału dowodowego jest wówczas wątpliwa. Dzięki nowej funkcji synchronizacji czasu problem ten zostaje rozwiązany.*

Wśród dodatkowych funkcji znajdują się: udoskonalony kreator do wyszukiwania i wybierania podłączonych urządzeń oraz nowa wersja modułu *Logic*, służąca do dodawania nowych użytkowników kart dostępu.

Oprogramowanie SAMS pozwala na całościowe zarządzanie systemem kontroli dostępu, a także może dostarczać szczegółowe raporty dotyczące aktywności posiadacza karty. Raporty te mogą zostać wyeksportowane do formatu Excela lub pliku tekstowego w celu zintegrowania danych z innymi pakietami oprogramowania, np. listą obecności, zaawansowanym zarządzaniem zasobami (ERP) lub systemem księgowym.

Systemy kontroli dostępu firmy Samsung są oparte na technologii RFID oraz technologii biometrycznej. Dostarczają oszczędne rozwiązania do dowolnego zastosowania kontroli dostępu w zakresie od 1 do 28 000 przejść, wraz z szerokim wyborem technologii odczytu (w tym rozpoznawania linii papilarnych), inteligentnych kart zbliżeniowych oraz kodów PIN, jak również opcji do obsługi list obecności.

System kontroli dostępu Samsung Techwin został ostatnio zintegrowany z oprogramowaniem rozliczania czasu pracy (RCP) polskiej firmy IFTER.

Bezpośr. inf. David Solomons
DRS Marketing

TARGET TRAINING przyczynia się do rozwoju branży zabezpieczeń

W ciągu dwóch lat swojej działalności szkoleniowej firma **TARGET TRAINING** znacząco rozwinęła swoją ofertę szkoleniową w dziedzinie zabezpieczeń technicznych na rynku zachodniopomorskim. 31 sierpnia 2011 r. zakończony został projekt realizowany ze środków Europejskiego Funduszu Społecznego pod nazwą „WIEM – POTRAFIĘ – PRACUJĘ". W jego ramach prowadziliśmy na terenie województwa zachodniopomorskiego kurs „Pracownik zabezpieczenia technicznego pierwszego stopnia", który istotnie wpłynął na wzrost zainteresowania rozwojem zawodowym w branży ochrony osób i mienia. W grudniu 2011 r. zostaliśmy wyróżnieni nominacją w kategorii „Projektodawca PO KL" w konkursie „Zachodniopomorskie Magnolie EFS", organizowanym przez Wojewódzki Urząd Pracy w Szczecinie.

Zainteresowanie prowadzonymi przez nas szkoleniami z zakresu branży zabezpieczeń technicznych objęło obszar kolejnych województw: pomorskiego, wielkopolskiego, lubuskiego i kujawsko-pomorskiego. Dzięki nawiązaniu współpracy z czołowymi producentami i dystrybutorami urządzeń i systemów zabezpieczeń, takimi jak: Satel, DPK System, Sejfpol, Aplisens, Suma oraz AAT Holding, wyposażenie naszej bazy dydaktycznej zostało znacznie wzbogacone o urządzenia i systemy umożliwiające realizację dodatkowych zadań. Tym samym nasza oferta szkoleniowa została poszerzona o kształcenie w zawodach: „instalator systemów alarmowych", „instalator systemów telewizji dozorowej" oraz „monter/konserwator urządzeń zabezpieczeń technicznych osób i mienia". W niedalekiej przyszłości zamierzamy prowadzić szkolenia w zawodach: „instalator systemów alarmowych przeciwkradzieżowych", „pracownik zabezpieczenia technicznego drugiego stopnia", „projektant systemów alarmowych" oraz „instalator systemu zarządzania inteligentnym budynkiem".

Gwarancją jakości szkoleń oferowanych przez firmę TARGET TRANING jest uzyskana w grudniu akredytacja Zachodniopomorskiego Kuratora Oświaty, który w ten sposób docenił naszą pracę i wysiłek włożony w rozwój firmy i rynku szkoleń. Uzyskanie akredytacji umożliwiło nam skierowanie otwartej oferty do uczelni wyższych, szkół i ośrodków kursowych, obejmującej realizację części zajęć programowych, praktyk zawodowych oraz warsztatów szkoleniowych w oparciu o naszą bazę dydaktyczną. Absolwentom naszych szkoleń oferujemy możliwość udziału w prezentacjach nowoczesnych urządzeń i systemów oraz szkoleniach doskonalących, które organizujemy z udziałem współpracujących z nami firm.

Bezpośr. inf. Tadeusz Taniewski, Maja Kornel
TARGET TRAINING

Bosch dla polskiej prezydencji

Cyfrowa sieć kongresowa DCN-NG oraz system do tłumaczeń **Integrus** firmy **Bosch** były wykorzystywane podczas spotkań w ramach polskiej prezydencji w Radzie Unii Europejskiej.

Dwa systemy firmy Bosch: DCN-NG (czyli *Digital Congress Network – Next Generation*) oraz *Integrus* (cyfrowy system dystrybucji tłumaczeń symultanicznych w podczerwieni), zapewniały najwyższą jakość usług konferencyjnych podczas oficjalnych i nieoficjalnych spotkań przedstawicieli UE w Polsce. Systemy firmy Bosch, zgodnie z zamówieniami publicznymi, zostały wybrane przez firmę świadczącą usługi konferencyjne podczas prezydencji.

Cyfrowy system kongresowy DCN-NG wyróżnia się nowoczesną konstrukcją i ergonomią. Zapewnia bezpieczeństwo transmisji danych oraz jest odporny na zakłócenia wywoływane przez telefony komórkowe, dzięki czemu zapewnia doskonałą jakość odbioru. DCN-NG to rozwiązanie w pełni multimedialne. System może być sterowany za pośrednictwem ekranów dotykowych, a dzięki projektorom lub ekranom plazmowym pozwala na graficzne wyświetlanie informacji (np. wyników głosowania). To nowoczesne rozwiązanie techniki cyfrowej posiada wszystkie funkcje niezbędne do przeprowadzenia głosowań oraz rejestracji obecności z wykorzystaniem kart identyfikacyjnych.

Bezprzewodowy system Integrus zapewnia doskonałą jakość dźwięku oraz jest odporny na zakłócenia generowane przez oświetlenie. System obsługuje 31 kanałów tłumaczeń oraz kanał języka oryginalnego i z łatwością łączy się z systemem DCN-NG oraz innymi systemami kongresowymi. Integrus może być wykorzystywany zarówno jako instalacja stała, jak i mobilna. Ma szerokie zastosowanie w dziedzinie tłumaczeń symultanicznych – od centrów kongresowych, przez siedziby organizacji międzynarodowych, po wydarzenia plenerowe. Transmisja w podczerwieni gwarantuje ochronę informacji (sygnały nie przenikają przez ściany i sufity sali konferencyjnej) oraz swobodę ruchu dla uczestników (połączenie przez podczerwień jest bezprzewodowe).

Oba systemy są w pełni mobilne, dlatego mogą być wykorzystywane w różnych miejscach i o różnym czasie. Podczas polskiej prezydencji systemy Bosch były wykorzystywane na spotkaniach m.in. w Warszawie, Sopocie, Poznaniu i Krakowie.

Systemy kongresowe i systemy dystrybucji tłumaczeń firmy Bosch były niejednokrotnie stosowane podczas wielu ważnych wydarzeń w Polsce, takich jak np. szczyt NATO w Krakowie, obchody 20. rocznicy obalenia komunizmu – na Zamku Królewskim na Wawelu, a także 70-tej rocznicy wybuchu II wojny światowej – na Westerplatte. W Europie jednym z najbardziej spektakularnych wydarzeń z wykorzystaniem systemów firmy Bosch była konferencja klimatyczna w Kopenhadze, w której uczestniczyło dwa tysiące delegatów.

Stałe instalacje systemów firmy Bosch w Polsce znajdują się m.in. w Ministerstwie Spraw Wewnętrznych, Ministerstwie Obrony Narodowej oraz Centrum Nauki Kopernik.

Bezpośr. inf. Łukasz Kałucki
Robert Bosch

Samsung wprowadza linię kamer i rejestratorów HD-SDI umożliwiających korzystanie z jakości Full HD poprzez okablowanie analogowe

Dotychczas generowanie, przeglądanie i rejestrowanie obrazów o wysokiej rozdzielczości było zarezerwowane dla systemów sieciowych IP. Jednakże technologia zastosowana w nowych **rejestratorach** oraz **kamerach HD-SDI** firmy **Samsung** umożliwia transmisję nieskompresowanych obrazów w rozdzielczości Full HD (1080P) poprzez tradycyjne okablowanie analogowe.

Jedną z głównych zalet technologii HD-SDI jest bezstratność podczas cyfrowej transmisji obrazów oraz brak opóźnienia podczas ich podglądu. Dzięki temu nowe kamery Samsung – SCB-6000 w obudowie standardowej oraz kopułkowe kamery do zastosowań wewnętrznych SCD-6080 – są idealne wszędzie tam, gdzie wymagane jest uzyskanie najwyższej jakości obrazów możliwych do wykorzystania jako materiały dowodowe, lecz gdzie przesyłanie obrazów za pomocą sieci IP jest niewykonalne bądź nieopłacalne z uwagi na uwarunkowania wynikające z istniejącej już infrastruktury. Przykładami takich aplikacji są np. lotniska, porty, banki, kasyna czy centra handlowe.

Aby zapewnić kompletne rozwiązanie HD-SDI, firma Samsung wprowadziła także czterokanałowy **rejestrator DVR SRD-480D**, który oferuje rozdzielczość zapisu 1080p w czasie rzeczywistym na wybranych kanałach lub rozdzielczość 720p w czasie rzeczywistym na wszystkich kanałach.

– Pomimo że w przyszłości znakomita większość systemów nadzoru wizyjnego będzie niewątpliwie wykorzystywała sieć IP, to jednak zawsze będą występować sytuacje, w których rozwiązania analogowe okażą się najlepsze dla specyficznych projektów – powiedział **Peter Ainsworth**, senior product manager w Samsung Techwin Europe. – *Wbudowana w nową linię kamer i rejestratorów Samsunga technologia HD-SDI umożliwia instalatorom oferowanie klientom wszelkich zalet megapikselowych kamer HD bez konieczności posiadania specjalistycznej wiedzy z zakresu okablowania sieciowego, przełączników, gniazd czy serwerów związanych z systemami bazującymi na technologii IP. Co równie ważne, rozwiązanie HD-SDI firmy Samsung jest w pełni kompatybilne z jej bezlicencyjnym oprogramowaniem Net-i Viewer, pozwalającym użytkownikom przeglądać obrazy w technologii analogowej, sieciowej lub HD-SDI na wspólnej platformie w ramach całego nadzorowanego obiektu.*

Kamera stacjonarna **SCB-6000** oraz wewnętrzna **kamera** kopułkowa **SCD-6080** to profesjonalne kamery dzienno-nocne, które mogą generować i transmitować obrazy zgodne ze standardem Full HD poprzez analogowe okablowanie na odległość do 100 metrów, w czasie rzeczywistym przy 25 kl./s. Oba modele wyposażono w technologię redukcji szumów SSNRIII (*Super Noise Reduction*), SSDR (*Samsung Super Dynamic Range*) oraz system kompensacji prześwietlonych obszarów HLC (*Highlight Level Compensation*), przy jednoczesnym pięciokrotnym zwiększeniu rozdzielczości obrazu w porównaniu z kamerami analogowymi o rozdzielczości standardowej.

Maksymalną odległość transmisji pomiędzy kamerami SCB-6000 lub SCD-6080 a urządzeniem rejestrującym można zwiększyć do 200 metrów poprzez zainstalowanie niskostratnego **kabla koncentrycznego L-6CHD**. Dystans transmisji zostanie niebawem dodatkowo zwiększony po wprowadzeniu do oferty firmy Samsung **wzmacniacza SPH-120R**, co nastąpi już w niedalekiej przyszłości.

Bezpośr. inf. David Solomons
DRS Marketing

AXIS Q1922/-E – nowe kamery termowizyjne o rozdzielczości VGA

Firma **Axis Communications** wprowadziła na rynek udoskonalone termowizyjne kamery sieciowe **AXIS Q1922 i AXIS Q1922-E.** Urządzenia pracujące w rozdzielczości VGA zapewniają wysoką jakość obrazu i szeroki zakres detekcji. Możliwość zainstalowania jednego z czterech obiektywów oraz zaawansowany przetwornik obrazu zapewniają elastyczność i niezawodność tego rozwiązania, ułatwiając jednocześnie jego integrację z inteligentnymi aplikacjami do rejestrowania i analizy materiału wizyjnego. Nowe kamery doskonale sprawdzą się w ekonomicznych systemach monitorowania całodobowego i nadzoru stref zamkniętych w takich miejscach, jak lotniska, elektrownie i porty.

– *Po wprowadzeniu z sukcesem na rynek pierwszej linii termowizyjnych kamer sieciowych rozszerzamy ofertę o nowe urządzenie AXIS Q1922/-E. Model ten zapewnia rozdzielczość VGA, która umożliwia uzyskanie znacznie wyższej jakości obrazu w stosunku do starszych rozwiązań, skuteczne wykrywanie obiektów znajdujących się w polu widzenia kamery oraz istotne zwiększenie zakresu pracy. Nowy produkt zapewni także łatwą i niezawodną integrację z rozwiązaniami innych firm, oferowanymi przez naszą sieć partnerów tworzących aplikacje* – powiedział **Erik Fränlid**, dyrektor ds. zarządzania produktami w firmie Axis. *AXIS Q1922/-E zapewnia łatwą integrację systemu nadzoru termowizyjnego z dowolną siecią monitoringu wizyjnego i umożliwia rozszerzenie funkcji zabezpieczeń całodobowych nawet w wymagających lokalizacjach..*

Termowizyjne kamery IP tworzą obraz na podstawie ciepła wydzielanego przez obserwowane obiekty, pojazdy i ludzi. Dzięki temu „widzą" one w całkowitej ciemności. Zapewniają obrazy umożliwiające operatorom wykrycie podejrzanych działań i podjęcie odpowiednich czynności nawet w trudnych warunkach klimatycznych. Sprawdzają się również we mgle, kurzu czy dużym zadymieniu monitorowanego obszaru.

Kamera AXIS Q1922 jest przeznaczona do monitorowania pomieszczeń, natomiast model AXIS Q1922-E, posiadający stopień ochrony IP66, do systemów zewnętrznych. Cztery dostępne obiektywy, wysoka rozdzielczość równa 640×480 (VGA) i zaawansowany przetwornik obrazu zwiększają efektywny zakres nadzoru i stwarzają możliwość ochrony obwodowej. Zróżnicowanie rodzajów obiektywów zapewnia elastyczny wybór pola widzenia i zasięgu urządzeń, wynoszącego, w zależności od wybranej opcji, od 300 do 1800 m. Kamery obsługują też najważniejsze funkcje systemu nadzoru wykorzystującego protokół IP, takie jak standardy kompresji H.264 i Motion JPEG, zapewniają dwukierunkową transmisję dźwięku, są wyposażone w lokalną pamięć masową i mogą być zasilane metodą *Power over Ethernet*. Inteligentne aplikacje wizyjne są kluczowym elementem każdej kamery termowizyjnej. AXIS Q1922/-E ma wbudowany system generujący alarmy, który jest uruchamiany w chwili wykrycia próby manipulacji przy urządzeniu. Kamera została również wyposażona w funkcję wykrywania ruchu, a także może współpracować z platformą AXIS Camera Application Platform.

Termowizyjne kamery sieciowe AXIS Q1922/-E pozwalają też na skorzystanie z najbogatszej na rynku oferty oprogramowania do zarządzania materiałem wizyjnym, dostępnego w ramach programu Application Development Partner Program firmy Axis, jak również oprogramowania AXIS Camera Station. Urządzenia zbudowane zostały w oparciu o standard ONVIF, który zapewnia zgodność operacyjną z innymi sieciowymi produktami wizyjnymi.

Bezpośr. inf. Krzysztof Pietrzak
Grayling Poland







Po nagrody do Lund

Na zaproszenie **Axis Communications**, firmy tworzącej urządzenia do sieciowych systemów wizyjnych, najlepsi polscy partnerzy firmy udali się do Lund, miasta w południowo-zachodnim regionie Szwecji, na północny wschód od Malmö, gdzie firma ma swoją główną siedzibę, po odbiór przyznanych im nagród. Dziesięciu przedstawicieli firm i dwie przedstawicielki prasy branżowej, w tym autorka niniejszego reportażu, pod życzliwą opieką **Agaty Majkucińskiej** – menedżera ds. kluczowych klientów, wyleciało 5 grudnia do Kopenhagi. Z lotniska odebrała nas **Irina Källberg Rönning**, która od tego momentu pełniła rolę naszego przewodnika i gospodarza. Najpierw pojechaliśmy autobusem do Malmö, mostem Øresund Bridge – najdłuższym mostem na świecie (razem ze sztuczną wyspą i tunelem ma ponad 14 km długości), który 2 lipca 2000 roku spiął brzegi Szwecji i Danii. Przejazd słynnym mostem był dla nas wielką atrakcją.

Zanim dotarliśmy do celu podróży, zawieziono nas do uroczego, oddalonego od cywilizacji hotelu Lodge, który znajduje się w pobliżu wsi Genarp, około 30 minut jazdy z Lund, gdzie po krótkiej powitalnej prezentacji firmy Axis udaliśmy się na spacer po okolicy, a następnie oddaliśmy się relaksowi, korzystając z hotelowej sauny i jacuzzi. To cudowne, oddalone od zgiełku miasta miejsce sprawiło, że przez moment zapomnieliśmy o pracy, goniących nas terminach i domowych obowiązkach. Wieczorem uczestniczyliśmy w uroczystej kolacji, podczas której byliśmy świadkami niezwykłego ceremoniału, który normalnie odbywa się 13 grudnia, w najdłuższą noc w roku (przygotowano go specjalnie dla nas). Tego szczególnego dnia dziewczynka ubrana w białą suknię i z wieńcem na głowie, w który wplecione są świece, rozdaje domownikom tradycyjne szwedzkie przysmaki: bułeczki z rodzynkami, pierniczki, inne ciasta oraz glögg. Towarzyszy temu śpiew – wykonywana jest tradycyjna pieśń *Santa Lucia*.

Kolejnego dnia, 6 grudnia, odwiedziliśmy siedzibę główną Axis Communications, gdzie powitał nas prezes **Ray Mauritsson**, który przedstawił m.in. strukturę działania i dalszego rozwoju firmy, która zatrudnia obecnie ponad tysiąc osób, a założyciel firmy i prezes zarządu **Martin Gren** zapoznał nas z jej historią i misją. **Anders Vigren**, menedżer produktu, oprowadził nas po przedsiębiorstwie, pokazał między innymi, jak dużym zespołem dysponuje dział Badań i Rozwoju, w którym setki inżynierów pracuje nad nowymi technologiami. Przedstawiciele polskich firm stwierdzili, że możliwość zobaczenia na własne oczy laboratoriów, gdzie testowane są nowe urządzenia, znacznie zwiększyła ich zaufanie do firmy i jej produktów. Zwrócili również uwagę na kulturę pracy oraz warunki, w jakich inżynierowie tworzą oprogramo-

wanie do kamer i same kamery. W Experience Center można było zobaczyć, jak kamery pracują w różnych warunkach. Zainteresowanie wzbudziła między innymi kamera wielkości ziarnka grochu, którą można łatwo ukryć i która świetnie rejestruje twarze, przez co umożliwia precyzyjną identyfikację złodzieja. Kamera ta jest przeznaczona do zastosowania m.in. w punktach handlowych. **Patrik Anderson** i **Johan Akesson**, menedżerowie produktu, opowiedzieli o zrealizowanych projektach oraz doświadczeniach zdobytych podczas wdrażania rozwiązań IP w ich codziennej pracy. Kładli duży nacisk na potencjał, jaki kryje się w tej technologii. O obsłudze klientów Axisa i oferowanej przez firmę pomocy technicznej opowiedział inżynier serwisu **Andrei Matveyeu**.

Martin Gren wręczył nagrodzonym pamiątkowe statuetki i dyplomy oraz pakiet oprogramowania **AXIS Camera Station Base Pack 4 channels EN**.

Wśród nagrodzonych firm znaleźli się:

1) DG ELPRO[1]
2) MVB[2]
3) Techniserv[3]
4) Honeywell[4] – w kategorii „Największy projekt 2011”,
5) Śląska Sieć Metropolitalna – w kategorii „Najbardziej innowacyjny projekt 2011”[5],

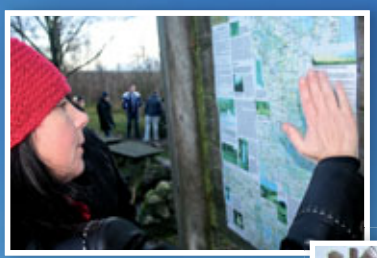
1) Nagroda za dobre wyniki. Firma DG ELPRO jest firmą handlowo-usługową działającą na rynku od 1990 r. Zajmuje się integracją systemów zabezpieczeń i automatyki budynku (od projektu po kompleksową instalację).

2) Nagroda za dobre wyniki. MVB to nowoczesny, kompleksowy integrator systemów zabezpieczeń, technologii i urządzeń IT, automatyki przemysłowej oraz elektroenergetyki. Dostarcza optymalnych rozwiązań technologicznych stosowanych w inteligentnych budynkach.

3) Nagroda za dobre wyniki. W projekcie tym wykorzystano kamery Axis. Celem jest monitorowanie kolejek przy kasach w jednej z największych sieci handlowych w Polsce.

4) Realizacja nowego terminalu pasażerskiego T2 na lotnisku Gdańsk – Rębiechowo obejmuje dostarczenie przez Honeywell oraz Andrem zintegrowanego systemu bezpieczeństwa oraz automatyki bazującej na oprogramowaniu Enterprise Building Integrator R 410.2 oraz Digital Video Manager R 400.2. System będzie zarządzać systemem antywłamaniowym, systemem kontroli dostępu, telewizją dozorową IP, systemem do analizy treści obrazu, automatyką wentylacji oraz klimatyzacji, energetyką oraz będzie zbierał informacje z liczników mediów. Cały system jest połączony za pośrednictwem sieci z licznymi stacjami operatorskimi, które umożliwiają podgląd i sterowanie wymienionymi systemami. Jednym z największych wyzwań jest uruchomienie 460 kamer IP firmy Axis Communications oraz przechowywanie nagrań przez 30 dni.

5) Przedmiotem zadania jest inwestycja miasta Gliwice określona jako „rozbudowa systemu detekcji na terenie miasta Gliwice wraz z modernizacją wybranych sygnalizacji świetlnych”.






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

6) TOP-KEY[6] – w kategorii „Najbardziej aktywny partner 2011”,
7) Siemens[7] – w kategorii „Partner o najbardziej dynamicznym wzroście 2011”.

Nagrodzeni mieli możliwość zaprezentowania swoich firm i nagrodzonych projektów zgromadzonym.

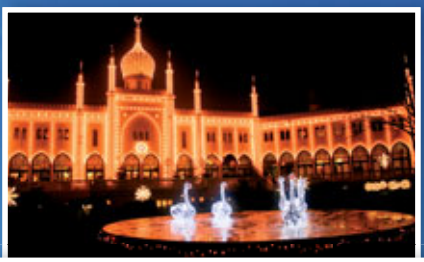
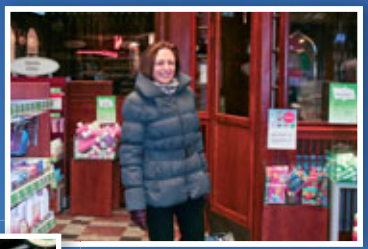
Po emocjach związanych z wizytą w firmie Axis i zażyciu tam sporej dawki wiedzy pojechaliśmy zwiedzać świątecznie udekorowane Malmö. Oprócz pań Iriny i Agaty naszym przewodnikiem była **Edyta Tomczak**, nasza rodaczka mieszkająca od wielu lat w Skandynawii, obecnie pracująca w firmie Axis. Ukoronowaniem wieczoru była kolacja w słynnej tradycyjnej szwedzkiej restauracji Sankt Markus Wine Cellar.

Kolejnym punktem programu (7 grudnia) była wizyta w siedzibie głównej **Milestone Systems** w Brondby (dzielnica Kopenhagi), gdzie powitał nas Country Manager North East Europe – **Anders Johansson**. Milestone Systems jest uznanym na całym świecie producentem profesjonalnego oprogramowania do zarządzania systemami telewizji dozorowej IP. Wszystkie produkty firmy mają otwartą architekturę i są kompatybilne z większą liczbą kamer IP, wideoserwerów i cyfrowych rejestratorów wizyjnych (DVR) niż jakiekolwiek inne rozwiązania. Zapytałam kilku uczestników wyjazdu, czy dowiedzieli się czegoś nowego podczas pobytu w firmie. Jedna z osób poinformowała mnie, że dzięki tej wizycie dowiedziała się o kilku modułach programowych obsługujących systemy przeznaczone dla specyficznych branż i klientów. Szczególnie zainteresował ją moduł służący do rozpoznawania tablic rejestracyjnych pojazdów będących w ruchu, gdyż korzysta z podobnego rozwiązania, które jednak jest wydzielonym programem nie współpracującym z systemem Milestone, który zarządza systemem monitoringu w jego firmie. Zdaniem innej osoby, którą zapytałam o wrażenia, ważny był nacisk położony podczas prezentacji na skuteczność analitycznych systemów wizyjnych. W zależności od wymagań narzuconych przez dany projekt konkretne rozwiązanie będzie

Wdrożenie systemu automatyczno-dynamicznego sterowania ruchem na terenie Gliwic zapewni zwiększenie przepustowości kluczowych odcinków dróg miejskich oraz poprawi bezpieczeństwo ruchu i wpłynie na skrócenie czasu przejazdu, co będzie miało bezpośredni wpływ na obniżenie kosztów transportu samochodowego oraz ochronę środowiska.

6) Firma TOP-KEY funkcjonuje na rynku od 1991 roku, a od 1997 zajmuje się profesjonalnymi systemami zliczania klientów/pojazdów. Jako firma zlicza klientów w ponad 60 centrach handlowych oraz w ponad 1000 sklepach. W bieżącym roku wdrożyła między innymi największy system zliczania klientów znajdujący się pod jednym dachem, tj. 200 kamer liczących Axis w Centrum Futura Park w Krakowie.

7) Siemens oferuje kompleksowe rozwiązania z dziedziny ochrony życia i mienia oraz automatyki budynkowej (zapewnia wykonanie systemu pod klucz, jego serwis i konserwację).


odpowiednio dokładne. Użytkownik końcowy powinien być świadomy tego, że systemy analityczne mogą mieć bardzo różną stopę dokładności (ang. *accuracy rate*). Na rynku praktycznie nie istnieją systemy działające ze stuprocentową dokładnością. Użytkownik końcowy powinien zdawać sobie z tego sprawę, gdyż ma to decydujący wpływ na powodzenie danego projektu. Mi osobiście podobało się krótkie, ale bardzo treściwe i dotyczące produktów Milestone podsumowanie jednego z uczestników wyjazdu: „Milestone ma sporo rozwiązań dla wymagających użytkowników, a ich oprogramowanie ułatwia pracę tam, gdzie rozbudowane systemy są trudne do ogarnięcia".

Na zakończenie pobytu uczestnicy wyjazdu mieli okazję poznać Kopenhagę. Ambasada RP w Kopenhadze zarekomendowała naszą rodaczkę, od wielu lat mieszkająca w Danii, która okazała się wspaniałym przewodnikiem. Jej wiedza na temat tego kraju jest imponująca. Opowiedziała nam i pokazała wszystko to, co powinniśmy wiedzieć i zobaczyć, abyśmy mogli powiedzieć, że poczuliśmy to wspaniałe, piękne, kolorowe i gwarne miasto. Na tyle nas zaciekawiło, że wielu z nas ma ochotę do niego wrócić. Mnie osobiście najbardziej zainteresowali ludzie – uśmiechnięci i chętni do zabawy pomimo niesprzyjającej aury. Zachwycił nas park rozrywki Tivoli, położony w samym centrum Kopenhagi, będący jedną z największych atrakcji turystycznych Danii. Udekorowano go kilometrami świetlnych dekoracji. Można było poczuć w nim świąteczną atmosferę i prawdziwie duńską tradycję. Wieczorem, w restauracji na terenie Ogrodów Tivoli, odbyła się uroczysta pożegnalna kolacja.

Wyjazd był bardzo udany. Jak zgodnie stwierdzili uczestnicy, część merytoryczna była przygotowana perfekcyjnie, a organizatorzy wykazali się bardzo dużym zaangażowaniem, doświadczeniem i pasją. Mieliśmy możliwość pobieżnego zapoznania się z produktami firm Axis i Milestone. Podczas prezentacji poruszono bardzo ciekawe tematy, które odpowiadały zainteresowaniom uczestników. Nie bez znaczenia było znakomite przygotowanie teoretyczne i doświadczenie prowadzących, którzy na co dzień realizują wielkie projekty. Bardzo ważna była też możliwość podzielenia się doświadczeniami i zawarcia nowych znajomości. Podkreślał to każdy z uczestników. Nie sposób opisać atmosfery tych kilku dni spędzonych razem. Grupa świetnie się zintegrowała, mimo iż większość osób nie znała się wcześniej. Nawiązane kontakty są bezcenne i mam nadzieję, że zaowocują wieloma wspólnymi projektami.

Redakcja czasopisma *Zabezpieczenia* dziękuje firmie Axis Communications za zaproszenie. Wszystkim nagrodzonym gratulujemy i życzymy, aby nagrody zostały im przyznane ponownie za rok.

Teresa Karczmarzyk

Monitoring wizyjny w „Chmurze”

podłącz, zaloguj, zobacz

Daniel Kamiński

Monitoring wizyjny online zdefiniowany jako VSaaS (*Video Surveillance as a Service*) był według ISM Research najszybciej rozwijającą się usługą w 2010 roku. Prawdopodobnie tak samo będzie w kolejnych latach. Głównym argumentem przemawiającym za tym stwierdzeniem jest to, że usługa narodziła się jako wynik trzech głównych trendów rozwojowych, wcześniej przewidzianych przez ISM Research, czyli: szybkiego rozwoju kamer IP, szybkiego rozwoju programów zajmujących się zarządzaniem strumieniami wizyjnymi VMS (*Video Management Software*) oraz uruchomienia usług umożliwiających pracę w tzw. „Chmurze" (*Cloud Computing*)

Inny model biznesowy – monitoruj się sam

Główną ideą VSaaS jest udostępnienie klientowi końcowemu usług monitoringu wizyjnego, do tej pory zarezerwowanych dla wyspecjalizowanych firm. W przypadku VSaaS klient, który chciałby mieć możliwość obserwacji zdarzeń w obiekcie, nie musi już inwestować w specjalistyczne rejestratory, macierze dysków czy kamery przemysłowe. Może kupić kamerę IP wraz z dostępem do aplikacji sieciowej pozwalającej na podgląd i rejestrację zdarzeń, podłączyć tę kamerę samodzielnie do zasilania oraz do sieci Internet, zalogować się na stronę dostawcy usług i rozpocząć przeglądanie obrazów z zamontowanych kamer.

Idea VSaaS spodoba się zarówno obecnym użytkownikom systemów CCTV, jak i klientom, którzy dopiero rozważają skorzystanie z nich. Oprócz bowiem małych punktów handlowych i gastronomicznych, w których do tej pory najczęściej były stosowane te systemy, można będzie z powodzeniem instalować je w mieszkaniach i domach jednorodzinnych. Stanie się to możliwe ze względu na niższy koszt systemu (klient inwestuje tylko w kamery), dużą elastyczność montażu (wykorzystanie istniejącej sieci komputerowej lub sieci WiFi) oraz możliwość korzystania z wielu wbudowanych funkcji (czujek ruchu, toru dźwiękowego, lokalnej pamięci flash).

Należy się spodziewać, że w Polsce rozwiązanie VSaaS będą promować głównie firmy zajmujące się monitorowaniem alarmów, operatorzy telekomunikacyjni oraz instalatorzy i integratorzy. Obecnie możemy brać przykład z innych krajów UE (takich jak Wielka Brytania, Holandia, Hiszpania, Niemcy), w których dostawcy usług obsługują już nawet po 30 tysięcy kamer. Podobnie jak w Wielkiej Brytanii mogą również powstać dedykowane centra monitoringu wizyjnego RVRC (*Remote Video Response Centre*). W części krajów UE (Wielkiej Brytanii, Holandii i Hiszpanii) rozwój monitoringu wizyjnego jest dodatkowo promowany przez ustawodawców,

Fot. 1. Zdjęcie przykładowej kamery IP firmy Axis serii M10 (fot. Axis)

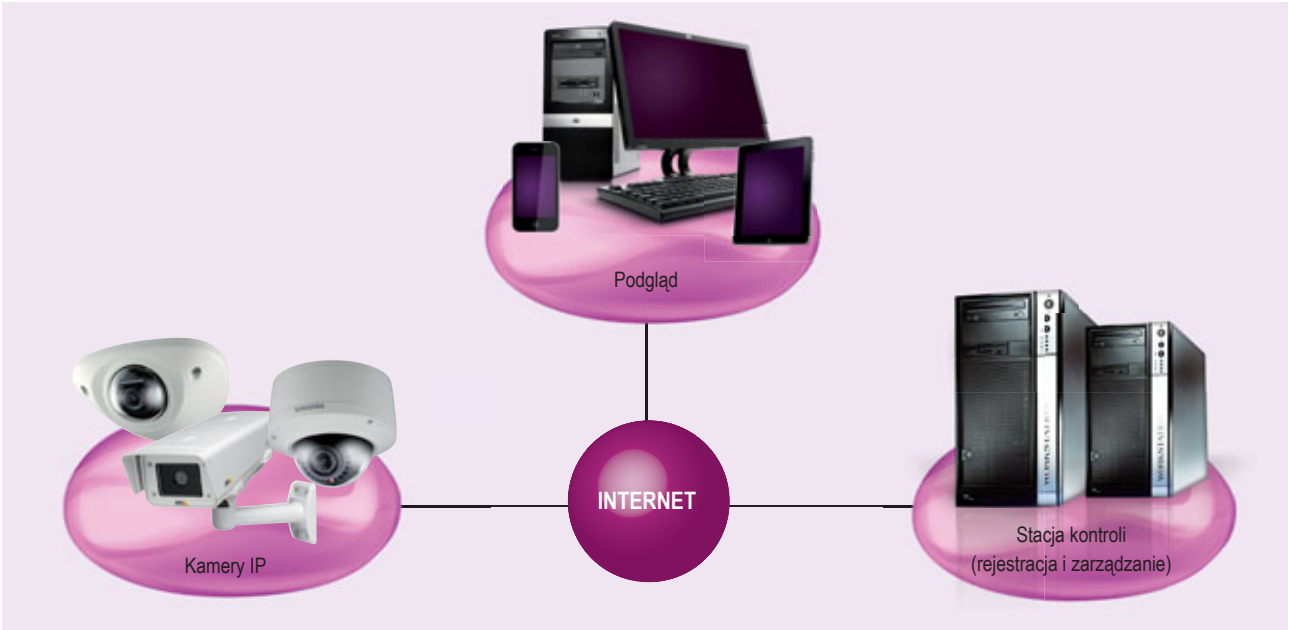
którzy w tych krajach w ramach walki z fałszywymi alarmami podjęli decyzję o stosowaniu weryfikacji wizyjnej w przypadku przyłączania systemów alarmowych do systemu monitoringu.

