CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 6(82)/2011

ZABEZPIECZENIA

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

W NUMERZE:

- Zapomniane ultradźwięki
- PoE bez tajemnic (część 1)
- O legitymowaniu na osiedlach chronionych
- Bezprzewodowa transmisja obrazu z kamer IP HD

JVC

Authorised Professional Dealer
euroalarm

www.euroalarm.com.pl

5 LAT GWARANCJI

Czy wiesz, że:
- dla kamer serii SuperLoLux , MTBF (średni czas bezawaryjności) wynosi 93000 godz (ok 10 lat),
- dla kamery TK-C9300 SuperLoLux wydłużyliśmy gwarancję do 5 lat,
- już w lutym 2012 r, JVC wprowadzi do oferty aż osiem nowych modeli kamer IP Super LoLux HD

Wrocław 71 3492772 / Bydgoszcz 52 3254010 / Koszalin 94 3458330 / Gorzów Wlkp. 95 7298337 / Toruń 56 6641214

Spis treści

Wydarzenia, Informacje 4

Publicystyka

O legitymowaniu na osiedlach chronionych
– *Jan Rybczyński* 22

Telewizja dozorowa

PoE bez tajemnic (część 1)
– *Andrzej Walczyk* 26

Bezprzewodowa transmisja obrazu z kamer IP HD
– *Agnieszka Gralak, CAMSAT* 32

Aplikacja iPOLiS MOBILE
– *James Smith, Samsung Techwin Europe* 36

Hemisferyczna technologia monitoringu wizyjnego
– *Linc Polska* 40

Kamera stworzona z myślą o profesjonalistach
– *Jan T. Grusznic, Bosch Security Systems* 44

Systemy zintegrowane

Chomguard Security – pakiet przeznaczony do zarządzania systemami technicznych zabezpieczeń obiektu
– *Tomasz Krawczyk, chomtech.pl* 48

Monitorowanie systemów sygnalizacji włamania i napadu z wykorzystaniem sieci Ethernet (część 3)
– *Adam Rosiński, Maciej Maszewski* 52

Kontrola dostępu

SKD i RCP w małych i średnich obiektach z wykorzystaniem rozwiązań firmy ROGER
– *Kamil Stadnicki, ROGER* 58

KaDe zintegrowane z RCP
– *Ryszard Sobierski, AAT Holding* 64

SSWiN

Zapomniane ultradźwięki – zastosowanie dopplerowskich czujek ruchu w systemach alarmowych w obiektach budowlanych
– *Marcin Buczaj, Politechnika Lubelska* 68

Aper Home Alarm
– *Artur Jajszczak, SPS Electronics* 72

Porady

Oświetlenie w systemach nadzoru wizyjnego (część 2)
– *Agata Majkucińska, Axis Communications* 76

Ochrona przeciwpożarowa

UCS 6000. Oddymianie pod kontrolą (część 2)
– *Mariusz Sowiński, POLON-ALFA* 82

Karty katalogowe 89

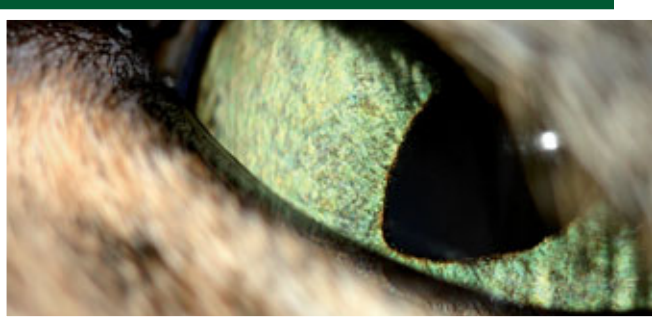
Spis teleadresowy 100

Cennik i spis reklam 110

CZASOPISMO ZABEZPIECZENIA 6/2011

O legitymowaniu na osiedlach chronionych **22**

PoE bez tajemnic (część 1) **26**



Kamera stworzona z myślą o profesjonalistach **44**

Zapomniane ultradźwięki – zastosowanie dopplerowskich czujek ruchu w systemach alarmowych w obiektach budowlanych **68**

Zapraszamy do udziału w konkursie

Polski Mistrz Techniki Alarmowej 2012

Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „**POLALARM**" zaprasza producentów oraz dystrybutorów elektronicznych i elektromechanicznych urządzeń oraz systemów przeznaczonych do ochrony osób i mienia do udziału w **XIV edycji konkursu Polski Mistrz Techniki Alarmowej 2012**.

Zgłoszenia będą przyjmowane do dnia **20 lutego 2012 roku** na drukach *Wniosku o udział w konkursie*. Wypełniony wniosek (wraz z załącznikami) należy przesłać na adres biura zarządu stowarzyszenia POLALARM (ul. Nowogrodzka 18 lok. 8, 00-511 Warszawa, e-mail: *polalarm@polalarm.com.pl*).

Przyznanie tytułów, nagród i wyróżnień w konkursie nastąpi do dnia 3 kwietnia, a uroczystość wręczenia nagród laureatom odbędzie się w pierwszym dniu międzynarodowej wystawy zabezpieczeń SECUREX 2012, tj. 23 kwietnia 2012 roku, na terenie Międzynarodowych Targów Poznańskich.

Na stoisku POLALARMU podczas wystawy SECUREX 2012 będziemy prezentować urządzenia i systemy, które zajęły I miejsce w grupie, oraz laureata głównej nagrody Złota Zbroja.

W miarę możliwości postaramy się zaprezentować wszystkie produkty zgłoszone do konkursu. Wszyscy uczestnicy konkursu będą mieli możliwość umieszczenia na naszym stoisku ulotek i folderów reklamowych z informacją o zgłoszonych do konkursu produktach. *Regulamin konkursu* oraz *Wniosek o udział w konkursie* zamieszczone są na stronie *www.polalarm.org*.

Informacji na temat konkursu udziela biuro zarządu stowarzyszenia POLALARM – tel./faks: 22 626 90 31, 22 625 57 43.

Bezpośr. inf. POLALARM

SCO-2080RH – nowa kamera firmy Samsung

SCO-2080RH to nowa kamera firmy **Samsung** w obudowie typu pocisk (*bullet*). Kamera jest przystosowana do pracy w temperaturach od -50°C do +50°C i doskonale sprawdza się w miejscach narażonych na skrajnie niekorzystne warunki atmosferyczne.

Zastosowanie wentylatora, grzałki i osłony przeciwsłonecznej sprawia, że kamera SCO-2080RH pracuje efektywnie w najbardziej wymagających miejscach, takich jak lotniska, porty, parkingi oraz wszelkie inne otwarte i nieosłonięte obszary. Obudowa o stopniu szczelności IP66 pozwala na bezpośredni montaż na zewnątrz, a wbudowany promiennik podczerwieni LED umożliwia uzyskanie doskonałej jakości obrazu obiektów oddalonych nawet o 50 metrów i znajdujących się w całkowitej ciemności.

Kamera SCO-2080RH typu „wszystko w jednym", która dostarczana jest w komplecie ze zmiennoogniskowym obiektywem, osłoną, uchwytem oraz kablem o długości jednego metra, to znakomita kamera dzienno-nocna z mechanicznym filtrem podczerwieni umożliwiającym uzyskanie wyraźnego, kolorowego obrazu zarówno w dzień, jak i w nocy. Podwójna szklana osłona przednia eliminuje problem występujący w przypadku wielu konkurencyjnych kamer typu pocisk, polegający na tym, że wewnętrzny promiennik podczerwieni oświetla kropelki skondensowanej pary wodnej, która osiada na przedniej szybie obudowy.

W kamerze można ustawić osiem stref detekcji ruchu i dwanaście stref prywatności, natomiast możliwość sterowania poprzez kabel koncentryczny pozwala na zdalne zarządzanie kamerą poprzez menu ekranowe, z poziomu centrum monitorowania. Do tego celu wystarczy kompatybilny rejestrator DVR, np. wybrany model z serii SRD firmy Samsung.

Zastosowanie najnowszej generacji procesora DSP Samsung serii W-V w modelu SCO-2080RH zapewnia uzyskanie kolorowego obrazu o bardzo wysokiej jakości, o rozdzielczości 600 linii TV w ciągu dnia oraz obrazu monochromatycznego o rozdzielczości 700 linii TV w nocy. Trzeciej generacji technologia cyfrowej redukcji szumów SSNRIII (*Samsung Super Noise Reduction III*) pozwala wyeliminować szumy obrazu przy niewystarczającym oświetleniu, bez „efektu ducha" lub rozmycia, oraz umożliwia zmniejszenie rozmiarów plików zapisywanych na dyskach rejestratorów nawet do 70% w porównaniu z kamerami nie wyposażonymi w podobną technologię.

Nowy model ma także funkcję *Highlight Compensation*, która jest odpowiedzialna za rozpoznanie i neutralizację prześwietlonych obszarów obrazu. Dzięki niej można dostrzec uprzednio niezauważone szczegóły. W kamerze SCO-2080RH zastosowano również technologię SSDR (*Samsung Super Dynamic Range*), która automatycznie rozjaśnia zaciemnione obszary kadru, pozostawiając naświetlenie pozostałych stref na niezmienionym poziomie. Dzięki temu zaciemnione obszary stają się lepiej widoczne, co pozwala operatorowi dostrzec obiekty pozostające w cieniu.

Bezpośr. inf. David Solomons
DRS Marketing

AXIS Q1602/-E

kamery do nadzoru wizyjnego o bezkonkurencyjnej czułości na światło

Firma **Axis Communications** proponuje stacjonarną kamerę sieciową **AXIS Q1602/-E**, która wykorzystuje technologię Lightfinder. Dzięki rejestracji kolorowego obrazu nawet w warunkach słabego oświetlenia nowa kamera sprawdzi się zarówno w wewnętrznych, jak i zewnętrznych systemach nadzoru, umożliwiając skuteczną identyfikację postaci i obiektów.

Technologia Lightfinder sprawia, że kamera AXIS Q1602 tworzy materiał wizyjny przy bardzo słabym oświetleniu i „widzi" nawet w ciemności. Kamera pracuje zarówno w świetle dziennym, jak i w podczerwieni, wytwarzając obraz o rozdzielczości D1 (720×576).

Zaawansowana technologia Lightfinder jest szczególnie przydatna w systemach nadzoru wizyjnego instalowanych w lokalizacjach wymagających dokładnej obserwacji, takich jak place budowy, parkingi i systemy monitoringu miast i ich obrzeży. Konwencjonalne kamery pracujące w trybie dzień/noc reagują na spadek poziomu oświetlenia przełączaniem się w tryb monochromatyczny. Kamera AXIS Q1602 może wytwarzać kolorowy obraz nawet w warunkach bardzo słabego oświetlenia. Jej użycie jest doskonałym rozwiązaniem w sytuacjach, w których czynnik koloru decyduje o poprawności identyfikacji osób lub przedmiotów. Wykorzystanie technologii Lightfinder znacznie zwiększa szanse na rozpoznanie osób, pojazdów i zarejestrowanie incydentów. Ze względu na wyjątkowo wysoką czułość kamer na światło w wielu przypadkach nie ma potrzeby stosowania dodatkowych lamp emitujących światło podczerwone. Zmniejsza to koszty i stopień skomplikowania instalacji całego systemu nadzoru wizyjnego.

Wewnętrzna kamera AXIS Q1602 i przygotowana do montażu na zewnątrz kamera AXIS Q1602-E mogą przesyłać wiele indywidualnie konfigurowalnych strumieni wizyjnych skompresowanych metodami H.264 i Motion JPEG jednocześnie. Obydwie kamery mogą pracować w trybach dzień/noc i umożliwiają dwukierunkową transmisję dźwięku i są wyposażone w obiektyw o regulowanej ogniskowej z funkcją zdalnej regulacji ostrości. Kamera AXIS Q1602-E ma stopień szczelności IP66 i jest dostarczana razem z uchwytem ściennym oraz osłoną przeciwsłoneczną. Jej obudowa jest odporna na działanie pyłu, deszczu, śniegu i słońca. Urządzenie może pracować w ekstremalnych temperaturach od -40°C do 50°C.

Bezpośr. inf. Kamila Wierzbicka
Grayling Poland

Siemens i Bosch sponsorami projektów nowych polskich norm

Spółki **Siemens** i **Robert Bosch**, postanowiwszy przeznaczyć środki na opracowanie projektów polskich wersji dwóch norm europejskich z grupy norm dot. systemów alarmowych, stworzyły warunki umożliwiające swojej organizacji – Polskiej Izbie Systemów Alarmowych (**PISA**) – zawarcie z Polskim Komitetem Normalizacyjnym (**PKN**) kolejnych umów dotyczących opracowania projektów polskich norm.

Siemens Sp. z o.o. finansuje prace nad normą EN 50132-1:2010 *Systemy alarmowe – Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 1: Wymagania systemowe*, a **Robert Bosch Sp. z o.o.** nad normą EN 50131-2-6:2008 *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 2-6: Czujki stykowe rozwierne (magnetyczne)*.

W europejskiej normie **EN 50132-1:2010** określono minimalne wymagania dotyczące systemów dozorowych CCTV w zastosowaniach związanych z zabezpieczaniem oraz wyszczególniono minimalne wymagania eksploatacyjne, a także wymagania funkcjonalne (w formie wymagań użytkowych, do uzgodnienia pomiędzy klientem a dostawcą).

Norma **EN 50131-2-6:2008** dotyczy rozwiernych czujek stykowych (magnetycznych) wykorzystywanych jako część alarmowych systemów włamania i napadu (I&HAS) instalowanych w budynkach. Zawiera wymagania dla określonych stopni zabezpieczenia i czterech klas środowiskowych, obejmując zastosowania w przypadku lokalizacji wewnątrz pomieszczeń oraz na zewnątrz.

W listopadzie 2011 r. Polski Komitet Normalizacyjny opublikuje w języku polskim Specyfikację Techniczną PKN-CLC/TS 50131-7:2010 Systemy alarmowe – *Systemy sygnalizacji włamania i napadu – Część 7: Wytyczne stosowania*. Dokument normalizacyjny został opracowany przez PKN na podstawie umowy z Polską Izbą Systemów Alarmowych.

Wytyczne stosowania mają służyć pomocą przy projektowaniu, instalacji, obsłudze i konserwacji alarmowych systemów włamania i napadu (I&HAS). Są uporządkowane w kolejności logicznej, odpowiadającej czynnościom towarzyszącym projektowaniu i instalowaniu I&HAS. Każda procedura jest przedstawiona osobno w kolejnych wytycznych, jednak w praktyce można wykonywać niektóre procedury równocześnie z innymi. W *Załączniku K* w formie schematu opisane są główne procesy i dokumentacja objęte wytycznymi stosowania.

Bezpośr. inf. PISA

Wandaloodporna kamera sieciowa Samsung SNV-5010 została zaaprobowana do użytku w europejskim przemyśle kolejowym

Testy przeprowadzone przez dwie niezależne instytucje, w tym badania sprawdzające odporność na ekstremalne wibracje, zaowocowały wydaniem certyfikatów potwierdzających, iż wandaloodporna **sieciowa kamera kopułkowa Samsung SNV-5010** jest w stanie niezawodnie pracować w uciążliwych warunkach, jakie mogą występować w wagonach, na dworcach i w innych miejscach na kolei.

Niemiecki koncern TUV SUD przetestował kamery SNV-5010 pod kątem ich przydatności na stacjach kolejowych (pod katem zgodności z normą EN-50121), natomiast koncern SGS Korea Co Ltd., po przeprowadzeniu niezależnych badań, wydał certyfikat zgodności z normą EN-50155, potwierdzając tym samym, że model SNV-5010 doskonale poradzi sobie w rygorystycznych warunkach pracy w składach pociągów.

SNV-5010 dołącza do długiej listy profesjonalnych produktów firmy Samsung z zakresu zabezpieczeń, którym, po przetestowaniu, przyznano certyfikat zgodności z normą EN-50121.

Wandaloodporna 1.3-megapikselowa kamera kopułkowa Samsung SNV-5010 ma stopień szczelności IP66. Jej wymiary to zaledwie 100×115×42 mm. Została zaprojektowana z myślą o instalacji w miejscach o ograniczonej dostępności. Wykorzystuje ona technologię skanowania progresywnego w celu uzyskania ostrego, wysokiej jakości obrazu ruchomych obiektów. W standardzie kamera oferuje bezlicencyjną i bezpłatną inteligentną analizę obrazu (IVA) z optyczną barierą wirtualną i możliwością detekcji kierunku wejścia/wyjścia. Jest wyposażona także w funkcję detekcji pojawiania się/znikania obiektów. IVA powoduje też, że w razie prób zamaskowania obiektywu (na przykład zamalowania go farbą) lub w przypadku nieautoryzowanej zmiany pola widzenia kamery wywoływany jest alarm.

Bezpośr. inf. David Solomons
DRS Marketing

Firma S.P.S. Trading Sp. z o.o. zmieniła nazwę na SPS Electronics Sp. z o.o.

W drugiej połowie września bieżącego roku firma S.P.S. Trading Sp. z o.o. zmieniła nazwę na **SPS Electronics Sp. z o.o.** Decyzja Udziałowców i Zarządu spółki o przekształceniu obecnej nazwy to konsekwencja wnikliwej obserwacji dynamicznego rozwoju rynku systemów zabezpieczeń.

Protoplastą SPS Electronics Sp. z o.o. była firma Sanservice Sp. z o.o. dystrybutor elektroniki użytkowej i klimatyzacji marki SANYO. W 1997 r., w wyniku konsolidacji Sanservice Sp. z o.o. oraz firmy Sanpro Sp. z o.o., producenta telewizorów na licencji SANYO, firma Sanservice Sp. z o.o. została przekształcona w S.P.S. Trading Sp. z o.o. W 2011 r. potrzeba uwydatnienia profilu działalności firmy silnie powiązanej z obszarem elektronicznych systemów zabezpieczeń stała się inspiracją do wzmocnienia jej wizerunku pod nową nazwą SPS Electronics Sp. z o.o.

W SPS Electronics Sp. z o.o. znajdą Państwo bogate portfolio innowacyjnych i optymalnie dobranych produktów. Kompleksowość rozwiązań o wszechstronnych zastosowaniach i doradztwo techniczne na każdym etapie realizacji projektu to nasze atuty, dzięki którym pozostajemy Państwa wiarygodnym partnerem w biznesie.

Bezpośr. inf. SPS Electronics Sp. z o.o.

SPS electronics

Nowe rejestratory cyfrowe marki NOVUS

W ofercie handlowej firmy **AAT Holding** pojawiły się nowe rejestratory cyfrowe marki **NOVUS**. Seria E, ciesząca się dużym uznaniem instalatorów oraz klientów końcowych, została rozszerzona o nowe modele 4-, 8- i 16-kanałowe o nazwach, odpowiednio, **NDR-EA2104**, **NDR-EA2208** i **NDR-EA2416**.

Wśród wielu nowo dodanych funkcji są dwa niezależne wyjścia monitorowe z gniazdami BNC i VGA, dzięki którym można wyświetlać dwa niezależne, różnie podzielone obrazy. Na jednym z monitorów można odtwarzać obrazy zarejestrowane na dysku, a na innym obserwować na bieżąco obrazy z kamer, zastosowawszy dowolny podział ekranu.

Rejestratory wzbogacono również o funkcję wyświetlania materiałów reklamowych według zdefiniowanego harmonogramu. W przypadku nieprowadzenia obserwacji oba monitory mogą być wykorzystane do wyświetlania materiałów reklamowych. Ta funkcja jest szczególnie przydatna w przypadku obiektów publicznych, takich jak sklepy, biura etc.

W przypadku rozbudowanych systemów składających się z dwóch lub większej liczby rejestratorów istnieje możliwość połączenia ich przez sieć IP i wyświetlenia obrazów ze wszystkich kamer na monitorze VGA lub BNC podłączonym do jednego z rejestratorów. Oznacza to, że do połączenia sieciowego operator nie potrzebuje komputera PC z dedykowanym oprogramowaniem.

Bezpośr. inf. Patryk Gańko
AAT Holding

Pełny obraz sytuacji

Kamera IP **Dinion HD 1080p** z funkcją dzień/noc to najnowsza kamera HD firmy Bosch. Ta wysokiej jakości kamera ma najwyższe w swojej klasie parametry użytkowe. Wytwarza obraz w rozdzielczości Full HD, doskonale działa w warunkach słabego oświetlenia oraz zapewnia bardzo dobrą reprodukcję kolorów.

Dinion HD 1080p charakteryzuje się wysoką jakością obrazu także podczas monitorowania scen o zróżnicowanej kolorystyce i dużej dynamice. Termin 1080p odpowiada – zgodnie ze standardem HD – rozdzielczości równej dwóm megapikselom. Wszystkie komponenty biorące udział w powstawaniu obrazu – od obiektywu aż do cyfrowego przetwornika obrazu – gwarantują dużą ostrość całej obserwowanej sceny. Umożliwia to identyfikację twarzy, obiektów oraz informacji alfanumerycznych – także z dużej odległości.

Specjalnie dobrany przetwornik obrazowy zapewnia doskonałą detekcję i analizę obserwowanych obiektów. Obrazy mają wyjątkową wyrazistość umożliwiająca identyfikację szczegółów. Nawet w gorszych warunkach oświetleniowych można łatwo rozróżnić poszczególne odcienie kolorów.

Sytuacje alarmowe są wykrywane łatwo i niezawodnie. Zintegrowany i zoptymalizowany pod kątem rozdzielczości HD układ inteligentnej analizy obrazu (*Intelligent Video Analysis – IVA*) wyświetla na ekranie informację o każdej sytuacji alarmowej, wskutek czego operatorzy już nie przeoczą żadnych podejrzanych działań. IVA rejestruje istotne szczegóły scen, które można zapisać w celu późniejszej analizy za pomocą funkcji *Forensic Search*.

Kamera IP Dinion HD 1080p z funkcją dzień/noc wyróżnia się także obudową. Precyzyjnie skonstruowana kamera ma estetyczny i profesjonalny wygląd. Szeroki zakres temperatur roboczych umożliwia stosowanie jej w różnych warunkach klimatycznych.

Przyjazny dla użytkownika panel sterowania sprawia, że instalacja i konfiguracja kamery jest niezwykle prosta i szybka. Najlepszy w swojej klasie elektryczny napęd układu automatycznej regulacji ostrości ułatwia uzyskanie ostrego obrazu. Zastosowanie PoE oznacza, że kamera nie wymaga dodatkowego kabla zasilającego i jest energooszczędna.

Kamera IP Dinion HD 1080p z funkcją dzień/noc ma szeroki zakres zastosowań. Jest polecana zwłaszcza do monitorowania złożonych scen o zróżnicowanej kolorystyce lub scen rozgrywających się przy słabym oświetleniu. Można ją zastosować między innymi w monitoringu miejskim, na stadionach, lotniskach, w instytucjach finansowych oraz kasynach gier.

Bezpośr. inf. Bosch Security Systems

Samsung wprowadza dwa nowe, łatwe w obsłudze sieciowe rejestratory obrazu

Seria dwóch nowych rejestratorów sieciowych **Samsung** została opracowana tak, aby przypominały one w użyciu rejestratory DVR, ale jednocześnie miały wszelkie atuty systemów NVR.

W przeciwieństwie do większości rejestratorów sieciowych, które mogą być obsługiwane wyłącznie zdalnie, z wykorzystaniem dodatkowego komputera PC, dwa nowe modele mogą być konfigurowane również lokalnie, kontrolowane za pomocą myszy i obsługiwane w wyjątkowo łatwy sposób poprzez wielojęzyczny interfejs graficzny.

Zarówno czterokanałowy **SRN-470D**, jak i szesnastokanałowy **SRN-1670D** wykorzystują kompresję H.264, przez co umożliwiają lepsze wykorzystanie pasma sieciowego z jednoczesnym zachowaniem wysokiej jakości obrazu. Ponadto oferują opcję kompresji MPEG-4 lub MJPEG. Pasmo sieciowe dostępne dla procesu rejestracji jest równe 64 Mb/s co umożliwia jednoczesny zapis obrazów ze wszystkich podłączonych kamer, w czasie rzeczywistym, z rozdzielczością 704 x 480 lub zapis z rozdzielczością Full HD (1920×1080) obrazów z kamer IP wybranych z bogatej oferty firmy Samsung – megapikselowych kamer o rozdzielczości Full HD, megapikselowych kamer o rozdzielczości HD, kamer o rozdzielczości 4-CIF oraz kamer o rozdzielczości VGA.

Dodatkową zaletą modeli SRN-470D i SRN-1670D jest możliwość automatycznej detekcji i rejestracji wszystkich zainstalowanych kamer, zatem można skrócić proces instalacji.

Model SRN-470D jest przystosowany do współpracy z jednym dyskiem 2 TB SATA, natomiast SRN-1670D umożliwia podłączenie maksymalnie pięciu dysków SATA, więc można przechowywać nawet 10 TB danych. Obydwa modele mogą zapisywać dźwięk na wszystkich kanałach i mają wbudowany napęd DVD Winter, porty USB ułatwiające eksportowanie obrazu, a także wyjście HDMI o rozdzielczości 1080 pikseli, które umożliwia bezpośrednie podłączenie monitora LCD.

Pełna kompatybilność z nie wymagającym licencji i bezpłatnym oprogramowaniem CMS NET-I Viewer zapewnia użytkownikom dostęp do urządzeń NVR typu SRN-470D lub SRN-1670D z dowolnego miejsca na świecie poprzez komputer PC z dostępem do Internetu, dzięki czemu można utrzymać całodobowe połączenie z systemami bezpieczeństwa bez względu na ich lokalizację.

Bezpośr. inf. David Solomons
DRS Marketing

Produkty Bosch otrzymują certyfikat CERTALARM

Dwie czujki dymu oraz dźwiękowy system ostrzegawczy **Praesideo** firmy **Bosch** otrzymały znak jakości **CERTALARM**. Są one jednymi z pierwszych produktów, które otrzymały certyfikat ogólnoeuropejski. CERTALARM ma aprobatę Komisji Europejskiej, a jego celem jest harmonizacja certyfikacji w europejskiej branży systemów pożarowych oraz systemów zabezpieczeń.

Wśród produktów firmy Bosch, które noszą znak CERTALARM, znajduje się konwencjonalna optyczna czujka dymu **FCP-O 320**, adresowalna optyczna czujka dymu **FAP-O 420** oraz system **Praesideo 3.5**. Czujki dymu z sukcesem przeszły test zgodności z normą EN 54-7, natomiast system Praesideo – z normą EN 54-16. W teście potwierdzono także zgodność izolatorów zwarć optycznej czujki dymu FAP-O 420 z normą EN 54-17.

CERTALARM jest organizacją niedochodową, która opracowuje procedury testowe i certyfikacyjne dla systemów pożarowych i systemów bezpieczeństwa; celem tych działań jest osiągnięcie zunifikowanych metod badań tego typu systemów w całej Europie i wypromowanie jednolitego znaku jakości. Przyznanie znaku jakości następuje po przeprowadzeniu testów przez niezależne laboratoria, które sprawdzają zgodność produktu z normami europejskimi – normą EN 54 w przypadku elementów systemów sygnalizacji alarmów pożarowych oraz normą EN 50131 w przypadku elementów systemów sygnalizacji włamania i napadu. Schemat certyfikacyjny CERTALARM został przyjęty przez organizację European Cooperation for Accreditation (EA) jako „schemat branżowy".

Bezpośr. inf. Bosch Security Systems

Aktualizacja oprogramowania Samsung NET-i Ware

Najnowsza wersja oprogramowania rejestrującego **Net-i Ware** firmy **Samsung** zwiększa możliwości związane z nagrywaniem dzięki przepustowości 250 Mbps oraz zapewnia pasmo dostępne dla rejestracji obrazu z najnowszej generacji kamer megapikselowych HD marki Samsung.

Wersja 1.33 oprogramowania Net-i Ware umożliwia rejestrację w czasie rzeczywistym przez sieć IP i równoczesne nagrywanie i odtwarzanie doskonałych jakościowo obrazów z najnowszych kamer sieciowych Samsung Full HD w rozdzielczości od VGA do trzech megapikseli. W rzeczywistości Net-i Ware może przetwarzać i nagrywać strumienie z 64 1.3-megapikselowych kamer Samsung HD w czasie rzeczywistym, jeśli zostanie zastosowana platforma komputerowa o odpowiedniej wydajności.

Zarządzające rejestracją oprogramowanie NET-i Ware zostało zaprojektowane w celu ułatwienia administrowania systemem, zapewnienia pełnej kontroli, monitorowania i nagrywania obrazów wygenerowanych przez megapikselowe oraz standardowe sieciowe kamery Samsung iPOLiS, a także w celu umożliwienia nagrywania i odtwarzania obrazów poprzez sieć, z wykorzystaniem komputera jako stacji roboczej. Projektanci firmy Samsung wyposażyli oprogramowanie NET-i Ware w dodatkowe funkcje, aby zapewnić operatorom pełne wykorzystanie najnowszej technologii IP, m.in. w spersonalizowane konta użytkowników oraz wbudowaną przeglądarkę, dzięki czemu można zalogować się do systemu za

pośrednictwem dowolnego komputera w dowolnym miejscu na świecie.

Proces rejestracji urządzenia z oprogramowaniem NET-i Ware umożliwia operatorowi wyjątkowo proste dodanie, modyfikację oraz usunięcie nawet 64 urządzeń sieciowych, a także indywidualne skonfigurowanie każdego z nich do rejestracji w trybie prealarmowym i postalarmowym. Program wspiera następujące algorytmy kompresji: H.264, MPEG-4 oraz MJPEG. Obsługiwane są także liczne formaty kopii zapasowych, zarówno obrazu, jak i nagrań dźwięku, np. G.726, G.711, G.723 oraz PCM.

Bezpośr. inf. David Solomons
DRS Marketing

AXIS M1043-W i AXIS M1044-E

małe kamery bezprzewodowe umożliwiające lokalne przechowywanie nagrań

Firma **Axis Communications** wprowadziła na rynek małe kamery sieciowe AXIS M1043-W i AXIS M1044-W oferowane w atrakcyjnej cenie. Wyposażono je w funkcje lokalnego nagrywania obrazu i dźwięku, komunikacji bezprzewodowej i inteligentnego nadzoru wizyjnego. Kamery są przeznaczone do nadzoru małych firm, butików, restauracji, hoteli i mieszkań prywatnych.

Najnowsze modele kamer z serii AXIS M10 zapewniają doskonałą jakość obrazu wyświetlanego z prędkością 30 klatek na sekundę, z rozdzielczością SVGA (AXIS M1043-W) i HDTV 720p (AXIS M1044-W). Kamery są wyposażone w funkcje łączności bezprzewodowej zgodne ze standardem *WiFi Protected Setup*, który upraszcza proces ustawiania zabezpieczeń sieciowych. Obsługa bezprzewodowych standardów 802.11n i WPS gwarantuje łatwą konfigurację i wysoki poziom bezpieczeństwa.

Dzięki obsłudze kart pamięci micro-SDHC kamery mogą lokalnie przechowywać dane cyfrowe. Możliwe jest także zapisywanie danych w zasobach sieciowych, takich jak pamięci NAS (*Network-Attached Storage*). Opcja lokalnego przechowywania danych umożliwia budowę tanich i niezawodnych systemów rejestrujących obrazy z kamer. Ponadto kamery **AXIS M1043-W** i **AXIS M1044-W** są wyposażone w pasywny czujnik podczerwieni (PIR), wykrywający intruzów nawet w zupełnej ciemności, jak również oświetlacze LED pracujące w świetle białym, automatycznie oświetlające scenę po wykryciu ruchu lub na życzenie użytkownika. Kamery zapewniają dwukierunkową transmisję dźwięku. Mają zintegrowany mikrofon i głośnik, dzięki czemu użytkownicy mogą samodzielnie prowadzić nasłuch obserwowanego obszaru oraz komunikować się z gośćmi lub intruzami przebywającymi w pobliżu kamer. Kamery wyposażono też w porty I/O (1 wejście, 1 wyjście) służące do podłączenia takich urządzeń jak czujniki i przekaźniki zewnętrzne, które umożliwiają włączanie oświetlenia lub otwieranie i zamykanie drzwi.

Bezpośr. inf. Kamila Wierzbicka
Grayling Poland

Punkty kamerowe PTZ Videotec są zgodne z wymaganiami ONVIF

Firma **Videotec** oznajmia, że sieciowe punkty kamerowe **ULISSE**, **ULISSE COMPACT** i **MAXIMUS** spełniają wymagania wynikające ze specyfikacji **ONVIF**, dzięki czemu mogą być łatwo zintegrowane ze wszystkimi urządzeniami kompatybilnymi z ONVIF. Zwiększa to elastyczność systemów dozorowych oraz stwarza możliwość ich wieloletniego funkcjonowania.

Firma Videotec partycypuje w pracach ONVIF i PSIA. Ma głęboką wiarę w sens tworzenia protokołów prowadzących do standaryzacji i integracji sieciowych urządzeń zabezpieczających. To wszystko przynosi korzyści użytkownikom końcowym, gdyż upraszcza sterowanie i zarządzanie systemami dozorowymi, umożliwia swobodniejszy wybór urządzeń oraz wydłuża okres ich eksploatacji. Firma podjęła współpracę z wieloma producentami, takimi jak na przykład **Milestone**, w celu ujednolicenia protokołów komunikacyjnych w produktach pracujących w sieci IP, takich jak punkty kamerowe ULISSE PTZ, urządzenia ALBERT, które analizują sygnały wizyjne, czy klawiatury sterujące DCZ.

Wszystkie produkowane przez firmę Videotec sieciowe punkty kamerowe z funkcjami PTZ mogą być łatwo zintegrowane z cyfrowymi systemami dozorowymi i zapewniają możliwość sterowania funkcjami PTZ za pośrednictwem sieci IP. Wszystkie sygnały wizyjne i sterujące są kodowane i przesyłane poprzez sieć. Oglądane na żywo obrazy są wydajnie skompresowane w standardzie MPEG-4. Maksymalna liczba klatek na sekundę wynosi 25, zaś obrazy mają rozdzielczość Full D1.

Dzięki nieustannemu wprowadzaniu zmian technologicznych punkty kamerowe firmy Videotec odznaczają się bardzo dobrymi parametrami i konkurencyjnymi cenami. W klasie urządzeń przeznaczonych do pracy w warunkach zewnętrznych stanowią one unikatowe rozwiązania, niedostępne u innych producentów.

Bezpośr. inf. Martina Panighel
VIDEOTEC SpA
Tłumaczenie: Redakcja

AXIS P3367-V/-VE

stacjonarne kamery kopułkowe z matrycą 5 Mpx i mechanizmem precyzyjnego sterowania przysłoną

Firma **Axis Communications** proponuje stałopozycyjne sieciowe kamery kopułkowe z matrycą o rozdzielczości 5 megapikseli i mechanizmem precyzyjnego sterowaniem przysłoną. Zarówno wewnętrzna kamera sieciowa **AXIS P3367-V**, jak i dostosowany do instalacji zewnętrznych model **AXIS P3367-VE** to urządzenia odporne na akty wandalizmu. Oferując obraz o wysokiej szczegółowości, świetnie sprawdzą się w systemach nadzoru na dużych obszarach, takich jak terminale lotnicze, dworce kolejowe, parkingi, korytarze szkół i kampusy uczelniane.

Stałopozycyjne kamery kopułkowe przystosowane do pracy w trybie dzień/noc dostarczają materiał wizyjny o rozdzielczości 5 megapikseli z prędkością 12 klatek na sekundę lub obraz o rozdzielczości HD 1080p z prędkością 30 klatek na sekundę. Dzięki kompresji H.264 i opcji przesyłania wielu strumieni wizyjnych jednocześnie można zwiększyć efektywność wykorzystania pasma sieciowego i pamięci masowej. Ponadto kamery AXIS P3367-V/VE realizują zaawansowane, zdalne cyfrowe funkcje PTZ, które umożliwiają między innymi powiększanie wybranych fragmentów obrazu, dostosowywanie kąta widzenia kamer i regulację ostrości poprzez sieć, eliminując potrzebę ręcznej regulacji kamer. Kamery mogą być zasilane metodą PoE – do ich zasilania i transmisji danych potrzebny jest tylko jeden kabel.

Kamery będą dostępne w dwóch wersjach – AXIS P3367-V, przeznaczonej do montażu w pomieszczeniach, oraz AXIS P3367-VE, dostosowanej do instalacji na zewnątrz dzięki spełnieniu norm IK10, IP66 i NEMA 4X.

Bezpośr. inf. Kamila Wierzbicka
Grayling Poland

AXIS P5544 daje obraz panoramiczny za jednym kliknięciem

Axis Communications proponuje nową sieciową kamerę kopułkową **AXIS P5544** z funkcją PTZ, wyposażoną w dwa różne obiektywy umożliwiające użytkownikom uzyskanie panoramicznego obrazu w obrębie kąta widzenia 360° oraz odrębnego obrazu z mechanicznie obracanej i pochylanej części kamery wyposażonej w obiektyw zmiennoogniskowy. Praca w rozdzielczości HD i 18-krotny zoom optyczny zapewniają dobrą rozróżnialność szczegółów i wysoką jakość materiału wizyjnego. Kamera jest przystosowana do instalacji w pomieszczeniach i sprawdza się w systemach nadzoru instalowanych na lotniskach, dworcach kolejowych, w centrach logistycznych i galeriach handlowych oraz we wszystkich obiektach, w których wymagany jest nadzór dużych obszarów oraz ostry obraz umożliwiający identyfikację postaci i ocenę zdarzeń.

Kamera AXIS P5544 wykorzystuje unikatową technologię Panopsis firmy Axis, dzięki której może pracować w trybie panoramicznym 360° z obiektywem szerokokątnym oraz pełnić funkcję szybkoobrotowej kamery kopułkowej z funkcją ciągłego obrotu, możliwością pochylenia do 180° oraz 18-krotnym zoomem optycznym, stosującej rozdzielczość HDTV 720p. Specjalnie opracowany interfejs użytkownika, zawierający funkcję szkła powiększającego i umożliwiający dokonywanie ustawień kamery, ułatwia monitorowanie dowolnego obszaru w trybie panoramicznym 360°. W trybie standardowym kamera może zostać natychmiast ustawiona w pozycji pozwalającej na obserwację wybranego fragmentu obszaru przy rozdzielczości HDTV i wytwarza obraz o proporcjach 16:9.

Kamera może pracować w trybie dziennym i nocnym, co gwarantuje wysoką jakość obrazu nawet przy słabym oświetleniu. Szeroki zakres dynamiki zapewnia lepszą widoczność obiektów znajdujących się zarówno w zacienionych, jak i oświetlonych obszarach sceny. Kamera AXIS P5544 umożliwia dwukierunkową transmisję dźwięku. Ma także

funkcję detekcji akustycznej, dzięki której alarm może zostać uruchomiony np. na skutek budzących wątpliwości, podejrzanych dźwięków. Do kamery można podłączyć urządzenia zewnętrzne, takie jak czujniki i przekaźniki, na przykład w celu automatycznego włączenia oświetlenia lub zablokowania drzwi. AXIS P5544 współpracuje z *AXIS Camera Application Platform*, która umożliwia instalację aplikacji do analizy obrazu, opracowanych przez partnerów firmy Axis. Kamera ma wbudowane gniazdo kart pamięci SD/SDHC, dzięki czemu nagrania można przechowywać lokalnie.

Prosta w montażu obudowa kopułkowa PTZ to konstrukcja o stopniu szczelności IP51, zapewniająca ochronę przed pyłem i kapiącą wodą. Obraz można rejestrować nawet po włączeniu systemu zraszaczy. Kamera jest zasilana jest przez sieć Ethernet (standard IEEE 802.3at), co znacznie upraszcza instalację dzięki zastosowaniu jednego standardowego kabla sieciowego do zasilania, przesyłania obrazu i sterowania mechanizmem PTZ.

Bezpośr. inf. Kamila Wierzbicka
Grayling Poland

6 edycja konkursu

KAMERA NR 1 ROKU 2012

Izba **T**echnicznej **O**chrony **M**ienia

Zaprasza wszystkich producentów i importerów do nadsyłania swoich nominacji do konkursu - Kamera Roku 2012.Dla przypomnienia, w poprzednich edycjach tytuł ten przypadł następującym firmom: Techwin (2007r.), Bosch (2008r.), Siemens (2009r.), Mintron (2010r.), Ganz (2011r.).

Warto nadmienić, że w pięciu dotychczasowych edycjach konkursu, ten prestiżowy tytuł - Kamery Roku, tylko jeden raz przypadł kamerze IP(Ganz Pixel**P**ro).