Usługi wykorzystujące VSaaS są skierowane głównie do odbiorców z rynku masowego. Rozwiązanie jest przeznaczone dla obiektów, w których będą zamontowane maksymalnie cztery kamery. Szczególnie istotne są łatwość korzystania z systemu (dostęp przez stronę internetową) oraz możliwość obsługi wielu lokalizacji w jednym oknie. W związku z taką charakterystyką klientów inny będzie również model sprzedaży, a opisane poniżej rozwiązania będą oferowane w sklepach internetowych oraz sklepach z elektroniką, czyli miejscach, w których użytkownik końcowy może sam dokonać zakupu.

Kamery IP – OneClick Connection

Model sprzedaży ukierunkowany na klienta masowego wymusza również inne podejście do montażu i uruchomienia kamer. W przypadku usług VSaaS najlepiej sprawdzają się kamery przygotowane do samodzielnego uruchomienia. Kamery te często są wstępnie skonfigurowane i łączą się

Rys. 1. Przykład idei VsaaS



Rys. 2. Przykład idei hostingu wizyjnego

z dedykowanym serwerem; użytkownik końcowy ma tylko ustawić je we właściwym miejscu, podłączyć zasilanie oraz zapewnić dostęp do Internetu. Połączenie z Internetem można wykonać przewodowo lub przez wbudowany moduł WiFi. Instalacja jest tak prosta, że często kamery te określa się mianem *One Click Connection*.

Wiele osób zada sobie pytanie, czy kamery przeznaczone do samodzielnego montażu to jeszcze ochrona. Jednak po bliższym zapoznaniu się z tematem większość wątpliwości znika. Tego typu kamery są produkowane przez największych dostawców rozwiązań IP w branży zabezpieczeń, takich jak: Axis, Panasonic, Sony. Dostępne są również u innych producentów, coraz lepiej rozpoznawalnych, jak: Vivotec, Brickcom, Acti, D-link i wielu innych.

Kamery te bardzo często są wyposażone we wbudowaną pamięć flash (do 32 GB), zintegrowaną czujkę ruchu, promiennik światła, mikrofon i głośnik oraz możliwość uruchomienia algorytmu analityki w kamerze, tak aby ograniczyć liczbę transmisji zdalnych powiadomień o zdarzeniach.

Klienci, którzy niedawno zainwestowali w kamery analogowe, nie muszą zmieniać całego systemu. Specjalnie dla nich pojawiły się kodery IP, które zamieniają analogowy sygnał wizyjny na postać cyfrową i pozwalają na komunikację wykorzystującą ten protokół.

Hosting wizyjny

Najważniejszym elementem usługi VSaaS jest platforma informatyczna, która pozwala na archiwizację zdarzeń z wielu tysięcy kamer jednocześnie, umożliwia zdalny dostęp do obrazu w trybie online oraz zdalne przeglądanie archiwum zdarzeń przez dziesiątki tysięcy klientów.

Wiąże się to z przygotowaniem serwerowni, która z jednej strony ma odpowiednio dobraną pojemność dysków przeznaczonych do archiwizacji danych, a z drugiej strony jest wyposażona w przyłącze teleinformatyczne o przepustowości pozwalającej na rejestrację zdarzeń wizyjnych z podłączonych kamer, obserwację w trybie online obrazów z kamer oraz przeglądanie archiwum.

Przy tworzeniu takiej serwerowni trzeba wziąć pod uwagę następujące kwestie: ciągłość działania (niezbędna jest rezerwowa serwerownia i kilku dostawców usług internetowych), bezpieczeństwo dostępu do danych znajdujących

Fot. 2. Przykład aplikacji VSaaS (fot. Cameramanager)

się na serwerze, odporność na dużą liczbę wywołań strony internetowej oraz skalowalność systemu (przygotowanie się na wzrost zapotrzebowania na pasmo sieciowe i przestrzeń dyskową wraz ze wzrostem liczby klientów).

Właśnie do tego celu idealnie nadają się profesjonalne centra danych, które wynajmują (hostują) serwery, przestrzeń dyskową, pasmo oraz zajmują się obsługą i wsparciem technicznym infrastruktury. W przypadku dużych centrów danych, które pracują w tzw. „Chmurze", dostępnych jest wiele rozproszonych po świecie serwerowni. W tak niezawodną i skalowalną infrastrukturę nie jest w stanie zainwestować żadna firma – z tego względu popularny stał się też hosting.

Usługi dodane

Klienci, którzy zakupią kamerę i usługę VSaaS, uzyskują dostęp do narzędzi znajdujących się na serwerze u dostawcy usługi. Mogą administrować danymi kontaktowymi, zdalnie konfigurować opcje kamery oraz obserwować obraz z kamery online.

Klienci bardziej wymagający mogą wykupić dodatkowe licencje pozwalające na zdalną rejestrację zdarzeń na serwerze dostawcy usługi, na tworzenie harmonogramów czuwania systemu oraz na konfigurowanie powiadomień e-mailem lub MMS-em dotyczących zdarzeń wizyjnych.

Nowością wśród tego typu usług są funkcje analizy obrazu, takie jak *licznik klientów, wirtualny płot* itp. Funkcje analizy obrazu są konfigurowane w różny sposób w zależności od rodzaju chronionego obiektu (magazyn, punkt kasowy, ogrodzenie domu itp.).

Ogniwem łączącym usługi VSaaS ze zwykłym systemem monitorowania są reakcje grup interwencyjnych agencji ochrony. W takim przypadku oprogramowanie VSaaS jest integrowane poprzez dedykowany interfejs z programem stacji monitorowania, aby w przypadku alarmu wyświetlać obraz z kamery, która wygenerowała alarm. W przypadku kamer IP wykorzystywane są dwa strumienie wizji: pierwszy transmituje aktualny obraz sytuacji w obiekcie, a drugi pozwala stwierdzić, w jakiej sytuacji wywołany był alarm (tzw. prealarm).

Prywatność

Klient, który zdecyduje się na usługi interwencyjne agencji ochrony, musi udostępnić obraz z kamer stacji monitorowania. W takiej sytuacji rodzi się wiele pytań dotyczących prywatności chronionych osób. Część kamer jest wyposażonych w przycisk prywatności (tzw. Madonna button), który powoduje, że na żądanie klienta kamera jest odłączana. Oczywiście można tak skonfigurować kamerę, aby w momencie załączania systemu w dozór obraz z kamer stawał się dostępny dla stacji monitorowania, a w momencie gdy system jest wyłączony, takiego dostępu nie było.

Mobilność

Korzystanie z monitoringu wizyjnego online na bazie kamer IP pozwala na dużą swobodę dostępu do kamer zainstalowanych w chronionych obiektach. Obraz z kamer można obserwować lokalnie na komputerze lub zdalnie przez Internet. W takim przypadku dostępne są dwa rozwiązania: komputery osobiste oraz urządzenia przenośne.

Fot. 3. Zdjęcie przykładowej kamery z opcją prywatności (fot. Panasonic)

Mobilność rozwiązania jest szczególnie istotna, gdy klient nadzoruje kilka lub kilkanaście obiektów w różnych lokalizacjach i chciałby sprawdzić, czy np. pracownicy punktualnie otworzyli jego sklepy. Wtedy może zdalnie połączyć się z systemem i uzyskać dostęp do różnych kamer. Najistotniejsze jest to, że osoba nadzorująca system nie jest przywiązana do jednego miejsca – może się połączyć z podlegającymi jej kamerami nawet podczas kontroli dowolnego obiektu (oczywiście pod warunkiem, że jest w zasięgu sieci 3G lub WiFi)

Podsumowanie

Usługa VSaaS może wydawać się mało profesjonalna, gdyż przy pierwszym kontakcie ma się wrażenie, że zastosowane kamery wyglądają jak kamery internetowe, a korzystanie z wynajętych serwerów może podważać wyuczone zasady bezpieczeństwa. Jednakże po bliższym zapoznaniu się z rozwiązaniami okazuje się, że kamery są w pełni profesjonalne, a zdarzenia wizyjne przechowywane w tych samych centrach danych, w których obsługiwane są dane finansowe wielu strategicznych instytucji.

Dużą zaletą rozwiązań VSaaS są nowe funkcje pozwalające na zdalną archiwizację zdarzeń wizyjnych (co jest szczególnie przydatne w momencie kradzieży). Istotne są funkcje analizy obrazu, które mogą być uruchamiane na serwerze lub w kamerze (aby ograniczyć ilość transmisji). Ważne są opcje związane z generowaniem alarmów, gdyż mamy tu do czynienia z alarmami aktywowanymi za pomocą dźwięków (np. nadzór nad niemowlętami i małymi dziećmi), przez wizyjne detektory ruchu, a także wbudowane bądź przyłączone czujki.

Najbliższe lata pokażą, czy usługa się przyjmie w Polsce, ale ze względu na wzrastającą liczbę usługodawców uważam za wysoce prawdopodobne, że zdominuje ona rynek masowy. Dodatkowo kryzys i związane z nim ograniczenia nakładów na ochronę mogą powodować, że część klientów będzie wybierała rozwiązanie VSaaS ze względów ekonomicznych.

Daniel Kamiński
OCHRONA JUWENTUS

Cień GPS
podąża za obiektem jak cień

Anna Szymczak

System monitoringu został stworzony, aby zapewnić ludziom bezpieczeństwo, chronić wartościowe przedmioty oraz usprawnić pracę w firmach, które swoją działalność w dużej mierze opierają na usługach transportowych. Dzięki uproszczeniu obsługi urządzeń oraz znacznemu obniżeniu ich cen z zaawansowanych technologii mogą dziś korzystać nie tylko specjaliści, ale także prywatni użytkownicy. Firma Monitech stworzyła zaawansowany technologicznie, bezabonamentowy system Cień GPS, który stanowi odpowiedź na zapotrzebowanie rynku na niedrogą usługę umożliwiającą łatwe lokalizowanie ludzi i pojazdów

Skuteczna kontrola ludzi i pojazdów

Monitorowanie położenia obiektów jest w dzisiejszych czasach bardzo użyteczną funkcją. Dzięki urządzeniom, które ustalają pozycję obserwowanego obiektu, można bez problemu kontrolować jego przemieszczanie się. Takie rozwiązania są szczególnie użyteczne wówczas, gdy chcemy wiedzieć, gdzie w danej chwili przebywa nasze dziecko lub osoba starsza, która wymaga stałej opieki. Oprócz tego urządzenia monitorujące można stosować jako zabezpieczenie przed ewentualną kradzieżą. Włożone do torebki czy laptopa, umożliwią zlokalizowanie przedmiotów w razie ich zaginięcia. System monitorowania wykorzystujący takie urządzenia jak Cień GPS może być również wykorzystany do lokalizacji pojazdów firm transportowych lub taksówek należących do korporacji. Ułatwia on pracę dyspozytorowi, który, obserwując pojazdy na mapie cyfrowej, może bez problemu koordynować działania kierowców. To także idealne rozwiązanie dla wypożyczalni motocykli czy quadów – monitorowanie udostępnionego sprzętu zapobiega bowiem jego użytkowaniu na niedozwolonym terenie lub w warunkach niezgodnych z umową oraz pomaga w przypadku ewentualnej kolizji lub próby kradzieży sprzętu.

Cień GPS – jak cień

System Cień GPS charakteryzuje się przede wszystkim niezwykłą prostotą działania – wystarczy aktywować urządzenie, zarejestrować się na stronie internetowej i można rozpocząć jego użytkowanie. Aktywacja jest bezpłatna. Dostęp do systemu jest darmowy i nieograniczony. Umożliwia to stosunkowo niskie koszty eksploatacji, stałe połączenie z serwerem oraz pełny wgląd w działania obserwowanego obiektu. Samo urządzenie – o kompaktowych rozmiarach 67×40×21 mm i masie zaledwie 60 g – łatwo umieścić tak, by było niewidoczne dla osób trzecich. Solidna obudowa ma zwiększoną wytrzymałość na wilgoć i pył, a dzięki specjalnie wykonanym gumowym narożnikom chroni urządzenie przed uszkodzeniami w przypadku jego upadku. Maksymalny czas działania baterii to pięć dni, zaś ich ładowanie trwa około pięciu godzin.

System monitoruje przemieszczanie się obiektu i w razie zaistnienia zdarzeń, które zostały oznaczone jako niepożądane, alarmuje poprzez wysyłanie SMS-ów lub też przekazywanie informacji na specjalnie przygotowanej platformie internetowej. Z wykorzystaniem systemu Cień GPS można stworzyć tzw. wirtualne ogrodzenie. W momencie jego przekroczenia przez obserwowany obiekt system wyśle powiadomienie o naruszeniu granic obszaru.

Dostępne są dodatkowe akcesoria do systemu Cień GPS, takie jak wodoszczelna obudowa, zewnętrzna antena GPS czy ładowarka samochodowa, które zwiększają możliwości użytkowe sprzętu oraz poszerzają zakres jego działania. Gwarantuje to dłuższe działanie systemu Cień GPS oraz pozwala na swobodne użytkowanie nawet w bardzo trudnych warunkach, np. w miejscach wilgotnych czy z ograniczonym dostępem do sieci.

Rys. 1. Wodoszczelna obudowa z baterią

Rys. 2. Cień GPS + ładowarka samochodowa + zewnętrzna antena GPS

Darmowy i nieograniczony dostęp przez stronę WWW – system Geoloc

Cień GPS wykorzystuje technologię systemu Geoloc, który umożliwia sprawne i precyzyjne lokalizowanie obiektów na mapach cyfrowych. Obsługa odbywa się za pośrednictwem strony internetowej *www.ciengps.pl*, na której można na bieżąco sprawdzać lokalizację obserwowanych obiektów. Interfejs portalu jest niezwykle prosty w obsłudze, wszystkie zakładki są dobrze opisane, a poruszanie się po nim jest bardzo intuicyjne. Zarejestrowane w systemie urządzenie odbiera sygnały z systemu GPS, a następnie przekazuje je poprzez sieć GSM do serwera, na którym w specjalnych bazach przechowywane i gromadzone są dane. Dzięki takiemu rozwiązaniu użytkownik jest w stanie w każdej chwili i w każdym miejscu na kuli ziemskiej sprawdzić oraz przeanalizować informacje. W zakładkach można dodać i skonfigurować urządzenia Cień GPS, wyznaczyć obszar wirtualnego ogrodzenia czy też prześledzić historię przemieszczania się obiektu. W portalu można ustawić powiadomienia, które będą informowały użytkownika o przekroczeniu dozwolonego obszaru, rozpoczęciu i zakończeniu przemieszania się lub o niskim poziomie baterii. W ramach funkcji wirtualnego płotu można wyznaczyć obszar, po którym obiekt będzie poruszać się swobodnie. Po przekroczeniu granicy tego terytorium zostanie włączony alarm.

Po każdym dniu użytkownik może wygenerować raport, w którym zawarte będą wszystkie istotne dla niego informacje. Zestawienie może zawierać opis trasy przejazdu z wyszczególnieniem nazw ulic oraz miejsc postoju, informację zbiorczą o czasie przejazdu i czasie parkowania, wykresy prędkości i przebytego dystansu, określać moment przekroczenia prędkości ustawionej przez administratora.

Cień GPS wraz z systemem Geoloc to doskonałe rozwiązanie dla wszystkich osób, które potrzebują stałego monitoringu osób lub pojazdów. Dzięki prostej obsłudze i szerokiemu zakresowi działania urządzenie jest uważane za niezwykle funkcjonalne i uniwersalne – nadaje się zarówno dla osób prywatnych, które chcą mieć pod stałą opieką swoje dzieci, jak i dla właścicieli firm transportowych czy wypożyczalni. Wieloletnie doświadczenie producenta, firmy Monitech, umożliwiło stworzenie platformy. Właśnie dlatego system Cień GPS jest odpowiedzią na zapotrzebowanie rynku na usługę lokalizowania ludzi i pojazdów w sposób łatwy i efektywny, która nie jest przy tym kosztowna – wymaga tylko zakupu urządzeń oraz dostępu do Internetu.

Do nabycia u dystrybutorów, m.in. AlfaTronik i Multitech.
http://www.alfatronik.com.pl/
http://www.multitech.pl/.

Anna Szymczak

Rewolucja
sektora nadzoru wizyjnego

Agata Majkucińska

Analizując wyniki badań i rozwój technologii, śmiało można powiedzieć, że miniony rok był przełomowy dla rynku nadzoru wizyjnego. Już teraz systemy bazujące na cyfrowych kamerach sieciowych zaczynają zastępować systemy analogowe w coraz większej liczbie dużych i średnich firm. Powód tego jest prosty: sieciowy system monitoringu nie tylko oferuje większą elastyczność, skalowalność i łatwiejszą obsługę, lecz także pozwala na osiągnięcie znacznie lepszych efektów, jeśli chodzi o jakość obrazu i pracę w trudnych warunkach – a co za tym idzie, zapewnia wysoką wiarygodność identyfikacji rejestrowanych obiektów i osób

Do lamusa odchodzi przekonanie, że analogowy system monitoringu jest znacznie tańszy niż rozwiązania sieciowe. Rzeczą oczywistą jest, że urządzenia cyfrowe kosztują więcej niż ich analogowe odpowiedniki. Warto jednak zwrócić uwagę, że w przypadku zaawansowanych kamer kopułkowych PTZ różnica w cenie nie jest wcale tak wyraźna, a ponadto nie można oceniać opłacalności zakupu wyłącznie na podstawie cen samych urządzeń. Amortyzacja kosztów budowy, eksploatacji lub rozszerzenia całego systemu w przypadku większych instalacji przechyla szalę wyraźnie na korzyść rozwiązań IP. Przyczyna jest prosta: zarówno montaż, jak i obsługa systemów bazujących na nowoczesnych rozwiązaniach są znacznie wygodniejsze i nie wymagają „kilometrów" nowego okablowania.

Natomiast rozwiązania IP dają znacznie większe korzyści: dzięki nowoczesnym kamerom w niemal każdych warunkach oświetleniowych czy atmosferycznych można uzyskać jakość obrazu, która pozwala wykorzystać nagranie jako niezbity dowód przestępstwa podczas rozprawy sądowej.

Zalety cyfryzacji systemów nadzoru dostrzegają już nie tylko szefowie firm potrzebujących dużych, skomplikowanych instalacji; wzrasta również zainteresowanie ich stosowaniem w mniejszych przedsiębiorstwach. Odpowiadając na potrzebę rynku, największe koncerny oferujące rozwiązania sieciowe proponują od pewnego czasu również niedrogie kamery przeznaczone dla punktów sprzedaży detalicznej, stacji benzynowych, małych pensjonatów itp. Axis Communications, lider na rynku sieciowych systemów nadzoru wizyjnego, również posiada w swojej ofercie szereg ekonomicznych produktów przeznaczonych dla małych i średnich przedsiębiorstw.

Rys. 1. AXIS Q1602 – pierwsze kamery wyposażone w unikalną technologię Lightfinder

Rys. 2. Termowizyjna kamera sieciowa AXIS Q1922-E o rozdzielczości VGA

Proponowane rozwiązania pozwalają wykorzystać już istniejącą infrastrukturę. Kamery są zasilane metodą Power over Ethernet; większość z nich spełnia wszystkie najnowsze wymagania, m.in. obsługuje dwukierunkową transmisję dźwięku i standardy kompresji H.264 i MJPEG oraz współpracuje z Axis Camera Application Platform – dając możliwość doboru urządzeń i wybranych aplikacji np. analitycznych.

To wszystko sprawia, że mimo ogólnoświatowego kryzysu zainteresowanie systemami nadzoru wykorzystującymi protokół IP nie tylko nie spada, ale wręcz rośnie. W trzecim kwartale ubiegłego roku Axis Communications odnotował 32-procentowy wzrost sprzedaży netto. To wyraźny dowód na to, że osoby odpowiedzialne za bezpieczeństwo w firmach rozumieją już, iż cyfryzacja systemów nadzoru jest jedynym właściwym i przyszłościowym kierunkiem.

Badania, które grupa badawcza Lusax przeprowadziła na Uniwersytecie w Lund, wykazały, że koszty wdrożenia i utrzymania systemów cyfrowych są średnio o 13% niższe niż w przypadku ich analogowych odpowiedników.

Lepszy obraz, łatwiejsze przechowywanie

Zalety systemów wykorzystujących protokół IP to nie tylko opłacalność ekonomiczna. Najważniejsza jest jakość nagrań oraz łatwość ich przechowywania i analizy. Najnowsze osiągnięcia w zakresie poprawy zarówno rozdzielczości kamer,

Rys. 3. Szeroki wybór oprogramowania pozwala błyskawicznie analizować ruch osób w sklepach, na parkingach i w większych obiektach, takich jak lotniska czy stacje metra

Fot. 4. AXIS M1043-W – nowoczesne kamery sieciowe dostosowane do potrzeb małych firm, punktów sprzedaży, a nawet prywatnych mieszkań

jak i możliwości identyfikacji zarejestrowanych obiektów są nie do przecenienia. Wprowadzone na rynek pod koniec 2011 roku kamery z unikatową technologią Axis Lightfinder (w tym pierwsze takie urządzenia: AXIS Q1602 i AXIS 1602-E) pozwalają uzyskać wyraźny i kolorowy obraz nawet w warunkach bardzo słabego oświetlenia, gdy najlepsze na rynku kamery analogowe dają obraz czarno-biały z dużą zawartością szumów. W sytuacjach gdy konieczna jest weryfikacja osób widocznych na nagraniu, wykrywanie ewentualnych zagrożeń czy identyfikacja pojazdów przy słabym oświetleniu, tego typu rozwiązanie jest nie do zastąpienia.

Łatwość integracji nowych urządzeń z istniejącymi już sieciami monitoringu powoduje, że coraz częściej będzie się zdarzać stosowanie wielu rodzajów kamer cyfrowych w jednym systemie. Co więcej, możliwe jest stworzenie systemu hybrydowego – nie zachodzi więc konieczność wymiany całego stosowanego do tej pory sprzętu.

Trzeba również powiedzieć, że urządzenia cyfrowe znacznie lepiej niż analogowe radzą sobie we wszelkich sytuacjach nietypowych – takich jak skrajnie zmienne warunki oświetleniowe. Na przykład światło przechodzące przez okno lub przeszklone drzwi tworzy jednocześnie strefy mocno i słabo oświetlone. Identyfikacja obiektów w takich warunkach przy zastosowaniu tradycyjnych metod monitoringu jest bardzo trudna.

Fot. 5. Nowoczesne sieciowe kamery kopułkowe można zaobserwować już w wielu punktach użyteczności publicznej

Fot. 6. AXIS Q1604-E – kamera sieciowa

Dzięki zastosowaniu zaawansowanych przetworników oraz technologii rozszerzającej zakres dynamiki obrazu (*Wide Dynamic Range Capture*) polegającej na wzajemnym połączeniu kilku klatek różniących się poziomem ekspozycji, możliwe jest uzyskanie obrazów o wyjątkowej przejrzystości. Tego typu rozwiązanie, kojarzące się dotychczas bardziej z filmami SF niż ze współczesnymi urządzeniami, zastosowano już w modelach dostępnych w sprzedaży. Mowa tu o kamerach AXIS Q1604 i Q1604-E (odpowiednio do zastosowań wewnętrznych i zewnętrznych).

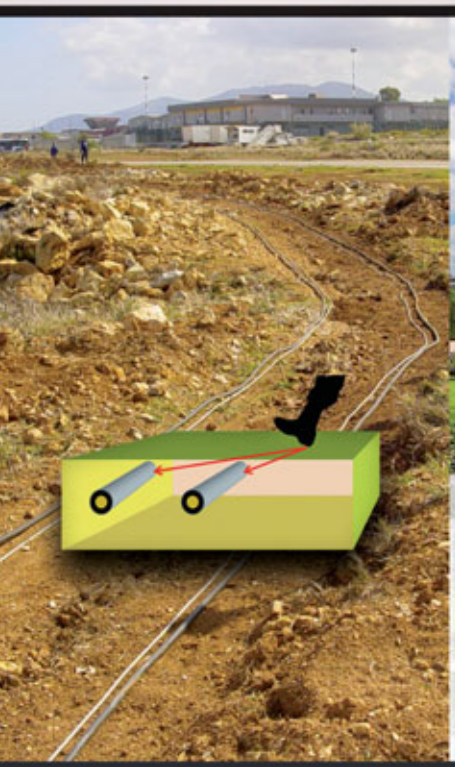
Ze względu na to, że w cyfrowych kamerach przemysłowych wprowadzono obsługę brzegowych pamięci masowych (EDGE Storage), oraz dzięki współpracy firmy Axis Communications z wiodącymi producentami oprogramowania do zarządzania materiałami wizyjnymi (w tym Aimetis, Genetec, Milestone, OnSSI czy SeeTec) możliwe jest bezproblemowe lokalne przechowywanie nagrań i ich późniejsza analiza, a także synchronizacja materiału nagranego lokalnie z materiałem przechowywanym na serwerze lub macierzy np. po awarii systemu. Jeśli połączymy to z technologiami automatycznego wykrywania ruchu oraz rozpoznawania obiektów i osób, okazuje się, że wprowadzenie sieciowego nadzoru wizyjnego nie tylko pozwoli na zwiększenie bezpieczeństwa mienia, lecz także przyniesie inne korzyści. Umożliwia pozyskanie wielu informacji, które mogą być podstawą do optymalizacji procesów transportowych na terenie fabryki, zmiany sposobu aranżacji punktu sprzedaży detalicznej, czy nawet zmian w infrastrukturze zakładu. Poparcie decyzji czysto biznesowych danymi uzyskanymi z systemów telewizji dozorowej jest możliwe także dzięki ogromnej bazie oprogramowania do nadzoru wizyjnego, stworzonego w ramach programu Application Development Partner firmy Axis.

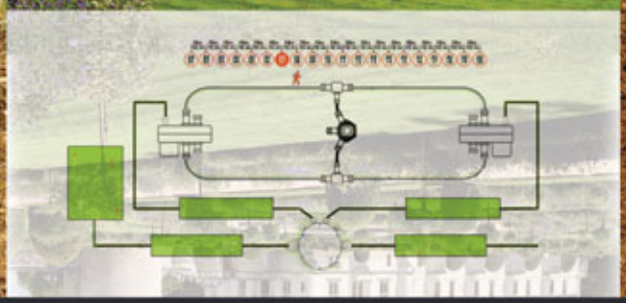
Nie ma wątpliwości, że przyszłość rynku nadzoru jest związana za cyfryzacją. Już teraz jesteśmy świadkami dynamicznych zmian. Stopniowe odchodzenie od rozwiązań analogowych już się rozpoczęło – pozwoli to zwiększyć bezpieczeństwo wszędzie tam, gdzie tradycyjne kamery okazywały się niewystarczające. Dzięki łatwej integracji i szybkiemu zwrotowi kosztów inwestycji kamery sieciowe przestały być kosztowną zachcianką szefów ochrony – stały się urządzeniami wykorzystywanymi na co dzień. Jest to oczywiste dla coraz większej liczby menedżerów IT, security, szefów ochrony i innych osób odpowiedzialnych nie tylko za bezpieczeństwo, ale także za optymalizację procesów biznesowych w dużych i małych firmach.

Agata Majkucińska
Axis Communications

OCHRONA OBWODOWA OBIEKTÓW

ZBAR





ZAKOPYWANE CZUJNIKI CIŚNIENIOWE

- dwie rurki zakopane na maksymalnej głębokości 30 cm (zależnie od podłoża), biegną równolegle w maksymalnej odległości 1,5 metra od siebie
- końce kanału połączone są z sensorem i zaworem
- działanie systemu oparte jest na wykrywaniu zmian ciśnienia, przy przejściu intruza
- sygnały przesyłane do zespołu sterowniczego są analizowane w dziedzinie czasu i częstotliwości oraz poziomów energii
- możliwość określenia punktu przejścia przez strefę detekcji
- konfiguracja „stand alone" lub sieciowa

Zapraszamy do odwiedzenia naszego stoiska nr **65**, pawilon nr **7**
Międzynarodowe Targi Poznańskie
SECUREX 2012
23-26 kwietnia 2012

94-214 Łódź, Poland, Krakowska 60
Tel. + 48 **426 111 298**, Fax +48 **426 111 297**
e-mail: zbar@zbar.com.pl

sprawdź pełną ofertę na **www.zbar.com.pl**

CIAS SCHRACK SECONET SENSTAR GPS STANDARD Protech

Sieciowe systemy wizyjne

nowe możliwości biznesowe dla instalatorów i integratorów

James Smith

Wzrasta zapotrzebowanie na zintegrowane, sieciowe systemy bezpieczeństwa. Użytkownicy końcowi także oczekują podwyższenia jakości zintegrowanych zabezpieczeń. W związku z tym postaram się pokrótce przedstawić niektóre najnowsze rozwiązania, które instalatorzy i integratorzy mogą zaproponować użytkownikom końcowym

Fot. 2. SNV-7080R HD – wandaloodporna megapikselowa kamera sieciowa z wbudowanym diodowym oświetlaczem pracującym w podczerwieni

Dotychczas sieciowe systemy wizyjne były postrzegane jako rozwiązania przydatne w dużych projektach, jednak firma Samsung dostrzega coraz większe możliwości wykorzystania tej technologii w małych i średnich instalacjach. W trudnych warunkach gospodarczych klienci oczekują maksymalnych korzyści wynikających z poczynionych inwestycji. Firma Samsung przyjmuje, że sieciowe systemy bezpieczeństwa mogą obecnie zwiększyć zyski instalatorów i integratorów systemów bezpieczeństwa i jednocześnie są rozwiązaniem korzystniejszym niż tradycyjne rozwiązania analogowe ze względów finansowych i użytkowych. Dane pochodzące z rynku są jednoznaczne i dowodzą, że sieciowe systemy wizyjne weszły w okres intensywnego rozwoju i ta tendencja utrzyma się przez najbliższe lata, gdyż użytkownicy końcowi wybierają rozwiązania sieciowe zamiast tradycyjnych rozwiązań analogowych. Mając to na uwadze, firma Samsung pomyślnie nawiązuje partnerskie kontakty biznesowe z integratorami w całej Europie.

Oczywiście partnerska współpraca jest oparta na obustronnych korzyściach, dlatego firma Samsung zaadaptowała filozofię *Smarter Security*. Częściowo dotyczy ona oferowanych produktów, wśród których znajdują się kompletne rozwiązania sieciowe wykorzystujące darmowe oprogramowanie służące do przeglądania i rejestracji obrazów oraz rozwiązania hybrydowe wykorzystujące kodery wizyjne umożliwiające modernizację systemu bezpieczeństwa i przejście na rozwiązania sieciowe z zachowaniem istniejących kamer analogowych.

Oferowanie produktów i rozwiązań najwyższej klasy stanowi jedynie fragment strategii *Smarter Security*. Zgodnie z nią należy również przekonywać instalatorów i integratorów do tego, by rekomendowali instalowanie zintegrowanych, sieciowych systemów kontroli dostępu i dozoru wizyjnego. Ponadto powinno się oferować przedsprzedażowe i posprzedażowe usługi w postaci szkoleń technicznych, darmowego projektowania systemów, darmowego wsparcia technicznego oraz pełnej, trzyletniej gwarancji na wszystkie produkty.

Oferowane możliwości

Aby uzasadnić koszty, jakie będzie trzeba ponieść w najbliższej przyszłości, w trudnych warunkach ekonomicznych, osoby zarządzające bezpieczeństwem będą szukać zysków wynikających z zastosowania analogowych lub sieciowych systemów monitoringu.

W wielu przypadkach koszty wynikające z instalacji systemów bezpieczeństwa będą pokrywane z budżetów działów HR, IT i działu handlowego i zostaną zaakceptowane przez kierownictwo działu bezpieczeństwa, gdyż dzięki kamerom będzie można pozyskiwać cenne informacje, a następnie dzielić się nimi. Będzie to oczywiście wymagało zmiany podejścia dotyczącego wykorzystania rozwiązań, w których kamery i urządzenia rejestrujące współdziałają z wieloma systemami, takimi jak systemy kontroli dostępu, sygnalizacji włamania i napadu, sygnalizacji pożarowej, automatyki budynkowej, a także z systemami rozliczeniowymi w punktach sprzedaży.

Na całe szczęście technologie wykorzystywane w systemach dozorowych nadążają za rosnącymi wymaganiami użytkowników końcowych, które są związane z wprowadzeniem na rynek najnowszej generacji kamer HD tworzących obrazy o bardzo wysokiej jakości, co umożliwia nie tylko ocenę sytuacji w danym miejscu, lecz także wyciągnięcie znacznie istotniejszych wniosków.

Klienci na pewno docenią możliwość integracji produktów wykorzystywanych w różnych systemach bezpieczeństwa, możliwość modernizacji analogowych systemów wizyjnych i przejście na technologię sieciową. Nie ma także wątpliwości co do tego, że współpraca osób odpowiedzialnych za infrastrukturę IT oraz integratorów systemów sieciowych przyniesie realne korzyści, dzięki którym klientom szybko zwrócą się koszty

Fot. 1. Samsung NET-i Ware

Fot. 3. Aplikacja Samsung iPoLis App do telefonów komórkowych i tabletów

inwestycji związanych z systemami bezpieczeństwa. Czynnikiem ułatwiającym osiągnięcie tego celu jest rosnąca liczba niezależnych producentów oprogramowania oferujących otwarte platformy programowe, których głównym celem jest ułatwienie integracji sprzętu oraz systemów dostarczanych przez różnych producentów.

Fot. 5. Wandaloodporna kopułowa kamera sieciowa

Korzyści wynikające ze stosowania sieciowych systemów wizyjnych

Najbardziej oczywistą korzyścią wynikającą ze stosowania sieciowych, wizyjnych systemów dozorowych jest możliwość ograniczenia kosztów związanych z infrastrukturą kablową. Dodatkowe korzyści wynikają z tego, że pojedynczy kabel sieciowy jest w stanie transmitować sygnały wizyjne, akustyczne oraz dane sterujące. Ponadto taki kabel umożliwia zasilanie metodą PoE, dzięki której można jeszcze bardziej ograniczyć koszty – nie ma potrzeby zastosowania oddzielnych zasilaczy dla każdego z urządzeń peryferyjnych. Są jeszcze dwie inne korzyści, szczególnie istotne dla szefów służb ochrony. Pierwszą z nich jest możliwość sterowania kamerami oraz przeglądania bieżących obrazów z kamer i archiwalnych, zapisanych w rejestratorach obrazów z wykorzystaniem dowolnego komputera połączonego z siecią lub nawet smartfonu. Daje to możliwości trudne do uzyskania w systemie analogowym, w którym obrazy są tradycyjnie transmitowane do centralnego pomieszczenia sterującego, często z wykorzystaniem kosztownych, dzierżawionych linii przewodowych. Rozwiązania wykorzystujące sieci IP oferują wysoki stopień niezawodności, gdyż materiały wizyjne mogą być przechowywane w dowolnym miejscu w sieci i pobierane w dowolnym czasie przez autoryzowanych użytkowników. Jednoczesna rejestracja i przechowywanie materiałów wizyjnych w kilku lokalizacjach zapewnia wymagany poziom nadmiarowości.

Dodatkową, istotną korzyścią wynikającą ze stosowania sieciowych systemów wizyjnych jest możliwość skorzystania z kamer najnowszej generacji, odznaczających się wysoką rozdzielczością, dostarczających znacznie więcej informacji niż konwencjonalne kamery analogowe, wytwarzające obrazy o rozdzielczości 0,4 megapiksela. Na przykład kamera o rozdzielczości 1,3 megapiksela, w zależności od pola widzenia, może pełnić rolę kilku kamer analogowych, gdyż pozwala na skorzystanie z funkcji cyfrowego powiększenia obrazu bez wprowadzania zniekształceń wynikających z pikselizacji. Jakość obrazów dostarczanych przez kamery o rozdzielczości Full HD jest jeszcze wyższa. Trzeba to zobaczyć, żeby się przekonać. Możliwość wyświetlania obrazów zgodnych ze standardem 1080p oraz dostępność funkcji WDR w wybranych modelach kamer umożliwia wykorzystanie systemu w bardzo trudnych warunkach oświetleniowych. Kamery o rozdzielczości Full HD oraz kamery kopułowe wykorzystujące chipset WiseNet2 DSP firmy Samsung mogą wytwarzać obrazy o jakości tak wysokiej, że można wykorzystać je jako materiał dowodowy w sądzie. Bardzo wysoka jakość obrazów sprzyja też bezpieczeństwu i higienie pracy. Ponadto obrazy o wysokiej rozdzielczości mogą być przydatne w zarządzaniu, na przykład w handlu detalicznym – dzięki nim można obserwować zachowania klientów.

Fot. 4. Sieciowe rejestratory wizyjne, których obsługa jest tak łatwa jak obsługa rejestratorów DVR

Banki, kasyna, punkty sprzedaży, fabryki, centra miast, porty lotnicze i dworce kolejowe to jedynie nieliczne przykłady środowisk, w których wyjątkowa jakość obrazów wytwarzanych przez kamery sieciowe o rozdzielczości Full HD sprawi, że działanie wizyjnego systemu dozorowego z naddatkiem spełni oczekiwania użytkowników końcowych.

Mimo iż celem tego artykułu jest uwypuklenie zalet sieciowych systemów wizyjnych, warto również zwrócić przy okazji uwagę na to, że klienci są coraz bardziej zainteresowani korzyściami wynikającymi ze stosowania sieciowych systemów kontroli dostępu. Głównym celem jest poszukiwanie sposobów integracji i współdziałania wszystkich systemów bezpieczeństwa, oczywiście z wizyjnym systemem dozorowym włącznie, przy czym zdolność do przekazywania obrazów, danych dotyczących alarmów oraz informacji sterujących pomiędzy tymi systemami przynosi oczywiste korzyści operacyjne. Ponadto dzięki wizualnej weryfikacji tożsamości osób próbujących uzyskać dostęp do wydzielonych obszarów osoby zarządzające obiektem mogą uzyskać istotne informacje dotyczące na przykład miejsca przebywania i czasu pracy poszczególnych osób.

Aby utwierdzić użytkowników końcowych w przekonaniu o dużej przydatności informacji uzyskanych ze zintegrowanych i harmonijnie współdziałających systemów dozoru wizyjnego i kontroli dostępu, podkreślmy to, że wydarzenia odnotowywane w systemie kontroli dostępu są dokładnie i jednoznacznie zsynchronizowane z odpowiednimi obrazami pochodzącymi z systemu wizyjnego. Dotychczas nie istniały tanie metody uzyskiwania takich rezultatów i przez wiele lat użytkownicy cierpieli niewygody związane z wyszukiwaniem właściwych fragmentów nagrań i przyporządkowywaniem ich do wydarzeń zachodzących w obiekcie.

Firmy oferujące sieciowe systemy bezpieczeństwa mogą uzyskać dodatkowe dochody, proponując nowe produkty IP, które mogą stanowić uzupełnienie wcześniejszych rozwiązań. Wsparcie i doradztwo producentów, takich jak Samsung, a także szkolenia i dostępna pomoc umożliwią klientom wybór produktów najlepiej przystosowanych do realizacji określonych przez nich zadań. My wszyscy możemy zatem wziąć udział w rewolucji sieciowej.

James Smith
Samsung Techwin Europe
Tłumaczenie: Redakcja

Rejestratory wizyjne DIVAR HD serii 700

Do nagrywania obrazu w wysokiej jakości

DIVAR 700 serii HD to szybkie, łatwe w obsłudze urządzenie do zapisu obrazu HD i SD oraz zarządzania zarchiwizowanymi materiałami. Łatwe w konfiguracji i konserwacji rejestratory wizyjne serii 700 spełniają wymagania najbardziej zaawansowanych zastosowań CCTV. Posiadają cztery twarde dyski z możliwością ich wymiany od przodu, zabezpieczenie RAID-4 oraz zaawansowane funkcje integracyjne. Dzięki temu stanowią idealne rozwiązanie przy zastosowaniach wymagających bardzo wysokiej jakości nagranego obrazu. Zintegrowany i w pełni zautomatyzowany system zarządzania kamerami sieciowymi umożliwia obsługę 32 kamer H.264. Z kolei modele hybrydowe stanowią idealne i przyszłościowe rozwiązanie dla rosnącej liczby zastosowań wykorzystujących równocześnie kamery analogowe i sieciowe.
Rejestratory serii 700 są idealnym wyborem w przypadku średnich i dużych systemów.

www.boschsecurity.pl

BOSCH
Technologia bliżej nas

PoE bez tajemnic (część 2)

Andrzej Walczyk

W pierwszej części artykułu (*Zabezpieczenia* nr 6/2011) przedstawiłem czytelnikom wybrane zagadnienia teoretyczne związane z metodą zasilania urządzeń peryferyjnych zgodną ze standardem PoE. Przejdźmy teraz do zagadnień praktycznych. Zastanówmy się, w jaki sposób można zbudować sieć umożliwiającą zasilanie urządzeń peryferyjnych tą metodą

Najdoskonalszym, a jednocześnie chyba najkosztowniejszym sposobem praktycznego wykorzystania metody PoE jest zastosowanie odpowiednich przełączników sieciowych, czyli urządzeń pracujących w drugiej, a częściowo także w trzeciej warstwie sieci IP, fabrycznie wyposażonych w układy umożliwiające zasilanie urządzeń peryferyjnych za pośrednictwem interfejsu Ethernet. W takim przypadku mamy pewność, że zachowana jest zgodność ze standardem PoE, realizowane są wszystkie procedury związane z niezawodnością i bezpieczeństwem użytkowania, opisane w pierwszej części artykułu.

Zaletą takiego rozwiązania jest prostota. Jeśli urządzenia peryferyjne są podłączone do sieci IP za pomocą przełączników, których interfejsy dostarczają energię zasilającą zgodnie ze standardem PoE, żadne inne urządzenia nie są już potrzebne. Niestety w praktyce bywa inaczej.

Trudno rozstrzygnąć, czym kierowali się konstruktorzy i producenci przełączników sieciowych z opcją PoE. Wystarczy stwierdzić, że większość z tych urządzeń ma ograniczoną sumaryczną moc, jaką może dostarczyć do urządzeń podłączonych do ich interfejsów sieciowych. Na przykład popularny i często stosowany przełącznik typu FS108P firmy Netgear ma w sumie osiem interfejsów Fast Ethernet, z czego tylko cztery mogą służyć do zasilania urządzeń peryferyjnych metodą PoE.

Gdyby to było jedyne ograniczenie, nie byłoby żadnego problemu. Przecież nie wszystkie urządzenia sieciowe mogą być zasilane metodą PoE. Ponadto przełącznik musi być jakoś połączony z siecią, czyli z innymi urządzeniami tworzącymi infrastrukturę sieciową, zatem istnienie interfejsów nie zapewniających zasilania metodą PoE jest jak najbardziej uzasadnione.

Realne ograniczenie polega na tym, że sumaryczna moc zasilająca, jaka może być dostarczona do urządzeń peryferyjnych przez cztery interfejsy Ethernet z opcją PoE, wynosi tylko 32 W. W praktyce oznacza to, że przed podłączeniem urządzeń peryferyjnych należy sprawdzić, jaki jest ich sumaryczny pobór mocy. Przykładowo – limit zostaje osiągnięty, gdy dwa z tych interfejsów są obciążone mocą rzędu 15 W i żadne inne urządzenia zasilane metodą PoE nie mogą już być podłączone do tego przełącznika, mimo iż dwa interfejsy z opcją PoE nie zostały w ogóle wykorzystane. Przełącznik dostarczający 32 W mocy zasilającej będzie jednak tańszy od przełącznika, którego wszystkie interfejsy mogą być obciążone pełną mocą, czyli sumaryczne obciążenie może dochodzić do 60 W. Jeśli ograniczymy się do zastosowań związanych z telewizją dozorową, okaże się, że sytuacja nie jest tak krytyczna, jak mogłoby się wydawać. Należy pamiętać, że typowe kamery IP zasilane metodą PoE mają pobór mocy rzędu 8 W, dzięki czemu przełącznik dysponujący sumaryczną mocą 32 W może być w pełni wykorzystany bez przekraczania limitu.

Drugim istotnym ograniczeniem są parametry transmisyjne przełączników sieciowych. W tym momencie warto przypomnieć, że do poprawnej pracy sieciowego systemu monitoringu wizyjnego wymagana jest nieprzerwana, płynna transmisja ramek sieciowych w warstwie pierwszej i równie szybkie przetwarzanie pakietów w wyższych warstwach sieciowych, co wiąże się z koniecznością zastosowania wystarczająco szybkich procesorów i odpowiednich buforów przechowujących dane przeznaczone do transmisji. Nowoczesne metody kompresji obrazów, takie jak H.264, zmuszają do spełnienia dość rygorystycznych wymagań dotyczących przepustowości sieci. Co prawda średnia przepływność związana z transmisją obrazów z pojedynczej kamery jest niewielka, jednakże wartości chwilowe, z którymi mamy do czynienia podczas transmisji klatek referencyjnych, są wysokie. To zjawisko staje się szczególnie dokuczliwe w przypadku kamer o wysokiej rozdzielczości i uniemożliwia stosowanie prostych, tanich przełączników sieciowych, mimo iż ich średnia przepustowość jest wystarczająco duża. Innymi słowy – wymagania dotyczące prędkości transmisji pakietów w sieci, w której pracują kamery IP, są znacznie wyższe od wymagań wobec przełączników wykorzystywanych w biurach, gdzie urządzeniami końcowymi są komputery, drukarki, telefony VoIP i inne urządzenia biurowe.

Bardzo często zdarza się, że dobierając urządzenia przeznaczone do budowy sieci, w której mają pracować kamery IP, projektant czy instalator dysponuje przełącznikami o odpowiednich parametrach transmisyjnych, jednakże pozbawionymi możliwości zasilania kamer metodą PoE. Podobnie może być podczas prac modernizacyjnych, gdy w sieci są już zainstalowane przełączniki starego typu, bez opcji PoE, tymczasem nowe urządzenia peryferyjne wymagają zasilania tą metodą. W takim przypadku można posłużyć się dodatkowymi urządzeniami określanymi jako „midspan". To słowo nie ma dobrego odpowiednika polskojęzycznego. Można spotkać się z określeniami „panel zasilający" lub „zasilacz PoE", jednakże w materiałach reklamowych, a nawet w pracach o zacięciu naukowym najczęściej spotkamy określenie „midspan". Zastosowanie takich urządzeń rozwiązuje wiele problemów. Po pierwsze – dysponują one dużą sumaryczną mocą zasilającą i w większości przypadków wszystkie interfejsy sieciowe mogą być obciążone zgodnie z wymaganiami narzucanymi przez standard PoE. Po drugie – można zastosować dowolnego typu przełączniki sieciowe o odpowiednio dobranych parametrach transmisyjnych, nie dysponujące opcją PoE, co ułatwia pracę projektantom sieciowych systemów dozorowych. Po trzecie – ceny rynkowe paneli zasilających są na tyle niskie (w porównaniu z przełącznikami z opcją PoE), że ich zastosowanie znajduje uzasadnienie ekonomiczne.

Innym, równie popularnym sposobem wykorzystania metody PoE do zasilania pojedynczych kamer sieciowych jest zastosowanie specjalistycznych zasilaczy wyposażonych w dwa interfejsy Fast Ethernet. Pod względem transmisyjnym takie urządzenia są całkowicie pasywne, to znaczy w żaden sposób nie modyfikują ramek sieciowych, przy czym na jednym z interfejsów dostarczają energię zasilającą. Przykładem takiego zasilacza może być oferowany przez firmę Sony model SNCA-POE1, który działa zgodnie ze standardem PoE, realizuje wszystkie funkcje opisane w pierwszej części artykułu i jest przeznaczony do zasilania jednej kamery IP dowolnego producenta, przystosowanej do zasilania tą metodą.

Warto zastanowić się nad ekonomicznym aspektem stosowania takich zasilaczy PoE. Ich cena rynkowa dochodzi do kilkuset złotych, lecz ich użycie jest opłacalne, gdyż eliminuje kosztowny przełącznik sieciowy z opcją PoE. Ponadto na rynku pojawiły się ostatnio kamery IP, które mogą być zasilane tylko metodą PoE, więc użycie odpowiedniego zasilacza i tak jest konieczne. Należy tu zwrócić uwagę na pewien mechanizm rynkowy. Otóż kamery IP, które mogą być zasilane jedynie metodą PoE, są znacznie tańsze od kamer które mogą być zasilane na kilka sposobów (na przykład 12 V_{DC}/24 V_{AC}/PoE). Co prawda kamery umożliwiające swobodny wybór jednej z trzech dostępnych metod zasilania są bardziej uniwersalne, jednakże metody te nigdy nie są wykorzystywane jednocześnie, czyli to uniwersalne rozwiązanie jest w pewnym sensie rozrzutne i nieuzasadnione ekonomicznie.

Zasilanie urządzeń peryferyjnych metodą PoE staje się coraz bardziej popularne i przestaje dotyczyć tylko urządzeń o małym poborze mocy. Wersje HPoE i PoE plus, o których wspomniałem w pierwszej części artykułu, umożliwiają zasilanie kamer obrotowych, central alarmowych, kontrolerów w systemach kontroli dostępu, a nawet stacji roboczych i przenośnych komputerów. Metoda PoE znajduje bardzo szerokie zastosowanie w automatyce przemysłowej, a także w sprzęcie medycznym – jest przydatna wszędzie tam, gdzie prostota i bezpieczeństwo użytkowania urządzeń peryferyjnych ma zasadnicze znaczenie.

Z prognoz rynkowych wynika, że metoda PoE może stać się standardem w przypadku masowych usług teleinformatycznych, takich jak na przykład dostęp do Internetu w pokojach hotelowych czy poczekalniach na dworcach kolejowych i lotniczych (gdzie poprzez abonenckie gniazdo ethernetowe dostarczana będzie energia zasilająca). Może też być powszechnie wykorzystywana do zasilania tabletów, czytników książek elektronicznych, komputerów itp. W zasadzie trudno wymienić wszystkie możliwe zastosowania metody PoE w życiu codziennym. Zastosowania mogą być dziwaczne. Gromadząc materiały do tego artykułu, znalazłem opisy gitary Gibson z wmontowanym przedwzmacniaczem zasilanym metodą PoE, a także zdjęcia golarki elektrycznej z gniazdem RJ45, którą można podłączyć do gniazdka abonenckiego w pokoju hotelowym. Zachęcam czytelników do poszukiwania równie niecodziennych zastosowań tej metody zasilania.

Andrzej Walczyk

Kamery IP Full HD marki NOVUS

Fot. 1. Kamery IP Full HD: NVIP-2C2011D-P, IP-2DN2001D-2P, IP-2DN4001V/IRH-2P, IP-2DN3001H/IR-2P, IP-2DN5001C-1P

Patryk Gańko

Linia kamer dwumegapikselowych, o których obszernie pisałem na łamach *Zabezpieczeń* (3/2011) została uzupełniona pięcioma modelami kamer o tej samej nominalnej rozdzielczości, lecz zgodnych ze standardem Full HD. Dotychczasowe modele generowały dwumegapikselowy strumień wizyjny w rozdzielczości 1600×1200 (proporcje obrazu 4:3) i z prędkością do 15 klatek na sekundę. Seria kamer IP Full HD, którą poniżej szczegółowo scharakteryzuję, generuje dwumegapikselowe strumienie wizyjne w rozdzielczości HD 1920x1080 (proporcje obrazu 16:9) i z prędkością real-time (25 obrazów na sekundę)

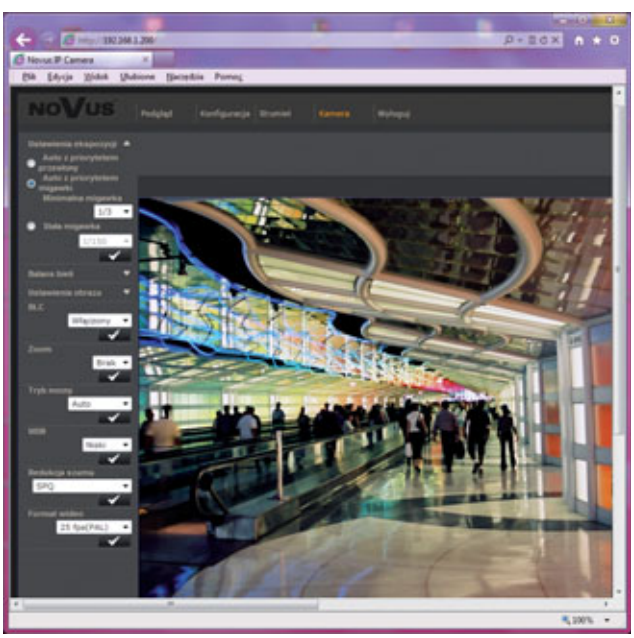
W powszechnej opinii osób instalujących systemy telewizji dozorowej (zarówno analogowe, jak i IP) to właśnie rozdzielczość, a więc zdolność do rozróżnienia szczegółów obserwowanej sceny jest głównym wyznacznikiem jakości obrazu. Z reguły dokonując wyboru urządzeń, pomija się inne, ważne kryteria decydujące o końcowej jakości obrazu, takie jak: dynamika obrazu, rozdzielczość bitowa etc. Wraz ze wzrostem rozdzielczości matryc kamer IP pojawiły się ograniczenia uniemożliwiające ich powszechne stosowanie. Bardzo dokładnie opisał to Andrzej Walczyk w artykule „*Piksel pikselowi wilkiem*" (*Zabezpieczenia* 1/2010), którego fragment *in extenso* chciałbym przytoczyć. „*Tendencją, którą można zaobserwować na współczesnym rynku CCTV, jest stopniowy wzrost rozdzielczości. (…) W procesie tym widać jednak wyraźną granicę, która przebiega na poziomie nazywanym umownie Full HD. Chodzi o wielkość matrycy równą 1920×1080 pikseli, stosowaną w telewizji programowej, a także w sprzęcie domowym. Ten sam format zaczyna być coraz liczniej reprezentowany w urządzeniach do monitoringu telewizyjnego. Przyczyn tej sytuacji jest wiele. Zauważany do niedawna pęd do bardzo dużych liczb pikseli, sięgających 16 mln, powoli ustępuje zdroworozsądkowym wymaganiom użytkowym, związanym z parametrami kamer, przepływnością typowych sieci IP oraz koniecznością ograniczenia przestrzeni dyskowej rejestratorów. Jakość obrazów z kamer wysokomegapikselowych jest relatywnie niska. Jedynym atutem tych kamer są duże rozmiary matrycy. Poza tym mają same wady. Odznaczają się bardzo niską czułością, niską poklatkowością, wymagają bardzo dobrze skorygowanych, drogich obiektywów, nie mogą być umieszczone w typowych obudowach stosowanych w CCTV, gdyż przednie szyby tych obudów powodują utratę rozdzielczości układu kamera – obudowa – obiektyw. Takie kamery bardziej przypominają wyspecjalizowane aparaty fotograficzne niż urządzenia telewizyjne. Na przykład typowe kamery z przetwornikiem 16 Mpix generują najwyżej trzy klatki obrazowe na sekundę przy pełnej rozdzielczości. Czy to w ogóle można nazwać telewizją?*"

Należy przypuszczać, że kamery Full HD w krótkim czasie staną się standardem w telewizji IP (oczywiście pod warunkiem, że przy takim tempie zmian można jeszcze w ogóle mówić o jakichkolwiek standardach). Technologia Full HD ma niezaprzeczalne zalety i przewagę w stosunku do ciągle dominującej na rynku telewizji analogowej, natomiast nie dziedziczy przedstawionych powyżej wad rozwiązań wielomegapikselowych. W związku z codziennymi kontaktami z instalatorami i inwestorami chciałbym podzielić się jeszcze osobistą refleksją. O wielomegapikselowe systemy monitoringu wizyjnego IP pytają zazwyczaj osoby niedoświadczone, inwestorzy końcowi, nigdy osoby, które mają już doświadczenie i znają ograniczenia, z jakimi spotkały się podczas uruchamiania sieciowych systemów dozoru wizyjnego.

Kolejnym mitem jest niska czułość kamer IP. Pokutuje przekonanie o niskiej czułości przetworników produkowanych w technologii CMOS w porównaniu z przetwornikami CCD stosowanymi w kamerach analogowych. Pod adresem *http://www.novuscctv.pl/pl/node/8027* znajdują się materiały filmowe porównujące czułość kamery analogowej serii B (NVC-BDN5404C) i kamery serii G (NVC-GDN5801C) oraz czułość kamery Full HD NVIP-2DN5001C-1P i standardowej kamery IP. Co prawda czułość kamery analogowej jest wyższa niż czułość kamery sieciowej, jednak nie ma różnicy znacznej, która mogłaby spowodować problemy z wykorzystaniem kamery IP w trudnych warunkach oświetleniowych. Czułość przykładowej kamery IP NVIP-2DN3001H/IR-2P o rozdzielczości Full HD wynosi 0,2 lx/F=1,2 w trybie kolorowym, 0,02 lx/F=1,2 w trybie monochromatycznym i nie odbiega od czułości typowych kamer analogowych.

Stosowane w kamerach sieciowych o rozdzielczości Full HD matryce CMOS mają format 1/2,7", dlatego wymagane jest zastosowanie obiektywów przystosowanych do formatów 1/2" lub 1/3", jednakże w tym przypadku nie dla całego zakresu ogniskowej obraz będzie prawidłowy. W przypadku formatu 1/3" przy minimalnych wartościach ogniskowej może pojawić się zjawisko winietowania, czyli zasłonięcia narożnych obszarów obrazu. W kamerach stosowane jest skanowanie progresywne, co umożliwia poprawną obserwację poruszających się obiektów przy poklatkowości 25 kl./s. W kontekście obserwacji scen o dynamicznie zmieniającym się poziomie oświetlenia bardzo istotne są funkcje automatycznej regulacji ekspozycji. Oprócz standardowego trybu pracy z priorytetem przysłony dostępne są opcje ze stałym czasem otwarcia migawki lub opcje mieszane, z priorytetem przysłony i z możliwością zmian czasu otwarcia migawki w ograniczonym zakresie. W standardowym trybie pracy z automatyczną lub ręczną regulacją czasu otwarcia migawki dostępne wartości mieszczą się w zakresie od 1/1,5 s do 1/10 000 s, zaś w trybie pracy z przedłużonym czasem otwarcia migawki w zakresie od 1/25 s do 1s. Po zmianie obiektywu należy przeprowadzić autokalibrację przysłony w celu zapewnienia prawidłowego punktu początkowego układów sterujących pracą przysłony. W przypadku kamer sieciowych dostępne są również typowe funkcje kamer analogowych, takie jak BLC i WDR, a także cyfrowa redukcja szumów DNR oraz możliwość regulacji równowagi barw.

Wszystkie modele kamer generują równocześnie maksymalnie dwa sieciowe strumienie wizyjne z możliwością



Rys. 2. Interfejs sieciowy pozwalający na zmianę ustawień ekspozycji kamery

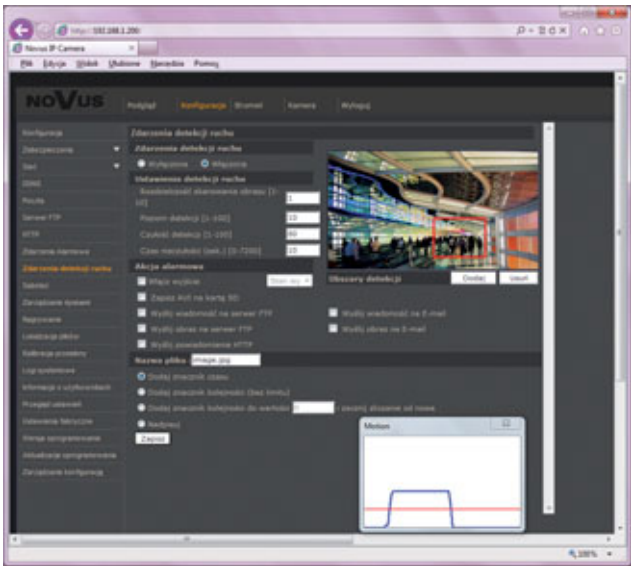
wykorzystania algorytmów kompresji H.264 lub M-JPEG. Jeśli jeden ze strumieni jest wykorzystany do transmisji obrazu o rozdzielczości Full HD (1080p, 25 kl./s), w drugim strumieniu można transmitować obrazy o rozdzielczości D1, także z prędkością 25 kl./s. Ponadto kamera klasyczna (typu *box*) ma dodatkowe wyjście BNC. Dla każdego strumienia wizyjnego możemy ustalić parametry dotyczące jakości (poziomu kompresji) obrazu i przepływności (wielkości generowanego strumienia danych), wybierając tryb CBR (stała wielkość strumienia danych) lub tryb VBR (zmienna wielkość strumienia danych).

Seria kamer IP Full HD ma funkcję detekcji ruchu. Szczególnie przydatny w procesie regulacji parametrów związanych z detekcją ruchu jest dynamiczny wykres obrazujący poziom ruchu w badanej scenie. Pozwala to na prawidłowe ustawienie progu aktywacji detekcji (czerwona linia na wykresie) oraz czułości detekcji ruchu w celu zredukowania liczby fałszywych alarmów. Kamery dysponują mechanizmem antysabotażowym, który umożliwia podjęcie akcji alarmowej w przypadku zasłonięcia obiektywu lub gwałtownej zmiany obserwowanej sceny. Akcja podejmowana na skutek alarmu jest taka sama jak w przypadku aktywacji wejścia alarmowego (dotyczy to wszystkich modeli za wyjątkiem NVIP-2C2011D-P), wykrycia ruchu lub sabotażu i obejmuje: uaktywnienie wyjścia, przejście do trybu nocnego, wysłanie e-maila lub e-maila z załącznikiem (załącznikiem są obrazy w formacie JPG), przesłanie informacji lub pliku na serwer FTP (plikami są obrazy w formacie JPG), wysłanie powiadomienia do serwera HTTP oraz zapis obrazu na karcie pamięci (w formacie AVI). Interfejs sieciowy pozwala na zdefiniowanie dwóch kont klienckich na serwerach poczty wychodzącej (w celu zdalnego powiadamiania użytkownika o zaistniałych zdarzeniach) oraz dwóch adresów serwerów FTP, na które będą przesyłane zdjęcia i nagrania alarmowe. Kamery mają również funkcję maskowania stref prywatności (można zamaskować maksymalnie pięć obszarów i wypełnić je dowolnym kolorem).

W przypadku wszystkich modeli kamer można dokonać zapisu obrazu na kartach pamięci typu microSD i microSDHC, co umożliwia tworzenie dodatkowych archiwów. Zapis może być realizowany w trzech trybach: alarmowym, ciągłym lub zgodnie z harmonogramem. Maksymalna pojemność pojedynczej karty pamięci może wynosić 16 GB, przy czym można posłużyć się funkcją nadpisywania, czyli ciągłego usuwania najstarszych zarejestrowanych nagrań.

Test	Strumień 1 (PAL)	Strumień 2 (PAL)
H.264 + MJPEG	1920×1080/25FPS	720×576/25FPS
	1920×1080/13FPS	1920×1080/13FPS
	1280×720/25PS	1280×720/25PS
MJPEG	1920×1080/25FPS	–
H.264 + H.264	1920×1080/25FPS	720×576/25FPS
	1920×1080/13FPS	1920×1080/13FPS
	1280×720/25PS	1280×720/25PS
H.264	1920×1080/25FPS	–

Tab 1. Tabela ilustrująca zależność między rozdzielczością i liczbą obrazów w jednostce czasu



Rys. 3. Ustawienia detekcji ruchu z wykresem

Przy projektowaniu kamer priorytetowo potraktowano kwestie bezpieczeństwa sieciowego. W urządzeniach zastosowano następujące mechanizmy zabezpieczające przed nieautoryzowanym dostępem do zasobów kamery:

- tworzenie kont dla użytkowników o różnym poziomie uprawnień,
- szyfrowanie połączeń metodą HTTPS wraz z automatyczną generacją certyfikatu,
- filtrowanie adresów IP umożliwiające stworzenie grup użytkowników mających dostęp i nie mających dostępu do kamery, uaktywnianie i definiowanie kluczy uwierzytelniających dla połączeń w sieci lokalnej lub Wi-Fi zgodnej z IEEE 802.1X.

Aby ułatwić zarządzanie kamerami sieciowymi zaimplementowano m.in. protokoły SNMP do zarządzania urządzeniami sieciowymi i UPnP do włączenia lub wyłączenia funkcji dostępu do kamery w otoczeniu sieciowym w systemach Windows XP, Vista i Win 7. Dodatkowo w menu służącym do programowania mechanizmu QoS można zdefiniować sieciowe priorytety dla usług transmisji wizji, dźwięku lub danych sterujących. Wszystkie modele kamer mogą być zasilane poprzez gniazdo sieciowe RJ45 z wykorzystaniem technologii PoE (IEEE 802.3af), a model NVIP-2C2011D-P może być zasilany tylko tą metodą.

Do pełnego scharakteryzowania kamer IP Full HD nie wystarczy jednakże sam opis. Dlatego też przygotowano materiały ilustrujące działanie wybranych modeli kamer w różnych warunkach oświetleniowych.

Wszystkie filmy można obejrzeć pod adresem *http://www.novuscctv.pl/pl/node/8027*.

Patryk Gańko
AAT Holding

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Kamery IP Full HD

Doskonała jakość obrazu, duża funkcjonalność!

Kamera standardowej rozdzielczości

Kamera IP Full HD marki NOVUS®

Full HD

Rozdzielczość megapikselowa 2.0 Mpx Full HD

Praca w trybie dwustrumieniowym

Typowa kamera megapikselowa

Kamera IP Full HD marki NOVUS®

Bardzo wysoka czułość

porównywalna z czułością kamer analogowych

NOVUS 3 teraz lata gwarancji

obiektyw należy do wyposażenia dodatkowego

NMS Compatible

ALNET Compatible

Oprogramowanie NMS (Novus Management System) do monitoringu wizyjnego IP w komplecie!