Warunkiem udziału w konkursie jest spełnienie następujących wymogów:

- proponowana kamera weszła do dystrybucji na polski rynek po 30.01.2011
- dostarczenie typowanej kamery wraz z kartą katalogową do 28.12.2011r na adres: I.T.O.M. ul. Piękna 25, 85-303 Bydgoszcz
- wniesienie opłaty za test porównawczy nadesłanej kamery na konto organizatora konkursu - I.T.O.M. (szczegóły pod tel. 52 3254010)

Wyniki 6 edycji konkursu zostaną ogłoszone na łamach czasopism branżowych wraz ze szczegółową prezentacją KAMERY NR 1 ROKU 2012.

STESKAL korzysta z systemu kontroli dostępu **CEM AC 2000 Lite**

System kontroli dostępu **CEM AC 2000 Lite** został wdrożony w Zakładzie Usług Produkcyjnych Piekarnia-Ciastkarnia STESKAL, który oferuje wyroby piekarnicze i cukiernicze i specjalizuje się w usługach gastronomicznych oraz sprzedaży hurtowej i detalicznej. System został zainstalowany przez firmę **AGIS Fire & Security** – autoryzowanego i wyłącznego dostawcę rozwiązań marki CEM w Polsce.

Głównym elementem systemu, w którym wykorzystano najnowocześniejsze rozwiązania, takie jak m.in. biometryczne czytniki linii papilarnych, jest AC 2000 Lite Controller. Jego funkcje pozwalają na obsługę i sterowanie pozostałymi elementami systemu z jednego miejsca. Umożliwia to m.in. generowanie raportów dotyczących ruchu gości w obiekcie czy nadawanie lub anulowanie uprawnień do poruszania się w określonych strefach – wszystkie polecenia wprowadzane są przez zarządcę w jednym miejscu, bez konieczności wprowadzania modyfikacji dotyczących każdego z zabezpieczonych przejść oddzielnie.

Dzięki zastosowaniu nowoczesnej technologii IP w systemie kontroli dostępu CEM AC 2000 Lite czytniki linii papilarnych i kontrolery systemu zostały przyłączone poprzez sieć Ethernet. Takie rozwiązanie zagwarantowało szybką instalację i umożliwia łatwą i szybką rozbudowę systemu w przyszłości.

Zaawansowane technologicznie rozwiązanie jest proste w obsłudze, m.in. dzięki udostępnionej przez dostawcę rozbudowanej polskiej wersji językowej oprogramowania przeznaczonego do zarządzania systemem kontroli dostępu AC2000.

W strefach wymagających ochrony zastosowano czytniki biometryczne sterowane za pomocą inteligentnych kontrolerów IP eDCM300. Dzięki temu inwestor może być spokojny nie tylko o zarządzanie ruchem osób w obiekcie, ale także o niezawodność systemu kontroli dostępu w przypadku awarii sieci – eDCM300 ma wbudowaną bazę danych użytkowników i w przypadku awarii sieci i braku komunikacji z serwerem głównym system kontroli dostępu nadal jest sprawny.

Kontroler AC2000 Lite umożliwia także integrację systemu kontroli dostępu CEM AC 2000 Lite z innymi rozwiązaniami w zakresie bezpieczeństwa (np. z systemem nadzoru wizyjnego, z systemem sygnalizacji włamania i napadu).

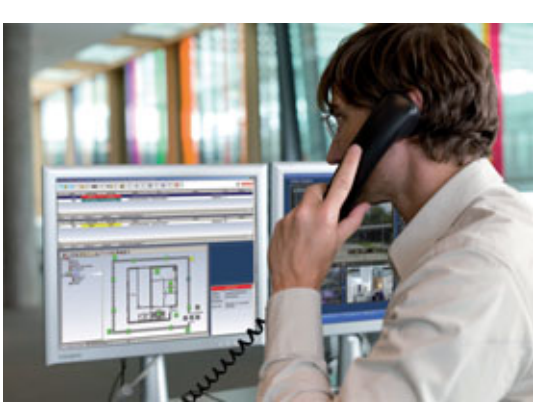
Bezpośr. inf. AGIS Fire & Security

Bosch przedstawia nową wersję systemu BIS

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

Rozszerzone funkcje wizyjne

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



Ulepszony interfejs użytkownika

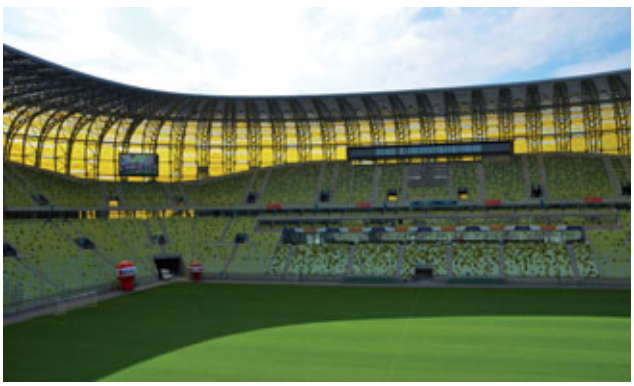
Dzięki wizualnemu „odświeżeniu" produktu obsługa jest szybsza i bardziej intuicyjna. Ponadto użytkownik może teraz korzystać z trzech skrzynek odbiorczych służących do odbioru komunikatów alarmowych. Komunikaty mogą być automatycznie przesyłane do jednej z tych skrzynek, w zależności od stopnia ważności, lub ręcznie przenoszone przez operatora metodą „przeciągnij i upuść", co znacznie przyspiesza obsługę. Skrzynki odbiorcze są konfigurowalne. Można określać pojemność skrzynek. Pojawiają się one na ekranie jedynie w przypadku nadejścia komunikatu o zdarzeniu.

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

Bezpośr. inf. Bosch Security Systems

Systemy sygnalizacji pożarowej Schrack Seconet na polskich stadionach

W związku z przygotowaniami do EURO 2012 budowane lub modernizowane są obiekty sportowe, w tym stadiony. W ostatnich tygodniach oficjalne otwarcia odbyły się w Gdańsku i we Wrocławiu. Oba obiekty zostały wyposażone w wysokiej klasy systemy sygnalizacji pożarowej Schrack Seconet.



We wrześniu 2011 r. **Schrack Seconet Polska** dodała do swojej listy referencyjnej kolejny obiekt sportowy – **stadion PGE Arena w Gdańsku**. Ten niezwykle nowoczesny stadion o całkowitej powierzchni użytkowej 36 tys. m^2 może pomieścić ponad 42 tys. widzów. Obiekt został zaprojektowany w taki sposób, aby pełnić rolę nie tylko bezpiecznego i komfortowego miejsca imprez sportowych – na jego terenie będzie można organizować między innymi zjazdy, konferencje i spotkania biznesowe. W projekcie uwzględniono nowoczesne sale konferencyjne, prestiżowe gabinety oraz 40 lóż dla VIP-ów.

Obiekt został wyposażony w najnowocześniejsze systemy bezpieczeństwa, między innymi w system sygnalizacji pożarowej Schrack Seconet. Na stadionie znajduje się 1,8 tys. inteligentnych multisensorowych czujek CUBUS MTD 533X, wykrywających wszystkie pożary testowe (TF1–TF9). Co więcej, mogą one być zastosowane jako czujki dymu, ciepła lub jako czujki dualne dymu/ciepła, a dzięki technice interaktywnego działania CUBUS Nivellierung mogą dostosowywać swoją czułość do zmieniających się warunków otoczenia. System składa się z sześciu modułowych central sygnalizacji pożarowej Integral IP MXF, których architektura została oparta na idei stuprocentowej redundancji sprzętowej i programowej, a dzięki zastosowaniu kart pamięci SD każda centrala ma zdolność zapamiętania do 65 tys. zdarzeń.

Kolejnym obiektem, który w ostatnich dniach znalazł się na liście referencyjnej Schrack Seconet Polska, jest **Stadion Miejski we Wrocławiu**. Pierwszy oficjalny mecz zostanie rozegrany we wrocławskim obiekcie pod koniec października br. Stadion we Wrocławiu został zaprojektowany tak, by zapewnić odpowiednie warunki do organizacji różnego typu najwyższej rangi wydarzeń sportowych, kulturalnych oraz rozrywkowych. Całkowita kubatura stadionu to ok. 489 tys. m^3, a trybuny zostały wyposażone w prawie 43 tys. miejsc siedzących. Obiekt wyposażono również w 2130 miejsc dla VIP-ów. Nad bezpieczeństwem widzów oraz całego obiektu czuwają nowoczesne systemy sygnalizacji pożarowej i sterowania gaszeniem firmy Schrack Seconet. Stadion został wyposażony w elementy peryferyjne wykorzystujące najnowszą technologię pętlową X-LINE, m.in. w prawie 4 tys. interaktywnych multisensorowych czujek CUBUS MTD 533X. Dla ułatwienia zarządzania bezpieczeństwem pożarowym w obiekcie zastosowano sieć SecoNET, która zintegrowała na poziomie cyfrowym system sygnalizacji pożarowej, składający się z sześciu central Integral IP MXF, oraz jeden z największych w Polsce systemów sterowania gaszeniem, składający się z czterech central Integral IP MXE, który steruje 32 strefami gaszenia.

Bezpośr. inf. Schrack Seconet Polska

Warsztaty Axisa – podsumowanie

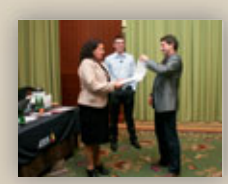
Dnia 16 listopada w Hotelu Hayatt Regency w Warszawie odbyło się spotkanie pod hasłem „**Nadzór wizyjny w trudnych warunkach oświetleniowych z Axis Communications**", zorganizowane przez firmę Axis, na które zaproszeni zostali przedstawiciele firm projektowych, instalacyjnych, dystrybucyjnych, a także prasy branżowej. W pierwszej części tego spotkania **Agata Majkucińska** omówiła asortyment produktów firmy Axis, kładąc szczególny nacisk na innowacyjność niektórych rozwiązań. Asystował jej **Daniel Lesisz**, który uzupełniał prelekcję szczegółowymi informacjami technicznymi, odpowiadał na pytania publiczności i demonstrował działanie wybranych urządzeń wizyjnych firmy Axis. Na spotkaniu była obecna **Edyta Tomczak** z centrali w Lund w Szwecji.

Największą atrakcją tej części spotkania była prezentacja odznaczającej się bardzo dużą czułością nowej kamery sieciowej firmy Axis. Po zasłonięciu okien okazało się, że na sali nadal jest zbyt widno i trzeba zastosować środki pomocnicze w postaci tekturowego kartonu, w którym umieszczono kamerę, kolorową maskotkę stanowiąca obserwowany obiekt i najważniejszą rzecz – czuły luksomierz, którego wskazania można było obserwować na ekranie monitora. Ten prosty eksperyment dowiódł, że prezentowana kamera doskonale odwzorowuje barwy, nawet przy oświetleniu spadającym poniżej 0,1 luksa. Udowodnił także, że prezenterzy potrafią znakomicie prowadzić tego typu spotkania, gdyż wszystko przebiegło niezwykle sprawnie.

Po przerwie wystąpił **Dmitry Moroz**, przedstawiciel wschodnioeuropejskiego oddziału firmy **AXXONSOFT**, który zaprezentował publiczności osiągnięcia tej firmy w dziedzinie oprogramowania zarządzającego dużymi systemami monitoringu wizyjnego. Wszystkim zaimponowały liczby – 180 tysięcy kamer w samej Moskwie, obsługiwanych przez 10 tysięcy serwerów, tworzących całkowicie automatyczny system monitoringu, który w powiązaniu z gigantycznymi bazami danych jest zdolny do nieprzerwanego patrolowania ulic tego miasta i do wykrywania potencjalnych zagrożeń, poszukiwania określonych samochodów na podstawie ich cech charakterystycznych i numerów z tablic rejestracyjnych czy poszukiwania osób na podstawie analizy wyglądu ich twarzy. Prezenter nie ukrywał, że nawet tak rozbudowany system nie jest w stanie samodzielnie zapewnić bezpieczeństwa mieszkańcom tak ogromnego obszaru, jakim jest Moskwa, jednak jest w stanie znacznie ułatwić pracę policji, służb ratunkowych i porządkowych, dostarczając danych dotyczących ruchu ulicznego, lokalizując groźne incydenty, wypadki etc. Na przykładzie funkcji automatycznego rozpoznawania poszukiwanych osób prelegent wyjaśnił, że system dostarcza głównie danych statystycznych, to znaczy określa częstotliwość pojawiania się danej osoby na jakimś obszarze, stopień podobieństwa tej osoby do wzorca pobranego z bazy danych oraz szacunkową stopę błędów podczas tych obserwacji.

Całość imprezy umiliły przerwy na kawę i znakomity obiad, podczas którego nie cichły dyskusje na temat zaprezentowanych nowości. Spotkanie należy uznać za bardzo udane.

Andrzej Walczyk
Redakcja



Forum Monitoringu Polskiego – podsumowanie

Kolejne **Forum Monitoringu Polskiego**, które odbyło się tradycyjnie w ośrodku Geovita w Jadwisinie pod Warszawą, cieszyło się niespotykaną dotąd popularnością i zgromadziło około dziewięćdziesięciu uczestników z całej Polski. Najwięcej było reprezentantów firm, których działalność jest bezpośrednio związana monitoringiem, ale nie zabrakło również bankowców, przedstawicieli ZPR (zainteresowanych monitoringiem kasyn gry), a także dystrybutorów prezentujących swoje oferty sprzętowe. Tematyka referatów była zróżnicowana i dotyczyła normalizacji, procedur ochrony obiektów, oprogramowania, sprzętu, a także monitoringu stadionów.

Z pozoru nudne zagadnienia normatywne wywoływały liczne dyskusje, zarówno podczas prelekcji, jak i później, w kuluarach, co świadczyło o dążności firm zajmujących się świadczeniem usług ochrony do spełniania wymogów wynikających z obowiązujących rozporządzeń oraz do ścisłego przestrzegania prawa regulującego monitoring.

Nieuzasadnione byłoby przytaczanie programu forum i tytułów kolejnych referatów. Wystarczy wspomnieć, że dyskusja, jaka rozwijała się w każdej przerwie, była na tyle gorąca, że powodowała istotne opóźnienia. Dyskutanci mieli równie sprecyzowane poglądy jak prelegenci i zaciekle ich bronili, dlatego konkluzje w toku spotkania bywały zaskakujące. Na przykład przetwarzanie danych w tak zwanej chmurze oraz tworzenie bardzo zaawansowanych technologicznie wirtualnych stacji monitoringu znalazło zarówno zagorzałych zwolenników, jak i oponentów. W tym kontekście na pierwszy plan wysuwały się zagadnienia dotyczące masowości usług związanych z monitoringiem obiektów oraz obsługi bardzo dużej liczby abonentów przez pojedyncze agencje ochrony.

Spotkanie uświetnił wieczorny bankiet połączony z udanymi występami iluzjonisty, w których partycypowali wybrani uczestnicy forum. Większą część sztuczek prezentowanych na estradzie widownia przyjmowała gromkimi okrzykami: „Wiemy jak to działa". „Ja też wiem" – odpowiadał iluzjonista i zabawa trwała dalej. Niech ten dialog stanowi podsumowanie naszego forum. Przecież naprawdę wiemy, jak to działa. Oczywiście monitoring nie jest iluzją, wręcz przeciwnie.

Andrzej Walczyk
Redakcja

Firma C&C Partners Telecom zaprezentowała sprzęt oraz oprogramowanie firmy SIQURA

SIQURA®
SURVEILLANCE SOLUTIONS

Na spotkaniu, które odbyło się 28 września w Warszawie, firma **C&C Partners Telecom** zaprezentowała sprzęt oraz oprogramowanie produkowane przez firmę **SIQURA** (dawniej Optelecom NKF) opierającą swoje działania w trzech dziedzinach – monitoringu ruchu drogowego, transportu publicznego i infrastruktury krytycznej – na trzydziestopięcioletnim doświadczeniu. Obecnie SIQURA zatrudnia stu sześćdziesięciu pracowników, z czego stu stanowi personel inżynieryjno-techniczny. Dzięki takiej strukturze zatrudnienia firma SIQURA w krótkim czasie opracowała urządzenia oraz oprogramowanie pozwalające na automatyzację procesów zarządzania bezpieczeństwem transportu, infrastruktury krytycznej, a także wielkich aglomeracji miejskich.

Wszystkie urządzenia oferowane przez firmę SIQURA są produkowane na terenie Holandii, co stanowi pewien odwrót od generalnej tendencji do ograniczania kosztów produkcji przez przeniesienie jej w odległe zakątki świata. W tym przypadku konieczność utrzymania jakości urządzeń na odpowiednim poziomie była powodem umieszczenia zakładu produkcyjnego na terenie Europy.

Podstawowym składnikiem systemów oferowanych przez firmę SIQURA są kamery telewizyjne o specjalnej konstrukcji, przystosowane do pracy w trudnych warunkach oświetleniowych, jakie często panują na drogach publicznych oraz na terenach obiektów przemysłowych. Obrazy wytwarzane przez te kamery są głównym, aczkolwiek nie jedynym źródłem danych, które umożliwiają ocenę sytuacji na chronionym obszarze i automatyczne podejmowanie decyzji dotyczących akcji ratowniczych czy zapobiegawczych, dlatego jakość tych obrazów ma decydujące znaczenie dla działania całego systemu.

By sprostać wysokim wymaganiom, konstruktorzy kamer produkowanych przez firmę SIQURA zdecydowali się na wykorzystanie przetworników obrazowych typu PIXIM, które odznaczają się bardzo wysoką dynamiką, praktycznie nieosiągalną dla przetworników innego rodzaju. W praktyce oznacza to, że kamery SIQURA mogą wytwarzać wyraźne obrazy telewizyjne podczas obserwacji scen odznaczających się bardzo wysokim kontrastem, z jakim mamy do czynienia w transporcie drogowym oraz w przemyśle.

Ponadto kamery SIQURA zostały wyposażone w interfejsy optyczne, które umożliwiają ich bezpośrednią współpracę z kablami światłowodowymi, co pozwala na rozmieszczanie kamer w znacznych odległościach od siebie i od jednostki centralnej systemu bez konieczności zastosowania dodatkowych urządzeń transkodujących.

Kamery SIQURA są wyposażone w procesory sygnałowe wykrywające potencjalnie niebezpieczne sytuacje już na poziomie kamery, bez konieczności angażowania w to serwerów stanowiących jednostkę centralną systemu. Taka architektura pozwala na bardzo szybkie podejmowanie właściwych decyzji w sytuacjach krytycznych, wymagających natychmiastowej reakcji.

Kolejnymi składnikami systemów oferowanych przez firmę SIQURA są kodery, przełączniki sieciowe i konwertery umożliwiające tworzenie rozległych sieci teleinformatycznych na bazie różnych nośników, na przykład takich jak kable koncentryczne, które pozostały po demontażu starych systemów CCTV. Cechą wspólną tych urządzeń jest ekstremalnie szeroki zakres temperatur pracy, dzięki któremu można instalować je w dowolnych lokalizacjach – także takich, które są narażone na oddziaływanie najsurowszych czynników klimatycznych.

Ostatnim, a zarazem najważniejszym składnikiem systemów oferowanych przez firmę SIQURA jest oprogramowanie systemowe, które przetwarza dane pochodzące z kamer i innych czujników. Przykładowo – systemy automatycznej analizy ruchu drogowego wykorzystujące oprogramowanie SIQURA realizują następujące funkcje:

- wykrywanie pojazdów pozostających przez dłuższy czas bez ruchu, na przykład na skutek kolizji,
- wykrywanie pojazdów jadących pod prąd lub niewłaściwym pasem drogi,
- wykrywanie pieszych na obszarach przeznaczonych wyłącznie dla ruchu kołowego,
- wykrywanie porzuconych przedmiotów lub paczek zalegających na drodze, stwarzających zagrożenie dla innych pojazdów,
- wykrywanie dymu (opcja wykorzystywana jedynie w tunelach),
- zliczanie pojazdów, obliczanie prędkości ruchu.

Należy zaznaczyć, że systemy SIQURA służą jedynie bezpieczeństwu ruchu drogowego, a nie wykrywaniu i ściganiu wykroczeń drogowych, dlatego nie dokonują one identyfikacji pojazdów, tylko stwierdzają ich obecność lub analizują parametry ich ruchu.

Na podobnej zasadzie można wykorzystywać systemy SIQURA do zarządzania bezpieczeństwem na terenie takich obiektów jak:

- elektrownie,
- zakłady przemysłowe,
- rafinerie i przepompownie paliw,
- porty (i w infrastrukturze portowej),
- krytyczne obszary zabudowy miejskiej.