- Matryca CMOS, 1/2.7" ■ 2.0 megapiksele (1920x1080) ■ Wydłużony czas ekspozycji (DSS) ■ 5 stref prywatności ■ Kompresja H.264 lub M-JPEG
- Prędkość przetwarzania do 25 kl/s (HD 1080p) ■ Praca w trybie dwustrumieniowym ■ Funkcje przed-alarmu i po-alarmu ■ Nagrywanie wideo w formacie AVI
- Funkcja harmonogramu ■ Detekcja ruchu ■ Obsługa kart SD/SDHC

NVIP-2C2011D-P
- Elektroniczna funkcja dzień/noc
- Czułość: 0.1 lx/F=1.5
- Wbudowany mikrofon
- Wbudowany obiektyw f=4 mm
- Zasilanie: PoE

NVIP-2DN2001D-2P
- Mechaniczny filtr podczerwieni
- Czułość: 0.02 lx/F=1.2
- Dwukierunkowa transmisja audio
- Wbudowany obiektyw f=3~9 mm
- Zasilanie: 12 VDC/24 VAC/PoE

NVIP-2DN4001V/IRH-2P
NVIP-2DN3001H/IR-2P
- Mechaniczny filtr podczerwieni
- Wbudowany oświetlacz podczerwieni
- Czułość: 0 lx, IR wł.
- Dwukierunkowa transmisja audio
- Wbudowany obiektyw f=3~9 mm
- Klasa szczelności: IP66
- Zasilanie: 12 VDC/24 VAC/PoE

NVIP-2DN5001-1P
- Mechaniczny filtr podczerwieni
- Czułość: 0.02 lx/F=1.2
- Dwukierunkowa transmisja audio
- Montaż obiektywu: CS
- Zasilanie: 12 VDC/PoE

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

DIVAR 700 HD

Łączy tradycyjne systemy analogowe z systemami sieciowymi

Radomir Dębek

Do niedawna projektowanie systemów CCTV wymagało od projektanta przestrzegania normy PN-EN 50132-1, traktującej dosyć ogólnie o całościowym ujęciu jakości systemu i sprecyzowaniu procedur testowych dla nowego systemu. Konieczne było również uwzględnienie kolejnej normy, PN-EN 50132-7, która określa rodzaj zastosowanych komponentów powstającego systemu telewizji dozorowej. Chodzi głównie o sprecyzowanie parametrów, jakimi ma się charakteryzować cały system, aby spełnić wymogi formalne i oczekiwania klienta. Jeszcze kilka lat temu wybór był prosty. Mniej skomplikowane systemy projektowano zwykle na bazie rejestratorów analogowych. Dla dużych systemów tworzono skomplikowane układy satelitarne, złożone z kilku krosownic, z których korzystało jednocześnie wielu operatorów. Same rejestratory stanowiły wówczas uzupełnienie systemu o funkcjonalność rejestracji sygnału wizyjnego. Z biegiem czasu wykorzystanie protokołu TCP/IP oraz sieci LAN wytworzyło generację sieciowych rejestratorów wizyjnych (tzw. *Network Video Recorder*) przechwytujących strumienie wizyjne w MPEG-4, a później także H.264 (*Bosch Recording Station*).

Takie rejestratory zapisywały materiał wizyjny na dysku lokalnym (kontroler RAID) lub zewnętrznej macierzy SCSI. W dalszej kolejności pojawiły się macierze iSCSI oraz autorskie oprogramowanie firmy Bosch, czyli *Video Recording Manager*, zawiadujące zapisem na tych macierzach.

Czy zatem rejestratory w ich oryginalnej formie mają jeszcze realne szanse jeśli muszą konkurować z technologią IP oraz z wielkim wyścigiem rozdzielczości od 540 linii telewizyjnych do 1920×1080 pikseli?

Obserwacja rozwoju technologii, nie tylko na rynku branży bezpieczeństwa, może wzbudzić co do tego pewne wątpliwości. Powstało wiele rozwiązań bazujących na coraz bardziej popularnym standardzie HD-SDI. Opracowany przez stowarzyszenie SMPTE standard 292M w teorii pozwala na przesłanie cyfrowego sygnału z punktu kamerowego do rejestratora na odległość dochodzącą do 100 metrów przy zastosowaniu przewodu RG-6/RG-11 (dla przepływności 1,5 Gb/s).

Czyżby znaleziono panaceum na wszystkie problemy, jakie niesie ze sobą zastosowanie systemu IP?

Otóż niezupełnie. Większość systemów analogowych wykorzystuje okablowanie wykonane z użyciem kabli typu RG-59 lub RG-6, a pozostałe korzystają z konwerterów przewodu koncentrycznego na przewód sieciowy odpowiedniej kategorii. Problem w tym, że przewody w większości starych instalacji mają złą jakość, a rdzenie samych przewodów RG często nie są już miedziane, lecz miedziowane! Jakość oplotu pozostawia również wiele do życzenia. W efekcie okazuje się, że dopuszczalna odległość między kamerą pracującą w standardzie HD-SDI a rejestratorem spada do kilkudziesięciu metrów.

Czy można zatem zaprojektować nieskomplikowany system odpowiadający obecnym trendom?

Zdecydowanie tak. Firma Bosch, począwszy od 2009 roku, skutecznie promuje platformę pod nazwą kodową Midas. Jako następca Divara-2 nowy rejestrator Divar-XF zapoczątkował kolejny rozdział w historii rejestratorów analogowych. Standardowa funkcjonalność pozwalająca na obsługę ekspandera portów klawiaturowych lub menedżera monitorów, uzupełniona serwerem WWW oraz mechanizmem inteligentnego przeszukiwania (*SmartSearch*), to standard. Jako nowość pojawiła się możliwość wykorzystania macierzy RAID-4, co znacząco podniosło bezpieczeństwo przechowywanych danych. Wymogiem było użycie czterech dysków twardych w rejestratorze i dodatkowa licencja.

Po raz pierwszy pojawiła się możliwość rejestracji nie tylko obrazów z kamer analogowych, ale także – po dodaniu odpowiednich licencji – strumieni wizyjnych z kamer IP z kompresją H.264. Dzięki temu rejestrator stał się urządzeniem hybrydowym pozwalającym na rejestrację obrazów z maksymalnie 16 kamer analogowych oraz osiem kamer sieciowych. W 2010 roku platforma Midas została zmodernizowana i pojawił się rejestrator Divar 700. Wraz z prezentacją nowej wersji pojawiły się zupełnie nowe możliwości w sferze protokołu TCP/IP. Nowa wersja pozwoliła na rejestrację obrazów z 16 kamer analogowych oraz strumieni wizyjnych z 16 kamer IP. W sytuacji gdy projektant tego wymagał, możliwe stało się zastosowanie modelu w pełni sieciowego, rejestrującego strumienie wizyjne z 32 kamer IP. Jeżeli objętość pamięci, na którą składały się cztery dyski HDD (każdy po maksymalnie 2 TB), okazywała się niewystarczająca, z pomocą przychodziły macierze iSCSI.

Firma Bosch oferuje dwie linie modelowe. Na pierwszą składa się typoszereg DLA1200/DLA1400, stanowiący ekonomiczny wariant macierzy iSCSI, będący uzupełnieniem rejestratora i zapisujący maksymalnie 12,8 TB materiału wizyjnego dla najbardziej rozbudowanej wersji. W przypadku systemów profesjonalnych dedykowanym rozwiązaniem są macierze FAS2020/FAS2040. Jeden rejestrator może obsłużyć do 60 jednostek logicznych, co przy ograniczeniu wielkości jednej jednostki logicznej do 8 TB daje w efekcie astronomiczną pojemność 480 TB. Dodatkową zaletą jest możliwość wyboru wersji z dwoma portami sieciowymi o przepustowości 1 Gb/s. Wówczas drugi interfejs sieciowy umożliwia podłączenie macierzy bezpośrednio do rejestratora (*Direct-Attached Storage*), a jednocześnie zmniejsza ruch w sieci i podnosi poziom bezpieczeństwa zapisu dla kamer analogowych w momencie awarii przełącznika sieciowego.

Najnowsza wersja sprzętowa rejestratorów DIVAR serii 700, wprowadzona w listopadzie 2011 r., umożliwia rejestrację obrazu z kamer HD pracujących w standardzie 720P czy 1080P zarówno w wersji stałopozycyjnej, jak i PTZ, w tym także obrazu archiwalnego, zarejestrowanego tymczasowo w pamięci kamery. Projektant musi jedynie pamiętać o sumarycznej przepływności strumieni wizyjnych (w wersji hybrydowej 36 Mb/s, a w wersji sieciowej 72 Mb/s) dla wybranego rejestratora. Z myślą o możliwości monitorowania stanu rejestratorów została także wprowadzona obsługa komunikatów protokołu SNMP. Aby w pełni korzystać z jakości HD, została zaprojektowana aplikacja *Bosch Video Client*, stanowiąca programowe centrum zarządzania rejestratorem. Od momentu wprowadzenia wersji 3.43 oprogramowania rejestratora interfejsem WWW stała się także aplikacja BVC. Wówczas nie jest konieczna instalacja jakiegokolwiek oprogramowania na stanowisku odbiorczym. Sama aplikacja (instalowana na komputerze) stanowi pewnego rodzaju platformę integrującą w jeden system nie tylko rejestratory z rodziny Divar 700, ale również systemy zapisu DLA 1200/1400 lub dekodery wizyjne VIP-XDHD wraz z kamerami prowadzącymi rejestrację na wewnętrznych kartach pamięci.

Zatem decydując się na użycie Divar 700, możemy łatwo zbudować analogowy system szyty na miarę nawet wygórowanych potrzeb. Co więcej, na bazie tego rejestratora można zaprojektować i zrealizować w pełni profesjonalny system IP wykorzystujący najnowsze zdobycze technologii, włącznie z macierzami iSCSI czy kamerami HD. Razem z nową aplikacją, tworzącą pomost między światem analogowym a IP, projektant otrzymuje solidne rozwiązanie do budowy systemu w pełni zgodnego ze współczesnymi trendami technologicznymi pomimo użycia tradycyjnego rejestratora. A w dziedzinie funkcjonalności zarówno samego Divara 700, jak i aplikacji BVC firma Bosch nie powiedziała jeszcze ostatniego słowa…

Radomir Dębek
Bosch Security Systems

Czujki ruchu GRAPHITE i IVORY

GRAPHITE – nowa rodzina zaawansowanych czujek ruchu

Czujki GRAPHITE należą do serii zaawansowanych czujek ruchu oferowanych przez firmę SATEL. Są to pasywne czujki podczerwieni (tzw. PIR) wykorzystujące układ optyczny z płaskimi soczewkami Fresnela. Czujki GRAPHITE wykorzystują w pełni cyfrowe przetwarzanie sygnału przez mikroprocesor, co zapewnia stałość i powtarzalność ich parametrów. W przeciwieństwie do czujek analogowych i prostych czujek cyfrowych procesor przetwarzający sygnał w czujkach GRAPHITE analizuje wiele różnych parametrów. Dzięki temu czujka jest w stanie precyzyjnie odróżnić impuls wytwarzany przez poruszające się w polu jej widzenia osoby od zakłóceń wywołanych światłem słonecznym, konwekcją powietrza z grzejników czy pracą wentylacji.

Ważną cechą czujek GRAPHITE jest funkcja cyfrowej kompensacji temperatury, dzięki której zapewniona jest pełna skuteczność wykrywania intruza niezależnie od temperatury panującej w chronionym pomieszczeniu.

Dzięki dużemu obszarowi detekcji (ponad 100 m^2) można jedną czujką GRAPHITE zabezpieczyć nawet bardzo duże pomieszczenie. Ogranicza to liczbę potrzebnych urządzeń, a dzięki temu ułatwia instalację i pozwala obniżyć całkowite koszty inwestycji. Płynna regulacja czułości umożliwia dopasowanie parametrów pracy czujki do wielkości pomieszczenia i panujących w nim warunków, dzięki czemu czujka ta sprawdzi się doskonale także w mniejszych pomieszczeniach.

Atutem czujek GRAPHITE jest funkcja zdalnego uruchamiania sygnalizowania diodą LED w trybie testowym (bez konieczności uprzedniego otwierania obudowy i przełączania zworki lub mikroprzełącznika). Dzięki temu w normalnej sytuacji czujka zachowuje się w maksymalnie dyskretny sposób, nie sygnalizując naruszeń. Po uruchomieniu testu z manipulatora czujka sygnalizuje wykrycie ruchu wbudowaną diodą, co pozwala łatwo zweryfikować jej poprawne działanie – na przykład po zmianie aranżacji pomieszczenia. Kontrola i pewność poprawnego działania czujek ruchu gwarantuje odpowiedni poziom zabezpieczenia.

Pamięć alarmu to sygnalizowanie wbudowaną diodą LED uruchomienia alarmu przez czujkę. Pamięć ta umożliwia sprawdzenie, która z czujek w systemie uruchomiła alarmowanie – nie trzeba sprawdzać tego w centrali alarmowej. Jest to szczególnie przydatne, jeżeli z jakiegoś powodu kilka czujek podłączono do wspólnego wejścia, co uniemożliwia identyfikację alarmującej czujki w centrali.

Czujki GRAPHITE są wyposażone w system wymiennych soczewek Fresnela. Dzięki temu można je dostosować także do nietypowych zastosowań – np. funkcji kurtyny lub bariery pionowej. Firma SATEL oferuje przydatny w pracy zestaw wymiennych soczewek.

Specjalnym wariantem czujki GRAPHITE jest GRAPHITE PET. Od wersji podstawowej różni się dodatkową funkcją ignorowania sygnałów pochodzących od poruszających się w polu jej widzenia małych zwierząt domowych – np. psów lub kotów. Dzięki tej czujce nie trzeba już więcej wybierać między posiadaniem ulubionego zwierzaka a komfortem wynikającym z poczucia bezpieczeństwa, jakie daje skuteczny system alarmowy.

Warto wspomnieć również o certyfikatach uzyskanych przez czujki GRAPHITE w wyniku długotrwałych testów w niezależnym europejskim akredytowanym laboratorium badawczym. Dzięki nim czujki GRAPHITE mogą być stosowane w systemach alarmowych wymagających zgodności z normą EN50131 – nawet w tak wymagających obiektach jak banki czy budynki użyteczności publicznej.

Fot. 1. Czujki ruchu IVORY i GRAPHITE

IVORY – udane połączenie polskiej myśli technicznej z japońską technologią

Najbardziej zaawansowaną spośród oferowanych przez firmę SATEL pasywnych czujek podczerwieni jest IVORY, która wykorzystuje rozwiązania zastosowane wcześniej w czujkach GRAPHITE. Do jej budowy wykorzystano specjalne zwierciadło sekcyjne opracowane w ramach współpracy firmy SATEL z japońskim producentem precyzyjnych układów optycznych, firmą JAPANPLALENS. Kooperacja zaowocowała opracowaniem zwierciadła przewyższającego parametrami stosowane w tradycyjnych czujkach soczewki Frensela.

Główną zaletą nowego zwierciadła jest znacznie poprawiony w porównaniu z wcześniej stosowanymi soczewkami przestrzenny rozkład stref wykrywania. Oznacza to, że czujka IVORY wykryje intruza szybciej i skuteczniej. Zwiększenie skuteczności będzie szczególnie zauważalne w przypadku pomieszczeń o zróżnicowanej zabudowie. Ponadto uwzględnienie strefy podejścia pozwala efektywnie zabezpieczyć obszar praktycznie bezpośrednio pod czujką. Zaawansowane zwierciadło umożliwia także skuteczniejsze ogniskowanie energii podczerwieni na elemencie fotoczułym. Czujka IVORY pracuje dzięki temu z silniejszym sygnałem, co z kolei zwiększa odporność na fałszywe alarmy spowodowane przez różnego rodzaju zaburzenia w chronionej przestrzeni.

Kolejną zaletą IVORY jest sposób analizowania sygnału przez procesor czujki. Przetwarza on na bieżąco sygnał pochodzący z pyroelementu na postać cyfrową. Sygnał ten jest następnie poddawany szczegółowej analizie w celu określenia, czy jego wystąpienie ma związek z obecnością człowieka przemieszczającego się w polu widzenia czujki, czy jest to tylko typowe zakłócenie spowodowane np. przez przeciąg lub światło reflektorów samochodowych. Dzięki tym mechanizmom czujka IVORY jest jednym z najbardziej niezawodnych urządzeń tego typu, zapewniając skuteczność działania charakterystyczną dla najwyższej klasy czujek ruchu.

Dzięki estetycznej, zgrabnej obudowie czujka IVORY świetnie prezentuje się zarówno we wnętrzach nowoczesnych, jak i w tych urządzonych klasycznie. Ponadto mechaniczna konstrukcja czujki zapewnia zamknięcie przestrzeni układu optycznego nie tylko przy zamkniętej obudowie, ale też w czasie montażu, gdy obudowa jest zdjęta. Ogranicza to możliwość wniknięcia drobin kurzu czy pyłu budowlanego do newralgicznych miejsc, wydłużając żywotność i zwiększając niezawodność precyzyjnego układu optycznego czujki.

W typowych zastosowaniach czujki GRAPHITE i IVORY zapewnią bardzo dużą skuteczność i niezawodność. Warto o tym pamiętać, ponieważ to właśnie czujki będą decydować o jakości zabezpieczenia. Użycie nawet najbardziej zaawansowanej centrali w połączeniu z czujkami słabej jakości spowoduje, że system nie będzie wystarczająco skuteczny lub przysporzy niepotrzebnych problemów związanych z koniecznością interwencji serwisowych.

SATEL

Systemy alarmowe **Satel**

czujki ruchu: **AMBER, AQUA, GRAPHITE, SILVER, IVORY**

Połączenie pasji i zaawansowanej inżynierii pozwoliło firmie SATEL na zaprojektowanie szerokiej gamy czujek - od prostej i niezawodnej czujki **AMBER**, przez czujkę **IVORY** będącą owocem współpracy polsko-japońskiej, po zaawansowaną czujkę **SILVER** zapewniającą najwyższej klasy bezpieczeństwo. Nieustanne dążenie do innowacji zaowocowało m.in. takimi unikalnymi rozwiązaniami jak energooszczędne oświetlenie awaryjne LED zintegrowane z czujką ruchu w urządzeniu **AQUA Luna**.

Wszystkie czujki w ofercie firmy SATEL łączy niezawodność i korzystny stosunek możliwości do ceny - dlatego są tak chętnie wybierane przez profesjonalistów branży zabezpieczeń.

Skuteczna detekcja

- ponad 20 lat doświadczenia
- kontrola jakości na każdym etapie produkcji
- 100% przetestowanych urządzeń

Satel®

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

Galaxy Flex

nowy system sygnalizacji włamania i napadu przystosowany do małych i średnich instalacji

Tomasz Szklarz

Seria central Galaxy Flex firmy Honeywell to rozwiązania w pełni integrujące system alarmowy i system kontroli dostępu, które oferują nowy poziom wygody i elastyczności działania w mniejszych systemach bezpieczeństwa. Trzy bogate w funkcje modele Galaxy Flex mają budowę modułową, więc można dostosować je do specyficznych potrzeb użytkownika. Klienci i instalatorzy ceniący rozwiązania Honeywell w większych instalacjach mogą od tej chwili zastosować je w systemach, w których znajduje się 20, 50 lub 100 linii oraz do ośmiu przejść

Fot. 1. Centrala Galaxy Flex z klawiaturami i systemem bezprzewodowym

Oparte na sprawdzonej technologii urządzenia Galaxy Flex są skalowalne, kompatybilne z innymi centralami Galaxy, identyczne z nimi w sposobie łączenia i konfigurowania i wyposażone w takie same klawiatury oraz takie same moduły rozszerzeniowe i komunikacyjne. Dopełniają serię Galaxy, która może być odtąd stosowana w instalacjach o dowolnej wielkości. Dzięki wspólnym dla całej serii urządzeniom peryferyjnym można obniżyć koszty magazynowania. Osoby doświadczone w pracy z modelami Dimension czy G3 mogą skonfigurować model Flex bez problemu, dzięki czemu firmy instalatorskie mogą ograniczyć koszty szkolenia personelu.

Rzućmy okiem na poszczególne modele. Galaxy Flex 20 to produkt przystosowany do małych systemów obejmujących do 20 linii oraz dwóch przejść. Obsługuje do 25 użytkowników, czytników i klawiatur z wbudowanymi czytnikami bezpośrednio do magistrali danych.

Warto nadmienić, że opisywana linia central była przygotowywana z myślą o zapewnieniu projektantom i instalatorom maksymalnej wygody i komfortu podczas pracy. Wymieńmy najistotniejsze z tego punktu widzenia cechy i funkcje. Wygodna i odporna obudowa centrali Galaxy Flex umożliwia zredukowanie czasu i kosztów instalacji oraz okablowania. Moduły bezprzewodowe i komunikacyjne można zamocować wewnątrz specjalnie zaprojektowanych zatrzaskowych slotów. Akumulator może być zainstalowany wewnątrz obudowy. Sposób podłączenia do magistrali RS485 urządzeń peryferyjnych w postaci klawiatur, czytników, modułów rozszerzeń czy modułów komunikacyjnych można nazwać metodą *plug and play* – elementy

Fot. 2. Klawiatura jako uzupełnienie eleganckiego wnętrza

posiada rejestr 500 zdarzeń alarmowych oraz dodatkowy rejestr 500 zdarzeń kontroli dostępu. Model Flex 50 jest przeznaczony dla średnich systemów obejmujących do 50 linii i ośmiu przejść. Obsługuje do 50 użytkowników, a rejestry mogą obejmować po 1000 zdarzeń. Model Flex100 obsługuje do 100 linii i ośmiu przejść. Pracuje z maksymalnie 100 użytkownikami, zapisuje w logach po 1000 zdarzeń. Dodajmy, że rekomendowanym sposobem kontrolowania drzwi przez system Flex jest wykorzystanie znanego od lat modułu DCM (*Door Control Module*) C080. Do tego modułu można podłączyć dwa czytniki. Jest on kompatybilny z większością urządzeń zgodnych ze standardem Wiegand. Istnieje również możliwość podłączenia peryferyjne są automatycznie wykrywane po podłączeniu ich do źródła zasilania. To także pozwala zaoszczędzić czas i ułatwia pracę mniej doświadczonym instalatorom. Gdy prowadzenie przewodów jest niemożliwe, np. ze względów estetycznych, Galaxy Flex pozwala na bezprzewodowe przyłączenie odpowiednich elementów systemu – bez obniżenia niezawodności. Opatentowana technologia dwukierunkowej komunikacji radiowej z inteligentnym routingiem zapewnia instalatorowi niezwykłą wygodę, a użytkownikowi pewność funkcjonowania. System sam rozpozna najlepszą ścieżkę transmisji radiowej, a jeśli dojdzie do zmiany otoczenia wpływającej na propagację sygnału, ścieżka ta zostanie zaktualizowana bez konieczności

Fot. 3. Klawiatury TouchCenter, MK8 i MK7

jakiejkolowiek ingerencji użytkownika. Centrale Flex mogą obsłużyć do ośmiu modułów bezprzewodowych działających na częstotliwości 868 MHz, co umożliwia obsługę do 100 bezprzewodowych linii i do 98 pilotów. System jest kompatybilny ze wszystkimi sensorami Honweywell z protokołem Alpha.

Kolejną istotną cechą central Flex jest różnorodność zapewnianych przez nie opcji komunikacyjnych. GSM/GPRS, Ethernet oraz linia telefoniczna umożliwiają maksymalne dopasowanie centrali do warunków użytkowania i niezawodną transmisję sygnału w każdej sytuacji. Centrala Flex, podobnie jak inne centrale Galaxy, może być programowana i monitorowana poprzez oprogramowanie Remote Servicing Suite (RSS). Używając tego software'u instalator może sprawnie skonfigurować system dzięki intuicyjnemu interfejsowi, łącząc się z centralą zdalnie – poprzez wyżej wymienione kanały komunikacyjne – lub lokalnie – za pomocą typowego przewodu mini-USB. Należy zwrócić uwagę na niespotykaną w systemach tej wielkości możliwość zdalnej diagnostyki stanu systemu. Monitorowanie stanu zasilania, akumulatorów, bezpieczników, przełączników sabotażowych, poziomów napięć, wartości rezystancji linii itp. jest możliwe bez użycia dodatkowych narzędzi czy mierników oraz bez konieczności odwiedzania chronionego obiektu. Daje to oczywiste i przeliczalne na gotówkę oszczędności firmom zajmującym się instalacją i konserwacją systemów zabezpieczeń. Zdalne monitorowanie zasilania i stanu akumulatorów jest możliwe w przypadku zastosowania dedykowanych zasilaczy P025 (lub P026 w wersji z koncentratorem linii). Zarówno rutynowa inspekcja, jak i zaplanowana konserwacja, czy też proste sprawdzenie statusu systemu, mogą być sprawnie wykonane zdalnie lub lokalnie, za pomocą stacjonarnego lub przenośnego PC.

Inną istotną cechą central Galaxy Flex jest wysoki poziom wygody zapewniany użytkownikowi końcowemu. Przyczynia się do tego rozbudowana seria urządzeń sterujących. Klawiatura MK7 jest produktem obecnym na rynku od lat i sprawdzonym. Urządzenie to ma tradycyjny wygląd, trwałą konstrukcję i klapkę zabezpieczającą, dlatego sprawdza się w środowisku przemysłowym. MK8 to klawiatura o nowoczesnym wyglądzie, przeznaczona do użycia we wnętrzach, w których liczy się estetyka. TouchCenter jest klawiaturą graficzną z ekranem dotykowym, która zapewnia pełną, wygodną i niezwykle intuicyjną obsługę systemu, jednocześnie będąc doskonałym uzupełnieniem prestiżowych wnętrz.

Centrale Galaxy Flex spełniają oczekiwania współczesnego rynku. Są odpowiednie do małych i średnich instalacji, a jednocześnie pozwalają korzystać ze wszystkich zalet rozbudowanych central Galaxy. Są zgodne z normą EN50131 Grade2.

Tomasz Szklarz
ADI Global Distribution

Galaxy® Flex

Seria central do małych i średnich systemów bezpieczeństwa

	Flex 20	Flex 50	Flex 100
Maksymalna liczba linii	12-20	12-50	12-100
Moduły bezprzewodowe	8	8	8
Grupy	3	4	8
Zasilacz na płycie	1 A	1 A	2 A
Użytkownicy	25	50	100
Schematy tygodniowe	2	4	4
Połączenia programowe	5	5	5
USB port	Tak	Tak	Tak
Moduł Telekom	Tak	Tak	Tak
IP	Opcja	Opcja	Opcja
GSM/GPRS	Opcja	Opcja	Opcja
Klawiatury	3	4	8
KeyProx	3	4	8
Drzwi	2	8	8
TouchCenter	1	1	1
Zgodność z EN	Grade2	Grade2	Grade2

Honeywell

Seria central Galaxy Flex firmy Honeywell to rozwiązanie w pełni integrujące system alarmowy i kontroli dostępu, które daje nowy poziom elastyczności i łatwości instalacji wśród systemów małych i średnich, przy pełnej zgodności z EN50131 Grade2.

Linia Galaxy Flex składając się z trzech modeli i zapewniając modułową budowę systemu pozwala na dostosowanie możliwości instalacji do wszelkich specyficznych potrzeb klienta.

ADI GLOBAL DISTRIBUTION

ADI Global Distribution
Lubieszyn 8, 72-002 Dołuje /k Szczecina
Tel: +48 91 485 40 60-79
Warszawa, 03-310 ul. Odrowąża 15
Tel: +48 22 519 76 57-58

www.adiglobal.com/pl

Zdalny dostęp do central alarmowych

Szybsza i tańsza konfiguracja oraz serwis

Artur Płatek

Konfiguracja współczesnych rozbudowanych central alarmowych realizujących zaawansowane funkcje bywa zadaniem czasochłonnym i podatnym na błędy, gdy jest realizowana w tradycyjny sposób za pomocą manipulatora. Producenci central alarmowych starają się rozwiązać problem, dostarczając ułatwiające i automatyzujące ten proces oprogramowanie na komputery PC. Jedyne, co trzeba zrobić w celu dokonania zmian, to ustanowić połączenie z centralą za pomocą dedykowanego dla niej interfejsu bądź zdalnie dokonać autoryzacji. Niniejszy artykuł omawia niektóre techniczne aspekty różnego rodzaju metod dostępu. Przedstawiony zostanie transmiter GPRS LX20G-3C firmy EBS, umożliwiający zdalny dostęp do centrali alarmowej za pośrednictwem połączenia GPRS

Dostęp do centrali za pomocą połączenia lokalnego

Najpopularniejszą metodą uzyskiwania dostępu do centrali alarmowej – oprócz konfiguracji za pomocą manipulatora – jest lokalne połączenie dedykowanym kablem. Niewątpliwą zaletą takiej metody jest łatwość uzyskania połączenia. Nie są do tego potrzebne żadne dodatkowe elementy oprócz komputera i specjalizowanego kabla. Szybkość połączenia jest zazwyczaj duża, a opóźnienia transmisji niewielkie. Niestety, instalator musi znajdować się w obiekcie, w którym jest zainstalowana centrala alarmowa – a w sytuacji gdy niezbędna jest bardzo szybka reakcja serwisowa, nie zawsze istnieje taka możliwość. Wtedy nieoceniona staje się możliwość zdalnego dostępu.

Zalety zdalnego dostępu

Szybka reakcja na awarie to nie jedyna sytuacja, w której zdalny dostęp może być przydatny. Połączenie takie może być używane także do:

- okresowych audytów systemu alarmowego polegających na kontroli poszczególnych jego elementów, o ile centrala alarmowa na to pozwala,
- odczytu historii zdarzeń,
- zmiany konfiguracji systemu alarmowego ze względu na stwierdzone błędy konfiguracji podczas instalacji lub zmiany konfiguracji obiektu,
- zaprogramowania konfiguracji zgodnie z wymaganiami klienta po instalacji i wstępnej konfiguracji systemu alarmowego przez mniej wykwalifikowany personel.

Dzięki możliwości zdalnej konfiguracji można znacząco zredukować koszty obsługi przez zmniejszenie liczby wyjazdów serwisowych bądź też realizację ich przez mniej wykwalifikowany personel.

Obecnie zdalny dostęp do centrali alarmowej można uzyskać za pomocą:

- analogowej linii telefonicznej,
- sieci Internet,
- sieci GSM/GPRS.

Dostęp za pomocą linii telefonicznej

Obecnie możliwość zrealizowania połączenia za pomocą analogowej linii telefonicznej jest najbardziej rozpowszechnionym sposobem zdalnego dostępu. Dzieje się tak, ponieważ zdecydowana większość central alarmowych jest wyposażona w dialer telefoniczny, służący do raportowania zdarzeń do centrum monitorowania. Z tego względu koszty związane z instalacją dodatkowych urządzeń transmisyjnych po stronie systemu alarmowego mogą zostać wyeliminowane.

Niestety, w Polsce – mimo powszechnej obecności dialerów w centralach alarmowych – linia telefoniczna (PSTN) bardzo rzadko jest przyłączana do systemu alarmowego. Wynika to z wysokich kosztów utrzymania linii telefonicznej oraz niedostępności jej w danej lokalizacji lub dostępności tylko w technologii VoIP (*Voice over Internet Protocol*), uniemożliwiającej poprawne przesłanie raportów zdarzeń do centrum monitorowania. W tych realiach obwód dialera telefonicznego w centrali alarmowej jest traktowany najczęściej jako interfejs do alarmowych nadajników radiowych, GSM/SMS lub GPRS czy Ethernet, symulujących odbiornik telefoniczny i przekazujących zdarzenia do stacji monitorowania za pomocą medium, które nadajnik obsługuje.

Jeśli jednak analogowa linia telefoniczna (PSTN) jest podłączona do centrali alarmowej, zdalny dostęp jest realizowany przez wykonanie połączenia telefonicznego do systemu alarmowego. Za realizację połączenia odpowiada analogowy modem telefoniczny po stronie jednostki realizującej zdalny dostęp. Z jednej strony modem jest przyłączony do komputera operatora/instalatora, a z drugiej do analogowej linii telefonicznej PSTN. Eliminuje to możliwość zdalnego dostępu spoza biura, np. w trakcie podróży służbowej. Schemat połączeń obrazuje rys. 1.

Zestawienie połączenia z centralą alarmową, inicjowanego zdalnie przez instalatora, może być zrealizowane przez:

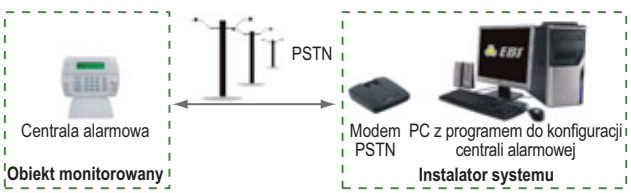
- wykonanie połączenia, które zostanie automatycznie odebrane przez centralę alarmową po skonfigurowanej liczbie sygnałów dzwonka,
- odrzucenie pierwszego zrealizowanego połączenia do centrali i automatycznie odebranie drugiego połączenia, jeśli zostanie ono wykonane w zadanym czasie,
- zrealizowanie połączenia zwrotnego (tj. od centrali alarmowej do instalatora), które zostanie zainicjowane przez użytkownika, lub automatycznie przez centralę alarmową.

Należy pamiętać, że centrale alarmowe niektórych typów wymagają zezwolenia użytkownika na zdalny dostęp do nich. Jednak w większości przypadków centrala alarmowa akceptuje przychodzące połączenia, a autoryzacja jest realizowana na podstawie wymienianych na początku transmisji kodów dostępu. Niejednokrotnie nie ma możliwości uzyskania zdalnego dostępu do centrali alarmowej, gdy jest ona w trybie dozoru.

Po zestawieniu połączenia z centralą alarmową dane są przesyłane w zdecydowanej większości przypadków za pomocą protokołu Bell103, rzadziej V.21. Czasami, zazwyczaj w bardziej rozbudowanych centralach alarmowych, stosowane są protokoły zapewniające wyższe prędkości transmisji kosztem mniejszej odporności na zakłócenia.

Bell103 jest formatem opracowanym w 1962 roku w AT&T i oferuje prędkość transmisji 300 b/s. Protokół ten jest chętnie stosowany, ponieważ wykorzystuje go także transmisja zdarzeń alarmowych w formacie SIA-FSK, dzięki czemu implementacja modemu w centrali alarmowej nie wiąże się praktycznie z żadnymi dodatkowymi kosztami. Mimo swojej prostoty protokół ten jest bardzo odporny na zakłócenia. Z doświadczenia autora wynika, że przy dobrze zaprojektowanym modemie i dialerze centrali możliwa jest poprawna transmisja danych podczas prowadzonej w tle rozmowy głosowej. Dodatkowo, dzięki prostocie protokołu koszt elementów niezbędnych do realizacji modemu 300 b/s w centrali jest niewielki.

Bell103 wykorzystuje modulację FSK (*Frequency Shift Keying*). Możliwa jest komunikacja *full duplex* (jednoczesna transmisja danych w dwóch kierunkach), polegająca na tym, że jedna strona używa częstotliwości nośnej 1170 Hz, a druga – 2125 Hz. Dane są kodowane za pomocą ośmiu bitów



Rys. 1. Schemat połączeń

danych z bitem startu na początku (o wartości zero) i bitem stopu na końcu (o wartości jeden). Bitowi jeden odpowiada częstotliwość nośna plus 100 Hz, a bitowi zero – częstotliwość nośna minus 100 Hz. Gdy nadajnik nie ma danych do wysłania, wystawia sygnał o częstotliwości odpowiadającej logicznej jedynce (częstotliwość nośna plus 100 Hz). Mówimy wtedy, że nadajnik podtrzymuje sygnał nośny. Protokół V.21 to zmodyfikowana wersja protokołu Bell103 – zmienione zostały używane częstotliwości nośne (1080 Hz i 1750 Hz).

Dane wymieniane między komputerem do konfigurowania centrali a samą centralą alarmową są przekazywane w trybie żądanie – odpowiedź, czyli w takim przypadku można użyć komunikacji typu *half duplex* (w danej chwili tylko w jedną stronę).

Niestety większość central alarmowych po wysłaniu danych, których zażądało oprogramowanie konfigurujące, zamiast podtrzymywać, wyłącza sygnał nośny w oczekiwaniu na następne żądanie. Nie każdy modem potrafi sobie poradzić z taką sytuacją i może to powodować:

1) wygenerowanie błędnych danych przy zaniku sygnału nośnego centrali alarmowej,
2) rozłączenie połączenia, bo zanik sygnału nośnego stanowi kryterium zerwania połączenia.

Jeśli występuje zjawisko opisane w punkcie 2, można podczas konfigurowania modemu zdefiniować maksymalny dozwolony czas zaniku sygnału nośnego (poleceniem ATS10=X, gdzie X przyjmuje wartości od jednego do 255 i oznacza czas w wielokrotnościach 1/10 sekundy). Jednak nie wszystkie modemy poprawnie obsługują to polecenie. W związku z powyższym aby zrealizować połączenie z centralą, należy zainstalować modem poprawnie działający – zazwyczaj producent centrali rekomenduje typ modemu właściwie współpracującego z jego centralami lub oferuje własny modem.

Ze względu na małą prędkość transmisji (300 b/s, czyli 30 bajtów na sekundę) czas transmisji danych konfiguracyjnych w zależności od typu centrali może wynosić od pojedynczych minut do godziny. Koszt połączenia zależy oczywiście od taryfy i operatora – opłatę naliczaną za czas połączenia ponosi strona inicjująca połączenie. Transmisja realizowana z prędkością 300 b/s jest odporna na zakłócenia, a więc stabilna, co oznacza, że gdy połączenie zostanie zestawione, to przy dobrej jakości modemie i dobrze zaprojektowanej centrali alarmowej nie powinno zostać zerwane.

Dostęp za pomocą Internetu

Bardziej rozbudowane centrale alarmowe są wyposażone w moduł umożliwiający podłączenie do sieci LAN, dzięki której dostęp do centrali można uzyskać za pośrednictwem Internetu. W lokalizacjach, w których Internet jest dostępny, stanowi to idealne rozwiązanie ze względu na znikome koszty związane z transmisją oraz zapewnioną wysoką jej prędkością, która może przewyższać nawet prędkość umożliwianą przez połączenie lokalne za pomocą dedykowanego kabla.

W rozwiązaniu takim oprogramowanie do konfiguracji centrali zawiera niezbędne środki gwarantujące zestawienie połączenia z centralą alarmową. Dane wymieniane między oprogramowaniem do konfiguracji a centralą alarmową są transmitowane za pomocą protokołu zdefiniowanego przez producenta centrali.

Aby jednak połączenie doszło do skutku, należy zapewnić połączenie w sieci między centralą alarmową a oprogramowaniem do konfiguracji. Można to zrealizować na kilka sposobów:

1) Centrala alarmowa staje się serwerem – konfigurator centrali inicjuje połączenie z centralą. W takim przypadku konfigurator musi znać jej adres i port, a ruch przychodzący do centrali musi być odblokowany (udostępniony).
2) Konfigurator staje się serwerem – centrala inicjuje połączenie z konfiguratorem centrali. W takim przypadku centrala musi znać jego adres i port, a ruch przychodzący do konfiguratora musi być odblokowany (udostępniony).
3) Komunikacja przez serwer pośredniczący, zazwyczaj dostarczany przez producenta centrali. W takim przypadku zarówno centrala, jak i konfigurator łączą się z serwerem pośredniczącym, który realizuje wymianę danych między centralą alarmową a konfiguratorem.
4) Inne, np. zestawienie między sieciami tunelu, w którym znajduje się konfigurator i centrala alarmowa.

Każda z tych metod ma swoje zalety i wady. Zastosowaną metodę zestawienia połączenia narzuca producent centrali alarmowej. Mimo obecności sieci komputerowej może się okazać, że ze względów bezpieczeństwa wymagany przez producenta sposób realizacji połączenia nie może zostać wykonany, np. w przypadku instytucji bankowych jest małe prawdopodobieństwo, aby można było zestawić połączenie za pomocą metody z punktu 1.

Dostęp za pomocą sieci GSM/GPRS

Malejące koszty modemów GSM powodują, że centrale alarmowe coraz częściej są w nie wyposażane. Umożliwia to oprócz monitorowania w sieci GSM zdalne sterowanie systemem alarmowym oraz jego konfigurację za pomocą sieci GSM/GPRS i dostępnych w niej usług. W przypadku tej drogi transmisji bazuje się na infrastrukturze sieciowej operatora GSM, a więc system alarmowy nie musi korzystać z sieci komputerowej klienta. Dzięki temu zapewnienie łączności z centralą może okazać się znacznie prostsze niż w przypadku zdalnego dostępu przez Internet. W centrali musi znaleźć się karta SIM, dzięki której centrala uzyska dostęp do sieci GSM/GPRS.

Do uzyskiwania dostępu do centrali za pomocą sieci GSM wykorzystywane są najczęściej trzy usługi:

– SMS,
– połączenie CSD (*Circuit Switched Data*),
– połączenie GPRS.

Droga SMS-owa służy najczęściej do zdalnego sterowania wyjściami lub załączaniem i wyłączaniem systemu. Ze względu na małą przepustowość raczej nie jest używana do pobierania historii zdarzeń ani zdalnej konfiguracji. Niewątpliwe zalety to dostępność usługi (SMS-a można wysłać z dowolnego telefonu komórkowego) oraz łatwość dostępu do centrali (jednostka, która chce uzyskać zdalny dostęp do systemu alarmowego, musi znać tylko numer telefonu karty SIM zainstalowanej w centrali alarmowej). Autoryzacja dostępu do systemu alarmowego może być zrealizowana za pomocą kodów dostępu i (lub) listy dozwolonych numerów telefonów, z których zdalny dostęp jest możliwy.

Połączenie CSD w sieci GSM to odpowiednik połączenia poprzez modem analogowy. Tak samo jak w przypadku połączenia linią telefoniczną, po stronie zdalnej wymagany jest modem – tym razem modem GSM z aktywną kartą SIM, na której uruchomiona jest usługa CSD. Usługa CSD musi być także aktywowana na karcie SIM włożonej do centrali alarmowej. Wymiana danych jest kontrolowana za pośrednictwem oprogramowania do konfiguracji centrali alarmowej, dostarczanego przez producenta centrali. Prędkość transmisji uzyskiwana za pomocą CSD to 9600 b/s lub 14 400 b/s, w zależności od operatora i typu modemu GSM po stronie centrali alarmowej oraz stanowiska, z którego uzyskiwany jest dostęp. Jeśli protokoły wymiany danych między centralą a oprogramowaniem konfigurującym nie zostaną dobrze zaprojektowane, może się okazać, że – mimo większej prędkości transmisji niż w przypadku prędkości oferowanej przez standardowe dialery PSTN w centralach alarmowych (300 b/s) – zysk wynikający z większej prędkości transmisji nie przełoży się na proporcjonalnie krótszy czas wymiany danych. Dzieje się tak dlatego, że w odróżnieniu od połączenia analogową linią telefoniczną dane wysyłane za pomocą modemu GSM trafiają do odbiorcy z dużym opóźnieniem, sięgającym nawet jednej sekundy. Jeśli zastosowany przez producenta centrali alarmowej charakter wymiany danych za pośrednictwem CSD to żądanie – odpowiedź, może się okazać, że efektywna prędkość transmisji jest niewiele większa niż w przypadku analogowej linii telefonicznej. Autoryzacja, podobnie jak w przypadku SMS-ów, może zostać zrealizowana przez kody dostępu i (lub) listy dozwolonych numerów telefonów.

Najmniej kosztownym i najbardziej efektywnym sposobem uzyskania dostępu do systemu alarmowego za pomocą sieci GSM jest wykorzystanie technologii GPRS. Jeśli usługa GPRS jest uruchomiona na karcie SIM zainstalowanej w centrali alarmowej, centrala może w technologii GPRS uzyskać dostęp do sieci IP – może to być prywatna sieć wydzielona przez operatora GSM dla agencji ochrony, do której należy karta SIM, lub publiczna sieć Internet. Tym samym centrala uzyskuje dostęp do sieci IP analogicznie jak centrale, które można przyłączyć do sieci LAN – ale ten dostęp do sieci jest realizowany w innej technologii. W odróżnieniu jednak od central alarmowych umożliwiających wpięcie do sieci LAN, w tym przypadku centrala alarmowa nie jest dołączana do sieci klienta końcowego, lecz bezpośrednio do publicznej sieci Internet lub sieci agencji ochrony. Ma to niebagatelne znaczenie, gdyż zdalny dostęp do centrali alarmowej może być zrealizowany znacznie łatwiej (nie musi podlegać polityce bezpieczeństwa sieci IP instytucji, w której system alarmowy jest zainstalowany). Centrala alarmowa może być cały czas połączona z docelową siecią IP – w przypadku technologii GPRS opłata jest pobierana za liczbę przesłanych danych.

Przy uzyskiwaniu zdalnego dostępu do centrali alarmowej obowiązują takie same zasady jak w przypadku dostępu do central alarmowych podłączanych do sieci LAN omówionych w poprzednim rozdziale.

Prędkość transmisji, jaką można uzyskać w sieci GPRS, to maksymalnie ok. 48 kb/s w jedną stronę. Niemniej jednak technologia ta cierpi ze względu na duże opóźnienia, które są tylko odrobinę mniejsze niż w przypadku technologii CSD. Dodatkowo opóźnienia te oraz prędkość transmisji mogą się zmieniać w zależność od ruchu w sieci GSM – połączenia GPRS mają w niej najniższy priorytet.

Dostęp do istniejących central za pomocą transmiterów IP/GSM/GPRS

Większość istniejących instalacji oraz tańsze centrale alarmowe nie są wyposażone ani w zintegrowany moduł umożliwiający podłączenie ich do sieci LAN, ani w modem GSM. Mimo że posiadają dialer telefoniczny, nie są także przyłączane do sieci telefonicznej. Aby w takim przypadku uzyskać zdalny dostęp do centrali, system alarmowy musi zostać wyposażony w urządzenie transmisyjne, które taki dostęp zapewni. Ponieważ w zdecydowanej większości takich instalacji montowane są transmitery IP/GSM/GPRS raportujące zdarzenia do stacji monitorowania, wydaje się oczywiste, że to one powinny zapewnić także możliwość zestawienia połączenia z centralą alarmową.

Interfejsem łączącym centralę z transmiterem może być interfejs do lokalnego konfigurowania lub dialer telefoniczny. Ze względu na różnorodność interfejsów do lokalnego konfigurowania systemów, ich różną konfigurację i wymagane prędkości transmisji oraz fakt, że niektóre starsze lub prostsze centrale mogą nie być w taki interfejs wyposażone, najczęściej rolę interfejsu pełni dialer. Mimo małej przepustowości jest on idealnym rozwiązaniem ze względu na jeden obowiązujący w nim protokół wymiany danych (w większości przypadków Bell103 lub V.21) oraz łatwość przyłączenia – wymagane są tylko dwa przewody podłączane do listwy ARK w centrali i transmiterze. Mała prędkość transmisji, wprawdzie niezbyt korzystna dla użytkownika końcowego, może być zbawienna ze względu na niwelację opóźnień w sieci GSM/GPRS. Dzięki interfejsowi, jaki zapewnia dialer telefoniczny, teoretycznie możliwe jest zdalne połączenie z dowolną centralą alarmową, w której *downloading* (*zgrywanie do centrali*) jest realizowany z prędkością 300 b/s.

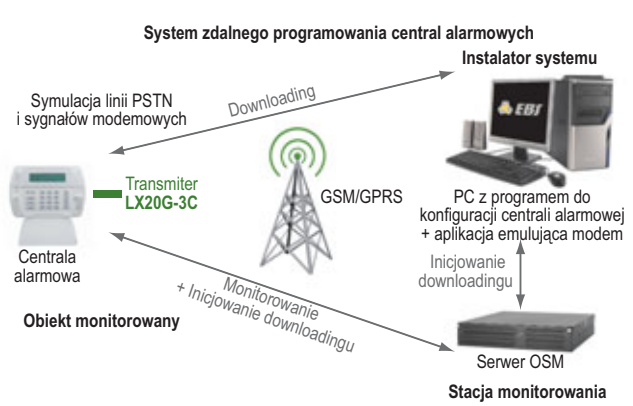
Gdy transmiter GSM jest podłączony do centrali alarmowej przez dialer, dostęp do centrali może zostać zrealizowany za pomocą CSD lub GPRS. Choć połączenie CSD zapewnia łatwiejsze uzyskanie zdalnego dostępu do centrali (wystarczy znać numer telefonu karty SIM zainstalowanej w transmiterze), a raz zestawione będzie miało w trakcie trwania mniej więcej te same parametry (tj. czas opóźnienia) – to jednak ze względu na koszty znacznie korzystniejsze jest połączenie GPRS. W przypadku połączenia GPRS opłata jest pobierana za liczbę przesłanych danych, a w przypadku CSD za czas połączenia. Aby porównać koszty, załóżmy skrajny przypadek, gdy dla bardzo rozbudowanej centrali alarmowej dane między centralą a oprogramowaniem konfigurującym są wymieniane przez godzinę. Przy założeniu, że koszt połączenia wynosi 29 gr za minutę, w przypadku połączenia CSD za transfer zapłacimy 60×29 gr = 17,40 zł! A ile będzie kosztować taka sama operacja wykonana za pomocą połączenia GPRS? Aby to wyliczyć, należy przede wszystkim oszacować ilość danych przesłanych za pomocą połączenia GPRS. Prędkość transmisji za pomocą linii telefonicznej wynosi 300 b/s (30 bajtów na sekundę), transmisja jest typu *half-duplex* (tylko w jednym kierunku w danej chwili), w ciągu godziny może zostać przetransmitowanych maksymalnie $3600 \times 30 = 108\,000$ bajtów = 105 kB. Ponieważ opłata jest

pobierana za dane przesyłane liczone na poziomie protokołu IP, należy doliczyć jeszcze bajty niezbędne do zbudowania nagłówków TCP lub UDP. Dane powinny być przesyłane w małych kawałkach (aby zapewnić wrażenie płynności), więc należy doliczyć spory narzut na nagłówki protokołów TCP/UDP, powodujący, że w przypadku rozpatrywanego transferu liczba bajtów przetransferowanych może sięgnąć nawet 1 MB – nie jesteśmy w stanie tego jednoznacznie określić. Nawet przy założeniu, że przetransferowany został 1 MB danych, to przy cenie transmisji wynoszącej 1 gr/10 kB, całkowity koszt przesłania danych wynosi 1 zł, czyli jest 17 razy niższy niż w przypadku połączenia CSD. Realizując połączenie GPRS, należy jednak zapewnić połączenie w sieci IP transmitera ze stanowiskiem, z którego uzyskiwany jest zdalny dostęp (co zostało już omówione). Trzeba się liczyć z możliwością zerwania połączenia GPRS w przypadku, gdy ruch w sieci GSM się nagle zwiększy w miejscu, w którym zainstalowany jest transmiter. Spowoduje to bowiem tak znaczne zwiększenie się opóźnień w dostarczaniu pakietów, że oprogramowanie do konfiguracji centrali przestanie je tolerować.

Należy pamiętać, że zdalny dostęp do centrali alarmowej jest kontrolowany przez oprogramowanie, które dostarcza producent centrali, nie uwzględniające faktu, że połączenie będzie się odbywać za pomocą dodatkowego transmitera IP, GSM lub GPRS. Aby komunikacja stała się możliwa, trzeba też zapewnić interfejs programowy między oprogramowaniem do konfiguracji centrali alarmowej a transmiterem. Najczęściej jest to oprogramowanie, które emuluje modem analogowy – wtedy aplikacja do konfiguracji centrali działa tak, jakby miała do czynienia z modemem i transmisja była realizowana przez linię telefoniczną. Program emulujący modem w odpowiedzi na żądania konfiguratora centrali alarmowej inicjuje i kończy sesję *downloadingu*, a w trakcie przesyłania danych zarządza transmisją, tj. dzieli dane na mniejsze pakiety, buforuje dane itp. Aby pokazać konkretne rozwiązanie, przedstawiony zostanie transmiter GPRS LX20G-3C firmy EBS.

LX20G-3C jest w ofercie firmy EBS najbardziej zaawansowanym transmiterem, cieszącym się dużym zainteresowaniem zarówno na rynku krajowym, jak i zagranicznym. Podstawowym jego zadaniem jest transmisja sygnałów alarmowych, które są pobierane z dialerów central alarmowych w protokołach ContactID oraz SIA-FSK i przesyłane do dedykowanego serwera (OSM.2007) drogą szyfrowaną za pomocą GPRS lub SMS. Dodatkowo transmiter ten może pełnić następujące funkcje:

– bramki GSM, umożliwiającej realizację połączeń głosowych wychodzących i przychodzących przy użyciu wbudowanego modemu oraz dowolnego urządzenia abonenckiego przyłączonego do zacisków transmitera, na których symulowana jest miejska linia telefoniczna;
– zdalnie sterowanej (przez GPRS) transmisji danych przez wbudowany port szeregowy RS485 lub RS232 ze sprzętową kontrolą przepływu z prędkością do 115 200 b/s, umożliwiającą zbudowanie na jego podstawie dowolnego urządzenia telemetrycznego;
– zdalnej konfiguracji central alarmowych wyposażonych w dialer z modemem 300 b/s (Bell103 i V.21) za pomocą połączenia GPRS;
– inne opisane w instrukcji instalacji dostępnej na stronie producenta http://www.ebs.pl.



Rys. 2. Schemat wymiany komunikatów w transmiterze LX20G-3C

Zdalna konfiguracja centrali jest realizowana za pomocą połączenia GPRS. W trakcie normalnej pracy transmiter utrzymuje łączność przez połączenie TCP z serwerem OSM.2007, do którego przesyłane są raporty o zdarzeniach alarmowych, dalej przekazywane do stacji monitorowania. Aby zrealizować zdalny dostęp do centrali alarmowej, należy na stanowisku, z którego będzie on uzyskiwany, oprócz konfiguratora centrali alarmowej uruchomić dostarczaną przez firmę EBS aplikację ModemEmu, która symuluje modem PSTN. W aplikacji do konfiguracji centrali alarmowej należy wskazać port szeregowy utworzony przez ModemEmu jako ten, do którego podłączony jest modem PSTN.

Aby zainicjować połączenie z centralą alarmową, jako jej numer telefonu należy podać numer seryjny transmitera, za pośrednictwem którego jest ona przyłączona, i zainicjować połączenie telefoniczne. W tym momencie aplikacja ModemEmu za pośrednictwem serwera OSM.2007 wysyła komendę do transmitera, aby ten zestawił bezpośrednie połączenie TCP z ModemEmu i wystawił sygnał dzwonienia na zaciskach symulowanej linii telefonicznej, do których podłączony jest dialer centrali alarmowej. Centrala widzi to tak, jakby zainicjowane zostało przychodzące połączenie telefoniczne. Po zaprogramowanej liczbie dzwonków centrala alarmowa przejmuje linię telefoniczną, co jest jednoznaczne z odebraniem tak zasymulowanego połączenia przychodzącego. Po odebraniu połączenia dialer centrali synchronizuje sygnały nośne z transmiterem LX20G-3C. Po zsynchronizowaniu sygnałów nośnych odpowiednia informacja jest wysyłana do ModemEmu – połączenie zostało ustanowione. Od tego momentu dane mogą być wymieniane między centralą alarmową a aplikacją do jej konfiguracji. Schemat wymiany komunikatów obrazuje rysunek 2.

Zakończenie sesji *downloadingu* przez wykonanie odpowiedniej komendy w programie do konfiguracji centrali jest przesyłane do transmitera LX20G-3C, który wraca do normalnej pracy.

Rozwiązanie wygląda tak, jakby modem analogowy został podzielony na dwie części – interfejs do centrali alarmowej (znajdujący się w transmiterze LX20G-3C) oraz interfejs do aplikacji konfigurującej centralę alarmową (w aplikacji ModemEmu) – połączone za pomocą połączenia TCP.

Artur Płatek
Starszy konstruktor R&D
EBS

INNOWACYJNOŚĆ
TECHNOLOGIA
ELASTYCZNOŚĆ
– PRODUKTY OEM/ODM

Nowości produktowe

Energys by EBS

System dedykowany dla energetyki, stanowiący zabezpieczenie antykradzieżowe dla transformatorów NN.

- Dostępne 2 wersje o różnym stopniu rozbudowania funkcjonalności
- Minimalizacja strat związanych z wandalizmem i kradzieżami
- Wygodna aplikacja powiadamiająca zainstalowana na komputerach dyspozytorów ruchu
- Grupowanie urządzeń na potrzeby klienta
- Liczne czujniki i moduły alarmujące o zanikach napięcia, wstrząsach i innych nieprawidłowościach w zależności od wybranej wersji urządzenia

LX20G-3C

Innowacyjny transmiter wprowadzający nową na polskim rynku funkcjonalność – możliwość zdalnej kontroli dowolnej centrali alarmowej z poziomu stacji monitorowania.

- Szybka reakcja na wszelkie awarie i nieprawidłowości w funkcjonowaniu centrali
- Oszczędność wynikająca z transmisji danych konfiguracyjnych/historii zdarzeń centrali alarmowej za pomocą GPRS
- Zdalny odczyt historii zdarzeń, zdalne przeprowadzanie okresowych audytów
- Brak konieczności podłączania linii telefonicznej do centrali alarmowej
- Brak konieczności posiadania modemu PSTN
- Współpracuje z najpopularniejszymi centralami dostępnymi na rynku (m.in. Napco, Paradox, Satel, DSC, Pyronix, Risco, GE)

EBS

CREATING A SENSE OF SECURITY
SINCE 1989

EBS Sp. z o.o.

ul. Bronisława Czecha 59
04-555 Warszawa, Polska

tel.: +48 22 518 84 00
fax: +48 22 812 62 12
e-mail: office@ebs.pl
website: www.ebs.pl

Bariery podczerwieni i czujka 3 x PIR

ATSUMI®

seria NR-TS/NR-TM

seria NR-QS/NR-QM

SIR10S

Wyłączny dystrybutor produktów Atsumi 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

Red Barrier

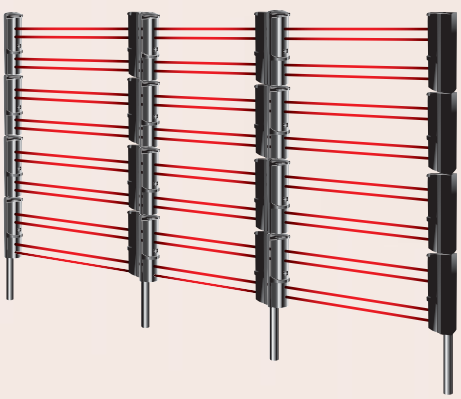
Zbuduj niewidzialny system detekcji z ATSUMI

Zewnętrzne bariery podczerwieni

dwuwiązkowe serii **NR-TS** i **NR-TM**
czterowiązkowe serii **NR-QS** i **NR-QM**

Bariery podczerwieni ATSUMI posiadają niezawodne, kontrolowane cyfrowo układy, które zapewniają bezawaryjną pracę i doskonałą ochronę nawet w najtrudniejszych warunkach środowiskowych.

- Sferyczne soczewki Fresnela
- Skuteczna detekcja nawet przy 99% poziomie tłumienia wiązki, podczas pracy w trudnych warunkach atmosferycznych (deszcz, mgła, śnieg itp.)
- Układ automatycznej regulacji wzmocnienia (AGC)
- Podwójna modulacja częstotliwości wiązki i funkcja kontroli mocy sygnału wiązki (NR-QS, NR-QM)
- Obwód EDC (NR-QS, NR-QM)
- Wybór kanału częstotliwości pracy (NR-QM, NR-TM)
- Tryb OR (NR-QM)
- Klasy szczelności IP54 (NR-QS, NR-QM) i IP55 (NR-TS, NR-TM)
- Łatwa instalacja
- Wysoce niezawodna ochrona obwodowa oparta na innowacyjnej technologii - możliwość instalacji do 4 barier w pionie (NR-QM)



Zewnętrzna pasywna czujka podczerwieni 3 x PIR

SIR10S

Czujka podczerwieni ATSUMI wykorzystuje nowo opracowaną metodę potrójnej detekcji PIR, dzięki czemu zapewnia niezawodną ochronę na zewnątrz obiektów i jednocześnie jest odporna na źródła fałszywych alarmów.

- Sferyczne soczewki Fresnela
- Zbieranie informacji przez 3 niezależne czujniki PIR
- Filtry światła białego
- Możliwość podłączenia do systemów CCTV lub innych aplikacji
- Klasa szczelności IP55
- Wszechstronność instalacji, możliwość montowania czujek jedna koło drugiej lub naprzeciwko siebie

Metoda zapobiegania fałszywym alarmom dzięki potrójnej detekcji PIR

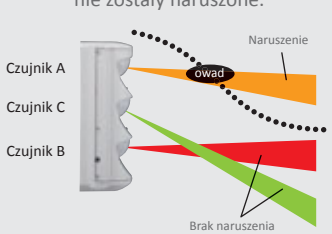
Bezpośrednie działanie promieni słonecznych

Naruszenie pól detekcji czujników A i B.
Pole detekcji czujnika C
nie zostało naruszone.

Nawet w przypadku, gdy czujniki A i B skierowane są bezpośrednio na działanie promieni słonecznych, czujka nie wchodzi w stan alarmu.

Owady, ptaki i zwierzęta

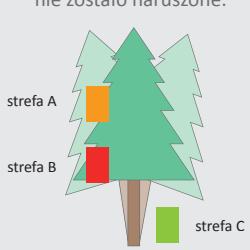
Naruszenie pola detekcji czujnika A.
Pola detekcji czujników B i C
nie zostały naruszone.



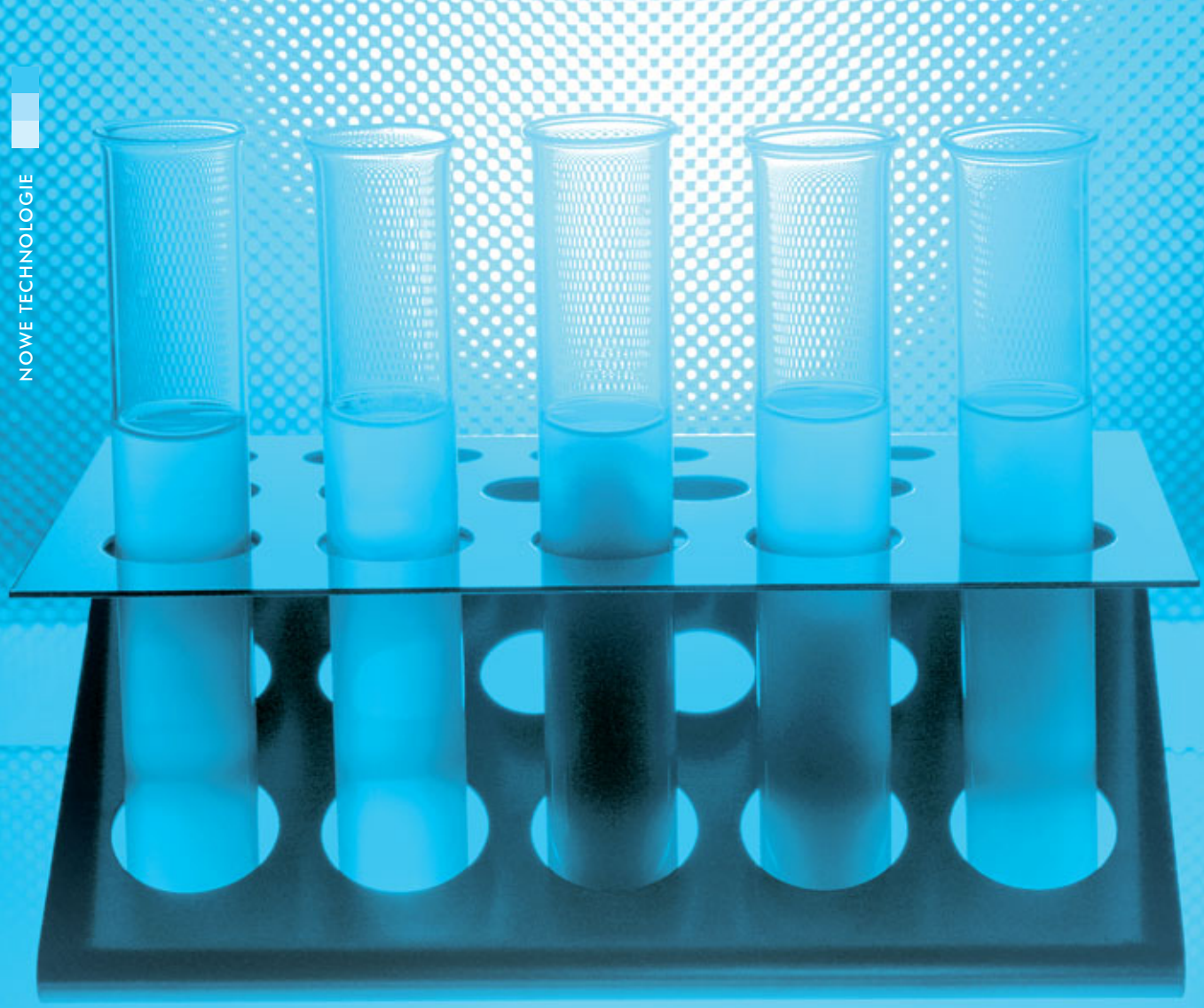
Latające ptaki, owady lub spadające z drzew liście nie powodują wejścia czujki w stan alarmu.

Poruszająca się roślinność

Naruszenie pól detekcji czujników A i B.
Pole detekcji czujnika C
nie zostało naruszone.



Kołysząca się roślinność nie powoduje wejścia czujki w stan alarmu.



DNA
w walce z przestępczością

Krzysztof Białek

Od odkrycia w 1953 roku struktury DNA rzesze naukowców pracują nad rozszerzeniem wiedzy na jej temat, by móc dzięki temu skuteczniej walczyć z chorobami. Dzięki poznaniu DNA możliwy jest również rozwój działalności związanej z klonowaniem organizmów. W ostatnim czasie ze środków masowego przekazu mogliśmy się dowiedzieć, że prawdopodobnie podjęta zostanie próba odtworzenia wymarłego przed tysiącami lat mamuta, dzięki odkryciu jego szczątków z bardzo dobrze zachowanym kodem. Jak odkryta przed kilkudziesięciu laty struktura kodu DNA może wspomóc nas w walce z kradzieżami?

Wydawałoby się, że w sferze zabezpieczania mienia wymyślono już wszystko, a to, co może nas zaskoczyć, to ewentualnie nowinka technologiczna lub lepsza integracja z systemami informatycznymi jednego z gamy produktów takich jak: zamki, systemy kontroli dostępu, telewizji dozorowej czy sygnalizacji włamania i napadu. Zabezpieczenia te są coraz bardziej skuteczne, jednak istnieją miejsca, w których ich zastosowanie nie jest możliwe, a jeśli nawet, to po udanym włamaniu lub napadzie dokonanym przez zamaskowanego intruza nie jest możliwa skuteczna identyfikacja sprawcy lub identyfikacja właściciela odzyskanego przedmiotu.

Od kilku lat w krajach takich jak Wielka Brytania, Niemcy oraz Holandia prowadzone są zaawansowane już programy związane z zabezpieczaniem mienia oraz wykrywaniem sprawców kradzieży i napadów z wykorzystaniem zupełnie nowego rozwiązania: substancji zawierających tzw. syntetyczne DNA. Są to substancje chemiczne – w pełni zsyntetyzowane w laboratorium, rozprowadzane w różnych formach, np. na bazie roztworu wodnego – które służą do znakowania wartościowych przedmiotów, a także ludzi. W pierwszej chwili można by pomyśleć, że ten sposób zabezpieczania mienia jest znany również w Polsce, bo przecież kilkanaście lat temu prowadzone były na szeroką skalę programy znakowania pojazdów i części zamiennych unikatowymi numerami, które w połączeniu z centralną bazą danych jednoznacznie wskazywały właściciela oznakowanego przedmiotu lub pojazdu. Dziś takich rozwiązań w zasadzie się nie stosuje, gdyż na rynku dostępnych jest wiele środków umożliwiających usunięcie tego typu napisów. System znakowania wykorzystujący substancje zawierające syntetyczne DNA ma podobny schemat zastosowania: wartościowe przedmioty również pokrywane są indywidualnie dobranym oznakowaniem. Różnic jest jednak wiele. Po pierwsze, usunięcie oznaczenia nie jest łatwe, ponieważ jego mikrocząsteczki wnikają głęboko w najmniejsze szczeliny pokrywanego materiału. Po drugie, takie oznakowanie nie jest zwykle widoczne dla ludzkiego oka. Można je zauważyć dopiero po oświetleniu pokrytego znacznikiem miejsca wiązką promieni UV. Po trzecie, identyfikatorem nie jest numer, lecz sekwencja znaków zapisana na mikrocząsteczce (możliwa do odczytania przy wykorzystaniu mocnego szkła powiększającego) lub unikatowy układ nukleotydów syntetycznego DNA (producent gwarantuje, że otrzymywany przez nas znacznik jest unikatowy). Na każdym pojemniku zawierającym znacznik znajduje się kod, który pozwala zidentyfikować niepowtarzalny skład zawartego w pojemniku środka. Kod ten znajduje się również w bazie danych, do której dostęp mają przedstawiciele organów ścigania. Dzięki temu możliwa jest identyfikacja właściciela porcji znacznika w przypadku odzyskania skradzionego przedmiotu lub zatrzymania oznakowanego przestępcy.