Systemy SIQURA są zawsze dostosowywane do charakteru i funkcji chronionych obszarów, czyli są projektowane na zamówienie, jednak zawsze wykorzystuje się inteligentną platformę CCTV, która jest najistotniejszą częścią każdego z tych systemów.

Uczestnicy spotkania zorganizowanego przez firmę C&C Partners Telecom mogli zapoznać się z kamerami i innymi urządzeniami firmy SIQURA. W spotkaniu wzięli udział przedstawiciele firm zainteresowanych zagadnieniami związanymi z bezpieczeństwem w ruchu drogowym i w przemyśle, a także przedstawiciele prasy.

Andrzej Walczyk
Redakcja

SIQURA

Rozwiązania
Budynkowe - zabe

Rozwiązania
Telekomunikacyjne

C&C solution partner
www.ccpartners.pl

C&C solution partner

Rozwiązania
Budynkowe - teleinformatyka

C&C solution partner

www.ccpart

16 września br. w warszawskim teatrze „Rampa" miała miejsce jubileuszowa uroczystość związana z 30-leciem działalności **Zakładu Elektroniki COMPAS**, którego właścicielami są **Anna i Jacek Szewczykowie**. Na imprezę przybyło wielu gości z całej Polski.

Część oficjalną rozpoczął gospodarz wieczoru Jacek Szewczyk, który bardzo serdecznie przywitał wszystkich przybyłych gości, a następnie przedstawił pokrótce historię firmy oraz specyfikę jej działalności od momentu jej powstania w 1981 roku (zarejestrowana pod nazwą AS, z siedzibą w bloku na warszawskiej Woli) poprzez okres transformacji gospodarki aż po dzień dzisiejszy. Jak się dowiedzieliśmy, Jacek Szewczyk miał pierwszy kontakt z branżą zabezpieczeń już w technikum elektronicznym, gdzie poznał Włodzimierza Lecha, z którym kilka lat później zakładał systemy alarmowe w domach jednorodzinnych i mieszkaniach. Ogłoszenia o swojej działalności zamieszczali w „Życiu Warszawy" w rubryce „Profesjonalne systemy alarmowe" i niecierpliwie czekali na zlecenia. Wychowywali małe wówczas dzieci i... marzyli o własnym fiacie 126p, popularnie zwanym maluchem.

Następnie (w latach 1985–1986), wraz z Wojciechem Kowalskim – wspólnikiem, w wynajętym garażu w Babicach Starych k/Warszawy rozpoczęli produkcję urządzeń do systemów alarmowych.

W roku 1989 państwo Szewczykowie spełnili swoje marzenie i przenieśli się do nowej, pięknej siedziby w Jabłonnie k/Warszawy, w której obecnie pracuje 14 osób, w tym również ich córka i syn, czyli kolejne pokolenie rodu Szewczyków. Jest to spełnienie ich kolejnego marzenia o tym, by przedsiębiorstwo pozostało w rękach rodziny.

W Jabłonnie powstał pierwszy polski system kontroli dostępu COMPAS2002, następnie COMPAS2026LAN, a obecnie trwają prace nad najnowszym produktem – systemem COMPAS2026LAN drugiej generacji. Oprócz własnych systemów firma integruje skomplikowane systemy nadzoru obiektów bazujące między innymi na amerykańskim systemie firmy Andover Controls. ZE COMPAS na stałe współpracuje z EPS LEVEL oraz Schneider Electric Polska.

Dzięki dwutorowości działań – produkcji i instalacji – COMPAS dzielnie opiera się wszelkim zawirowaniom politycznym i kryzysom gospodarczym. Ciągłość działania firmy to w znacznej mierze zasługa ciężkiej pracy jej szefa, który posiada wyjątkową, jak na nasze warunki, umiejętność zatrudniania najlepszych fachowców, a potem utrzymania ich w firmie. Tajemnicą poliszynela są również jego wzorowe, serdeczne kontakty z ludźmi z branży. Zawsze jest chętny do pomocy, dlatego i jemu nie odmawia się jej. Ludzie z branży znają jego niebanalne poczucie humoru, otwartość i nieustającą gotowość do zabawy. Od lat krąży (prawdziwa) anegdota o tym, jak to Jacek Szewczyk rozgrywał mecze tenisa stołowego z Henrykiem Brockim o... wysokość upustu.

Jubileusz 30-lecia działalności firmy COMPAS

Jak wspomniał Jacek Szewczyk, firma COMPAS zdobyła już wszystkie możliwe wyróżnienia, w tym: Złote Odznaki KIG, NOT, odznaczenia państwowe, puchary Targów Poznańskich, główne nagrody w Konkursie Mistrz Techniki Alarmowej, złote odznaki organizacji społecznych (AK) oraz zawodowych (POLALARM), Polskiej Izby Ochrony i wiele innych, co jest potwierdzeniem silnej pozycji firmy na polskim rynku oraz wyrazem uznania dla jej dokonań.

Na imprezie wręczono statuetki i dyplomy „Przyjaciel firmy COMPAS" wszystkim tym, których los w jakimś momencie życia zetknął z gospodarzami wieczoru. Gospodarze chcieli w ten sposób podziękować za to wszystko, co według nich przyczyniło się do sukcesu i rozwoju ich firmy.

Po oficjalnym spotkaniu odbył się spektakl teatralny pt. „Klimakterium... i już" (kompilacja teatralnej farsy, kabaretu i koncertu) w znakomitej obsadzie i mistrzowskim wykonaniu. Wybuchające co chwila salwy śmiechu i brawa były dowodem na to, że wybór przedstawienia był strzałem w dziesiątkę. Mężczyźni towarzyszący paniom bawili się równie dobrze, chociaż tekst mocno ich atakował. Po spektaklu można było porozmawiać z aktorkami oraz otrzymać autograf. Rozbawieni goście udali się następnie na bankiet, w przerwie którego można było posłuchać koncertu Cezarego Makiewicza – laureata przeprowadzonego na Pikniku Country w Mrągowie plebiscytu, podczas którego wybrano piosenkę XXX-lecia („Wszystkie drogi prowadzą do Mrągowa").

Jubileuszowa impreza była okazją do spotkania kolegów i koleżanek, z którymi wiele lat temu widywaliśmy się praktycznie co dzień, a obecnie nie widujemy się wcale lub kontaktujemy się sporadycznie. Przy obficie zastawionych stołach wspominaliśmy dawne czasy.

Dziękujemy Jackowi i Ani Szewczykom za zaproszenie, wspaniały wieczór oraz pamiątkowe statuetki, które nam ofiarowali. W imieniu swoim i całej redakcji życzę pomyślności i dalszego rozwoju firmy. Niech kompasy wskazują zawsze północ, a nasz branżowy COMPAS zawsze właściwy kierunek.....

Teresa Karczmarzyk

Międzynarodowe Targi Poznańskie

spotkaj przyszłość

securex 2012
POLAND
Międzynarodowe Targi Zabezpieczeń

23-26 kwietnia 2012
Poznań

zabezpiecz swój sukces

Dołącz do grona naszych wystawców już dziś!

www.securex.pl

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

O legitymowaniu na osiedlach chronionych

Jan Rybczyński

Czy pracownik ochrony ma prawo legitymowania osób wchodzących na teren chronionego osiedla z polecenia zarządu wspólnoty mieszkaniowej?

Zgodnie z ustawą z dnia 24 czerwca 1994 r. o własności lokali (Dz. U. z 2000 r. Nr 80, poz. 903 z późn. zm.) ogół właścicieli, których lokale wchodzą w skład określonej nieruchomości, tworzy wspólnotę mieszkaniową. Może ona również nabywać prawa i zaciągać zobowiązania (art. 6). Sprawami wspólnoty mieszkaniowej zajmuje się zarząd, który reprezentuje też wspólnotę na zewnątrz (art. 21 ust. 1). Jeśli zarząd jest kilkuosobowy, to zgodnie z ust. 2 ww. artykułu oświadczenia woli wspólnoty mieszkaniowej składają przynajmniej dwaj członkowie jej zarządu. Oczywiście wspólnota mieszkaniowa ma zdolność prawną jedynie w zakresie legalnych działań. Jej wszystkie czynności powinny być oceniane w tym świetle. Dotyczy to również sposobów ochrony osiedla.

Wszystkie zobowiązania firmy ochrony oraz zakres czynności pracowników ochrony są pochodną tzw. uprawnień właścicielskich mieszkańców.

Ochrona własności ma związek z bezwzględnym charakterem tegoż prawa własności. Właściciel może bowiem korzystać z rzeczy i rozporządzać rzeczą „z wyłączeniem innych osób" (art. 140 k.c.). Wypływa z tego obowiązek biernego poszanowania cudzego prawa własności przez osoby trzecie. Z uprawnień właścicielskich można korzystać w granicach określonych przez ustawy i zasady współżycia społecznego (spr. sygn. akt I CKN 745/00).

W kontekście niniejszej sprawy trzeba podkreślić, że choć członkiem wspólnoty nie jest najemca lokalu, korzysta on również z ochrony posesoryjnej.

A zatem – aby firma ochrony mogła zlecić swemu pracownikowi realizację zadań wynikających z art. 36 ust. 1 pkt 1 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, musi mieć umocowanie zawarte w poleceniu, planie ochrony osiedla, umowie dotyczącej ochrony czy uchwale właścicieli lokali. Są osiedla chronione, w których nie kontroluje się uprawnień do wejścia, a jedynie interweniuje na wniosek mieszkańców. Są również takie, gdzie zasadą jest kontrolowanie podczas wejścia i wyjścia – zresztą na różne sposoby.

Dochodzimy tu do kwestii praktycznej, która musi być rozwiązania wewnątrz wspólnoty. Mianowicie nie zawsze w interesie mieszkańca jest prowadzenie ewidencji jego gości przez pracowników ochrony.

Na podstawie swego uprawnienia właścicielskiego każdy mieszkaniec może indywidualnie decydować, czy i kiedy ochrona osiedla ma sprawdzać i ewidencjonować jego gości. Pracownicy ochrony powinni respektować jego wolę. Jego postanowienia mogą odnosić się do wszystkich odwiedzających go gości. Może też uczynić wyjątek odnoszący się jakiejś osoby.

Dobrym sposobem pierwotnego rozstrzygnięcia tej kwestii przed zawarciem umowy z firmą ochrony jest właśnie wspomniana uchwała właścicieli lokali. Zgodnie z art. 23 wskazanej na początku ustawy, uchwały właścicieli lokali są podejmowane bądź na zebraniu, bądź w trybie indywidualnego zbierania głosów przez zarząd. Uchwała może być wynikiem głosów oddanych częściowo na zebraniu, częściowo w trybie indywidualnego ich zbierania. Należy dodać, że zgodnie z ustawą właściciel lokalu może zaskarżyć uchwałę wspólnoty z powodu jej niezgodności z przepisami prawa lub z umową właścicieli lokali, lub gdy narusza ona zasady prawidłowego zarządzania wspólną nieruchomością bądź w inny sposób narusza jego interesy.

Bez specjalnego upoważnienia wspólnota nie może zastąpić kimś innym swojego członka jako strony postępowania w sytuacji, w której działa on w swym własnym interesie, który nie jest związany z nieruchomością wspólną, i sprawa nie dotyczy interesu prawnego wszystkich członków. Wydaje się, że prawo każdego mieszkańca do rozstrzygania o odstąpieniu od jakiegokolwiek sprawdzania uprawnienia gościa do wejścia mieści się w granicach jego interesu prawnego.

Przejdziemy obecnie do treści uprawnień, jakie wynikają z ustawy o ochronie osób i mienia.

W punkcie 1 ust. 1 artykułu 36 jest następujące stwierdzenie: „Pracownik ochrony przy wykonywaniu zadań ochrony osób i mienia w granicach chronionych obiektów i obszarów ma prawo do ustalania uprawnień do przebywania na obszarach lub w obiektach chronionych oraz legitymowania osób, w celu ustalenia ich tożsamości". Warunek podstawowy to działanie w granicach chronionego osiedla, a nie np. na terenie ogólnie dostępnym, poza władztwem wspólnoty mieszkańców.

Interpretując ten przepis, należy odnieść się do ogólnej definicji ochrony. Można tu przywołać tezę zaczerpniętą z wyroku WSA w Warszawie (sygn. VI SA/Wa 549/05), który stwierdza, że ustawowa definicja ochrony sprowadza się do działań wyłącznie prewencyjnych przy wykonywaniu zadań w granicach chronionych obiektów, do działania w celu zapobiegania, przeciwdziałania, niedopuszczania. W przypadku jakiegokolwiek przekroczenia tych granic nie można korzystać z ochrony prawnej wynikającej z wyżej wymienionego przepisu.

Trzeba również zaznaczyć, że czym innym jest legitymowanie dokonywane przez pracownika ochrony, a czym innym np. legitymowanie dokonywane przez policjanta, które jest określone w ustawie o policji. W kontekście przywołanego wyroku prawo policji do legitymowania służy innemu celowi, określonemu w art. 14 ust. 1 ustawy o policji („W granicach swych zadań policja w celu rozpoznawania, zapobiegania i wykrywania przestępstw i wykroczeń wykonuje czynności: operacyjno-rozpoznawcze, dochodzeniowo-śledcze i administracyjno-porządkowe").

Jest to więc cel inny niż wynikający z ustawy o ochronie osób i mienia, określony dla pracowników ochrony. Ponadto legitymowanie, do którego uprawnienie jest określone w art. 36 ust. 1 pkt 1 ustawy o ochronie osób i mienia, nie jest związane ze stosowaniem środków przymusu, tak jak legitymowanie dokonywane przez policjanta, które jest określone w art. 16 ustawy o policji, w którym jest napisane, że w razie niepodporządkowania się wydanym na podstawie prawa poleceniom organów policji lub jej funkcjonariuszy policjanci mogą zastosować środki przymusu bezpośredniego.

Osoba zamierzająca wejść na teren chronionego obiektu lub zatrzymana na terenie chronionym może odmówić poddania się legitymowaniu czy sprawdzeniu uprawnień do przebywania na takim terenie. Pracownik ochrony wzywa wówczas policję.

Należy podkreślić, że sposób ustalania uprawnień i legitymowania jest ściśle określony w przepisach rozporządzenia Rady Ministrów z dnia 18 listopada 1998 r. (Dz. U. Nr 144, poz. 933) w sprawie szczegółowego trybu działań pracowników ochrony, podejmowanych wobec osób znajdujących się w granicach chronionych obiektów i obszarów. W przypadku nieprzestrzegania tych przepisów przedsiębiorca lub pracownik ochrony może stracić swoją koncesję lub licencję.

Ustalenie uprawnienia osoby do przebywania na obszarze lub w obiekcie chronionym przez pracownika ochrony nie jest w zasadzie kontrowersyjne. Dokonuje się go przez:

– sprawdzenie, czy osoba posiada przepustkę, identyfikator albo inny dokument uprawniający do przebywania na obszarze lub w obiekcie chronionym, wystawiony przez osobę zarządzającą tym obszarem lub obiektem,
– porównanie okazanego dokumentu z określonym wzorem,
– sprawdzenie okazanego dokumentu pod względem zgodności zawartych w nim danych personalnych z tożsamością osoby oraz sprawdzenie terminu jego ważności.

Mieszkaniec może (ustnie lub pisemnie) wyrazić zgodę na przebywanie danej osoby na obszarze chronionym lub w obiekcie chronionym. Warto podkreślić, że na żądanie osoby, której uprawnienie do wejścia jest sprawdzane, pracownik ochrony musi podać swoje imię i nazwisko oraz okazać licencję lub inny potwierdzający jego uprawnienia dokument w taki sposób, aby osoba legitymowana miała możliwość odczytania i zanotowania zawartych w tym dokumencie danych. Pracownik ochrony musi też podać podstawę prawną i przyczynę swoich czynności. Ważne jest zatem związane z tym stanowisko wspólnoty mieszkaniowej.

Legitymowanie w związku z wchodzeniem na teren osiedla chronionego jest i pozostanie drażliwe, gdyż zgodnie z ustawową definicją ochrona sprowadza się do wyłącznie prewencyjnych działań w granicach chronionych obiektów, a więc działań, które mają na celu zapobieganie, przeciwdziałanie, niedopuszczanie. Zasada legitymowania wszystkich osób będzie zawsze oceniana jako skrajny sposób realizowania tak określonego celu.

Tożsamość osoby legitymowanej ustala się na podstawie dowodu osobistego, tymczasowego dowodu osobistego, tymczasowego zaświadczenia tożsamości, dokumentu stwierdzającego tożsamość cudzoziemca, paszportu lub innych dokumentów potwierdzających tożsamość, zaopatrzonych w fotografię i adres osoby legitymowanej.

Istnieje jeszcze jeden ważny przepis w tym rozporządzeniu, który odnosi się do zasad dokumentacji firmy ochrony, mianowicie zawarty w § 6 i brzmiący następująco: „Z czynności legitymowania pracownik ochrony sporządza notatkę służbową, zawierającą dane personalne osoby legitymowanej, wskazanie rodzaju dokumentu oraz jego numeru i serii, a także czasu, miejsca i przyczyny legitymowania". Ustalenie takiego obowiązku już w przypadku legitymowania pojedynczej osoby wskazuje na to, że legitymowanie ma się odbywać w wyjątkowych przypadkach. Można więc na przykład wylegitymować osobę, która nie została wylegitymowana wcześniej, gdyż przeszła przez płot. Nie jest zupełnie jasne, czy legitymowanie jest koniecznym elementem działań prewencyjnych w granicach chronionych obiektów, czy jest konieczne do zapobiegania, przeciwdziałania i niedopuszczania. W związku z nieostrością przepisu art. 36 ust. 1 pkt 1 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, a także brakiem szerszego orzecznictwa problem dotyczący korzystania z przedmiotowych uprawnień pozostanie.

Należy zatem pamiętać, iż dane osobowe pozyskane w trakcie czynności dokonywanych na podstawie art. 36 ust. 1 pkt 1 ustawy o ochronie osób i mienia podlegają ochronie na podstawie przepisów ustawy z dnia 29 sierpnia 1999 r. o ochronie danych osobowych.

Co prawda zbiory danych gromadzone w związku z ewidencją wejść można by uznać za zwolnione z obowiązku rejestracji w GIODO na mocy art. 43 ust. 1 pkt 4 ze względu na ich przetwarzanie w związku ze świadczeniem usług na podstawie umów cywilnoprawnych. Podlegają one jednak pełnej ochronie na podstawie przepisów rozdziału 5-tej ustawy, które dotyczą zabezpieczenia danych osobowych, oraz w związku z prawami osoby, której dane dotyczą (rozdział 4).

Sposób uregulowania trybu legitymowania w wyżej wymienionym rozporządzeniu Rady Ministrów wskazuje na jego wyjątkowość (obowiązek sporządzania notatki w każdym przypadku legitymowania).

Na tle tezy orzeczenia o sygn. VI SA/Wa 549/05, która sprowadza ochronę do wyłącznie prewencyjnych działań w granicach chronionych obiektów, do zapobiegania, przeciwdziałania i niedopuszczania, zachodzi poważna wątpliwość, czy legitymowanie wszystkich wchodzących na teren chronionego osiedla może być traktowane jako rutynowe i niekwestionowane prawo pracownika ochrony. Sprzeciwia się temu ugruntowana zasada, że każdy działa w dobrej wierze, zakaz nadużywania prawa podmiotowego, które jest dotkliwe dla obywateli, i uciążliwość takiego korzystania z uprawnień przez pracowników ochrony.

Przepisy omawianego rozporządzenia są w dużej mierze kalką przepisów wykonawczych uzupełniających ustawę o policji, a ponadto powstały, zanim rozpoczął się okres budowy licznych osiedli zamkniętych. Uważam, że pora określić odrębne zasady kontroli na osiedlach.

Jan Rybczyński
radca prawny

SCHRACK SECONET

Wszystkim Klientom, Współpracownikom i Przyjaciołom firmy życzymy pełnych ciepła, radości i spokoju Świąt Bożego Narodzenia.

Niech nadchodzący Nowy Rok będzie źródłem dalszych sukcesów i inspiracji w podejmowaniu nowych wyzwań.

Zespół Schrack Seconet Polska Sp. z o.o.

PoE
bez tajemnic (część 1)

Andrzej Walczyk

Na temat zasilania peryferyjnych urządzeń sieciowych metodą PoE napisano wiele publikacji, zaś projektantom i instalatorom sieciowych systemów teleinformatycznych ten temat jest powszechnie znany. Z technologii PoE korzysta na co dzień wiele osób i może im się wydawać, że wszystko jest proste – wtyka się wtyczkę i urządzenie działa. Jednak w rzeczywistości jest to dużo bardziej skomplikowane

Wyjaśnijmy najpierw sam termin. W encyklopedii znajdziemy następujący opis: „*Power over Ethernet* – technologia przesyłu energii elektrycznej do urządzeń peryferyjnych, będących elementami sieci Ethernet, takich jak telefony VoIP, bezprzewodowe punkty dostępowe, kamery internetowe i tym podobne, przy czym do przesyłu energii zasilającej służy ten sam kabel, którym transmitowane są dane cyfrowe". W praktyce zakres zastosowań metody PoE nie ogranicza się do przykładów podanych w encyklopedii. Popularność tej metody stale rośnie, pojawiają się jej nowe odmiany, takie jak PoE+ czy hPoE, zaś część urządzeń sieciowych w ogóle nie może być zasilana w inny sposób. Trudno się dziwić, gdyż brak dodatkowego okablowania i oddzielnych urządzeń zasilających bardzo upraszcza i przyspiesza instalację urządzeń sieciowych.

Główne założenia twórców technologii PoE można wymienić w kilku punktach:

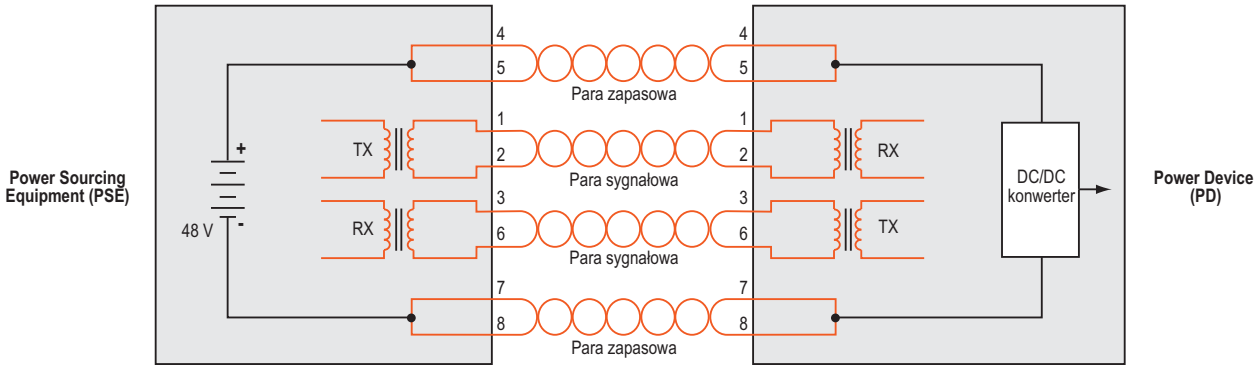
- możliwość zastosowania tej metody w każdej sieci Ethernet o prędkości transmisji 10, 100 lub 1000 Mb/s, zbudowanej z wykorzystaniem kabli miedzianych kategorii 5 lub 6;
- brak wpływu tej metody na parametry transmisyjne sieci Ethernet, w tym brak jakichkolwiek zakłóceń związanych z dostarczaniem energii;
- zapewnienie wysokiego poziomu niezawodności zasilania, niezależnie od długości i rodzaju zastosowanego okablowania, pod warunkiem zachowania zgodności z ogólnymi wymaganiami dotyczącymi okablowania w sieci Ethernet;
- zapewnienie wysokiego poziomu bezpieczeństwa, zarówno urządzeniom zasilanym tą metodą, jak i obsługującym je osobom;
- brak wpływu na działanie urządzeń nie przystosowanych do zasilania tą metodą, w tym zapewnienie bezpieczeństwa działania tych urządzeń.

Jak wynika z powyższych założeń, zasilanie urządzeń peryferyjnych metodą PoE może być realizowane w sieciach Ethernet określanych w literaturze jako 10 Base-T, 100 Base-Tx i 1000 Base-T, wykorzystujących kable miedziane. W takich sieciach pracuje większość współczesnych urządzeń peryferyjnych stanowiących wyposażenie mieszkań, biur, zakładów produkcyjnych, a nawet większych obiektów, takich jak na przykład stadiony.

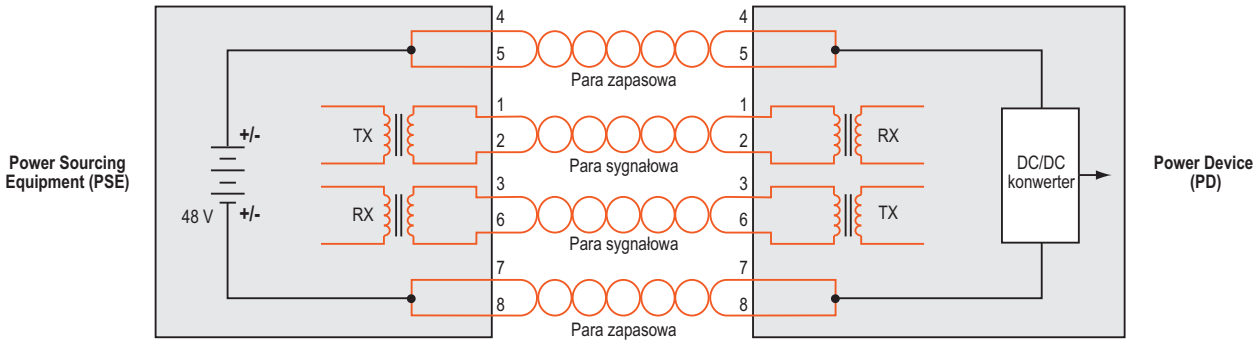
Z punktu widzenia użytkownika zasilanie urządzeń peryferyjnych metodą PoE nie nastręcza żadnych problemów. Jeśli wszystkie składniki sieci są do tego przystosowane, urządzenia peryferyjne zaczynają działać natychmiast po podłączeniu do sieci. Jedynym wyróżnikiem jest rodzaj złącza sieciowego, którym typowo jest gniazdo lub wtyk typu RJ45, i tylko na to musi zwrócić uwagę użytkownik. Innymi słowy, jeśli wtyki i gniazda do siebie pasują i urządzenie można fizycznie podłączyć do sieci, z pewnością zacznie ono działać.

Jak wiadomo, kabel sieciowy kategorii piątej lub szóstej składa się z czterech par przewodów miedzianych. Można rozróżnić trzy przypadki wykorzystania tych przewodów w PoE. W pierwszym z nich energia jest dostarczana za pośrednictwem wolnych par przewodów, nie używanych do transmisji danych, co jest możliwe tylko w sieciach o przepustowości 10 Mb/s lub 100 Mb/s. W drugim z omawianych przypadków energia jest dostarczana za pomocą dwóch par przewodów, używanych jednocześnie do transmisji danych i do zasilania. W sieciach o przepustowości 1000 Mb/s jest to jedyne możliwe rozwiązanie, gdyż do transmisji danych wykorzystane są wszystkie cztery pary przewodów. W trzecim z omawianych przypadków energia jest dostarczana za pomocą wszystkich czterech par przewodów, niezależnie od tego, czy te przewody są wykorzystywane do transmisji danych, czy pozostają niewykorzystane. Dzięki temu można ograniczyć straty energii wynikające z rezystancji przewodów, co jest szczególnie istotne w przypadku zasilania urządzeń peryferyjnych odznaczających się zwiększonym poborem mocy.

W literaturze spotyka się dwa określenia dotyczące składników sieci związanych z realizacją metody PoE, z którymi warto



Rys. 1. Zasilanie metodą PoE z wykorzystaniem wolnych przewodów



Rys. 2. Zasilanie metodą PoE z wykorzystaniem przewodów transmitujących dane

się zapoznać, gdyż są często stosowane (wymienione skróty będą używane także w dalszej części artykułu). Te określenia to:

– urządzenia dostarczające energię do kabla sieciowego metodą PoE, określane skrótowo jako PSE (od angielskich słów *Power Sourcing Equipment*);
– urządzenia wymagające zasilania metodą PoE, określane skrótowo jako PD (od angielskich słów *Powered Device*).

Dostarczanie energii służącej do zasilania peryferyjnych urządzeń sieciowych za pośrednictwem niewykorzystanych przewodów jest bardzo proste. Przypadek ten jest wyjaśniony na rys. 1.

W tym momencie należy podkreślić, że metoda PoE zasadniczo różni się od często stosowanych, prostych sposobów dostarczania energii do urządzeń sieciowych, które polegają na podłączeniu zewnętrznych zasilaczy do przewodów nie wykorzystywanych do transmisji danych. Ze względu na prostotę i niskie koszty implementacji takie sposoby są chętnie wykorzystywane przez producentów sprzętu sieciowego, w tym także wysokiej klasy profesjonalnego sprzętu sieciowego, przy czym nie są one kompatybilne z metodą PoE i nie spełniają typowych dla niej wymagań dotyczących niezawodności i bezpieczeństwa użytkowania.

Postawmy teraz pytanie: w jaki sposób można wykorzystać te same przewody do dostarczania energii zasilającej i równocześnie do transmisji danych sieciowych? Otóż wiadomo, że w konstrukcji interfejsów sieciowych stosowane są specjalne transformatory impulsowe, których zadaniem jest galwaniczne oddzielenie przewodów sieciowych od układów elektronicznych komputerów lub od innych urządzeń sieciowych. Jest to związane z koniecznością ochrony tych urządzeń przed przepięciami, jakie mogą się pojawiać w kablach sieciowych podczas burz lub w wyniku przepięć występujących w sieci energetycznej. Innym, równie istotnym powodem stosowania wspomnianych transformatorów jest konieczność dopasowania interfejsów sieciowych do impedancji falowej kabli transmisyjnych. Jednakże transformatory, których użycie gwarantuje poprawne działanie sieci Ethernet, mogą być wykorzystane także do innych celów. Ze środka pierwotnych uzwojeń tych transformatorów wyprowadzone są odczepy, przez które może przepływać prąd zasilający. Przypadek ten jest wyjaśniony na rys. 2.

Należy wyjaśnić, że oba opisane powyżej przypadki nie kolidują ze sobą. Urządzenia zasilające PSE i urządzenia peryferyjne PD mogą różnić się konstrukcją i mogą wykorzystywać różne sposoby transmisji danych, jednak nie ma to wpływu na praktyczną realizację metody PoE. Jeśli spełnione są wymagania dotyczące tej metody, urządzenia same negocjują warunki zasilania i wybierają odpowiednią formę połączenia.

Do zasilania urządzeń sieciowych metodą PoE wykorzystywane jest napięcie stałe o nominalnej wartości 48 V. Twórcy tej metody nie przypadkiem zdecydowali się na wybór takiej, a nie innej wartości napięcia – na tyle małej, by nie stanowiła zagrożenia dla zdrowia lub życia osób korzystających z urządzeń sieciowych, i na tyle dużej, by pozwalała na przekazanie relatywnie dużej mocy zasilającej przez przewody sieciowe kategorii piątej lub szóstej, których przekrój z natury rzeczy jest ograniczony. Z danych katalogowych pochodzących od producentów wynika, że w kablach sieciowych kategorii piątej lub szóstej średnica pojedynczych przewodów wynosi 0,5 mm lub 0,8 mm, przy czym ta druga wartość jest mniej popularna i rzadziej spotykana na rynku. Oznacza to, że w najgorszym przypadku przekrój pojedynczego przewodu wchodzącego w skład kabla sieciowego wynosi zaledwie 0,2 mm^2.

Wiadomo, że w sieci Ethernet długość pojedynczego odcinka kabla nie może przekraczać 100 m, co oznacza, że w najgorszym przypadku kabel może mieć właśnie taką długość. Biorąc pod uwagę bardzo mały przekrój przewodów, należy liczyć się ze znacznymi spadkami napięć w takich warunkach. Dlatego w metodzie PoE dopuszczono znaczną odchyłkę rzeczywistej wartości napięcia zasilającego od wspomnianej wcześniej wartości nominalnej. Napięcie doprowadzane do początkowej części kabla sieciowego powinno mieścić się w zakresie od 44 V do 57 V, zaś na końcu tego kabla – od 37 V do 57 V.

Kolejnym elementem wykorzystywanym w urządzeniach zasilanych metodą PoE są przetwornice napięcia stałego, zwane także konwerterami DC/DC. Pobierają one energię z kabla sieciowego i drogą niemal bezstratnej konwersji wytwarzają wszystkie napięcia niezbędne do zasilania układów wewnętrznych urządzeń peryferyjnych. Przetwornice muszą być przystosowane do pracy w warunkach dużych wahań napięcia wejściowego, co w chwili obecnej nie stanowi problemu technologicznego. Na rynku dostępne są liczne układy scalone wykonujące opisane powyżej zadania, dlatego to zagadnienie nie zostanie teraz dokładniej omówione.

Zastanówmy się teraz nad skutkami stosowania metody PoE podczas zasilania sieciowych urządzeń elektronicznych w aspekcie bezpieczeństwa ich użytkowania. Czy relatywnie duża wartość napięcia zasilającego, wynosząca nominalnie 48 V, może być przyczyną awarii przypadkowo podłączonych urządzeń nie przystosowanych do zasilania tą metodą? Czy napięcie występujące na końcach kabli sieciowych nie podłączonych do żadnych urządzeń może być przyczyną awarii

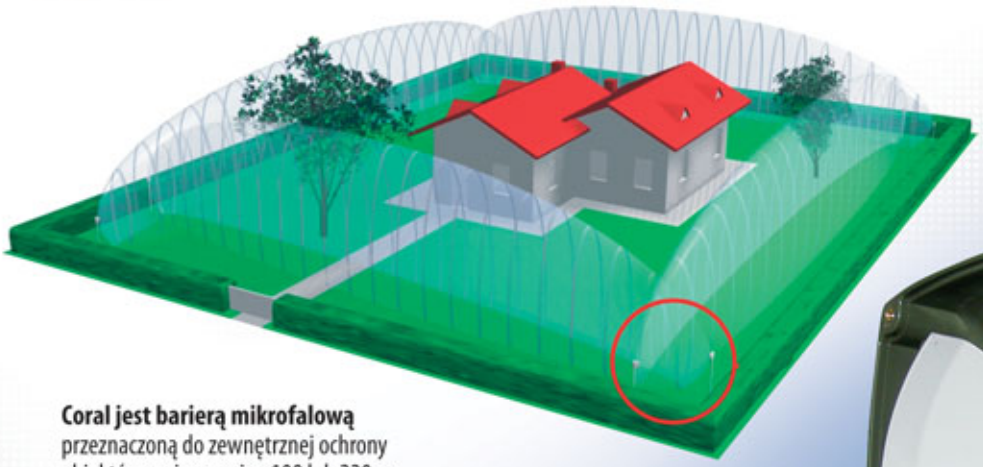
firma ATLine®

ZSJZ

www.atline.pl

AQAP 2110:2009
ISO 9001:2008

Firma ATLine sp.j. Sławomir Pruski
ul. Franciszkańska 125, 91-845 Łódź,
tel. +48 42 657 30 80, fax +48 42 655 20 99
e-mail: info@atline.pl, handel@atline.pl



Coral jest barierą mikrofalową przeznaczoną do zewnętrznej ochrony obiektów mającą zasięg 100 lub 220 m. Została zaprojektowana jako urządzenie przeznaczone do szybkiej i prostej instalacji oraz łatwego serwisowania.

Rewolucyjne rozwiązanie z anteną w kształcie skrzydeł motyla
oferuje jako jedyne na świecie unikalną, przestrzenną strefę detekcji i czyni barierę idealną do wielu zastosowań.

BARIERY MIKROFALOWE CORAL I CORAL PLUS

przypadkowo dotkniętych elementów? Otóż nie, żaden ze wspomnianych przypadków nie zachodzi. Urządzenia PSE dostarczające energię do kabla sieciowego realizują ściśle określone procedury, które pozwalają na uniknięcie tak przykrych doświadczeń.

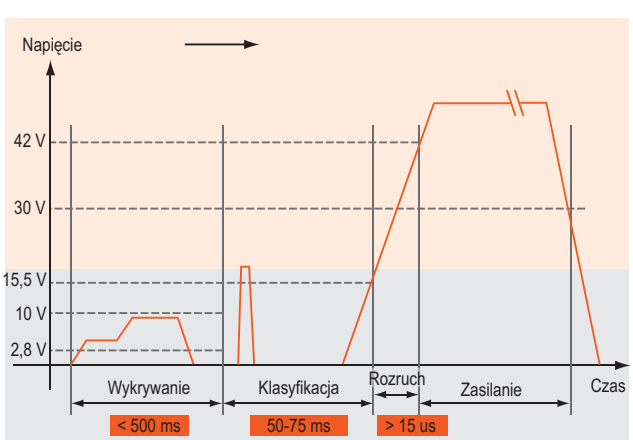
Pierwsza z tych procedur polega na dostarczaniu energii do kabla sieciowego tylko wtedy, gdy jest to potrzebne. Jeśli do kabla sieciowego podłączone jest urządzenie końcowe, które nie jest przystosowane do zasilania metodą PoE, urządzenie PSE nie dostarczy energii zasilającej. Przypadek ten obejmuje także sytuację, w której do końca kabla nie jest podłączone żadne urządzenie.

Druga z tych procedur polega na wykrywaniu i klasyfikacji urządzeń PD przystosowanych do zasilania metodą PoE i na dostosowaniu warunków zasilania do specyfiki tych urządzeń. Tę procedurę można rozbić na kilka etapów:

– wykrywanie urządzenia PD wymagającego zasilania metodą PoE;
– klasyfikacja urządzenia PD wymagającego zasilania metodą PoE, określenie nieprzekraczalnej wartości mocy zasilającej;
– rozruch urządzenia zasilającego PSE;
– dostarczanie energii zasilającej zgodnie z przeprowadzoną klasyfikacją.

Wykrywanie obecności urządzenia PD wymagającego zasilania metodą PoE polega na pomiarze wartości prądu pobieranego przez kabel sieciowy po przyłożeniu do niego niewielkiego napięcia, mieszczącego się w zakresie od 2,5 V do 10 V. Ze względów bezpieczeństwa na tym etapie wydajność prądowa urządzenia PSE jest ograniczana do 30 mA, zaś czas trwania impulsu próbkującego wynosi około 500 ms. Jeśli w takich warunkach nastąpi przepływ prądu, oznacza to, że do kabla sieciowego podłączone jest jakieś urządzenie i należy sprawdzić, czy jest ono przystosowane do zasilania metodą PoE. Innymi słowy – musi nastąpić jego klasyfikacja.

Klasyfikacja wykrytego urządzenia jest dokonywana po to, by ocenić, czy jest ono przystosowane do zasilania metodą PoE. Jeśli tak, ustalana jest nieprzekraczalna wartość mocy niezbędnej do zasilania go w warunkach normalnej pracy. Na tym etapie wszystkie urządzenia przystosowane do zasilania metodą PoE dołączają do kabla zasilającego pewną ściśle określoną rezystancję, która wynosi około 25 kΩ. Na podstawie dokładnego pomiaru tej rezystancji



Rys. 3. Wykres ilustrujący etapy realizacji metody PoE

każde z urządzeń można zakwalifikować do jednej z czterech klas, które różnią się wartością pobieranej mocy. Jeśli zmierzona wartość rezystancji nie mieści się w ściśle określonych granicach, oznacza to, że urządzenie podłączone do końca kabla sieciowego nie jest przystosowane do zasilania metodą PoE i energia zasilająca w ogóle nie zostanie dostarczona.

Na etapie rozruchu urządzenie zasilające PSE stopniowo zwiększa napięcie przykładane do kabla sieciowego. Zapobiega to przepływowi prądów rozruchowych o dużej wartości, a ponadto pozwala na łagodne uruchomienie przetwornicy i ustabilizowanie napięcia zasilającego na wymaganym poziomie.

Kolejny, ostatni etap polega na ciągłym dostarczaniu energii zasilającej do urządzenia peryferyjnego PD z zachowaniem limitu mocy ustalonego na etapie klasyfikacji. Wzrost poboru mocy powyżej ustalonej wartości oznacza awarię urządzenia peryferyjnego PD. Spadek poboru mocy poniżej pewnej wartości oznacza odłączenie urządzenia peryferyjnego PD. W obu przypadkach urządzenie zasilające RSE zareaguje odłączeniem zasilania.

Wszystkie opisane etapy działania urządzeń zasilanych metodą PoE są przedstawione na rys. 3.