Jak to działa?

Możliwości zastosowań tego rodzaju zabezpieczeń jest sporo, ponieważ nośnikami kodu mogą być:

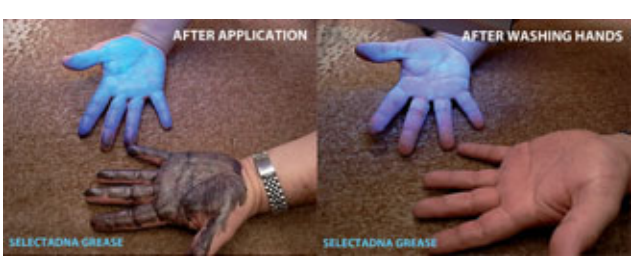
- klej (rozpuszczalny w wodzie) zawierający mikrocząsteczki z unikatową sekwencją znaków, marker UV i syntetyczne DNA z unikatowym kodem,
- pasty zawierające marker UV i syntetyczne DNA z unikatowym kodem,
- smary i żele zwierające marker UV i syntetyczne DNA z unikatowym kodem,
- spraye zawierające marker UV i syntetyczne DNA z unikatowym kodem.

Kleje, które po wyschnięciu stają się cienką, prawie niezauważalną dla użytkownika sztywną warstwą tworzywa, stosuje się do znakowania takich przedmiotów jak np. elementy składowe pojazdów samochodowych, motocykli, rowerów. Mikrocząsteczki identyfikacyjne są nanoszone tą metodą również na inne cenne przedmioty. W zagranicznych muzeach znakowane są tym sposobem dzieła sztuki, w korporacjach – m.in. laptopy i dyski twarde, zaś w gospodarstwach domowych – wartościowe mienie (RTV, antyki, kije golfowe, smartfony, komputery etc.). W Polsce pilotażowy program jest przygotowywany dla Muzeum Powstania Warszawskiego.

Pasty i żele stosuje się do zabezpieczania elementów infrastruktury, które najczęściej padają łupem złodziei. Pokrywane nimi są m.in. metalowe pokrywy studzienek kanalizacyjnych i telekomunikacyjnych, przewody elektryczne, kable telekomunikacyjne, transformatory, ale też kasy pancerne i sejfy.

W przypadku odnalezienia przedmiotu oznakowanego klejem zawierającym kod możemy zidentyfikować właściciela tej rzeczy praktycznie w czasie rzeczywistym – wystarczy odnaleźć oznakowane miejsce (gołym okiem lub stosując oświetlenie UV) i przez lupę odczytać unikalny numer znajdujący się na każdej z wielu niewielkich mikrocząsteczek. W przypadku zatrzymania podejrzanej osoby, która posiada przy sobie rzeczy oznakowane pastą lub żelem zawierającym syntetyczne DNA, możemy nie tylko zidentyfikować ją jako sprawcę kradzieży, ale również odnaleźć właściciela skradzionych przedmiotów. Pasta lub żel bowiem przy zetknięciu się z innym materiałem (ludzką skórą, częścią ubioru) zostawiają na nim ślad, który utrzymuje się jeszcze przez kilkadziesiąt dni, mimo wielokrotnej próby usunięcia zabrudzenia. W ten sposób sprawca zostaje oznakowany (w Wielkiej Brytanii policja zanotowała przypadki, gdy próbki SelectaDNA zostały skutecznie pobrane od przestępców po sześciu miesiącach od daty przestępstwa).

Spraye są stosowane do bezpośredniego oznaczania intruza lub wartości pieniężnych tuż przed zagarnięciem. Urządzenia zawierające spray umieszcza się nad otworami drzwiowymi lub okiennymi, a strumień nietoksycznego roztworu wodnego uwalniany jest w chwili, gdy sprawca znajduje się w pobliżu aplikatora. Aplikator jest zwykle uruchamiany przez system alarmowy



Fot. 1. Wygląd dłoni bezpośrednio po zetknięciu z przedmiotem oznakowanym smarem (prawa ręka poddana w obu przypadkach oświetleniu promieniami UV) oraz po zmyciu smaru. Pomimo usunięcia zabrudzenia ślady mikrocząsteczek – niewidoczne gołym okiem – nadal widoczne są po podaniu promieni UV.

wzbudzony przez czujkę ruchu (zwykle tzw. cichy alarm). Oczywiście może się zdarzyć, że środkiem tym zostaną spryskane osoby nie będące sprawcami przestępstwa, jednak grono podejrzanych jest zawężane dzięki zebraniu zeznań świadków zdarzenia lub przeanalizowaniu materiału zarejestrowanego przez systemy telewizji dozorowej. Niewielkie pojemniki ze sprayem uwalnianym pod wpływem uaktywnienia czujnika alarmowego są również wykorzystywane w obudowach urządzeń do przechowywania wartościowych przedmiotów (np. metalowych kasetek, szuflad multisejfów). W ten sposób widocznym pod wpływem promieniowania UV oznakowaniem zostają pokryte zarówno środki pieniężne, jak i dłonie kasjera oraz napastnika. W przypadku ujęcia osoby podejrzanej o przestępstwo policja ma możliwość zweryfikowania, czy jest ona rzeczywistym jego sprawcą i czy posiadane przez nią środki pieniężne są wynikiem kradzieży.

Fot. 2. Oznakowanie informujące o zastosowaniu zabezpieczeń z wykorzystaniem syntetycznego DNA, stosowane w Polsce

W Polsce tego rodzaju zabezpieczenia nie są jeszcze powszechne, ale cieszą się coraz większym zainteresowaniem. Jednym z głównych powodów niechęci był do tej pory brak centralnej bazy danych zawierającej informacje o numerach kodowych substancji wykorzystywanych przez konkretnych użytkowników. Kolejną przeszkodą był brak odpowiednich przepisów prawa oraz brak regulacji w zakresie współpracy z policją. W październiku 2011 roku odbyło się spotkanie przedstawicieli organów ścigania z jednym z producentów tego typu rozwiązania. W trakcie spotkania zaprezentowano produkty, sposoby i przykłady ich użycia, a także procedury działania związane z pobieraniem próbek i procedurami dowodowymi. Zaprezentowano też opinię prawną sporządzoną na zlecenie Polskiego Towarzystwa Kryminalistycznego przez prof. Ewę Gruzę z Uniwersytetu Warszawskiego, potwierdzającą legalność stosowania pułapek kryminalistycznych z zastosowaniem produktów SelectaDNA oraz potwierdzającą ich zdolność dowodową przed polskimi sądami. Warto zaznaczyć, że produkty SelectaDNA jako jedyne w swojej klasie zdobyły rekomendację Polskiego Towarzystwa Kryminalistycznego. Na spotkaniu zaprezentowano również Bezpieczny Rejestr Mienia (*Secure Assets Register*), który prowadzony jest centralnie dla całego świata oraz posiada akredytację LPS 1224 nadaną przez LPCB (*Loss Prevention Certification Board* – niezależną organizację certyfikującą produkty związane z bezpieczeństwem). Baza danych umożliwia organom ścigania dostęp telefoniczny i online do numerów kodowych oraz informacji potwierdzających własność konkretnej próbki z unikatowym kodem. Już z początkiem 2012 roku polskie organa ścigania powinny uzyskać dostęp do centralnej bazy danych na takich samych zasadach jak policje w Wielkiej Brytanii, Niemczech czy Holandii. Obecnie systemy znakowania SelectaDNA są testowane przez laboratoria i wydziały szkoleniowe wielu służb w Polsce, a wdrożenia planowane są już na luty bieżącego roku.

Ile to kosztuje?

Jak się okazuje, zaawansowane technologicznie rozwiązania wcale nie muszą być drogie. Użytkownicy detaliczni mogą na przykład zakupić „starter” zawierający pojemnik z klejem zawierającym mikrocząsteczki już za umiarkowaną kwotę, a zawartość jednego opakowania umożliwia oznakowanie do 50 przedmiotów. Każdy słoiczek zawierający mikrocząsteczki z unikatową sekwencją znaków, marker UV i syntetyczne DNA posiada unikalny kod. Właściciel „startera” może go zarejestrować w globalnej bazie danych, do której dostęp posiadają organa ścigania wielu krajów. W przypadku odnalezienia oznakowanych takim klejem przedmiotów pochodzących z kradzieży służby bezpieczeństwa są w stanie odszukać właściciela przedmiotów. Dla dużych odbiorców stosuje się inne wielkości opakowań, a ceny znaczników zawierających syntetyczne DNA są negocjowane indywidualnie.

Jaka jest skuteczność takich rozwiązań?

Producenci tego rodzaju zabezpieczeń podają, że w miejscach objętych programem znakowania liczba kradzieży znacząco się zmniejszyła. W jednej z dzielnic Londynu od chwili uruchomienia projektu liczba włamań spadła o 85%, a liczba kradzieży pojazdów mechanicznych o przeszło 50%. Znany światowy koncern farmaceutyczny wskazuje na spadek o 92% liczby kradzieży sprzętu informatycznego (przede wszystkim komputerów przenośnych) od momentu oznakowania go szybko schnącym klejem zawierającym mikroznaczniki i syntetyczne DNA. Bank of New Zealand zdecydował się na zamontowanie systemów sprayowych we wszystkich swoich placówkach, a kolej niemiecka (Deutsche Bahn AG), zachęcona sukcesem programu wdrożonego przez koleje holenderskie, rozpoczęła właśnie program znakowania kilkuset kilometrów infrastruktury. Za granicą systemy znakowania są z powodzeniem stosowane w kasynach, sklepach (Lidl, Spaar), na stacjach benzynowych (Shell, Texaco, Q8) czy nawet w restauracjach McDonald's. W Polsce ta dziedzina jeszcze raczkuje, co oznacza duże możliwości pozyskania nowych klientów. Niewątpliwie do znacznego zmniejszenia liczby przestępstw w miejscach zabezpieczonych substancjami zawierającymi syntetyczne DNA przyczyniła się prowadzona równolegle z procesem znakowania akcja informacyjna. Wiadomość o tym, że przedmioty poddawane są znakowaniu niemożliwemu do usunięcia, dotarła nie tylko do „zwykłych” klientów i użytkowników, ale również do przestępców, którzy zostali skutecznie odstraszeni. W wielu miejscach pojawiały się bilboardy zachęcające do udziału w projekcie, a instytucje i domy biorące w nim udział zostały oznaczone naklejkami i emblematami akcji. W podobny sposób zostały oklejone urządzenia poddane znakowaniu. Firma wdrażająca te programy nazywa efekty działania programów informacyjnych „DNA Fear Factor”.

Elementy takie jak technologiczna nowość, przystępna cena, a przede wszystkim skuteczność rozwiązania potwierdzona wynikami programów pilotażowych w innych krajach powodują, że w najbliższym czasie możemy być świadkami dużego rozwoju tego typu zabezpieczeń na naszym rynku.

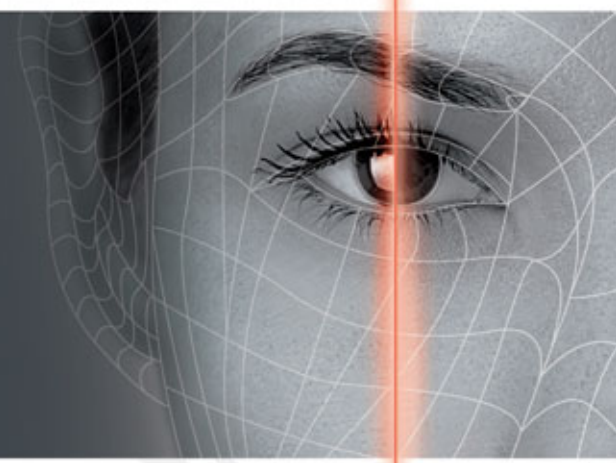
Krzysztof Białek

Międzynarodowe Targi Poznańskie

spotkaj przyszłość

securex 2012

Międzynarodowe Targi Zabezpieczeń



23-26 kwietnia 2012
Poznań

ZABEZPIECZ SWÓJ SUKCES!

Weź udział w najważniejszym spotkaniu profesjonalistów branży zabezpieczeń!

• Bezpieczeństwo • Ochrona • Monitoring •

www.securex.pl

ZŁOTY MEDAL MTP 2012

Szukaj na targach produktów oznaczonych Złotym Medalem MTP

Międzynarodowe Targi Poznańskie Sp. z o.o. | ul. Głogowska 14, 60-734 Poznań | tel. +48 61 869 26 00, fax +48 61 869 29 53

Nieprawidłowości na etapach tworzenia, eksploatacji i konserwacji systemu sygnalizacji pożarowej

Krzysztof Marchlewski

W skład systemów sygnalizacji pożarowej wchodzą obecnie bardzo zaawansowane technicznie urządzenia, które pod żadnym względem nie przypominają tych stosowanych jeszcze dwie dekady temu. Coraz większe wymagania wobec urządzeń, a także ich coraz większa funkcjonalność sprawiają, że wzrasta prawdopodobieństwo pojawienia się błędów na różnych etapach powstawania instalacji sygnalizacji pożarowej. W zależności od etapu przyczyny mogą być różne, podobnie jak konsekwencje

Projektowanie

Pierwszym etapem tworzenia instalacji jest opracowanie projektu ochrony obiektu. Projektowanie systemu jest tym etapem, który pozwala na najdokładniejsze określenie wymagań oraz sposobu ich realizacji.

Projekt powinien uwzględniać m.in.:

– przeznaczenie obiektu,
– konstrukcję obiektu pod kątem budowlanym,
– charakterystykę personelu i osób przebywających w obiekcie,
– przewidziane współpracujące ze sobą systemy bezpieczeństwa,
– utworzenie matrycy sterowań dla odpowiednich scenariuszy pożarowych,
– ustalenie zakresów odpowiedzialności projektanta i instalatora,
– przygotowanie szczegółowych planów rozmieszczenia urządzeń,
– bilansy prądowe urządzeń.

Najwięcej problemów z prawidłową realizacją pojawia się w związku z wybraniem bezpośrednio współpracujących ze sobą systemów bezpieczeństwa obiektu, które będą działać według opracowanego wcześniej scenariusza działań pożarowych, i późniejsze stworzenie matrycy powiązanych sterowań na podstawie scenariusza i projektu.

Z doświadczenia konsultantów firmy Polon-Ala wynika, że projektowanie sposobu współpracy systemów bezpieczeństwa ze sobą nie jest łatwe i wymaga wiedzy dotyczącej charakterystyki pracy każdego z nich. Wiedza ta powinna dotyczyć możliwości dopasowywania urządzeń w ramach systemu danego producenta oraz możliwości odbierania i wysyłania przez system informacji do dalszego przetwarzania lub poleceń do wykonania przez instalacje współpracujące.

Systemy bezpieczeństwa pożarowego budynków, które nie wchodzą bezpośrednio w skład systemu wykrywania pożaru, zazwyczaj są od niego zależne. Ponadto producenci tych systemów często wymagają różnych sposobów uruchomienia, na przykład za pomocą ciągłego lub impulsowego wysterowania prądowego lub styku bezpotencjałowego. Brak szczegółowej wiedzy na temat współpracy systemów i możliwości sterowania na poziomie systemu sygnalizacji pożarowej może spowodować, że urządzenia nie będą współdziałać, a systemy nie zostaną zintegrowane.

Utworzenie matrycy, która prawidłowo zrealizuje wymagany scenariusz pożarowy, jest szczególnie istotne w przypadku obiektów, w których system sygnalizacji pożarowej z powodu braku komputerowego systemu zarządzania budynkiem, czyli BMS przeznaczono do kontrolowania całości powiązanych ze sobą systemów automatyki i bezpieczeństwa budynku. Nieuwzględnienie szczególnych właściwości sprzętu danego producenta staje się często powodem późniejszych kłopotów. Przykładem może być brak możliwości reagowania centrali sygnalizacji pożarowej na sygnały przychodzące z systemów zewnętrznych poprzez moduły kontrolne.

Stworzenie szczegółowych planów rozmieszczenia urządzeń na etapie projektowania jest często niemożliwe, ale zazwyczaj nie wynika to z winy projektanta. Okazuje się bowiem, że na etapie projektowania systemu zabezpieczającego budynek często nie ma szczegółowych planów organizacji wnętrza. Późniejsze krystalizowanie się wyglądu i przeznaczenia konkretnych pomieszczeń sprawia, że zaplanowane w jakiś konkretny sposób rozmieszczenie urządzeń, np. czujek, okazuje się całkowicie nieodpowiednie do faktycznej organizacji i architektury wnętrza. W takich przypadkach konieczne jest tworzenie późniejszych projektów powykonawczych instalacji systemu sygnalizacji pożarowej i powiązanych z nim współpracujących gałęzi automatyki budynku.

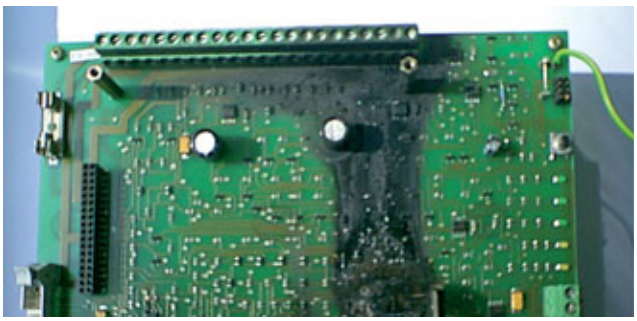
Wykonawstwo

Także na etapie wykonawstwa może wystąpić wiele nieprawidłowości. Oczywiście wcześniej mają miejsce procedury przetargowe i wyłaniany jest kontrahent. Ponieważ w myśl obowiązujących przepisów i powszechnie stosowanych zasad podstawowym kryterium wyboru oferty i oferenta jest jak najniższa cena, podczas przetargu urządzenia przewidziane w projekcie bywają zastępowane urządzeniami innego producenta. To z kolei powoduje, że trzeba dopasować urządzenia od nowa i dokonać korekty w matrycy sterowań.

Dobierane na podstawie kryterium cenowego urządzenia często nie odpowiadają wszystkim wymogom w przeciwieństwie do urządzeń, których wykorzystanie zaplanowano i uwzględniono w projekcie pierwotnym.

Ważniejsze nieprawidłowości występujące na etapie wykonywania instalacji:

– zamiana urządzeń jednego na urządzenia innego producenta bez uwzględnienia ich dopasowania;
– zmiany w projekcie bazowym bez konsultacji z projektantem;
– brak dokumentacji powykonawczej;



Fot. 1. Skutek nieprawidłowych połączeń

Fot. 2. Nieuwzględnienie zaleceń zawartych w dokumentacji dotyczącej urządzenia – zniszczenie uszczelnień gniazda czujki

Fot. 3. Samodzielne malowanie czujek

cząсej urządzenia – zniszczenie uszczelnień gniazda czujki

– niewłaściwy sposób wykonania instalacji pomimo słusznych zaleceń zawartych w projekcie;
– niedostosowanie się do zaleceń producenta dotyczących sposobu instalacji urządzeń;
– nieprawidłowe przyłączenie urządzeń do źródła zasilania (za/przed głównym wyłącznikiem pożarowym, nieodpowiedni rodzaj zastosowanych przewodów).

Każdy z błędów popełnionych podczas tworzenia instalacji może mieć poważne konsekwencje w przypadku wystąpienia pożaru.

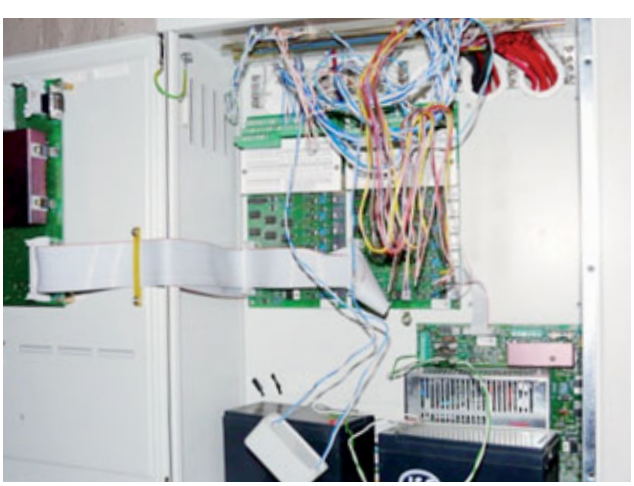
Zrezygnowanie z pierwotnie zaplanowanych funkcji przypisanych urządzeniom wybranym na początku, a co za tym idzie niezrealizowanie zaprojektowanego algorytmu sterowań, może spowodować, że podczas eksploatacji system sygnalizacji pożarowej wraz ze współpracującymi w obiekcie systemami bezpieczeństwa będzie uruchamiał się w niewłaściwych momentach lub uszkodzi elementy budynku. Znane są przypadki, w których w trakcie prób pożarowych wystąpiły uszkodzenia urządzeń pracujących w ramach zabezpieczenia pożarowego budynku tylko dlatego, że matryca sterowań nie była prawidłowo uzupełniona.

Braki w dokumentacji powykonawczej dadzą znać o sobie po pewnym czasie eksploatacji obiektu. Nieprawidłowości w tego rodzaju dokumentacji powodują, że późniejsza konserwacja systemu jest utrudniona, a ewentualne modernizacje wymagają znacznego nakładu pracy oraz poniesienia znacznych kosztów. W wielu przypadkach długotrwałe nieprawidłowe działanie systemu i brak możliwości lub umiejętności odpowiedniego konserwowania skutkuje wyłączeniem części najbardziej kłopotliwych elementów systemu, jednocześnie „oślepiając" go i powodując, że budynek zostaje częściowo pozbawiony zabezpieczenia pożarowego.

Niechlubny prym w tej kategorii wiodą bardzo stare systemy sygnalizacji pożarowej, których czas pracy w obiekcie przekracza kilkanaście lat. Rzut oka na panel czołowy przynosi na myśl bożonarodzeniową choinkę ze względu na liczbę świecących kolorowych lampek oznaczających stany uszkodzenia i blokowania.

Eksploatacja i konserwacja

Jeśli nawet instalacja sygnalizacji pożarowej jest oparta na bezbłędnym projekcie i wykonana całkowicie poprawnie, po pewnym czasie zawiedzie, jeżeli nie będzie regularnie konserwowana i poddawana testom na poprawne funkcjonowanie. Odpowiednie przepisy określają częstość i sposób konserwacji systemów



Fot. 4. Niedbałe pozostawienie przewodów instalacyjnych, które może skutkować zakłóceniem pracy centrali

Fot. 5. Zakrycie czujki folią

bezpieczeństwa pożarowego w obiekcie (Rozporządzenie Ministra Spraw Wewnętrznych i Administracji, Dz.U. nr 109, czerwiec 2010). W praktyce to właśnie zaniechania dotyczące konserwacji mają największy wpływ na funkcjonowanie instalacji. Błędy i uchybienia na etapie eksploatacji i konserwacji są największą bolączką wielu firm użytkujących SSP.

Podczas eksploatacji instalacja może być narażona na wiele oddziaływań powodujących jej wadliwe działanie. Przykłady:
– blokowanie wybranych elementów systemu bez konsultacji z odpowiednimi służbami i projektantem;
– zaklejanie czujek folią lub inna fizyczna i granicząca z sabotażem ingerencja w elementy systemu;
– wykonywanie prac konserwacyjnych przez firmy nie posiadające odpowiedniej wiedzy dotyczącej urządzeń sygnalizacji pożarowej;
– zmiana przeznaczenia pomieszczeń (w przypadku takiej zmiany powinno się zmienić również scenariusz pożarowy i matrycę sterowań);
– niekonserwowanie systemu sygnalizacji pożarowej przez kilka lat;
– zasłonięcie czujek lub ręcznych ostrzegaczy meblami lub elementami wystroju wnętrza;
– nieprzeszkolenie wybranej części personelu pod kątem odpowiedniej reakcji na sygnały centrali;
– likwidowanie uszkodzeń linii dozorowych poprzez łączenie kabli „na skrętkę".

To tylko niektóre, wybrane, najczęściej występujące problemy pojawiające na etapie eksploatacji systemu sygnalizacji pożarowej. Okazuje się jednak, że są one również najbardziej niebezpieczne. Szczególnie niebezpieczna okazuje się fizyczna ingerencja w instalację i w działanie urządzeń automatyki pożarowej, która tylko na krótko może dać efekt pozytywny. Jeśli system sygnalizacji pożarowej zostanie „oślepiony", to nie uruchomi odpowiednich urządzeń i nie zapewni bezpiecznej ewakuacji w przypadku rzeczywistego zagrożenia. Skutki mogą być tragiczne.

Podsumowanie

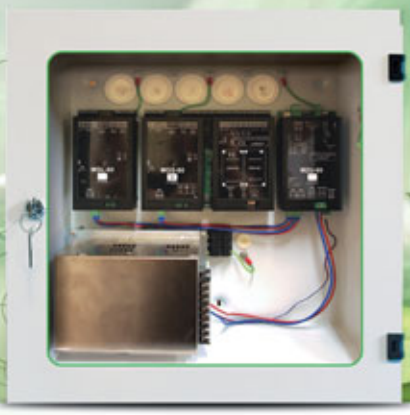
Należy starać się wyeliminować nieprawidłowości na etapie tworzenia, eksploatacji i konserwacji systemu sygnalizacji pożarowej. Dopóki system istnieje tylko na papierze i możliwe są konsultacje specjalistów w sprawie współdziałania urządzeń, wyeliminowanie nieprawidłowości jest stosunkowo proste. Na późniejszych etapach rozwiązanie problemów może być dużo trudniejsze, o ile w ogóle możliwe. Na pewno będzie wiązało się z dużymi kosztami. Z kolei ich zignorowanie może mieć poważne konsekwencje w przypadku pożaru.

Krzysztof Marchlewski
POLON-ALFA

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

UCS 6000

UNIWERSALNA CENTRALA STERUJĄCA



WEJŚCIA	UCS 6000	WYJŚCIA
• **praca samodzielna** czujki przyciski oddymiania		• **sterowanie 24 V** klapy z siłownikami dwukierunkowymi 2 lub 3 przewodowymi klapy z siłownikami ze sprężyną sterowanie elektrotrzymaczami itp.
• **praca jako element adresowalny w systemie POLON 4000**		
czujnik deszczu i/lub wiatru przyciski przewietrzające	• ponad 20 wersji • niemal dowolna konfiguracja • dedykowany program konfiguracyjny • 5 lat gwarancji	• **sterowanie 230 V~** wentylatory, kurtyny itp.

WSPÓŁPRACA Z CENTRALAMI SYGNALIZACJI POŻAROWEJ WSZYSTKICH PRODUCENTÓW

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.

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

CONTROL SYSTEM FMN
Autoryzowany serwis i dystrybutor drukarek HID Fargo

Najnowsza drukarka retransferowa do pracy ciągłej

Fargo HDP8500

Grzegorz Nowacki

Na listopadowych targach Cartes 2011 w Paryżu firma HID Global zaprezentowała nowy, przemysłowy model drukarki retransferowej do kart plastikowych z serii HDP (*High Definition Printing*). Następczyni bardzo dobrze znanych na rynku światowym modeli HDP600 i HDP5000 będzie miała symbol HDP8500. Drukarka będzie dystrybuowana przez firmę CONTROL SYSTEM FMN już od marca 2012 roku

Fot. 1. Drukarka FARGO HDP8500

Nowa generacja drukarek

Nowa drukarka została zaprojektowana z uwzględnieniem wymagań sektora produkującego na skalę przemysłową, wymagającego wysokiego stopnia niezawodności, sprawności urządzenia oraz dużej wydajności w cyklu pracy przy zachowaniu najwyższej jakości obrazu. Producent wziął pod uwagę wymagania związane z realizacją rządowych programów dotyczących kart identyfikacyjnych i legitymacji, specyfikę warunków pracy w dużych biurach obsługi, w punktach personalizacji kart na wyższych uczelniach oraz w korporacjach.

Firma HID wprowadza na rynek zupełnie nową, niezawodną, solidnie wykonaną, wysokiej klasy **przemysłową drukarkę do kart plastikowych**, którą docenią nawet najbardziej wymagający odbiorcy. Fargo HDP8500 jest objęta **trzyletnią gwarancją**. Jest to pierwsza w historii firmy HID drukarka do kart plastikowych, w przypadku której okres gwarancji jest tak długi.

Fargo HDP8500 jest zwiastunem nowej generacji drukarek retransferowych do kart plastikowych, powstających w laboratoriach HID. Drukarka ma zwiększoną pojemność podajników kart. Zastosowano dodatkową filtrację powietrza chłodzącego elementy drukarki i inne mechanizmy zwiększające odporność i niezawodność jej pracy. Materiały eksploatacyjne mają dużą wydajność.

Nowe rozwiązania techniczne

Konstruktorom przyświecała idea zaprojektowania urządzenia maksymalnie wydajnego, niezawodnego i zapewniającego bezpieczeństwo całego procesu produkcji kart. Środkiem do osiągnięcia założonego celu stało się oparcie architektury logicznej i rozwiązań konstrukcyjnych na autorskiej platformie HID zwanej *HID Global Trusted Identity Platform*. Dzięki temu pojawiła się możliwość logicznego zabezpieczenia dostępu do drukarki kodem PIN. Dopiero po prawidłowym wprowadzeniu przez operatora PIN-u na wyświetlaczu LCD drukarka będzie akceptowała i przetwarzała przesyłane do niej polecenia. Wprowadzono również fizyczną kontrolę dostępu obejmującą materiały eksploatacyjne: taśmy kolorowe, film retransferowy, taśmy laminacyjne oraz karty w podajniku i odbiorniku. Ponadto zastosowano kilka cennych rozwiązań, które skutecznie zabezpieczają dane przesyłane do drukarki HDP8500, między innymi algorytm szyfrowania danych AES (ang. *Advanced Encryption Standard*) z 256-bitowym kluczem oraz system wymazywania/zacierania danych na panelach jednokolorowych (resinowych), który uniemożliwia fizyczne odczytanie danych osobowych ze zużytych taśm.

Drukarka ma możliwość tzw. „bezpiecznego drukowania" oraz „bezpiecznego laminowania", która polega na wykorzystaniu paneli z barwnikiem widocznym wyłącznie w świetle UV oraz na stosowaniu holograficznych filmów retransferowych i holograficznych taśm laminacyjnych. Dzięki nim możliwe staje się zabezpieczenie karty na aż trzech poziomach (jawnym, tajnym i kryminalistycznym) oraz zwiększenie wytrzymałości mechanicznej powierzchni karty i tym samym jej trwałości.

Do modelu HDP8500 wprowadzono już piątą generację silnika – mechanizmu nadruku *High Definition Printing*. Ze względu na swoją elastyczność umożliwia on wykorzystanie kart wielu typów, wykonanych z różnych materiałów.

Konstruktorzy **Fargo HDP8500** skupili się również na warunkach środowiska, w jakich pracują drukarki do plastikowych kart. Pomieszczenia nieklimatyzowane, mocno ogrzewane, brudne i zakurzone stwarzają duże prawdopodobieństwo wystąpienia zakłóceń i usterek. Najczęściej powodują one obniżenie wydajności cyklu produkcyjnego oraz pogorszenie jakości nadrukowywanego na karcie obrazu. Zmodernizowany system wentylacji w modelu HDP8500 utrzymuje wewnątrz obudowy idealne warunki funkcjonowania poszczególnych podzespołów. W drukarce zamontowano specjalne czujniki do ciągłego monitorowania temperatury wnętrza. System wentylacji wyposażono w kurtyny i filtry chroniące najbardziej czułe elementy drukarki przed kurzem i innymi zabrudzeniami.

We wnętrzu HDP8500, na ścieżce do prowadzenia karty, zastosowano kilka modułów czyszczących. Ich zadaniem jest usuwanie zanieczyszczeń, które mogą znajdować się na powierzchni kart. Specjalna pokrywa drukarki zabezpiecza sensory rejestrujące pozycję czystego blankietu, radykalnie ograniczając liczbę błędów w nadruku oraz zacinanie się kart. Do zdarzeń tego typu dość często dochodzi podczas pracy ciągłej każdej z drukarek. Zastosowanie silników krokowych o większej mocy i najwyższej jakości zaowocuje poprawą sposobu prowadzenia kart, nawet w przypadku bardzo długich cykli produkcyjnych.

Wysoka wydajność

Celem zastosowania nowych rozwiązań jest przede wszystkim podniesienie wydajności urządzenia i skrócenie czasu

Fot. 2. Panel sterowania drukarki

zaangażowania operatora w czynności typowo eksploatacyjne. Cel ten osiągnięto między innymi dzięki pracy drukarki w trybie wielowątkowym, który znacznie zwiększa jej wydajność. Drukarka zintegrowana z odpowiednim środowiskiem informatycznym jest w stanie kodować jedną kartę podczas odbywającego się nadruku drugiej oraz laminacji trzeciej.

HDP8500 może drukować także w dwóch niestandardowych trybach. Tryb *Performance* zapewnia maksymalne prędkości produkcyjne – wykonanie około 1000 sztuk jednostronnych kart kolorowych w ciągu jednej zmiany (osiem godzin). Tryb *Premium* zapewnia najwyższą jakość wydruku w przypadku szczególnie wymagającej grafiki.