Opisany mechanizm działa w pierwszej, fizycznej warstwie sieci Ethernet[1]. Łatwo zauważyć, że jest to dość prosty mechanizm, który w trudniejszych przypadkach może zawieść. Na przykład urządzenie PSE może wyłączyć zasilanie, gdy urządzenie peryferyjne PD przejdzie w stan wyczekiwania, co byłoby oczywistym błędem. Znana jest również bardziej skomplikowana, doskonalsza procedura klasyfikacji urządzeń peryferyjnych zasilanych metodą PoE, realizowana w pierwszej i drugiej warstwie sieciowej. W tej metodzie urządzenia zasilające PSE i urządzenia peryferyjne PD wymieniają między sobą dane cyfrowe pozwalające na bardziej precyzyjne ustalenie parametrów zasilania. Szczegółowy opis tej metody negocjacji wykracza poza zakres niniejszego artykułu[2]. Ta klasa urządzeń jest określana w literaturze jako PoE+ i jest warta uwagi, gdyż technologia PoE stale się rozwija, pojawiają się jej nowe odmiany, takie jak hPoE, konstruktorzy sprzętu dążą do przekazania jak największej mocy zasilającej do urządzeń peryferyjnych bez konieczności modyfikacji okablowania. W literaturze można spotkać wzmianki o próbach przekazywania mocy rzędu 60 W przy napięciu 48 V, co umożliwia zasilanie kontrolerów drzwiowych i zwór elektromagnetycznych w systemach kontroli dostępu, a także ciężkich kamer szybkoobrotowych wyposażonych w grzałki i oświetlacze IR w systemach monitoringu wizyjnego. Zakres zastosowań metody PoE stale się rozszerza, nic więc dziwnego, że ulega ona ciągłym modyfikacjom. Praktyczne aspekty wykorzystania tej metody zostaną omówione w kolejnej części artykułu.

Andrzej Walczyk

1) Podział na warstwy jest zgodny z modelem OSI ISO sieci teleinformatycznej.

2) Zainteresowanych odsyłam do strony http://www.eetimes.com/design/analog-design/4010400/Power-over-Ethernet-PoE-grows-up-it-s-now-PoE-

Bezprzewodowy system do kamer megapikselowych IP HD.

Cyfrowy system bezprzewodowy pracujący w wolnym paśmie 5,6 GHz o mocy 1W, przeznaczony do płynnego przesyłania sygnałów wizyjnych z kamer IP HD do 5M pikseli.

- stabilna wysokiej jakości transmisja obrazu w jakości powyżej Full HD
- obsługiwane rozdzielczości do 2560x2048 pikseli
- rodzaj pracy: Punkt - Punkt oraz Punkt - Wielopunkt
- zasięg w wersji standardowej 2km (opcja 5km)
- osiem kanałów pracy
- zintegrowana antena dualna oraz dodatkowe złącza antenowe RP-SMA
- cyfrowa modulacja OFDM
- możliwość podłączenia dwóch kamer IP (dwa wejścia RJ45)
- zabezpieczenia transmisji 64/128/152 bitowym kodem
- obudowa zewnętrzna IP 55

CDS-5IP

www.camsat.com

Bezprzewodowa transmisja obrazu z kamer IP HD

Agnieszka Gralak

Branża telewizji dozorowej charakteryzuje się bardzo dynamicznym rozwojem, a wymagania techniczne wobec urządzeń są coraz wyższe. Łatwo zauważyć, jak bardzo w ciągu kilku lat zmieniły się właściwości rejestrowanego obrazu, np. rozdzielczość i kompresja sygnału. Korzyści płynące ze zwiększenia rozdzielczości obrazu do poziomu HD są oczywiste, jednak powodują także pewne problemy z przetwarzaniem dużej ilości danych i transmisją obrazu. Dlatego należy pamiętać o odpowiednim doborze pozostałych elementów systemu, aby odpowiadały one wysokim parametrom współczesnych kamer

Żadna, nawet najlepsza kamera nie zapewni nam obrazu o wysokiej jakości, jeżeli pozostałe urządzenia nie będą mogły go przesłać i odtworzyć w jakości niezmienionej. O ile obecnie można przesyłać za pomocą sieci przewodowej obrazy z kamer o wysokiej rozdzielczości i dowolnie dobranej kompresji, w przypadku transmisji bezprzewodowej sytuacja nie przedstawia się już tak dobrze. Dostępne na rynku bezprzewodowe kamery IP nie charakteryzują się zadowalającymi parametrami technicznymi i często nie mogą sprostać wymaganiom klientów. Brak płynności ruchu na obrazie, zrywanie transmisji, słaba przepustowość łącza i mały zasięg skutecznie odstraszają instalatorów od tego typu rozwiązań. Mimo to zapotrzebowanie na stabilne bezprzewodowe łącze IP jest bardzo duże, ponieważ nie zawsze możliwe jest wykorzystanie okablowania do przesyłu sygnału z kamery IP. Punkt odbiorczy może znajdować się w dużej odległości od monitorowanego obiektu lub nie ma możliwości modyfikacji istniejącego okablowania. Zdarza się także, że łącza nie mogą sprostać wymaganiom kamer o wysokiej rozdzielczości. Znów wracamy do punktu wyjścia, gdyż klient kupujący kamerę IP nie chce utraty jakości obrazu na skutek złego działania toru transmisyjnego łączącego kamerę z rejestratorem.

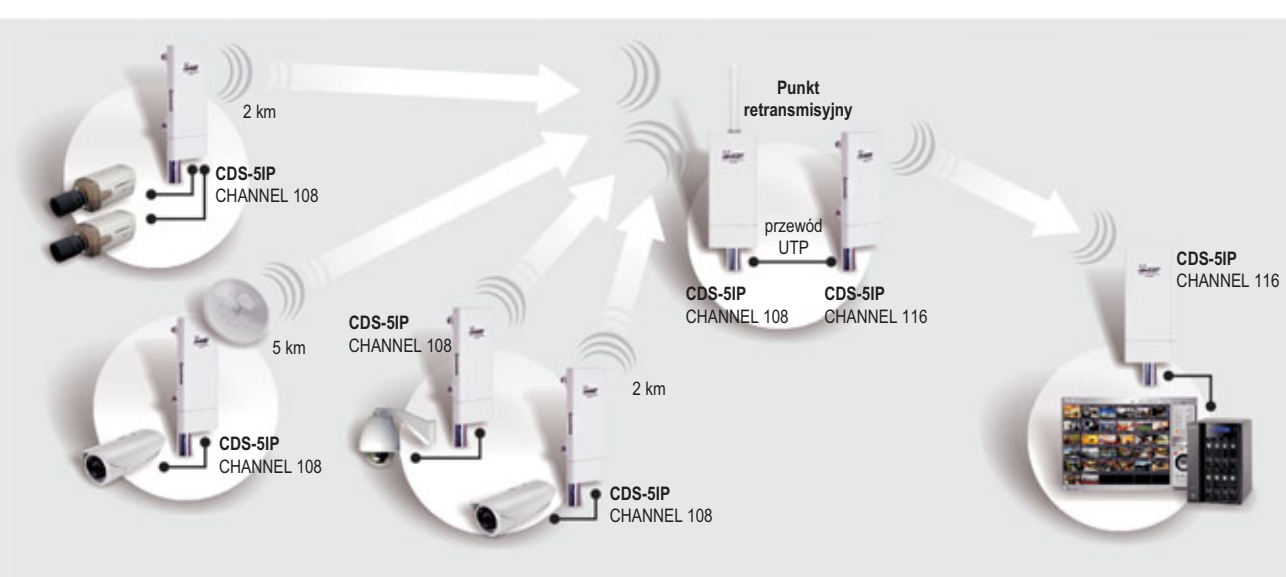
Firma Camsat, producent systemów bezprzewodowych, długo pracowała nad właściwym i pewnym rozwiązaniem problemu przesyłu sygnału z kamer IP o wysokiej rozdzielczości za pośrednictwem łącza radiowego. Prace nad udoskonaleniem oprogramowania oraz wykorzystanie najnowocześniejszych komponentów pozwoliły na wprowadzenie na rynek jednego z najlepszych rozwiązań związanych z transmisją bezprzewodową – urządzenia CDS-5IP.

CDS-5IP to bezprzewodowy zestaw pracujący w paśmie 5.6 GHz, o mocy 1 W, przeznaczony do przesyłania sygnału fonicznego i wizyjnego z kamer o różnych rozdzielczościach – od VGA 640×480 przez Full HD 1080p do QSXGA 2560×2048. Urządzenie pozwala na uzyskanie płynnej transmisji obrazów z prędkością 25 kl./s. Aby zminimalizować opóźnienia transmisji, zastosowano procesory taktowane z częstotliwością aż 400 MHz, co gwarantuje transmisję sygnałów ze znikomymi opóźnieniami. Jest to bardzo ważne w przypadku kamer obrotowych.

W CDS-5IP zastosowano zintegrowaną dwupolaryzacyjną antenę kierunkową, która pracuje w systemie MIMO, odznacza się zyskiem energetycznym 16 dBi i zapewnia stabilną transmisję na odległość dochodzącą do dwóch kilometrów. Dwa zewnętrzne wyjścia RP-SMA umożliwiają podłączenie anten zewnętrznych w przypadku potrzeby zwiększenia zasięgu lub instalacji anten dookolnych, niezbędnych podczas pracy w układzie punkt – wielopunkt. Warto podkreślić, że jest to rozwiązanie, które czyni urządzenie CDS-5IP bardzo wszechstronnym, elastycznie dopasowującym się do wymagań danego systemu monitoringu i umożliwia doskonałą pracę systemu na dużych, otwartych przestrzeniach. Ponadto anteny stanowią zwarcie dla prądu stałego, co zabezpiecza urządzenia przed uszkodzeniami na skutek przepięć czy wyładowań atmosferycznych, często paraliżujących działanie systemów bezprzewodowych.

Warunkiem optymalnego wykorzystania możliwości, które daje urządzenie CDS-5IP, jest precyzyjne skonfigurowanie zestawu z uwzględnieniem parametrów technicznych kamer. W zależności od potrzeb CDS-5IP może pracować w układzie punkt – punkt lub punkt – wielopunkt. Instalator ma do dyspozycji osiem częstotliwości. Każda z nich może być wykorzystana do transmisji obrazów z czterech czy też sześciu kamer. Liczba kamer IP zainstalowanych w jednym obiekcie zależy w dużym stopniu od ich rozdzielczości. Szczególnie polecanym przez producenta układem jest tryb VIDEO MOST. Daje on wiele możliwości. To od instalatora lub osoby zarządzającej będzie zależeć to, jaką liczbę kanałów roboczych uda mu się wykorzystać. W tym układzie na jednym kanale roboczym możemy uruchomić do czterech kamer IP, zapewniając przy tym wysoce stabilną transmisję.

Bardzo ważne jest zapewnienie bezpieczeństwa bezprzewodowej transmisji obrazu, dźwięku czy danych, dlatego w urządzeniach CDS-5IP zastosowano szereg zabezpieczeń, w tym 64/128/152-bitowy kod, firewall, a także funkcje rutowania. Zapewnia to maksymalną ochronę przesyłanych treści przed



Rys. 1. Przykład zastosowania CDS-5IP w konfiguracji PUNKT - WIELOPUNKT z retransmisją

ingerencją osób trzecich. Ponadto oprogramowanie urządzenia pozwala na zdalną konfigurację i precyzyjne ustawienie blokad dostępu.

Wielu instalatorów nie mających dużego doświadczenia w instalowaniu systemów bezprzewodowych ma pewne problemy z ich konfiguracją. Aby dodatkowo ułatwić instalację urządzenia CDS-5IP, wprowadzono szereg udogodnień. Zastosowano wskaźnik poziomu sygnału radiowego, który pozwala stwierdzić, że ustawienia anten są prawidłowe. Jest to niezwykle ważne dla prawidłowego działania systemu radiowego i daje gwarancję uzyskania poprawnej transmisji. Ponadto instalator ma możliwość regulacji mocy wyjściowej urządzeń radiowych w celu uzyskania optymalnych parametrów w danym obiekcie. CDS-5IP posiada dwa wejścia RJ45, które pozwalają na jednoczesną obsługę dwóch kamer IP bez konieczności doprowadzania dodatkowego zasilania. Można także wykorzystać jedno z wejść RJ45 do zasilania kolejnych urządzeń CDS-5IP. Jest to niezwykle dogodne rozwiązanie, które pozwala na montaż kamer w miejscach pozbawionych instalacji elektrycznej, do których nie można doprowadzić osobnych przewodów zasilających. Dzięki temu instalacja systemu bezprzewodowego IP HD jest nie tylko łatwiejsza, ale także bardziej ekonomiczna.

CDS-5IP wyróżnia się na tle innych, podobnych urządzeń dostępnych na naszym rynku. Oprócz transmisji obrazu z kamer IP oferuje szereg dodatkowych funkcji, takich jak kompleksowa obsługa kamer szybkoobrotowych czy dwukierunkowa transmisja danych. Wprowadzanie na rynek coraz doskonalszych systemów bezprzewodowych sprawia, że instalatorzy są do nich coraz przychylniej nastawieni. Dbałość o jakość urządzeń daje w rezultacie możliwość rozwiązania dotychczasowych problemów instalatorskich. Bezprzewodowe systemy dozorowe sprawdzą się w wielu miejscach, w których zastosowanie systemów przewodowych byłoby bardzo trudne, a tym samym kosztowne. W takich przypadkach użycie wysoce stabilnego i bezpiecznego łącza radiowego pozwala na transmisję obrazów o wysokiej jakości i jest uzasadnione zarówno ze względów technicznych, jak i ekonomicznych.

camSAT

CAMSAT,
Agnieszka Gralak
www.camsat.com

SZKOŁA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ TECHOM W WARSZAWIE

zaprasza na:

KURSY ZAWODOWE

w zakresie:

I STOPNIA: INSTALACJI, KONSERWACJI I EKSPLOATACJI SYSTEMÓW ALARMOWYCH DO STOPNIA ZABEZPIECZENIA 1-4 (KLASY SA-1 - SA-4)

II STOPNIA: PROJEKTOWANIA SYSTEMÓW ALARMOWYCH DO STOPNIA ZABEZPIECZENIA 1-4 (KLASY SA-1 - SA-4) DLA OBIEKTÓW CYWILNYCH I WOJSKOWYCH

RZECZOZNAWSTWO SYSTEMÓW TECHNICZNEGO ZABEZPIECZENIA OSÓB I MIENIA ORAZ ZARZĄDZANIA BEZPIECZEŃSTWEM OBIEKTU

UWAGA: TRWA NABÓR KANDYDATÓW NA KURS! (I SESJA - GRUDZIEŃ 2011R.)

NOWOŚĆ WARSZTATY DOSKONALĄCE PRAKTYCZNE UMIEJĘTNOŚCI Z ZAKRESU DIAGNOZOWANIA USZKODZEŃ ORAZ INSTALOWANIA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ

Udzielamy autoryzacji zakładom instalacji alarmowych

INFORMACJA ORAZ PRZYJMOWANIE ZGŁOSZEŃ:

tel.: 22 625 34 00
faks: 22 625 26 75
www.techom.com

Zespół ds. Szkoleń i Wydawnictw
Al. Wyzwolenia 12
00-570 Warszawa

techom@techom.com
a.bielecki@techom.com
k.doroba@techom.com

PRZECHWYĆ

ZAPISZ

POKAŻ

ZŁAP

iPOLiS

Rozwiązania sieciowe firmy Samsung

Obraz w rozdzielczości Full HD	Inteligentna Analiza Obrazu	Skalowalna rejestracja	Zdalny podgląd i sterowanie
FULL HD			

Kamery HD oraz monitory generują obrazy w formacie 16:9 i pozwalają operatorom określić z maksymalną dokładnością specyficzne obszary zainteresowania do bliższego zbadania – bez strat rozdzielczości i bez efektu „pikselacji" przy obserwacji. A dzięki zapisowi w rozdzielczości HD na materiale zarejestrowanym można wszystko zobaczyć z tą samą jakością.

Z pełnym zestawem kamer, wyborem opcji sprzętowych lub oprogramowania oraz monitorami HD, możesz stworzyć system bezpieczeństwa idealnie dopasowany do Twoich potrzeb.

Sieciowe rozwiązania bezpieczeństwa Samsung HD.
Inteligentniejsze bezpieczeństwo.

E STEsecurity@samsung.com
W samsungsecurity.com

Samsung Techwin Europe Ltd

SAMSUNG

Aplikacja iPOLiS MOBILE

James Smith

Fot. 1. Aplikacja iPoLis firmy Samsung, dla telefonów komórkowych i tabletów

Na przestrzeni ostatnich lat firma Samsung przeznaczyła duże nakłady finansowe na prowadzenie prac badawczych i rozwojowych związanych z elektronicznymi systemami bezpieczeństwa. Takie podejście zaowocowało wprowadzeniem na rynek konsumencki wielu nowych produktów. Innowacyjne technologie pozwoliły instalatorom, integratorom i użytkownikom systemów na uzyskanie namacalnych korzyści wynikających z uproszczenia codziennych czynności związanych z instalacją i obsługą systemów dozorowych

– *Wprowadzenie aplikacji iPOLiS MOBILE jest doskonałym przykładem innowacyjnego sposobu postrzegania rynku przez kadrę inżynieryjną zajmującą się projektowaniem nowych produktów, które pozwalają naszym klientom na możliwie najlepsze wykorzystanie rozwiązań firmy Samsung związanych z systemami dozorowymi* – powiedział Peter Ainsworth, Senior Product Manager w firmie Samsung Techwin Europe Ltd. – *Istnieje wiele sposobów wykorzystania tej aplikacji z korzyścią dla użytkowników. Może ona stanowić praktyczną pomoc, na przykład dla menadżerów odpowiedzialnych za bezpieczeństwo wielu obiektów, których z oczywistych przyczyn nie mogą oni nadzorować osobiście.*

Darmowa aplikacja iPOLiS MOBILE umożliwia zdalne przeglądanie materiału wizyjnego dostarczanego przez kamery sieciowe z rodziny iPOLiS na telefonach iPhone i smartfonach z systemem Android, takich jak Samsung Galaxy S. Aplikacje pozwalające użytkownikom na sterowanie funkcjami PTZ najnowszych kamer sieciowych firmy Samsung zainstalowanych w ich obiektach mogą być pobierane z portali iTunes i Android Market. Czynności związane z konfiguracją nie zajmują więcej niż kilkadziesiąt sekund, po czym możliwe jest przeglądanie strumieni wizyjnych z wybranych kamer za pośrednictwem bezprzewodowej sieci 3G.

W przyszłości wszystkie sieciowe kamery firmy Samsung należące do rodziny iPOLiS będą kompatybilne z tą aplikacją. Do kamer wyposażonych w najnowsze oprogramowanie, a tym samym kompatybilnych z iPOLiS, można zaliczyć najnowsze kamery o rozdzielczości HD, w tym modele realizujące funkcję PTZ.

Aplikacja iPOLiS MOBILE umożliwia także przeglądanie bieżących obrazów z kamer oraz sterowanie funkcjami PTZ za pośrednictwem cyfrowych rejestratorów wizyjnych z rodziny Samsung SRD.

Full HD – korzyści są wyraźnie widoczne

Technologia Full HD jest dziedziną, w której firma Samsung wykorzystała całe swoje doświadczenie techniczne. Firma wprowadziła na rynek kamery o rozdzielczości równej trzy megapiksele, kompatybilne z ONVIF, przystosowane do pracy w standardzie Full HD 1080p umożliwiającym uzyskanie obrazów o bardzo wysokiej jakości. Zarówno kamery stacjonarne, jak i kamery kopułowe wykorzystują procesor DSP typu WiseNet2 firmy Samsung Techwin, który daje użytkownikom możliwość skorzystania ze wszystkich zalet najnowszych kamer megapikselowych, między innymi z ich szerokiego zakresu dynamiki umożliwiającego prowadzenie obserwacji w trudnych warunkach oświetleniowych.

Fot. 2. Sieciowa, megapikselowa, wandaloodporna kamera kopułkowa typu SNV-7080R HD z wbudowanym oświetlaczem na diodach LED

Właściwie rozmieszczone kamery o rozdzielczości Full HD mogą zastąpić pięciokrotnie więcej standardowych kamer CCTV i mogą dostarczać obrazy o jakości dowodowej, które okażą się bezcenne w przypadku prowadzenia śledztwa o charakterze kryminalnym. Obrazy odznaczające się doskonałą jakością mogą być także przydatne dla organizacji dbających o bezpieczeństwo personelu oraz gości odwiedzających jakiś obiekt, zgodnie z ogólnie przyjętymi zasadami BHP. Ponadto mogą stanowić przydatne narzędzie w handlu detalicznym, gdzie osoby odpowiedzialne za ekspozycję towarów mogą wykorzystywać je do oceny zachowania klientów.