W drukarce Fargo HDP8500 znajduje się bardzo pojemny podajnik na 400 kart, co zmniejsza liczbę interwencji operatora w cyklu produkcyjnym.

Nowoczesnym rozwiązaniem jest wyświetlacz dotykowy, który ułatwia diagnostykę i dostęp do podstawowych informacji o statusie urządzenia i karty. Operator posiada pełen dostęp do ścieżki przebiegu karty we wnętrzu urządzenia. Dzięki temu może wizualnie ocenić prawidłowość przebiegu całego procesu nadruku. Jest to szczególnie ważne i wygodne w przypadku rozwiązywania problemów mogących pojawić się podczas eksploatacji.

Moduły

Wielką zaletą nowej drukarki Fargo HDP8500 jest jej elastyczność i modułowość. To właśnie te cechy wpływają na szeroki zakres możliwości integrowania jej z istniejącymi systemami oraz umożliwiają dalszą rozbudowę urządzenia w przypadku wzrostu wymagań i kompetencji systemu wydawania kart. Wśród opcji możemy wymienić:

– kodowanie paska magnetycznego w standardzie ISO,
– kodowanie kart stykowych i zbliżeniowych,
– system korygowania odkształceń karty w celu zachowania jej zgodności ze standardami ISO,
– system dodatkowych świetlnych wskaźników umożliwiających zdalne monitorowanie pracy urządzenia,
– moduł laminujący,
– **laser do grawerowania na powierzchni karty.**

Drukarka HDP8500 jest kompatybilna z innymi technologiami Genuine HID, co gwarantuje jej współdziałanie z wszystkimi produktami HID.

Najwyższa jakość i solidność wykonania, nowoczesność, elastyczność konfiguracji i implementacji, wysokie parametry techniczne i duże możliwości produkcyjne, dostępność zabezpieczeń wizualnych i logicznych, bezpieczeństwo użytkowania, zaawansowanie konstrukcyjno-technologiczne to zalety najnowszego modelu drukarki HID – Fargo HDP8500.

Krajowym dystrybutorem tych drukarek jest firma CONTROL SYSTEM FMN, która ma status Advantage Channel Partner HID.

Grzegorz Nowacki
Control System FMN

seria radius

RACS 4

System Kontroli Dostępu

- Do 250 podsystemów w jednym systemie.
- Do 32 kontrolerów dostępu w jednym podsystemie.
- Do 1000 kontrolerów w całym systemie.
- Bezpłatne oprogramowanie do zarządzania systemem KD.
- **INTEGRACJA** z innymi systemami:

RCP CCTV SSWiN

RCP Master *PR602LCD*

Rozwiązania Kontroli Dostępu i Rejestracji Czasu Pracy

roger®

www.roger.pl

20 YEARS 1991-2011

Wprowadzono do oferty **UT-4DR** – nowy interfejs komunikacyjny TCP/IP do systemu RACS4.

** - sugerowana cena detaliczna netto*

SUPER CENA 290 PLN*

Kilka słów o cyberprzestępczości

Monika Brzozowska

Kto z nas nie słyszał o atakach hakerskich, fałszywych profilach w portalach społecznościowych, wyłudzaniu danych osobowych, znieważaniu w sieci? W kancelarii coraz częściej zajmujemy się sprawami z zakresu szeroko pojmowanej cyberprzestępczości. Swoistą „karierę" na wokandach sądowych robią przestępstwa z zakresu pomawiania w sieci, a także „modne" ostatnio przestępstwa stalkingu czy tzw. kradzieży tożsamości. Sprawy z zakresu cyberprzestępczości nie są sprawami łatwymi. Poza kwestiami dowodowymi (tzw. dowody cyfrowe i możliwość ich zakwestionowania) istnieją także kwestie dotyczące ustalenia personaliów oskarżonego (jak wskazać dane osobowe przestępcy?), wskazania miejsca popełnienia przestępstwa, a także prawa właściwego (jeśli będziemy mieć do czynienia z aspektem międzynarodowym)

Do tej pory przestępstwa internetowe uznawano za przestępstwa bez użycia przemocy. Obecnie takie podejście się zmienia (w związku z nawoływaniem do przemocy, kierowaniem gróźb karalnych itp.). Wyjaśnię, co grozi za popełnianie przestępstw w Internecie i jak określone są przestępstwa internetowe w polskim prawie.

Kradzież tożsamości

Pojęcie kradzieży tożsamości długo istniało poza kodeksem karnym i dopiero nowelizacja w 2010 r. spenalizowała zachowanie polegające na fałszowaniu, defraudacji tożsamości. Zgodnie z art. 190 a § 2 kk karze pozbawienia wolności do lat trzech podlega każdy, kto podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej. Jeśli następstwem tego „podszywania się pod inną osobę" jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega wyższej karze, tj. karze pozbawienia wolności od roku do lat 10 (art. 190 a § 3 kk). Kradzież tożsamości polega na kradzieży lub wyłudzeniu danych osobowych i wykorzystaniu ich w celu podszywania się pod osobę, której dane dotyczą. Efektem takich działań może być np. zamawianie towarów w sieci, wykonywanie przelewów bankowych, zawieranie różnych umów przez Internet itp.

Należy rozróżnić kradzież danych od wyłudzenia danych osobowych. Kradzież danych zakłada pokonanie pewnego zabezpieczenia (np. włamanie się do systemu komputerowego danego użytkownika). Określając pewne przestępstwo jako wyłudzenie danych, zakłada się, że użytkownik sam przekazał swoje dane osobowe przestępcy – oczywiście nieświadomie, wbrew własnej woli, na przykład na skutek jakiegoś wprowadzenia go w błąd.

Stalking w Internecie

Stalking pojawił się pod koniec XX wieku. W wieku XXI, który przyniósł rozwój nowych technologii, stalking przeniósł się do cyberprzestrzeni.

Od 2010 r. w kodeksie karnym istnieje art. 190 a § 1, zgodnie z którym karze pozbawienia wolności do lat trzech podlega każdy, kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza w niej uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność. Ważne jest to, że stalking charakteryzuje się tzw. „uporczywością działań". Nie będzie więc uporczywym nękaniem jednorazowe działanie w Internecie, nawet jeśli wzbudza w ofierze poczucie zagrożenia.

O stalkingu możemy bowiem mówić w przypadku „działań trwających dłuższy czas"[1], „wielokrotności zachowań"[2]. Co może być takim uporczywym działaniem? Fantazja przestępców nie jest niczym ograniczona. W swojej praktyce spotkałam się np. z wysyłaniem znacznej liczby fałszywych e-maili, podawaniem prawdziwych danych ofiary w fałszywych ogłoszeniach (zarówno w ogłoszeniach o charakterze obojętnym, np. dotyczących sprzedaży rzeczy, jak i w ogłoszeniach matrymonialnych czy pornograficznych), prezentowaniem fotografii ze znieważającymi komentarzami, tworzeniem fałszywych profilów na portalach społecznościowych itp.

Pomówienia i znieważanie w sieci

Na salach sądowych pojawiły się sprawy z zakresu pomawiania czy znieważania w sieci. Są to dwa odrębne przestępstwa. Pomówienie to mówienie nieprawdy, zniewaga to mówienie prawdy, ale w obelżywy sposób. Może oczywiście dojść do prezentowania w Internecie nieprawdziwych informacji i to w sposób obelżywy – wówczas te dwa przestępstwa będą mogły stanowić jeden czyn zabroniony (prawo określa to jako tzw. zbieg przestępstw).

Na mocy art. 212 § 2 kk karze grzywny, ograniczenia wolności bądź pozbawienia wolności do roku podlega ten, kto (za pomocą środków masowego komunikowania) pomawia inną osobę, grupę osób, instytucję, osobę prawną lub jednostkę organizacyjną nie mającą osobowości prawnej o takie postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności.

Za środki masowego komunikowania uważa się „wszystkie środki, których działanie sprowadza się do masowego przekazywania rozmaitych treści. Czyli (…) prasę drukowaną, przekaz radiowy i telewizyjny, lecz także książkę, plakat, film oraz przekaz za pomocą Internetu"[3].

Do przestępstwa pomówienia może dojść wskutek publikowania w Internecie treści dotyczących sposobu czyjegoś postępowania, oceny czyjegoś postępowania, wskutek

1) Zgodnie z wyrokiem Sądu Apelacyjnego w Łodzi z dnia 18 stycznia 2001 r., II AKa 241/00, LEX 54979

2) Postanowienie Sądu Apelacyjnego w Krakowie z dnia 13 grudnia 2000 r.

3) Postanowienie Sądu Najwyższego z dnia 7 maja 2008 r., III KK 234/07, LEX 444478

przytaczania faktów, ale w sposób poniżający albo taki, który naraża poszkodowanego na utratę czyjegoś zaufania. Narażenie kogoś na utratę czyjegoś zaufania nie musi skutkować faktyczną utratą owego zaufania – wystarczy sam fakt narażenia.

Ofiarą pomówienia może być zarówno osoba fizyczna, jak i firma. Konkurencja i kryzys gospodarczy sprawiają, że walka o klienta przenosi się do sieci i często przekracza granice uczciwości i legalności. Pomówienie w Internecie, niepotwierdzone plotki, fałszywe oskarżenia, niesprawdzone pogłoski mogą narazić firmę na utratę zaufania klientów (którzy, zgodnie z kodeksem karnym, stanowią „opinię publiczną").

Jak bronić się przed cyberprzestępstwami?

Wyżej opisane sprawy są skomplikowane. Pomówienie i zniewaga są często ścigane dodatkowo na podstawie oskarżenia prywatnego.

Jeżeli akt oskarżenia musi zostać przygotowany przez samego pokrzywdzonego (ofiarę), warto skorzystać z uprawnienia, jakie daje art. 488 kpk. Zgodnie z tym artykułem pokrzywdzony może składać skargę na policji wraz z wnioskiem o ustalenie danych osobowych przestępcy oraz zabezpieczenie dowodów. Warto wspomnieć, że niezabezpieczenie dowodów może uniemożliwić skazanie za przestępstwo zniesławienia.

W przypadku kradzieży tożsamości czy też stalkingu ściganie odbywa się na podstawie wniosku pokrzywdzonego, co oznacza, że ofiara musi złożyć wniosek o ściganie i wówczas całe postępowanie prowadzi prokurator jako oskarżyciel publiczny.

Warto dodać, że jeśli nawet policja uzyska adres IP, który zidentyfikuje właściciela komputera oznaczonego tym adresem, nie będzie to jeszcze równoznaczne z identyfikacją sprawcy przestępstwa. Jeśli na przykład za pośrednictwem komputera (który znajduje się w mieszkaniu, w którym przebywają trzy dorosłe osoby) wysłano obrażające treści, a potencjalnych sprawców jest trzech, to za pomocą pośrednich dowodów trzeba określić, kto je wysłał. Może to okazać się trudne. Jeszcze trudniej ustalić sprawcę, jeżeli mamy do czynienia z podszywaniem się z wykorzystaniem cudzego adresu IP lub gdy jeden adres IP był przydzielony kilku komputerom (np. w sieci Wi-Fi).

adwokat Monika Brzozowska
kierownik Departamentu Prawa Własności Intelektualnej i Danych Osobowych w kancelarii Pasieka, Derlikowski, Brzozowska i Partnerzy

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Szybkoobrotowe kamery IP dzień/noc

Perfekcyjna jakość obrazu, szeroki zakres zastosowań!

Kompatybilne z oprogramowaniem NMS

Wraz z kamerą dostarczane jest w pełni funkcjonalne oprogramowanie NMS do zbudowania systemu monitoringu wizyjnego IP. W odróżnieniu od innych programów, bezpłatna licencja umożliwia podłączenie dowolnej liczby kamer IP oraz nie ma limitu przestrzeni do nagrywania. Nowoczesne i funkcjonalne oprogramowanie NMS o architekturze serwer - klient umożliwia m.in. rejestrację strumieni, odtwarzanie zarejestrowanego materiału, tworzenie map obiektów, sterowanie kamerami obrotowymi za pomocą myszki lub klawiatury z dżojstikiem.

Standardowa rozdzielczość HD 720p

Obraz w wysokiej rozdzielczości

Kamera NVIP-1DN6118SD posiada megapikselowy przetwornik obrazu. Dzięki temu może generować strumień wideo H.264 w jakości HD 720p. Panoramiczny obraz uzyskiwany z tej kamery ma w przybliżeniu 2 razy więcej pikseli niż kamera standardowej rozdzielczości, a co za tym idzie, umożliwia odwzorowanie znacznie większej liczby detali obserwowanej sceny.

Kompaktowa konstrukcja

Kamery zintegrowane są z metalową obudową z kloszem akrylowym. Uchwyt ścienny i osłona przeciwsłoneczna dostarczane są w komplecie. Wszystkie elementy potrzebne do zainstalowania punktu kamerowego znajdują się w zestawie. Opcjonalnie dostępne są adaptery umożliwiające instalację kamery na suficie, na rogu budynku lub na słupie.

NMS Compatible ALNET Compatible

Oprogramowanie NMS do monitoringu wizyjnego IP w komplecie!

- Mechaniczny filtr podczerwieni
- Typ obiektywu: motor-zoom z automatyczną przysłoną i ostrością
- 8 patroli (20 akcji na patrol), 8 tras automatycznego skanowania, 4 trasy obserwacji (do 1200 poleceń)
- Praca w trybie dwustrumieniowym - możliwość definiowania kompresji, rozdzielczości, prędkości i jakości dla każdego strumienia
- Sprzętowa detekcja ruchu
- Możliwość sterowania i konfiguracji bezpośrednio przez stronę www oraz z programu NMS
- Klasa szczelności: IP 67
- Zasilanie: 12 VDC

NVIP-DN6137SD

- Rozdzielczość przetwornika: 680 TVL
- Czułość: 0.06 lx/F=1.6
- Zoom: 37 x optyczny
- Rozdzielczość przetwarzania wideo: 720 x 576
- 127 presetów
- Szeroki zakres dynamiki (WDR)

NVIP-1DN6118SD

- Rozdzielczość przetwornika: 1.3 Mpx
- Czułość: 0.02 lx/F=1.6
- Zoom: 18 x optyczny
- Rozdzielczość przetwarzania wideo: 1280 x 960
- 98 presetów
- Szeroki zakres dynamiki (WDR)

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

RioPro – Profesjonalna drukarka do kart identyfikacyjnych

Profesjonalna drukarka zaprojektowana do seryjnego wydruku identyfikatorów. Rio Pro to niezawodna, szybka i łatwa w obsłudze drukarka umożliwiająca w każdym momencie użytkowania szybką zmianę trybu pracy na drukowanie dwustronne. Wbudowane opatentowane funkcje HoloKote i HoloKoteFlex zabezpieczają karty przed nieautoryzowanym kopiowaniem. Funkcje te dają również możliwość personalizacji znaku wodnego zawierającego tekst lub logo firmy. Standardowo, podczas procesu wydruku karta pokrywana jest cienką folią (overlay) zabezpieczającą nadruk przed uszkodzeniem mechanicznym i promieniami UV. Rio Pro i Rio Pro Duo wyposażone są w wyświetlacz LCD z menu w języku polskim informujący o statusie drukarki. Drukarki posiadają 3-letnią gwarancję łącznie z mechanicznymi uszkodzeniami głowicy. Drukarki posiadają certyfikat CE i RoHS.

Specyfikacja techniczna

- Wydruk karty w kolorze od krawędzi do krawędzi w 23 sekundy
- Monochromatyczny wydruk karty w 6 sekund
- Interfejs do PC: USB i Ethernet
- Menu wyświetlacza w języku polskim
- Sterowniki 32 i 64 bit w języku polskim: Windows 2000, XP, Vista, Windows 7
- Rozdzielczość wydruku: 300 dpi
- Podajnik na 100 kart
- Odbiornik na 70 kart
- Możliwość ręcznego podawania kart
- Zasilanie: 100-240 V / 50-60 Hz
- Wymiary / Masa: 470 mm x 220 mm x 250 mm / 4,9 kg
- Temperatura pracy: od 10°C do 30°C
- 5 wzorów znaków wodnych do wyboru
- Wydruk na kartach wielkości CR-80 oraz CR-79
- Automatyczna regulacja grubości karty
- 3 lata gwarancji z możliwością przedłużenia do 4 lat, łącznie z mechanicznymi uszkodzeniami głowicy

Opcje dodatkowe:

Możliwość aktualizacji do wersji dwustronnej

Możliwość drukowania dwustronnego (Rio Pro Duo)

Możliwość kodowania kart magnetycznych, chipowych i zbliżeniowych

Taśmy

- Kolorowa 5 paneli nadruk 300 kart (MA300YMCKO)
- Monochromatyczna czarna nadruk 1000 kart (MA1000K-BLACK)
- Monochromatyczna biała nadruk 1000 kart (MA1000K-WHITE)
- Monochromatyczna niebieska nadruk 1000 kart (MA1000K-BLUE)
- Monochromatyczna czerwona nadruk 1000 kart (MA1000K-RED)
- Monochromatyczna złota nadruk 1000 kart (MA1000K-GOLD)
- Monochromatyczna srebrna nadruk 1000 kart (MA1000K-SILVER)
- Monochromatyczna czarna plus overlay nadruk 600 kart (MA600KO)
- Kolorowa + czarna nadruk dwustronny 250 kart (MA250YMCKOK)
- Kolorowa 5 paneli nadruk 100 kart (MA100YMCKO)

Karty

Drukuje na wszystkich standardowych kartach PCV ISO CR-80 (85,6 x 54) oraz CR-79 (84,1 x 52,4) o grubości od 0,51 mm do 1,02 mm, kartach magnetycznych, zbliżeniowych, samoprzylepnych, HoloPatch

Zestaw czyszczący

- 1 szt. rolki czyszczącej dostarczana z każdą taśmą
- 10 szt. kart czyszczących, 1 flamaster (3633-0053)
- 5 szt. wałków czyszczących plus wymienna oś wałka

Dystrybucja:

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

GOLD-PLUS inteligentny tester akumulatorów z ręczną kalibracją

Inteligentny Tester Akumulatorów GOLD-PLUS został zaprojektowany do testowania akumulatorów 6-voltowych o pojemności od 1,2 h do 12 Ah oraz 12-voltowych o pojemności od 1,2 Ah do 100 Ah. Zastosowana technologia symulacji pełnego rozładowania skraca normalny test rozładowania z 20 godzin do 20 sekund. Automatycznie wyświetla napięcie akumulatora i aktualną pojemność. Dzięki funkcji kalibracji testera możliwe jest testowanie szczelnych akumulatorów (SLA) wykonanych w technologii AGM, żelowych do pracy cyklicznej oraz akumulatorów samochodowych. Akumulatory można testować wielokrotnie bez przerw pomiędzy pomiarami. Wbudowana dioda LED ostrzega przed odwróceniem polaryzacji.

Wymiana akumulatora jest zalecana, jeżeli jego współczynnik pojemności spada poniżej 65%. Na obudowie umieszczona jest tabela referencyjna wskazująca, kiedy akumulator powinien zostać doładowany lub wymieniony.

Cechy charakterystyczne

- Testuje w ciągu 20 sekund 6- i 12-voltowe szczelne akumulatory (SLA) - AGM i żelowe oraz akumulatory samochodowe,
- automatycznie wyświetla napięcie akumulatora i aktualną pojemność,
- może być skalibrowany do testowania akumulatorów szczelnych, żelowych i samochodowych o pojemności od 1,2 Ah do 100 Ah,
- zabezpieczony przed odwróceniem polaryzacji,
- testuje akumulatory szybko, dokładnie i jest łatwy w użyciu,
- zastosowanie – akumulatory w systemach alarmowych, zasilaczach UPS, samochodach elektrycznych i spalinowych.

Parametry techniczne	
Model	GOLD- PLUS
Typy akumulatorów	szczelne (SLA) – AGM i żelowe samochodowe akumulatory obsługowe
Pojemność akumulatorów	6 V 1,2 Ah – 12 Ah oraz 12 V 1,2 Ah – 100 Ah
Impulsowe obciążenie akumulatora podczas pomiaru	6 A dla akumulatorów 1,2 Ah – 9,9 Ah, 18 A dla akumulatorów 10 Ah – 100 Ah
Kalibracja Ah	Kalibrowany w pozycji 0 dla nowego, w pełni naładowanego akumulatora SLA o temperaturze 20-25 °C. Regulacja kalibracji w zakresie 00-99 dla akumulatorów żelowych i samochodowych
Wyświetlacz	podświetlany LCD
Ostrzeżenie o odwróconej polaryzacji	czerwona dioda LED
Ostrzeżenie o zbyt niskim napięciu akumulatora	dla 6 V < 5,25 V_{DC}, dla 12 V < 12,0 V_{DC}
Tolerancja pomiaru Ah	+/- 10 % (zależy od konstrukcji i parametrów produkcyjnych)
Tolerancja pomiaru VDC	+/- 2 %
Zabezpieczenie odwrócenia polaryzacji	tak
Zdolność wykonania kolejnych testów	natychmiastowa
Obudowa	ABS
Szczelność	IP54
Wymiary	210 mm × 110 mm × 41 mm
Masa	600 g (w opakowaniu)
Wyposażenie	Przewody testowe, futerał, certyfikat zgodności, etykiety na akumulatory
Gwarancja	1 rok

Dystrybucja: 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

Pronto – Drukarka do kart identyfikacyjnych

Pronto

MAGICARD

Mała, kompaktowa drukarka o nowoczesnym wyglądzie do zastosowania w każdej firmie i w każdym miejscu. Do szybkiego drukowania identyfikatorów oraz różnego rodzaju kart plastikowych. Drukarka Pronto jest łatwa w konfiguracji i użytkowaniu, posiada instrukcję i sterowniki w języku polskim do Windows 2000, XP, Vista, 7 i zapewnia niezawodne drukowanie kart przez wiele lat. Drukarka Magicard Pronto umożliwia wykorzystanie HoloKote i HoloPatch – opatentowanych zabezpieczeń przed nieautoryzowanym kopiowaniem kart.

Dzięki drukarce Pronto możesz samodzielnie wykonać kolorowe i monochromatyczne nadruki wysokiej jakości.

Specyfikacja techniczna

- Wydruk karty w kolorze od krawędzi do krawędzi w 35 sekund
- Monochromatyczny wydruk karty w 7 sekund
- TRW - Thermal Rewritable (wielokrotny zadruk termiczny)
- Interfejs do PC: USB rev. 1.1. (kompatybilny z USB 2.0)
- Sterowniki w języku polskim: Windows 2000, XP, Vista, 7
- Rozdzielczość wydruku: 300 dpi
- Zasilanie: 90-265 V / 47-63 Hz
- Wymiary / Masa: 270 mm × 215 mm × 233 mm / 4,4 kg
- Temperatura pracy: od 10°C do 30°C
- Gwarancja: 2 lata

Taśmy

- YMCKO 5 paneli nadruk 300 kart (MA300YMCKO)
- YMCKO 5 paneli nadruk 100 kart (MA100YMCKO)
- Monochromatyczna czarna nadruk 1000 kart (MA1000K-BLACK)
- Monochromatyczna czarna plus overlay nadruk 600 kart (MA600KO)
- Monochromatyczna biała nadruk 1000 kart (MA1000K-WHITE)
- Monochromatyczna czerwona nadruk 1000 kart (MA1000K-RED)
- 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)

Karty

Drukuje na wszystkich standardowych kartach PCV ISO CR-80 (85,6 × 54) oraz CR-79 (84,1 × 52,4) o grubości od 0,51 mm do 1,02 mm, kartach magnetycznych, zbliżeniowych, samoprzylepnych, HoloPatch i kartach do wielokrotnego zadruku TRW.

Zestaw czyszczący

- 1 szt. rolki czyszczącej dostarczanej z każdą taśmą
- 10 szt. kart czyszczących, 1 flamaster (CK1)
- 5 wałków czyszczących plus wymienna oś wałka

Dystrybucja:

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

Nowy, ekskluzywny panel wideodomofonowy iKALL

Wyposażony w wyświetlacz LCD o rozdzielczości 128×64 pikseli oraz 21-przyciskową, podświetlaną klawiaturę dotykową. W standardowej wersji modułu możliwe jest wprowadzenie do 3800 opisów do listy lokatorów oraz 6400 kodów otwarcia zamka. Opisy mogą być wyszukiwane za pomocą dwóch przycisków przewijania góra/dół lub po wprowadzeniu kilku początkowych liter szukanej nazwy. Po znalezieniu żądanego opisu wystarczy wcisnąć przycisk dzwonka aby nawiązać połączenie z lokalem. Możliwe jest również bezpośrednie połączenie z wybranym lokalem poprzez wprowadzenie numeru wywołania przypisanego do tego lokalu. Wszystkie funkcje, lista lokatorów oraz kody zamka programowane są za pomocą lokalnego menu. Dodatkowo lista oraz kody zamka mogą zostać przesłane z PC, dołączonego do portu USB, za pomocą oprogramowania 1249B.

iKALL wyposażony jest w dwa wyjścia: elektroniczne wyjście ryglowe (3A) oraz dodatkowe wyjście przekaźnikowe (10 A) np. do sterowania bramą. Dodatkowo moduł posiada wejście do podłączenia czujki drzwiowej sygnalizującej stan drzwi (czerwona dioda LED na aparatach wewnętrznych) oraz wejście umożliwiające podłączenie przycisku wyjścia.

Funkcja „wiadomość powitalna" pozwala na wprowadzenie dowolnego tekstu (np. adresu budynku), który będzie wyświetlany na ekranie panelu w trybie „standby". Menu ekranowe może być wyświetlane w jednym bądź naprzemiennie w dwóch wybranych językach.

Panel kompatybilny jest ze wszystkimi funkcjami i produktami systemów Simplebus Color oraz SimpleBus TOP.

iKALL - najważniejsze parametry i funkcje:

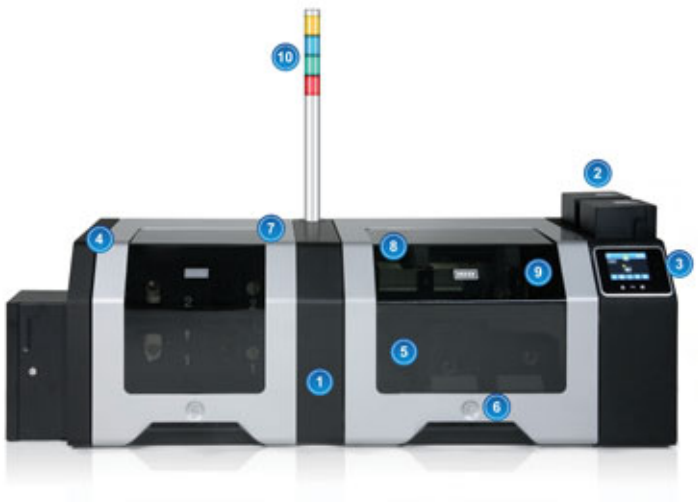
- dotykowe przyciski
- niebieskie podświetlanie
- wiadomość powitalna
- pamięć 3800 opisów oraz 6400 kodów zamka
- oświetlenie pola widzenia kamery 10 diodami LED
- szerokokątna kamera 1/4"
- elektroniczne wyjście napięciowe 3 A (AC lub DC)
- dodatkowe wyjście przekaźnikowe 10 A (NC/NO)
- wejście DO – czujka drzwiowa
- wejście RTE – przycisk wyjścia

Dystrybucja:

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

FARGO HDP8500
Nowa drukarka retransferowa do pracy ciągłej



Jedyna na rynku drukarka retransferowa do pracy ciągłej. Nowoczesna, wysokowydajna, szybka, odporna na zużycie. Posiada znakomite parametry techniczne, daje najwyższej jakości nadruk na kartach plastikowych. Przeznaczona dla wyspecjalizowanych centrów personalizacji kart, banków, wyższych uczelni, organizacji państwowych, wojska, korporacji.

Specyfikacja techniczna

- Wielowątkowy tryb pracy – symultaniczne kodowanie, drukowanie i laminowanie oraz dodatkowe dwa tryby drukowania (wysoka wydajność lub jakość nadruku)
- W standardzie wbudowany serwer ethernet-owy, moduł dwustronny oraz dwa zamykane podajniki o łącznej pojemności 400 kart
- Dotykowy wyświetlacz LCD z możliwością wprowadzenia kodu PIN-u
- 3 letni okres gwarancyjny oraz dożywotnia gwarancja na głowicę drukującą
- Zabezpieczenie nadruku wytrzymałymi materiałami eksploatacyjnymi
- Solidna metalowa obudowa ze specjalnymi zamknięciami ograniczającymi dostęp do kaset z materiałami eksploatacyjnymi
- System przepływu i filtracji powietrza: gęsty filtr powietrza, dwa wydajne wentylatory, specjalne uszczelnienia, wewnętrzne czujniki temperatury
- Więcej niż jeden moduł czyszczący i pełen wgląd w ścieżkę transportu karty we wnętrzu drukarki
- Szyfrowanie danych przesyłanych do drukarki za pośrednictwem sieci ethernet-owej oraz wymazywanie/zacieranie danych pozostałych po nadruku z panelu K
- Wiele dodatkowych opcji rozszerzenia funkcjonalności urządzenia
- Dystrybutor: Control System FMN - Advantage Channel Partner HID

Parametry techniczne	
Rodzaj nadruku	dwustronny, termosublimacja w technologii retransferu
Rozdzielczość	300 dpi
Ilość kolorów	16,7 mln / 256 odcieni na piksel
Obsługiwane typy taśm	YMC , YMCK , YMCKK , ymcKT , film retransferowy, taśmy fluorescencyjne/UV
Szybkość wydruku	YMCK do 1000 kart/8 godzin ciągłej pracy YMC do 1200 kart/8 godzin ciągłej pracy YMCKK do 720 kart/8 godzin ciągłej pracy
Obsługiwane typy kart	Rozmiar: CR-80 (85,6 mm x 54 mm), Grubość: 0,762 mm – 1,27 mm
Podajnik kart	400 kart (0,76 mm), dodatkowa sygnalizacja braku kart w podajniku
Odbiornik kart	200 kart (0,76 mm)
Moduł czyszczący	2 sztuki
Sterownik drukarki	Windows 7 (32 bit & 64 bit), Windows Vista™ (32 bit & 64 bit), Windows XP, Windows 2003 Server, Windows 2000, MAC OS X v10,4 / v10,5, Linux (Ubuntu 7.10, Red Hat Enterprise Desktop 5, Fedora Core 7, Fedora Core 8, openSUSE 10.3.)
Interfejs	USB 2.0 i Ethernet w standardzie
Pamięć drukarki	32 MB
Wyświetlacz	graficzny, dotykowy, pełnokolorowy LCD 3,2"
Masa	wersja podstawowa drukarki: 27,7 kg
Wymiary	wersja podstawowa: 39,4 cm x 71,6 cm x 35,6 cm
Zasilanie	100-240 V_{AC}, 50 Hz / 60 Hz
Gwarancja	3-lata na drukarkę, dożywotnia gwarancja na głowicę drukującą
Dodatkowe opcje	laminator, laminator dwustronny, dodatkowe wskaźniki świetlne do zdalnego nadzoru pracy urządzenia, korektor odkształceń kart (ISO Card Flattener), laser grawerujący
Opcje koderów	koder paska magnetycznego ISO, HiCo i LoCo, ścieżki 1, 2 i 3 czytnik/koder kart stykowych, czytnik/koder kart zbliżeniowych

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

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

Drukarki SD260 i SD360
małe, szybkie, wysokowydajne

Drukarki kart plastikowych SD260 (jednostronna) i SD360 (dwustronna) to najnowsze modele termotransferowe wprowadzane na rynek przez amerykańskiego producenta dużych systemów kartowych, firmę Datacard. Drukarki posiadają szereg nowatorskich rozwiązań technicznych oraz zwartą i ergonomiczną budowę, wykonane są z najwyższej jakości materiałów konstrukcyjnych. Przekłada się to bezpośrednio na łatwość i przyjemność obsługi nowych modeli z serii SD. Zastosowane innowacje pozwalają na osiągnięcie niespotykanej w innych drukarkach wysokiej jakości nadruku oraz wyjątkowych parametrów wydajności.

Zaletą tych drukarek jest długi okres gwarancyjny i niska cena. Biorąc pod uwagę prędkość drukowania oraz współczynnik jakości do ceny, prezentowane modele drukarek do kart plastikowych firmy Datacard są najlepszymi urządzeniami w swojej klasie.

SD260 i SD360 są szczególnie rekomendowane małym i średnim przedsiębiorstwom.

Dystrybutor: Control System FMN partner Datacard

Parametry techniczne	
Rodzaj nadruku	termosublimacja, termotransfer jednostronny (SD260), dwustronny (SD360)
Rozdzielczość	300 dpi
Ilość kolorów	16,7 mln / 256 odcieni na piksel
Obsługiwane typy taśm	YMCKT, ymcKT, KT, YMCKT-K, KTT, HQ, jednokolorowe, srebrna, złota, zdrapka
Szybkość wydruku	**do 200 kart/h** – jednostronnie pełen kolor (YMCKT) **do 830 kart/h** – jednostronnie jeden kolor (czarna HQ)
Obsługiwane typy kart	Rozmiar: CR-80 (85,6 mm x 54 mm) Grubość: 0,25 mm – 0,94 mm Rodzaj: PCV, ABS, PET, PET-G, PC, samoprzylepne
Podajnik kart	Automatyczny na 100 kart Dodatkowa sygnalizacja braku kart w podajniku**
Odbiornik kart	25 kart
Odbiornik odrzutów	nie – SD260, tak – SD360
Sterownik drukarki	Windows Vista™ (32 bit & 64 bit), Windows XP (32 bit & 64 bit), Windows 2003 Server, Windows 2008 Server, Windows 7 (32 bit & 64 bit)
Interfejs	**USB 2.0, Ethernet**
Pamięć drukarki	**128 MB**
Wyświetlacz	Graficzny jednokolorowy LCD
Masa	wersja bez koderów* 3,7 kg (zależnie od opcji)
Wymiary	wersja bez koderów* 39,1 cm×17,5 cm×22,4 cm
Gwarancja	**30 miesięcy**
Dodatkowe opcje	podajnik na **200 kart**** odbiornik na 100 kart zamek typu Kensington®
Opcje koderów	koder paska magnetycznego, czytnik kart procesorowych stykowych i zbliżeniowych, stacja dokująca*
Certyfikaty	cULus, FCC, I.C., CE, Ctick, VCCI, RoHS, WEEE, ENERGY STAR , CCC, KCC*

* dotyczy wyłącznie modelu SD260
** dotyczy wyłącznie modelu SD360

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

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

UT-4DR
Interfejs RS485-TCP/IP do systemu RACS4

Interfejs **UT-4DR** jest urządzeniem, które umożliwia komunikację z systemem kontroli dostępu RACS4 za pośrednictwem sieci komputerowej 10/100 BaseT Ethernet. Oprócz tej podstawowej funkcji, interfejs udostępnia 4 linie zewnętrzne, które mogą być skonfigurowane jako wejścia lub wyjścia i obsługiwane z poziomu przeglądarki sieciowej lub za pomocą komend protokołu Telnet.