Banki, kasyna, centra handlu detalicznego, zakłady produkcyjne, ruchliwe obszary miejskie, lotniska, stacje kolejowe stanowią zaledwie część środowisk, w których nadzwyczajna jakość obrazów dostarczanych przez kamery sieciowe pracujące w standardzie Full HD spowoduje, że działanie wizyjnych systemów dozorowych zaskoczy nawet najbardziej wymagających użytkowników.

Wszystkie modele kamer są zdolne do wytwarzania obrazów o rozdzielczościach od CIF (352×288), poprzez Full HD (1920×1080p) o proporcjach 16:9, do trzech megapikseli (2048×1536). Wszystkie modele mogą pracować w trybie dwustrumieniowym, z wykorzystaniem kompresji metodą H.264 i MJPEG. Tak więc te same kamery mogą być jednocześnie wykorzystane do monitoringu prowadzonego w czasie rzeczywistym, monitoringu mobilnego, rejestracji obrazów z zachowaniem wysokiej jakości lub wysokiej wydajności zapisu, rejestracji na kartach pamięci SD oraz do wysyłania powiadomień pocztą elektroniczną.

Ponadto opracowana przez firmę Samsung technologia kompresji Smart Codec pozwala na przechwytywanie obrazów z wyróżnionego, szczególnie istotnego fragmentu

Fot. 3. Sieciowe rozwiązania Samsunga

obserwowanej sceny z wyższą rozdzielczością niż z pozostałej części tej sceny. Oznacza to, że takie obszary jak drzwi wejściowe, okna, miejsca, w których są wyraźnie widoczne ludzkie twarze, mogą być obserwowane z wyższą rozdzielczością, zaś rozdzielczość pozostałej części obrazu może być zredukowana. Pozwala to na zmniejszenie objętości zapisywanych plików oraz na lepsze wykorzystanie dostępnego pasma sieciowego.

Technologia HD-SDI oferuje możliwość wyboru

Ze względu na rosnące wymagania użytkowników systemów dozorowych problem przechwytywania obrazów o rozdzielczości HD i większej nabrał dużego znaczenia. Dotychczas wysoka rozdzielczość obrazów była jednoznacznie przypisywana systemom wykorzystującym sieci IP, których tworzenie wymagało specjalistycznej wiedzy i było związane ze znacznymi kosztami w związku okablowaniem sieciowym i zastosowaniem urządzeń takich jak przełączniki sieciowe i serwery. Wprowadzenie technologii HD-SDI umożliwiło transmisję i rejestrację obrazów o rozdzielczości Full HD (1080p) z wykorzystaniem istniejącej infrastruktury analogowej, pozwalając użytkownikom czerpać korzyści wynikające z wysokiej rozdzielczości obrazów bez konieczności ponoszenia dodatkowych kosztów.

Fot. 4. Czytnik typu SSA-S3010 pracujący w systemie kontroli dostępu

Interfejs HD-SDI (*High Definition Serial Digital Interface*) stanowi standardowe wyposażenie w profesjonalnym, studyjnym sprzęcie telewizyjnym i służy do cyfrowej transmisji obrazów o wysokiej rozdzielczości w obrębie studia telewizyjnego. Interfejs pozwala transmitować sygnały wizyjne, które nie są skompresowane i podzielone na pakiety, przez co nie tracą na jakości i nie podlegają opóźnieniom podczas transmisji.

Proponowane przez firmę Samsung rozwiązania oparte na technologii HD-SDI zapewniają pięciokrotnie wyższą jakość obrazu w porównaniu z konwencjonalnymi systemami analogowymi i można je zastosować zamiast rozwiązań sieciowych, co jest łatwiejsze i tańsze.

Opracowane przez firmę Samsung kamery wykorzystujące technologię HD-SDI mogą dostarczać obrazy o rozdzielczości Full HD 1080p (1920×1080) w czasie rzeczywistym, z prędkością 25 obrazów na sekundę. Są to obrazy o rozdzielczości pięciokrotnie większej od tej, którą mogą osiągać najlepsze standardowe kamery analogowe. Wykorzystujące technologię HD-SDI cyfrowe rejestratory wizyjne firmy Samsung pozwalają na rejestrację obrazów o rozdzielczości HD 720p w czasie rzeczywistym, na wszystkich kanałach wejściowych, i jednoczesny podgląd zarejestrowanego materiału wizyjnego w rozdzielczości 720p.

Brak utraty jakości obrazu i opóźnień w transmisji

Ze względu na to, że sygnały wizyjne transmitowane z wykorzystaniem technologii HD-SDI nie są skompresowane i podzielone na pakiety, nie występują żadne przekłamania w treści obrazów ani żadne opóźnienia w ich transmisji. To oznacza, że użytkownicy mogą cieszyć oko obrazami o rozdzielczości Full HD 1080p i zerowym opóźnieniu. Ze względu na to, że w standardzie HD-SDI wykorzystywana jest cyfrowa transmisja sygnałów, z natury nieczuła na zakłócenia i na zjawisko tłumienia sygnału w kablach transmisyjnych, które jest typowe dla telewizji analogowej, obrazy nie podlegają nawet najmniejszym deformacjom.

Oparte na technologii HD-SDI systemy bezpieczeństwa firmy Samsung wykorzystują analogową infrastrukturę kablową, przez co stają się przydatne dla użytkowników pragnących poprawić jakość obrazów z zachowaniem istniejącego analogowego okablowania telewizyjnego lub dla użytkowników, którzy nie chcą instalować infrastruktury sieciowej w nowo budowanych obiektach. Ponadto pracujące w technologii HD-SDI kamery i cyfrowe rejestratory wizyjne firmy Samsung wykazują podobieństwo do standardowych kamer i rejestratorów analogowych. Dotyczy to zarówno ich instalacji, jak i obsługi, do której nie potrzeba żadnej specjalistycznej wiedzy ani wyjątkowych umiejętności.

Dostęp do w pełni zintegrowanych rozwiązań

Ze względu na to, że użytkownicy końcowi dążą do uzyskania możliwie największych korzyści z zainwestowanych środków finansowych, od każdego systemu kontroli dostępu oczekuje się, że będzie on interaktywnie współdziałał z innymi systemami bezpieczeństwa. Dominującym trendem jest powiązanie działania systemu kontroli dostępu z działaniem systemu monitoringu wizyjnego. Możliwość przepływu informacji

Fot. 5. Oprogramowanie sieciowe Samsung Net-i Viewer

pomiędzy tymi systemami wpływa korzystnie na ich cechy użytkowe. Poza oczywistą możliwością wizualnej weryfikacji tożsamości osób próbujących przedostać się do wnętrza chronionych obszarów można także uzyskać informacje umożliwiające kontrolę obecności, czasu pracy i inne działania dyscyplinujące pracowników.

By informacje dostarczane przez system monitoringu wizyjnego i system kontroli dostępu mogły być wiarygodne dla użytkowników końcowych, oba te systemy powinny harmonijnie współpracować. To oczywiste, że wydarzenia rejestrowane przez system kontroli dostępu powinny być zsynchronizowane z odpowiednimi fragmentami materiałów wizyjnych. Jak dotychczas nie wymyślono taniej metody realizacji tego celu.

Są już jednak pewne dobre wieści dla użytkowników, którym marzy się lepsze wykorzystanie systemów bezpieczeństwa. Obecnie firma Samsung – w ramach powiązania systemów kontroli dostępu i systemów wizyjnych wykorzystujących rejestratory SRD – oferuje już standardowo takie funkcje jak synchronizacja czasowa wydarzeń, rozpoznawanie linii papilarnych i możliwość zastosowania kart zbliżeniowych chronionych kodem PIN. Możliwe jest także podłączenie tych systemów do sieci IP z wykorzystaniem sieciowego enkodera z wbudowaną kartą pamięci SD, na której zapisywane są obrazy zsynchronizowane z próbami przekroczenia granic chronionych obszarów z użyciem ważnych lub nieważnych kart identyfikacyjnych, dzięki czemu użytkownicy zyskują możliwość przeglądania materiałów wizyjnych za pośrednictwem sieci. Ta łatwa do implementacji i użyteczna funkcja stwarza integratorom i instalatorom systemów okazję do zwrotu kosztów inwestycji, oferując możliwość tworzenia materiałów dowodowych o wysokiej jakości, w postaci danych pochodzących z systemu kontroli dostępu i powiązanych z danymi pochodzącymi z systemu monitoringu wizyjnego.

Fot. 6. Kompaktowa kamera typu SNO-5080R o rozdzielczości 1,3 megapiksela, odporna na czynniki klimatyczne

Oprogramowanie zarządzające pracą systemów kontroli dostępu

Systemy kontroli dostępu opracowane przez firmę Samsung służą do ochrony maksymalnie 128 tysięcy przejść, przy czym możliwy jest wybór rodzaju czytników. Można zastosować czytniki kart zbliżeniowych chronione kodem PIN, a także czytniki biometryczne, które reagują na kształt linii papilarnych. Wspomniane systemy mogą realizować funkcje kontroli obecności i rejestracji czasu pracy. Imponującą cechą czytników biometrycznych firmy Samsung jest możliwość zapamiętywania czterech tysięcy wzorów linii papilarnych z zachowaniem czasu odczytu na poziomie pół sekundy.

Oferowane są zarówno samodzielne kontrolery obsługujące pojedyncze przejścia, jak i urządzenia sieciowe, które umożliwiają tworzenie systemów chroniących wiele przejść. W przypadku zastosowania urządzeń sieciowych możliwe jest przekazywanie danych biometrycznych pomiędzy poszczególnymi kontrolerami bez konieczności stosowania komputera i specjalistycznego oprogramowania.

Dużym wyzwaniem jest przekonanie użytkowników o tym, że będą mieli pełną kontrolę nad złożonym systemem i będą mogli gromadzić, rejestrować i odtwarzać wiarygodne dane, które mogą okazać się niezbędne podczas postępowania dowodowego zmierzającego do ukarania nieproszonych gości, którzy dopuścili się działań o charakterze kryminalnym. Dobrą wiadomością jest to, że oprogramowanie Samsung Access Management Software (SAMS) umożliwia tworzenie szczegółowych raportów dotyczących aktywności poszczególnych użytkowników kart identyfikacyjnych. Raporty mogą mieć postać plików XLS lub PDF, przez co możliwa jest integracja z innymi pakietami programowymi, takimi jak Time & Attendance, ERP lub Payroll. Profesjonalna wersja SAMS Pro działa w podobny sposób, jednak realizuje pewne funkcje dodatkowe, w tym integrację systemów kontroli dostępu z systemami monitoringu wizyjnego. Umożliwia to operatorom systemów przeglądanie materiałów wizyjnych związanych z momentami wykorzystania kart identyfikacyjnych oraz ocenę aktywności ich posiadaczy. Stan czytników i kamer może być także monitorowany na specjalnej mapie zdefiniowanej przez użytkownika. Kolejną dobrą wiadomością jest to, że w przypadku systemów kontroli dostępu zintegrowanych z systemem monitoringu wizyjnego, które obsługują nie więcej niż 40 przejść i nie więcej niż 1000 użytkowników, dostępna jest bezpłatna wersja oprogramowania SAMS.

James Smith
Samsung Techwin Europe
Tłumaczenie: Redakcja

Hemisferyczna technologia monitoringu wizyjnego

Linc Polska

W swojej książce pt. *The Innovator's Technology* prof. Clayton Christensen (pracownik Harvard Business School) wprowadza określenie *disruptive technology*. Termin ten oznacza szczególnie innowacyjną, przełomową technologię – taką, która zmienia panujący *status quo*. Postęp uzyskany dzięki tej technologii znacznie przekracza naturalne tempo rozwoju uzyskiwane dzięki innym odkryciom. Tego typu innowacje można więc określić jako szczególnie błyskotliwe i istotne. Przyczyniają się one do tworzenia nowych produktów i nowych gałęzi rynku. W przypadku pojawienia się *disruptive technology* zmiany na rynku zachodzą spontanicznie, a nie na skutek badania oczekiwań konsumentów. Rynki, które dotychczas nie istniały, nie mogły zostać zbadane i przeanalizowane. W takim przypadku trudno cokolwiek zaplanować lub założyć. Wszystko to sprawia, że przełomowe technologie są tak nadzwyczajne i powodują gwałtowny rozwój w wielu nowych dziedzinach. Kamery hemisferyczne są właśnie takim przykładem

Rys. 1. Logika w kamerze: nagrywanie, zarządzanie, powiadamianie, wbudowany mikrofon i głośnik

Mimo iż technologia, którą wykorzystują kamery IP, nie jest przełomowa, w przypadku kamer hemisferycznych można już mówić o przełomie. Zapoczątkowały one ogromną zmianę w podejściu do projektowania i instalowania systemów nadzoru wizyjnego. Dzięki innowacyjnej technologii jedna kamera hemisferyczna może zastąpić 3 – 4 standardowe kamery wykorzystywane w systemach CCTV.

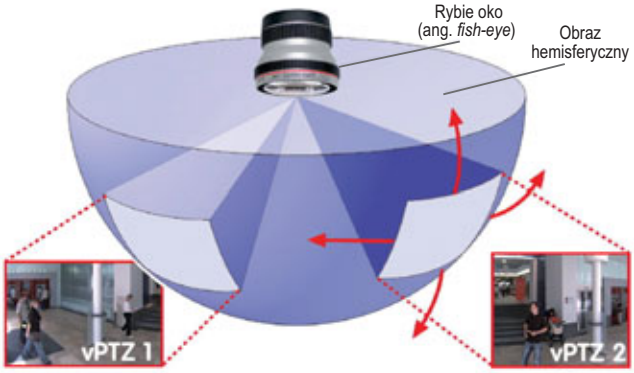
Kamera wykorzystująca technologię hemisferyczną może nagrywać i przechowywać nieskompresowane lub skompresowane obrazy na wewnętrznej pamięci kamery albo na dołączonej do kamery pamięci zewnętrznej. Dzięki temu sieć nie jest obciążana strumieniami wizyjnymi przeznaczonymi do rejestracji. Jeśli potrzebna jest pamięć o większej pojemności, można skorzystać z jednostek NAS (ang. *Network Attached Storage*), np. firmy Netgear, lub zewnętrznego serwera plików. Pozwala to obniżyć koszty związane z zakupem dedykowanego serwera do rejestracji obrazów oraz oprogramowania niezbędnego do rejestracji sekwencji wizyjnych na serwerze. Wszystkie operacje związane z korekcją obrazu są przeprowadzane w kamerze, a nie w komputerze, bowiem sama kamera jest już małym komputerem, który wykorzystuje system operacyjny Linux.

Większość dostępnych na rynku kamer nazywanych hemisferycznymi nie działa jednak w opisany wyżej sposób. Pojawia się pewien problem: w jaki sposób zarejestrować cały obraz, a następnie przesłać go przez sieć IP, zachowując wysokie parametry? Większość tego typu kamer obsługiwana jest przez komputery, do których są podłączone. To właśnie komputery są odpowiedzialne za wszystkie operacje związane z obróbką sygnału wizyjnego. Niesie to jednak za sobą konieczność przesłania przez sieć całego nieskompresowanego strumienia wizyjnego, który powoduje bardzo duże obciążenie sieci, a także bardzo duże obciążenie procesora w komputerze. W takim przypadku niemożliwe staje się podłączenie większej liczby kamer hemisferycznych do jednej jednostki centralnej. W przypadku wielu kamer liczba operacji związanych z korekcją zniekształceń obrazu jest zbyt duża, aby mógł poradzić sobie z nią jeden komputer. Warto też uświadomić sobie, że w przypadku takich kamer dla nieskompresowanej sekwencji o rozdzielczości 3 Mpx i prędkości nagrywania 12 klatek na sekundę wymagane pasmo sieciowe wynosi około 1 Gb/s. Nawet w przypadku zmniejszenia liczby klatek taki transfer przez sieć Ethernet jest zupełnie nieopłacalny. Jedynym rozwiązaniem jest zatem znaczne obniżenie rozdzielczości obrazu, dokonanie jego stratnej kompresji, np. z wykorzystaniem H.264, a następnie przesłanie go do serwera nagrywającego, który przeprowadzi ponowną analizę obrazu i dokona korekcji zniekształceń geometrycznych. Ze względu na niską jakość otrzymanego obrazu możliwości wykorzystania cyfrowych funkcji PTZ są bardzo ograniczone. Rozróżnialność szczegółów powstałego w ten sposób obrazu nie jest zadowalająca.

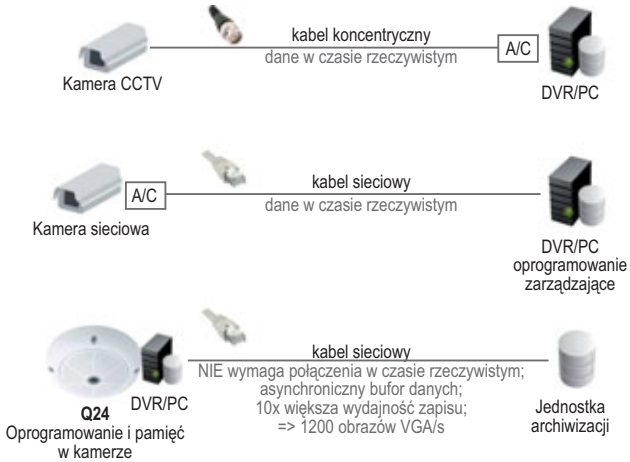
Przykładowo kamera hemisferyczna firmy Mobotix posiada układ logiczny znajdujący się w jej wnętrzu. Oprócz typowego procesora DSP (ang. *Digital Signal Processor*) w kamerze znajduje się także wbudowany mikrokontroler o architekturze ARM (ang. *Advanced RISC Machine*), która oferuje dużą moc obliczeniową przy małym zapotrzebowaniu na energię. Duża moc obliczeniowa procesorów ARM umożliwia wykorzystanie systemu operacyjnego z zaimplementowanymi mechanizmami wielowątkowości. Można wykorzystać wielowarstwową strukturę sieciową TCP/IP oraz odpowiedni system plików (np. FAT32).

Rys. 2. Megapikselowy widok od ściany do ściany (panorama180°)

Dzięki takiej budowie kamera staje się jednostką centralną na wzór komputera, która może dodatkowo sama przeprowadzać wszystkie operacje logiczne, morfologiczne oraz związane z korekcją zniekształceń geome-



Rys. 3. Technologia hemisferyczna, wirtualny PTZ



Rys. 4. Przeniesienie logiki do kamery hemisferycznej

trycznych obrazu. Cały obraz jest rejestrowany w pamięci wewnętrznej kamery – na karcie microSD o pojemności dochodzącej do 32 GB. Dzięki temu nie ma konieczności przesyłania całego strumienia wizyjnego przez sieć. Do komputera, do którego może być podłączona kamera, przesyłane są jedynie wybrane fragmenty obrazu lub pełen obraz panoramiczny po już dokonanej korekcji zniekształceń geometrycznych.

Oczywiście takie przeniesienie wszystkich działań związanych z obróbką obrazu do procesora sygnałowego (DSP) wbudowanego w kamerę odciąża procesor komputera. Dzięki temu jeden komputer może wyświetlać sekwencje z wielu kamer hemisferycznych.

Nie jest to jednak jedyna zaleta opisywanej kamery. Obsługa zdarzeń, na przykład wykrywanie incydentów na podstawie detekcji ruchu, także odbywa się w kamerze. Oczywiście wszystko to dzięki wbudowanemu DSP. Wysoka rozdzielczość dostarczanego obrazu umożliwia także użycie funkcji elektronicznego PTZ pozwalającej na płynne przeglądanie fragmentów obrazu hemisferycznego. Kamera oferuje także funkcje VOIP dzięki obsłudze protokołu VoIP/SIP – dwukierunkowej transmisji dźwięku. Ponadto wykorzystuje obiektyw typu rybie oko (ang. *fish-eye*).

Dzięki odpowiedniej architekturze kamer hemisferycznych można wykorzystać wszystkie ich zalety, w tym skorzystać z możliwości wytwarzania obrazów o wysokiej jakości. Kamery hemisferyczne są coraz bardziej popularne, gdyż zastąpienie czterech tradycyjnych kamer i rejestratora DVR jedną kamerą hemisferyczną ogranicza koszty. Co więcej, dostęp do obrazu z kamer za pośrednictwem urządzeń mobilnych (smartfonów, tabletów itp.) jest tym, czego obecnie oczekują użytkownicy.