Charakterystyka:

- Interfejs komunikacyjny TCP/IP do systemu RACS4
- Obniża znacznie koszt komunikacji TCP/IP w ramach systemu RACS4
- Łatwy w obsłudze i konfiguracji
- Konfiguracja z poziomu przeglądarki internetowej
- Praca w sieciach LAN/WAN 100/10Mbit/s Ethernet
- Stały lub dynamiczny adres IP
- 4 linie WE/WY ogólnego przeznaczenia
- Sterowanie liniami WE/WY z poziomu przeglądarki
- Sterowanie liniami WE/WY za pomocą komend protokołu Telnet
- Możliwość wykorzystania poza systemem kontroli dostępu RACS4 jako zdalnego portu WE/WY, sterowanego za pośrednictwem sieci komputerowej
- Obudowa przystosowana do montażu na szynie DIN 35 mm
- Moduł elektroniczny oparty na nowoczesnym 32-bitowym procesorze
- Obsługa interfejsu UT-4DR wymaga programu PR Master w wersji 4.4.6.xxx lub wyższej
- Zasilanie 10-15 V_{DC}

Producent: roger®

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

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

PR411DR-SET & PR402DR-SET
Zestawy kontroli dostępu

Akumulator widoczny na zdjęciu nie wchodzi w skład zestawu

PR411DR-SET i **PR402DR-SET** są zestawami złożonymi z kontrolera dostępu PR411DR lub PR402DR oraz zasilacza sieciowego PS-10ACDR (18VA) osadzonych fabrycznie w obudowie metalowej mogącej pomieścić akumulator awaryjny 7Ah/12V. Obudowa metalowa jest wyposażona w łącznik ochrony antysabotażowej oraz posiada wizjer do podglądu wskaźników statusowych zainstalowanych w niej urządzeń. Zestaw jest dedykowany do realizacji kontroli dostępu pojedynczego przejścia z jedno- lub dwustronną identyfikacją. Uzupełnieniem zestawu mogą być czytniki serii PRT produkcji ROGER lub inne czytniki pracujące w jednym z popularnych standardów takich jak Wiegand.

Zalety stosowania zestawów w rozwiązaniach kontroli dostępu:

- Atrakcyjna cena zestawu
- Kompletność rozwiązania – zestaw zawiera wszystkie (oprócz terminali) elementy potrzebne do realizacji punktu kontroli dostępu
- Możliwość instalacji na suficie
- Bezpośredni podgląd stanu pracy kontrolera dostępu dzięki wbudowanemu w obudowę wizjerowi
- Estetyczna metalowa obudowa
- Łatwa i szybka instalacja dzięki wyposażeniu w akcesoria montażowe

Zawartość zestawu:

- Kontroler dostępu PR411DR lub PR402DR
- Karta Master
- Komplet zworek do programowania adresu kontrolera
- Zasilacz transformatorowy PS-10ACDR
- Obudowa metalowa z wizjerem, łącznikiem antysabotażowym i szyną DIN 35mm
- Komplet wkrętów mocujących
- Opaski zaciskowe do zamocowania akumulatora
- Komplet przewodów do podłączenia akumulatora
- Instrukcje obsługi

Producent: roger®

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

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

CDV-40NM
monitor wideodomofonowy z rozszerzoną funkcjonalnością

Nowy monitor w ofercie firmy – model CDV-40NM - posiada 4-calowy ekran wysokiej rozdzielczości z podświetleniem LED. Oprócz standardowej funkcjonalności wideodomofonu (kontakt audiowizualny z osobą przy wejściu) został także wyposażony w szereg dodatkowych funkcji. Po zainstalowaniu w domu kilku odbiorników istnieje możliwość rozmowy pomiędzy ich użytkownikami (funkcja interkomu). Monitor obsługuje dwa wejścia (dwa panele audio/wideo) oraz dodatkowo dwie kamery CCTV, dzięki czemu użytkownik ma możliwość podglądu większego obszaru.

Dla wygody użytkownika urządzenie zostało wyposażone w pamięć wewnętrzną oraz czytnik kart Micro SD. Cechy te pozwalają na automatyczny lub ręczny zapis zdjęć oraz krótkich filmów (dodatkowa kontrola wejść – np. podczas nieobecności domowników). Zapisane obrazy można w prosty sposób przenieść na inne urządzenie (np. na komputer).

Zestaw wideodomofonowy może być rozbudowany o dodatkowe monitory z serii CDV-xxx oraz unifony DP-4VHP. Monitor współpracuje z dowolnym panelem wejściowym w systemie 4-żyłowym, dzięki czemu można skonfigurować odpowiedni zestaw dostosowany do własnych wymagań. 44 lata doświadczenia firmy COMMAX w projektowaniu elementów systemów wideodomofonowych pozwala cieszyć się użytkownikowi doskonałą jakością i bezawaryjną pracą przez długi czas.

Właściwości:

- monitor kolorowy
- wyświetlacz 4" Color TFT-LCD
- standard sygnału wizyjnego PAL/NTSC
- obsługa dwóch wejść (dwa panele wejściowe)
- obsługa kamer CCTV
- wbudowany moduł pamięci 128 obrazów oraz filmów
- czytnik kart Micro SD
- możliwość podłączenia dodatkowego monitora
- współpraca z unifonami DP-4VR, DP-4VH
- paging pomiędzy stacjami
- instalacja czteroprzewodowa + obwód elektrozamka
- współpracuje z kamerami analogowymi czteroprzewodowymi
- zasilanie 230 V
- wymiary: 249×158×47 mm

Dystrybucja: &GDE POLSKA

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

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

Zwory elektromagnetyczne SCOT

Zwory elektromagnetyczne SCOT są alternatywą dla powszechnie stosowanych w systemach kontroli dostępu elektrozaczepów. Zwora składa się z elementu wykonawczego zawierającego elektromagnes, montowanego na ramie drzwi, oraz metalowej płytki, umieszczanej na skrzydle drzwi. Zasilona cewka elektromagnesu przyciąga płytkę zabezpieczając w ten sposób wejście. W zależności od modelu zwory maksymalny nacisk na drzwi przy którym elektromagnes przyciąga metalową płytkę wynosi 180, 280, 350, 540 kg.

Oferta firmy została wzbogacona o najmniejszą zworę elektromagnetyczną - model EL-120S, charakteryzujący się maksymalnym naciskiem na drzwi wynoszącym 70 kg. Zwora taka znajduje zastosowanie przy niewielkich barierach oddzielających dwie strefy (np. baseny, wewnętrzne przejścia w obiektach użyteczności publicznej nadzorowane przez portiera itp.)

Zwory elektromagnetyczne SCOT przystosowane są do pracy z napięciem 12 lub 24 V_{DC}.

Zwory elektromagnetyczne stosuje się w systemach kontroli dostępu zamiennie z elektrozaczepami rewersyjnymi, czyli tam, gdzie przepisy bezpieczeństwa wymagają otwarcia drzwi po zaniku napięcia w systemie kontroli: wyjściach ewakuacyjnych, przeciwpożarowych, budynkach użyteczności publicznej.

Zwora elektromagnetyczna nie posiada ruchomych elementów mechanicznych, przez co praktycznie nie występuje zużycie elementów urządzenia. Z tego względu stosowana jest w miejscach o dużym natężeniu ruchu, gdzie kontrolowane drzwi są często otwierane, eliminując konieczność stałej konserwacji.

Dodatkowe uchwyty montażowe typu „L", „ZL", „UL" pozwalają na montaż zwory praktycznie na każdych drzwiach.

Sygnalizacja

Zwora elektromagnetyczna wyposażona jest w przekaźnik NO/NC, który może być wykorzystany w systemie kontroli dostępu informując o otwarciu/zamknięciu sterowanych drzwi. Dzięki temu możemy przekazać informację np. do systemu alarmowego, informując o stanie drzwi.

Dioda LED

Na obudowie zwory znajduje się dwukolorowa dioda informująca o stanie wejścia. Jeżeli drzwi są zamknięte, jest to sygnalizowane zielonym kolorem diody – jeżeli drzwi zostaną otwarte lub będą niedomknięte – dioda będzie świecić kolorem czerwonym. Jeżeli cewka zwory elektromagnetycznej nie jest zasilana (np. podczas trwania impulsu sterującego) – dioda jest wygaszona.

cecha / model	maksymalny nacisk na drzwi	sygnalizacja	dioda LED	zasilanie	wymiary
EL-120S	70 kg	NC		12 V_{DC} / 100 mA lub 24 V_{DC} / 60 mA	90 x 33 x 20 mm
EL-350	180 kg			12 V_{DC} / 300 mA lub 24 V_{DC} / 150 mA	170 x 41 x 20 mm
EL-350S	180 kg	NC		12 V_{DC} / 300 mA lub 24 V_{DC} / 150 mA	183 x 41 x 20 mm
EL-600SL	280 kg	NO/NC	✓	12 V_{DC} / 480 mA lub 24 V_{DC} / 240 mA	250 x 48 x 26 mm
EL-600TSL	280 kg	NO/NC	✓	12 V_{DC} / 480 mA lub 24 V_{DC} / 240 mA	250 x 48 x 26 mm
EL-800SL	350 kg	NO/NC	✓	12 V_{DC} / 500 mA lub 24 V_{DC} / 250 mA	285 x 55 x 29 mm
EL-800WS	350 kg	NC		12 V_{DC} / 500 mA	228 x 52 x 27 mm
EL-800DSL	2 x 350 kg	NO/NC	✓	2 x 12 V_{DC} / 500 mA lub 2 x 24 V_{DC} / 250 mA	570 x 55 x 29 mm
EL-1200SL	540 kg	NO/NC	✓	12 V_{DC} / 600 mA lub 24 V_{DC} / 300 mA	265 x 75 x 40 mm
EL-1200DSL	2 x 540 kg	NO/NC	✓	2 x 12 V_{DC} / 600 mA lub 2 x 24 V_{DC} / 300 mA	530 x 75 x 40 mm

Dystrybucja: GDE POLSKA

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

Kamera XGB-21CS

XGB-21CS to kamera o bardzo wysokiej czułości i rozdzielczości (580 TVL w trybie kolorowym, 650 TVL w trybie B/W), wyróżniająca się bardzo dobrym i wiernym odwzorowaniem kolorów oraz przemyślanym systemem mocowania poprzez zastosowanie uchwytu pośredniczącego. Ten lekki i niewielkich rozmiarów uchwyt przykręcamy do ściany i dopiero do niego mocujemy kamerę. Niebanalny i estetyczny wygląd kamery pozwala lepiej wkomponować się w elewacje nowo budowanych obiektów.
W kamerze zastosowano procesor obróbki sygnału Blue-I.
W XGB-21CS, podobnie jak w CCM-21VF czy CBM-25VD, zastosowano diody SR LED (Single Reflective LED). Mimo mniejszej liczby diod niż w rozwiązaniach z konwencjonalnymi diodami osiągnięto równomierne oświetlenie obserwowanej sceny, a dodatkową zaletą jest mniejsza emisja ciepła.

Zalety:

- wbudowany jasny obiektyw F1,2 o zmiennej ogniskowej 7,5÷50 mm z automatyczną przysłoną DC,
- dodatkowe serwisowe wyjście wideo,
- mechaniczny filtr podczerwieni IR - TDN(ICR),
- funkcja DSS (Digital Slow Shutter) regulowana w zakresie do 128 ramek zwiększająca czułość kamery,
- promiennik podczerwieni o zasięgu do 80 m,
- grzałka i wentylator,
- XWDR – poszerzony zakres dynamiki kamery,
- cyfrowa stabilizacja obrazu DIS,
- redukcja szumów 3D DNR, w porównaniu ze standardową redukcją DNR zapewnia zmniejszenie smużeń przemieszczających się obiektów,
- ukryty kabel w uchwycie.

Właściwości:

- bardzo wysoka rozdzielczość 580 TVL w trybie kolorowym oraz 650 TVL w trybie czarno-białym,
- 6,13-krotny cyfrowy zoom,
- menu ekranowe OSD,
- AGC, WDR, Eclipsa, BLC, AWB, 3D DNR, DIS, Flickerless, D/N, DZ – regulacja przez OSD,
- zasilanie 12 V_{DC}.

Model	XGB-21CS
Standard sygnału wideo	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/3" SONY Super HAD II CCD
Rozdzielczość efektywna	752(H)×582(V) 440K
Rozdzielczość	580 TVL kolor, 650 TVL B/W
Wyjście wideo	1,0V_{p-p}, 75 Ohm
Odstęp sygnał/szum	>52 dB (wył. AGC)
WDR	on (3 poziomy, maks. 60 dB) /off
Obiektyw	f=7,5~50 mm, F1,2
Tryb dzień/noc	auto
Czułość	0,05 lx (kolor) / 0,0002 (DSS on, BW) / 0,00 lx (IR LED włączone)
Menu OSD	angielski, chiński, koreański, rosyjski, hiszpański, francuski
Podczerwień	SR IR LED 12EA (850 nm), czujnik 1EA
Zasięg promiennika IR	maks. 80 m
Cyfrowa redukcja szumu	3D DNR, 63 poziomy / wył.
Funkcja DSS	do 128 ramek obrazu
Balans bieli	automatyczny
Automatyczna regulacja wzmocnienia (AGC)	wł./3 poziomy
Eclipsa	16 stref
Kompensacja światła tylnego	BLC/3 poziomy
Redukcja migotania	wł./wył.
Cyfrowa stabilizacja obrazu	wł./wył.
Cyfrowy zoom	6,13x
Strefy prywatności	8 programowalne strefy
Detekcja ruchu	4 programowalne strefy
Elektroniczna migawka	1/50~1/90 000 s
Stopień ochrony IP	IP67
Zasilanie	12 V_{DC}
Pobór prądu	maks. 1,7 A / 20 W
Wymiary (szer. x wys. x gł.)	125,7 x 222,3 x 372,4 mm
Temperatura pracy / Wilgotność	-30°C~50°C / 30%~80% RH
Masa	3,8 kg

Kamera IVC5055VR

CNB TECHNOLOGY Inc.

Kamera wandaloodporna IP IVC5055VR to kolejny model kamer IP firmy CNB. Kamera wyróżnia się rozdzielczością Full HD, poklatkowością 25 obrazów na sekundę, przetwornikiem CMOS ze skanowaniem progresywnym, dwustrumieniowością. Dodatkową zaletą jest możliwość awaryjnego zapisu obrazów na karcie SD oraz zasilanie PoE. Obraz z kamery cechuje naturalne odwzorowanie kolorów.

Zaletami kamery są:

- przetwornik CMOS 1/3" ze skanowaniem progresywnym
- rozdzielczość Full HD 1980×1080 pikseli przy 25 kl./s
- mechaniczny filtr podczerwieni
- dwa strumienie wizyjne z kompresjami H.264/MJPEG
- dwukierunkowa komunikacja głosowa
- zapis obrazów na kartach SD
- zgodność z protokołem ONVIF
- proporcje obrazu 16:9

Właściwości:

- kolorowa kamera dzień/noc
- automatycznie przełącza się w tryb BW
- dołączony bezpłatny program CMS (dwa monitory, 128 kanałów w tym 64 kamery IP, e-mapa, pełna zdalna obsługa kamery)
- dołączony bezpłatny program NVR CNB pozwalający na nagrywanie obrazów z 32 kamer bez ograniczeń wielkości bazy danych
- dołączony bezpłatny program NVR Axxon Smart Start pozwalający na nagrywanie obrazów z 16 kamer z możliwością analizy treści obrazu
- analogowe wyjście wizji PAL/NTSC
- regulacje jasności oraz koloru
- AGC, BLC, AWB, Flickerless, D/N, DSS
- zasilanie 12 V_{DC} albo PoE IEEE 802.3af
- grzałka
- obudowa kopułkowa wandaloodporna IP67

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

ABUS SECURITY CENTER
ABUS KEMAZ POLSKA Sp. z o.o.
ul. Wadowicka 8A
30-415 Kraków
tel. 12 640 15 60
faks 12 640 15 61
e-mail: tiglinski@abus-kemaz.pl
www.abus.pl

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

AGIS Fire & Security Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. 22 430 83 01
faks 22 430 83 02
e-mail: agisfs.pl@agisfs.com
www.agisfs.pl

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

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./faks 58 345 51 95
e-mail: ambient@ambientsystem.pl
www.ambientsystem.pl

ALPOL Sp. z o.o.
ul. Ścigały 10
40-208 Katowice
tel. 32 790 76 16
faks 32 790 76 60
e-mail: katowice@e-alpol.com.pl
www.e-alpol.com.pl

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

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

ul. Narwicka 5, 80-557 **Gdańsk**
tel. 32 750 30 81
faks 32 750 30 84
e-mail: gdansk@e-alpol.com.pl

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

ul. Paulinów 10, 67-200 **Głogów**
tel. 32 750 30 78
faks 32 750 30 69
e-mail: glogow@e-alpol.com.pl

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

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

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

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

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

ul. Długa 19, 63-400 **Ostrów Wlkp.**
tel. 32 750 30 25
faks 32 750 30 27
e-mail: ostrow@e-alpol.com.pl

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

ul. Młodzianowska 75d, 26-600
tel. 32 750 30 33
faks 32 750 30 35
e-mail: radom@e-alpol.com.pl

ul. POW 64, 98-200 **Sieradz**
tel. 32 750 30 55
faks 32 750 30 57
e-mail: sieradz@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. Polna 134/136, 87-100 **Toruń**
tel. 32 750 30 80
faks 32 750 30 73
e-mail: torun@e-alpol.com.pl

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

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

ul. Spółdzielcza 3, 87-800 **Włocławek**
tel. 32 750 30 43
faks 32 750 30 45
e-mail: wloclawek@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

ul. Dekoracyjna 3, 65-722 **Zielona Góra**
tel. 32 750 30 70
faks 32 750 30 71
e-mail: zielona@e-alpol.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.
Sławomir Pruski
ul. Franciszkańska 125
91-845 Łódź
tel. 42 657 30 80
faks 42 655 20 99
e-mail: info@atline.pl
www.atline.pl

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

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

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

CAMSAT
Gralak Przemysław
ul. Ogrodowa 2a
86-050 Solec Kujawski
tel. 52 387 36 58, 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: info@cbcpoland.pl
www.cbcpoland.pl

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

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

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

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

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

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

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

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

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

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

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

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
www.ebs.pl

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

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

PHU ELPROMA Sp. z o.o.
Biuro Handlowe:
ul. Syta 177
02-987 Warszawa
tel. 22 312 06 00
faks 22 312 06 02
e-mail: elproma@elproma.pl
www.elproma.pl

ELZA
ELEKTRO-SYSTEMY-INSTALACJE
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

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

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

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

GEO-KAT Sp. z o.o.
Al. Prymasa Tysiąclecia 145/149
01-424 Warszawa
tel. 22 877 08 80
faks 22 877 08 97
e-mail: info@geokat.com.pl
www.geokat.com.pl

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

HSA SYSTEMY ALARMOWE
Leopold Rudziński
ul. Langiewicza 1
70-263 Szczecin
tel. 91 489 41 81, 434 67 38
faks 91 489 41 84
e-mail: biuro@hsa.pl
www.hsa.pl

INSAP Sp. z o.o.
ul. Ładna 4-6
31-444 Kraków
tel. 12 411 98 44, 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 00
faks 32 324 89 01
e-mail: firma@kabe.pl
www.kabe.pl

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

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

MICROMADE
Gałka i Drożdż Sp. J.
ul. Wieniawskiego 16
64-920 Piła
tel./faks 67 213 24 14
e-mail: mm@micromade.pl
www.micromade.pl

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

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

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

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

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

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

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

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. Irysowa 11
02-660 Warszawa
tel. 22 831 15 35
faks 22 831 73 36
e-mail: biuro@polital.pl
www.polital.pl

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

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: norbert@pulsar.pl
www.pulsar.pl

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

RETT-POL Telewizja Przemysłowa i Telekomunikacja
ul. Podmiejska 21
01-498 Warszawa
tel. 22 664 84 63
faks 22 833 09 07
e-mail: michal.dziwniel@rettpol.com.pl
www.rettpol.com.pl

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

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

SAMSUNG TECHWIN EUROPE LIMITED
Biuro w Polsce
ul. Postępu 15c
02-676 Warszawa
tel. 22 20 50 777
faks 22 20 50 763
e-mail: STEsecurity@samsung.com
www.samsungsecurity.com

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

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

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

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

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

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

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

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

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

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

SCHNEIDER ELECTRIC POLSKA Sp. z o.o.
ul. Rzymowskiego 53
02-697 Warszawa
tel. 22 313 24 10
faks 22 314 24 11
e-mail: poland.helpdesk@schneider-electric.com
www.schneider-electric.pl/buildings

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

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

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

SPRINT S.A.
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

SPS Electronics Sp. z o.o.
ul. Wał Miedzeszyński 630
03-994 Warszawa
tel. 22 518 31 50
faks 22 518 31 70
e-mail: warszawa@spselectronics.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@spselectronics.pl

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

ul. Drewnowska 48, 91-002 **Łódź**
tel. 42 617 00 32
faks 42 659 85 23
e-mail: lodz@spselectronics.pl

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

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

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

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

P.P.H.U. SUMA Sp. z o.o.
ul. Panewnicka 109
40-761 Katowice
tel. 32 258 05 97
faks 32 258 05 98
e-mail: biuro@suma.com.pl
www.suma.com.pl

Biuro Handlowe:
ul. Makuszyńskiego 22a/23, 31-752 **Kraków**
tel. 12 684 00 23
e-mail: krakow@suma.com.pl

TAP- Systemy Alarmowe Sp. z o.o.
Os. Armii Krajowej 125
61-381 Poznań
tel. 61 876 70 88
faks 61 875 03 03
e-mail: sprzedaz@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
Robert Prandota, Henryk Prandota, Krystyna Prandota Spółka Jawna
ul. Słoneczna 4
40-135 Katowice
tel. 32 258 22 89
faks 32 357 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
faks 22 516 97 87
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl

UNICARD S.A.
ul. Wadowicka 12
30-415 Kraków
tel. 12 398 99 00
faks 12 398 99 01
e-mail: biuro@unicard.pl
www.unicard.pl

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

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

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

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
AAT Holding	–	TAK	TAK	–	TAK
ABUS	TAK	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	–
AGIS Fire & Security	TAK	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	–
Alarmnet	–	TAK	TAK	–	TAK
Alarmtech Polska	TAK	TAK	–	–	TAK
Alkam System	TAK	TAK	–	TAK	–
Alpol	–	–	TAK	–	TAK
Ambient System	TAK	TAK	TAK	TAK	TAK
Anma	–	TAK	–	TAK	TAK
ASSA ABLOY	–	–	TAK	–	TAK
ATLine	–	TAK	TAK	TAK	–
BOSCH	TAK	–	TAK	–	TAK
P.W.H. Brabork - Laboratorium	–	TAK	TAK	TAK	–
bt electronics	TAK	TAK	TAK	TAK	TAK
CAMSAT	TAK	–	TAK	–	–
CBC Poland	TAK	–	TAK	–	TAK
CMA	TAK	–	–	TAK	–
CONTROL SYSTEM FMN	–	TAK	TAK	TAK	TAK
D-MAX	–	TAK	TAK	–	TAK
D+H Polska	TAK	TAK	TAK	TAK	TAK
DG Elpro	–	TAK	TAK	TAK	TAK
DOM Polska	TAK	TAK	TAK	–	–
Dyskam-Ekotrade	TAK	TAK	–	TAK	–
Dyskret	–	TAK	TAK	TAK	TAK
EBS	TAK	TAK	TAK	–	–
ela-compil	TAK	–	TAK	–	TAK
El-Mont	TAK	–	–	TAK	–
Elproma	–	TAK	–	TAK	–
ELZA Elektro-Systemy-Instalacje	–	TAK	TAK	TAK	–
Eureka	–	TAK	–	TAK	–
Factor Polska	–	TAK	TAK	–	TAK
FES	–	TAK	TAK	TAK	TAK
GDE Polska	–	TAK	TAK	–	TAK
GEO-KAT	–	TAK	TAK	–	TAK
HSA	–	–	TAK	–	TAK
Insap	–	TAK	TAK	TAK	TAK
ISM EuroCenter	–	–	TAK	–	TAK

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Janex International	–	TAK	TAK	TAK	TAK
KABE	TAK	TAK	TAK	TAK	TAK
KATON	–	–	TAK	–	TAK
Kolektor MR	–	TAK	TAK	TAK	TAK
Legrand Polska	TAK	TAK	TAK	–	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	–	TAK	–	–
Nuuxe – Radioton	–	TAK	TAK	TAK	TAK
OBIS	–	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	–	–	–	–
Ramar	–	TAK	TAK	TAK	TAK
RETT-POL	–	–	TAK	TAK	–
RISCO	TAK	–	–	–	–
ROPAM Elektronik	TAK	–	TAK	–	–
Samsung	TAK	–	TAK	–	–
Satel	TAK	–	–	–	–
Sawel	–	TAK	TAK	TAK	TAK
Schrack Seconet Polska	TAK	TAK	–	–	TAK
Secural	TAK	TAK	TAK	–	TAK
S.M.A.	–	TAK	–	TAK	–
Schneider Electric Buildings Polska	–	–	TAK	–	–
Sprint	–	TAK	TAK	TAK	–
SPS Electronics	TAK	–	TAK	–	TAK
STRATUS	–	TAK	TAK	–	–
SUMA	–	–	TAK	–	–
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Tayama	–	–	TAK	–	–
Technokabel	TAK	–	–	–	–
UNICARD	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	–	–
Vision Polska	–	TAK	TAK	–	TAK
ZBAR	–	TAK	TAK	TAK	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ABUS	TAK	TAK	TAK	TAK	–	TAK	TAK	TAK	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, systemy rejestracji gości, karty magnetyczne i zbliżeniowe								
AGIS Fire & Security	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Alarm System	TAK	TAK	TAK	TAK	–	–	–	–	–
Alarmnet	–	TAK	TAK	–	–	TAK	–	–	–
Alarmtech Polska	TAK	–	–	–	–	–	–	–	–
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Ambient System	–	–	–	TAK	–	TAK	–	–	TAK
Anma	TAK	TAK	TAK	TAK	–	TAK	–	–	–
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
ATLine	TAK	TAK	–	–	TAK	TAK	TAK	TAK	–
BOSCH	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	TAK	–	–	–	–	TAK
bt electronics	–	–	TAK	–	–	TAK	–	TAK	–
CAMSAT	–	TAK	–	–	–	–	TAK	–	–
CBC Poland	–	TAK	–	–	–	–	–	–	–
CMA	TAK	–	TAK	–	–	–	TAK	–	–
Control System FMN	TAK	TAK	TAK	–	–	TAK	–	TAK	–
D-MAX	–	TAK	–	–	–	–	–	–	–
D+H Polska	–	–	–	TAK	–	TAK	–	–	TAK
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
DOM Polska	–	–	TAK	–	–	–	–	TAK	–
Dyskam-Ekotrade	TAK	TAK	–	TAK	–	–	TAK	–	–
Dyskret	TAK	TAK	TAK	TAK	–	TAK	–	TAK	TAK
EBS	Transmitery IP (ethernet), GSM/GPRS/SMS, zabezpieczenia bankowe, sygnalizatory, GPS, produkcja OEM/ODM, R&D								
ela-compil	–	–	–	–	–	TAK	–	–	–
El-Mont	TAK	TAK	TAK	–	–	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
ELZA Elektro-Systemy-Instalacje	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
Factor Polska	TAK	TAK	TAK	TAK	TAK	–	–	TAK	TAK
FES	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
GDE Polska	–	TAK	TAK	–	–	–	–	TAK	–
GEO-KAT	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
HSA	TAK	TAK	TAK	TAK	–	–	–	–	–
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
ISM EuroCenter	–	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
Janex International	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
KATON	–	TAK	TAK	–	–	TAK	–	–	–
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	–	–	–	–	TAK	–
Nuuxe – Radioton	–	TAK	–	TAK	–	–	–	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	–	–	TAK
OMC INDUSTRIAL	TAK	TAK	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	–	TAK	–	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	–	TAK	TAK	–	–	–
RETT-POL	TAK	TAK	TAK	TAK	–	–	TAK	–	–
RISCO	TAK	–	TAK	–	–	TAK	–	–	–
ROPAM Elektronik	TAK	TAK	TAK	TAK	–	–	TAK	–	–
Samsung	–	TAK	TAK	–	–	–	–	–	–
Satel	TAK	–	TAK	–	–	–	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	–	–
Sprint	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SPS Electronics	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	TAK	–	–	–
SUMA	–	TAK	–	–	–	–	–	–	–
Tap – Systemy Alarmowe	TAK	–	TAK	–	–	–	–	–	–
Tayama	–	TAK	TAK	–	–	–	TAK	–	–
Technokabel	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
UNICARD	TAK	TAK	TAK	–	–	TAK	–	TAK	–
W2	TAK	–	–	TAK	–	–	–	–	–
Vision Polska	–	–	–	TAK	–	TAK	–	–	–
ZBAR	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

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

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

Skład i łamanie
Tomasz Kaczmarczyk

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

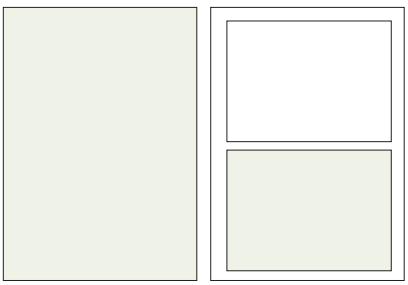
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

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

Cennik reklam

Reklama wewnątrz czasopisma:

cała strona, pełny kolor	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



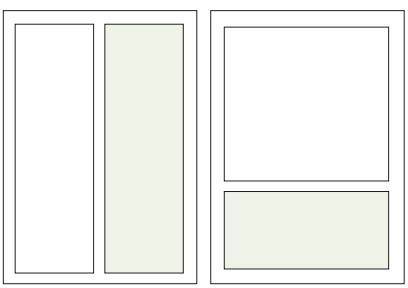
cała strona (200 x 282 mm + 3mm spad)

1/2 strony (170 x 125 mm)

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

Reklama na okładkach:

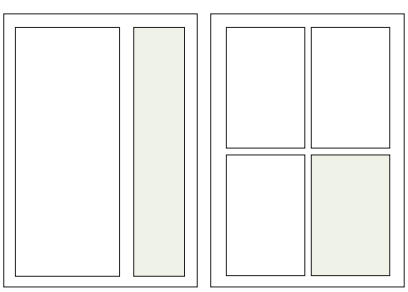
pierwsza strona	indywidualne negocjacje
druga strona	5000 zł
przedostatnia strona	5000 zł
ostatnia strona	5000 zł



1/2 strony (83 x 260 mm)

1/3 strony (170 x 80 mm)

Spis teleadresowy:
jednorazowy wpis 70 zł



1/3 strony (54 x 260 mm)

1/4 strony (83 x 125 mm)

Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Podane ceny nie uwzględniają podatku VAT (23%)

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

Spis reklam

PROMOCJA !

4 kanały IP w prezencie

AVC 16/400/4IP/LT

16 wejść wideo
kompresja sprzętowa H.264
480 kl/s dla standardowej jakości przy D1
320 kl/s dla najwyższej jakości przy D1
16 wejść audio
4 kanały IP

cena promocyjna 3000 PLN netto
cena detaliczna 4320 PLN netto
Okres promocji od 01.01.2012 do 29.02.2012 r.

Produkt w cenie promocyjnej dostępny wyłącznie w:

AAT SPS electronics

iPhone
symbian OS
android
BlackBerry

Ponad 60 000 instalacji na całym świecie

www.alnetsystems.com

ALNET SYSTEMS®

Profesjonalne systemy do cyfrowej rejestracji obrazu

NS NETSTATION
Sieciowy system cyfrowej rejestracji obrazu

NET HYBRID
Hybrydowy system cyfrowej rejestracji obrazu

NET HYBRID HD
Hybrydowy system cyfrowej rejestracji obrazu HD-SDI

CMS PROFESSIONAL
Profesjonalne oprogramowanie klienckie

CMS MOBILE
Oprogramowanie klienckie dla urządzeń mobilnych

Specyfikacje bez końca

Jedno rozwiązanie

Rozwiązania do migracji:

- Wyższy poziom bezpieczeństwa dzięki technologii 13,56 MHz
- Wiele aplikacji w ramach jednego systemu
- Bezproblemowa migracja z HID Prox lub MIFARE do HID iCLASS lub DESFire EV1

HID®

Nieważne, jakie wymagania pojawią się w przyszłości – nowe rozwiązania HID umożliwiają bezproblemową migrację do technologii smart card zaspokajającej przyszłościowe potrzeby z zachowaniem możliwości obsługi popularnych, starszych systemów po możliwie najniższych kosztach dla użytkownika.

Aby uzyskać informacje na temat, kiedy i jak migrować oraz aby poznać dostępne rozwiązania, należy odwiedzić stronę **hidglobal.com/onesolution-zab** i pobrać najnowszą dokumentację dotyczącą migracji.