Kluczową kwestię stanowi decentralizacja, czyli podział obciążenia przetwarzaniem danych, które przypadnie kamerze i komputerowi z oprogramowaniem zarządzającym. Dzięki ulokowaniu większej „inteligencji" w kamerze (przetwarzanie obrazu, zarządzanie rejestracją, detekcja ruchu itp.) wymagania dotyczące przepustowości sieci i zasobów sprzętowych są mniejsze. Dzięki temu na jednym komputerze można zapisać obraz z dużo większej liczby kamer. Ponadto buforowanie danych wizyjnych w kamerze zabezpiecza przed przerwami w transmisji danych.

Linc Polska

ULISSE RANGE

ZINTEGROWANE SYSTEMY POZYCJONUJĄCE

Dozór wizyjny w warunkach dziennych i nocnych ze sterowaniem analogowym lub sieciowym.

www.videotec.com

VIDEOTEC

Kamera stworzona z myślą o profesjonalistach

Jan T. Grusznic

Świadectwem klasy profesjonalisty jest jakość wykonywanych usług. Niska spowoduje utratę wiarygodności, wysoka zaowocuje rekomendacją u kolejnych zleceniodawców. Na ocenę wpływa jakość i parametry zastosowanych urządzeń. W dziedzinie systemów dozoru wizyjnego, gdzie subiektywna ocena obrazu jest ważniejsza od obiektywnej oceny możliwości użytej technologii, niedociągnięcia mogą kosztować utratę renomy. Chroniąc dobre imię profesjonalisty, darzone zaufaniem rozwiązania Boscha umożliwiają uzyskanie obrazów o wysokiej jakości, a także oferują wiele funkcji użytkowych

Automatyczna ostrość

Ostrość obrazu jest piętą achillesową instalacji CCTV. Źle lub niedbale ustawiona, znacznie zmniejsza postrzeganą rozdzielczość obrazu, a co za tym idzie możliwość rozpoznania obserwowanych osób lub obiektów. Wraz ze wzrostem rozdzielczości kamer problem narasta. Wynika to z braku odpowiednich narzędzi programowych w kamerach, które ułatwiałyby optymalne ustawienie punktu ostrości w dzień i w nocy. Rozwiązanie Lens Wizard jest kreatorem regulacji obiektywu w kamerach Dinion, który od lat pomaga w uzyskaniu wysokiej jakości obrazu. Doceniony przez profesjonalistów, doczekał się automatyzacji w kamerach NBN-832V-IP. Zastosowanie precyzyjnego mechanizmu regulującego położenie przetwornika względem zainstalowanego obiektywu zapewnia ustawienie ostrego obrazu zdalnie, za pomocą jednego przycisku w przeglądarce. Takie rozwiązanie niebywale przyspiesza instalację punktu kamerowego i umożliwia perfekcyjne ustawienie ostrości (oczywiście w przypadku zastosowania obiektywów o wysokiej rozdzielczości). Na uwagę zasługuje to, że poziom ostrości można ustawić oddzielnie dla warunków dziennych i nocnych na wypadek zastosowania obiektywu bez odpowiedniej korekcji chromatycznej. W przypadku wykorzystania obiektywów IR poziom ustawienia określany jest łącznie.

Analogowa czułość

Zwiększenie rozdzielczości kamery oznacza umiejscowienie większej liczby elementów światłoczułych w przetworniku obrazowym o określonych rozmiarach, co prowadzi do zmniejszenia aktywnej powierzchni pojedynczego fotoelementu. Wytworzenie obrazu HD (liczba aktywnych pikseli: 1920×1080) o nasyceniu porównywalnym z obrazem z przetwornika kamery PAL 1/3" (liczba aktywnych pikseli: 752×582) wymaga na ogół około pięciokrotnie silniejszego oświetlenia przetwornika. Przekłada się to na jeszcze silniejsze oświetlenie sceny[1], a w konsekwencji zwiększa koszty instalacji i eksploatacji punktu kamerowego. Co prawda niższą czułość kamer można próbować kompensować przez wzmocnienie sygnału, jednak powoduje to pogorszenie stosunku sygnału do szumu. To z kolei znacznie obniża jakość uzyskiwanego obrazu, na co nie godzą się profesjonaliści. Taki stan rzeczy spowodowany jest przez zachowanie tradycyjnych rozmiarów przetworników, znanych z rozwiązań analogowych – większy przetwornik pozwala na wygenerowanie obrazu o dobrej jakości przy słabszym oświetleniu. Tworząc technologię Dinion HD 1080p, wykorzystaliśmy przetworniki CMOS o wielkości 1/2,7", co umożliwia obserwację także słabiej oświetlonych scen. Czułość kamer NBN-832V-IP (na poziomie 0,22 lx dla trybu kolorowego i 0,05 lx dla trybu czarno-białego[2]) jest porównywalna z czułością kamer analogowych z przetwornikami CCD o wielkości 1/3".

Bezpieczeństwo zapisu

Dodatkowe funkcje, jakimi dysponuje kamera NBN-832V-IP, umożliwiają zapis materiału wizyjnego bez udziału serwera, co może być zrealizowane na kilka sposobów. Pierwszy z nich to bezpośredni zapis na macierzach dyskowych, do którego nie jest potrzebny dodatkowy serwer, co ogranicza koszty związane z utrzymaniem zapisanego materiału pochodzącego z kamer o wysokiej rozdzielczości. Harmonogram zapisu oraz parametry strumienia zapisywanych danych są ustalane bezpośrednio w kamerze, która samoistnie inicjuje proces rejestracji na dyskach sieciowych. Drugi z tych sposobów to lokalny zapis na karcie microSD XC (pojemność do 2 TB), która umieszczana jest bezpośrednio w kamerze. Zapis na karcie jest traktowany w identyczny sposób jak zapis na dyskach zewnętrznych i jest w pełni kompatybilny z dostępnym oprogramowaniem Boscha do zarządzania obrazem o rozdzielczości HD.

Połączenie tych dwóch rozwiązań – zapisu na macierzy i zapisu na karcie microSD – wprowadza dodatkową funkcję, jaką jest zapis redundantny. W przypadku awarii łącza służącego do transmisji danych pomiędzy kamerą a macierzą użycie lokalnej pamięci zapewni ciągłość rejestracji obrazu. Gdy dodatkowo procesem zapisu zarządza system *Video Recording Manager*, dane z karty zostają automatycznie przekopiowane do pamięci centralnej dzięki opatentowanej technologii ANR (ang. *Automatic Network Replenishment*).

Inteligentna Analiza Obrazu – dodatkowa para oczu

Precyzyjny i wydajny system Bosch IVA (ang. *Intelligent Video Analysis*) jest zaimplementowany niezależnie w każdej z kamer NBN-832V-IP. System ten jest dostosowany do rozwiązań HD i realizuje swoje funkcje bez wykorzystania centralnej,

1) Niższy współczynnik odbicia światła przez obserwowaną scenę determinuje większy stopień jej oświetlenia do uzyskania minimum światła docierającego do przetwornika. Jeżeli uzyskanie obrazu o optymalnym nasyceniu wymaga 1 lx światła docierającego do przetwornika, a poziom absorpcji sceny jest równy 80% (np. na parkingu z trawnikiem i drzewami), to minimalny poziom oświetlenia sceny wyniesie 5 lx (1 lx /1-0,8).

2) 30 IRE, współczynnik odbicia sceny 89%, temperatura barwowa 3200 K, przesłona F/1.2

analitycznej jednostki komputerowej. Dzięki dokonywaniu wielopoziomowej analizy danych z poszczególnych pikseli oraz analizy tekstury i ruchu w obrazie wewnątrz kamery, umożliwia śledzenie trajektorii (prędkości i kierunku) ruchu wszystkich obiektów i może wykryć obiekty ruchome, nieruchome oraz przekraczające granice chronionego obszaru. Technologia Bosch IVA w kamerach Dinion HD 1080p pomaga użytkownikowi szybko zareagować na podejrzane działania lub potencjalne zagrożenia. Każda kamera NBN-832V-IP pracująca w systemie monitoringu staje się aktywnym wirtualnym agentem ochrony, który identyfikuje zdarzenie w momencie jego zaistnienia, oraz powiadamia użytkownika o wykryciu zdarzenia o charakterze krytycznym przez wysłanie wiadomości alarmowej.

Mimo iż Bosch IVA jest bardzo nowoczesnym rozwiązaniem, jego wdrożenie, konfiguracja oraz wykorzystanie nie sprawiają trudności profesjonalistom. Precyzyjne dostosowanie obszarów detekcji do miejsc o charakterze krytycznym, analiza kształtów i sposobów poruszania się obiektów oraz obsługa urządzeń przez intuicyjny interfejs graficzny umożliwiają szybkie i precyzyjne dostosowanie systemu do indywidualnych potrzeb klienta. Wykorzystanie inteligencji rozproszonej (ang. *distributed intelligence*) w technologii Bosch IVA pozwala na stworzenie systemu, który nie zawiera centralnego serwera, a zatem wyeliminowany zostaje jeden z najbardziej krytycznych składników stanowiących potencjalne źródło awarii. IVA działa niezależnie w każdej kamerze NBN-832V-IP.

Przeszukaj archiwum w czasie krótszym niż dziesięć sekund

Jako integralne rozwiązanie systemowe IVA umożliwia gromadzenie szczegółowych informacji o monitorowanych miejscach, dzięki czemu można szybko wyszukać dowolne zdarzenia – nawet te, które we wcześniejszym procesie konfiguracji systemu nie zostały uznane za alarmowe. Dane wynikające z analizy treści obrazów są generowane i przechowywane razem z tymi obrazami w formie metadanych. Zawierają one szczegółowe informacje na temat wszystkich obiektów znajdujących się w obrębie monitorowanych obszarów i pojawiających się na nich lub je opuszczających. Analiza nie kończy się na obserwacji w czasie rzeczywistym – Bosch IVA może rozpoznawać zdarzenia także podczas odtwarzania nagrań. Zapisane metadane, które zawierają proste ciągi tekstowe opisujące określone szczegóły obrazu, zajmują o wiele mniej pamięci i są łatwiejsze do przeszukiwania niż zapisane obrazy. Podczas przeszukiwania metadanych za pomocą odpowiednich narzędzi, takich jak wyszukiwarki internetowe, IVA pozwala na szybkie odnalezienie odpowiedniego materiału wizyjnego bez konieczności ręcznego przeszukiwania całego archiwum.

Co dzieje się, gdy na monitorowanym obszarze ma miejsce zdarzenie, którego administrator systemu nie brał pod uwagę przy konfiguracji alarmu? Metoda wyszukiwania oferowana przez system Bosch IVA jest wyjątkowa, gdyż umożliwia przeglądanie archiwalnych obrazów z wykorzystaniem nowych kryteriów wykrywania zdarzeń. Dzięki temu można wyszukiwać zdarzenia inne niż te, które zostały wykryte podczas podglądu na żywo. Na przykład można skonfigurować system tak, aby wykrył pozostawiony obiekt podczas przeszukiwania archiwalnych obrazów, nawet jeśli system nie był wcześniej przygotowany do wykrywania tego typu zdarzeń.

Przejrzenie dziewięciogodzinnego nagrania w celu wykrycia określonego zdarzenia w normalnych warunkach zajmuje na ogół trzy godziny. Z wykorzystaniem IVA – zaledwie cztery minuty[3].

HD Boscha dla profesjonalistów

Silna pozycja rynkowa rozwiązań HD spowodowała, że większość dotychczasowych rozwiązań bazujących na kamerych megapikselowych została dostosowana do tego standardu. Dlatego też nowe produkty firmy Bosch są kompatybilne ze standardem HD.

Jan T. Grusznic
Bosch Security Systems

3) http://video.boschsecurity.com/search?title=Forensic+Search

Fot 1. Dualna kamera sieciowa Dinion HD 1080p

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Nowe rejestratory cyfrowe z serii E

Wyświetlanie plików reklamowych

Niezależne wyświetlanie na dwóch monitorach głównych

(np. „na żywo" i odtwarzanie lub „na żywo" i reklama)

Obsługa rejestratora z poziomu telefonu komórkowego

(np. podgląd „na żywo" i odtwarzanie obrazu z kamer, konfiguracja rejestratora, sterowanie PTZ i wyjściami alarmowymi)

Android Compatible

iPhone Compatible

E seria

E-Viewer Compatible

NOVUS 3 lata gwarancji teraz

NDR-EA2104
- Wejścia wideo: 4 x BNC
- Prędkość nagrywania do 100 kl/s
- Możliwość rejestrowania do 4 kanałów audio

NDR-EA2208
- Wejścia wideo: 8 x BNC
- Prędkość nagrywania do 200 kl/s
- Możliwość rejestrowania do 8 kanałów audio

NDR-EA2416
- Wejścia wideo: 16 x BNC
- Prędkość nagrywania do 400 kl/s
- Możliwość rejestrowania do 8 kanałów audio

▪ Pentapleks ▪ Kompresja H.264 ▪ Nagrywanie real-time ▪ Rozdzielczość nagrywania: 704 x 576, 704 x 288, 352 x 288 ▪ Funkcje przed-alarmu i po-alarmu
▪ Przechwytywanie danych tekstowych ▪ Praca w sieci komputerowej ▪ Menu w języku polskim ▪ Zasilanie: 12 VDC (zasilacz sieciowy w zestawie)

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

Chomguard Security

pakiet przeznaczony do zarządzania systemami technicznych zabezpieczeń obiektu

Tomasz Krawczyk

Obecnie rynek systemów do zarządzania bezpieczeństwem i automatyką budynku oferuje szereg rozwiązań czołowych światowych producentów (m.in. Siemens, Honeywell, TAC, Delta Controls itp.). Systemy te najczęściej są efektem doświadczeń zdobytych podczas projektowania systemów automatyki budynkowej (BMS – *Building Management System*), dlatego inwestorzy szukający specjalistycznych rozwiązań o mniejszym stopniu skomplikowania potrzebują oprogramowania, które będzie niezależnie od automatyki obiektu zarządzać technicznymi zabezpieczeniami w sposób intuicyjny i skuteczny. Takim właśnie produktem jest pakiet Chomguard Security

Charakterystyka programu

Chomguard Security jest najnowszej generacji specjalistycznym oprogramowaniem o architekturze modułowej, przeznaczonym do zarządzania bezpieczeństwem i automatyczną identyfikacją w dowolnej wielkości obiekcie lub na obszarze podlegającym ochronie. System jest odpowiedzialny za sterowanie, monitorowanie i wizualizację oraz zbieranie i zapis danych z systemów: telewizji dozorowej, kontroli dostępu, sygnalizacji włamania i napadu, sygnalizacji pożarowej, obsługi gości, drukowania identyfikatorów i zarządzania systemem kluczy, a także innych podsystemów działających na rzecz bezpieczeństwa obiektu.

Program integruje powyższe podsystemy w jednej spójnej i czytelnej dla użytkownika aplikacji. Zastosowanie jednego interfejsu dla tak wielu różnych podsystemów pozwala bardzo skutecznie zarządzać bezpieczeństwem, zapewniając użytkownikowi komfort pracy i bardzo szybki dostęp do każdej informacji o pracy systemu.

Dzięki takiemu rozwiązaniu inwestor otrzymuje pełne wsparcie od jednego dostawcy (posiadającego autoryzację producenta). Nie jest więc narażony na znaczne koszty wdrożenia każdego systemu osobno i żmudne szkolenia pracowników w zakresie obsługi zupełnie różnych od siebie i bardzo często mało intuicyjnych aplikacji.

Chomguard Security należy do klasy systemów, które pozwalają na swobodne definiowanie wielu stacji i poziomów pracy operatorów, gdy zachodzi potrzeba pracy rozproszonej. Pakiet łączy stabilność typową dla systemów z górnej półki z elastycznością produktów szytych na miarę. Aplikacja pracuje na platformach Windows i Linux.

Chomguard Security jest programem polskim, napisanym przez grupę informatyków i skonsultowanym ze specjalistami

Fot. 1. Widok menu głównego wizualizacji

Fot. 2. Widok okna do personalizacji identyfikatorów

ze służb mundurowych i z ekspertami z branży zabezpieczeń technicznych i ochrony mienia.

Architektura programu

Chomguard Security wykorzystuje najnowocześniejszą architekturę bazodanową i sprawdzone rozwiązania SQL i Oracle. Struktura systemu ma charakter otwarty i umożliwia korzystanie z dowolnego modułu, który jest w danej chwili potrzebny użytkownikowi (np. modułu kontroli dostępu), wraz z wymaganymi urządzeniami. Rozbudowa systemu o kolejne podsystemy na poziomie oprogramowania wiąże się tylko z instalacją kolejnych modułów aplikacji.

Chomguard Security pozwala na pracę z wykorzystaniem przeglądarki internetowej z kryptograficznym zabezpieczeniem transmisji – na takim poziomie jak w przypadku transakcji bankowych dokonywanych w Internecie. Komunikacja z urządzeniami oraz innymi systemami współdziałającymi jest możliwa za pośrednictwem sieci Ethernet 10/100/1000 Mb/s, portu szeregowego RS232 (systemy sygnalizacji pożarowej) lub RS422/485 oraz portu USB (np. w przypadku drukarek identyfikatorów czy czytników dowodów osobistych).

Do serwera systemu Chomguard można logować się jednocześnie w wielu miejscach sieci. Uwzględniana jest przy tym priorytetyzacja pracy według wcześniej zdefiniowanych uprawnień operatorów lub stanowisk. Dzięki temu jeden system może zarządzać wieloma lokalizacjami, do których dostęp mają wybrani operatorzy oraz stanowisko nadrzędne, z którego można zarządzać całym systemem.

Interfejs użytkownika

Interfejs użytkownika umożliwia sterowanie funkcjami systemu. Wymaga podania hasła i nazwy w celu identyfikacji. Gdy użytkownik zaloguje się do systemu, pakiet sprawdza jego uprawnienia i umożliwia mu wykorzystanie tylko wcześniej zdefiniowanych funkcji. Każda modyfikacja funkcji programu,

np. uprawnień, jest rejestrowana w bazie danych, co umożliwia administratorowi systemu sprawdzenie historii zmian funkcji według daty, rodzaju modyfikacji i użytkownika oraz wygenerowanie dotyczącego ich raportu. W praktyce pozwala to na dokładne zweryfikowanie działań użytkownika aplikacji i udowodnienie np. działań zabronionych.

Chomguard Security umożliwia operatorowi ograniczenie dostępu do wybranych danych. Można definiować wygląd danego okna lub skorzystać z możliwości pracy aplikacji na wielu monitorach jednocześnie, co daje operatorowi możliwość podziału ekranów monitorów do obserwacji każdej warstwy oddzielnie. Ograniczenia te ustanawia administrator systemu.

Interaktywna wizualizacja

Podstawową funkcją pakietu, która umożliwia zarządzanie bezpieczeństwem obiektu, jest wizualizacja zdarzeń. Aplikacja Chomguard Security pokazuje zdarzenia na monitorze komputera w czasie rzeczywistym i podejmuje zdefiniowane przez użytkownika akcje, odtwarza nagrane informacje o zdarzeniu, wyświetla informację graficzną (dynamicznie zmieniające się ikony oraz szczegółową informację o alarmie wraz z procedurami postępowania w osobnym oknie).

Program monitoruje szybkość reakcji użytkownika na zdarzenie alarmowe i w przypadku przedłużającego się braku reakcji może przesłać informację o alarmie do innych jednostek. W systemie rozróżniane są różne typy zdarzeń: od podstawowych (technicznych) o stanie urządzeń, poprzez informacje robocze o aktualnie wykonywanych przez poszczególne podzespoły systemu zadaniach i statusach, aż do informacji alarmowych (alarm napadowy, alarm włamaniowy, zbyt długo otwarte drzwi, próba użycia nieuprawnionej karty itp.).

Elementy systemów są zwizualizowane w postaci aktywnych punktów rozmieszczonych na planach obiektu. Sposób przedstawienia danego planu jest dowolny i zależy od preferencji użytkownika. Można włączyć wizualizację wszystkich podsystemów bądź każdego z nich w dowolnej kolejności, umożliwiając w ten sposób wyłączenie wszystkich niepotrzebnych komunikatów o poprawnie działających elementach i wskazanie tylko miejsca wystąpienia alarmu (zagrożenia).

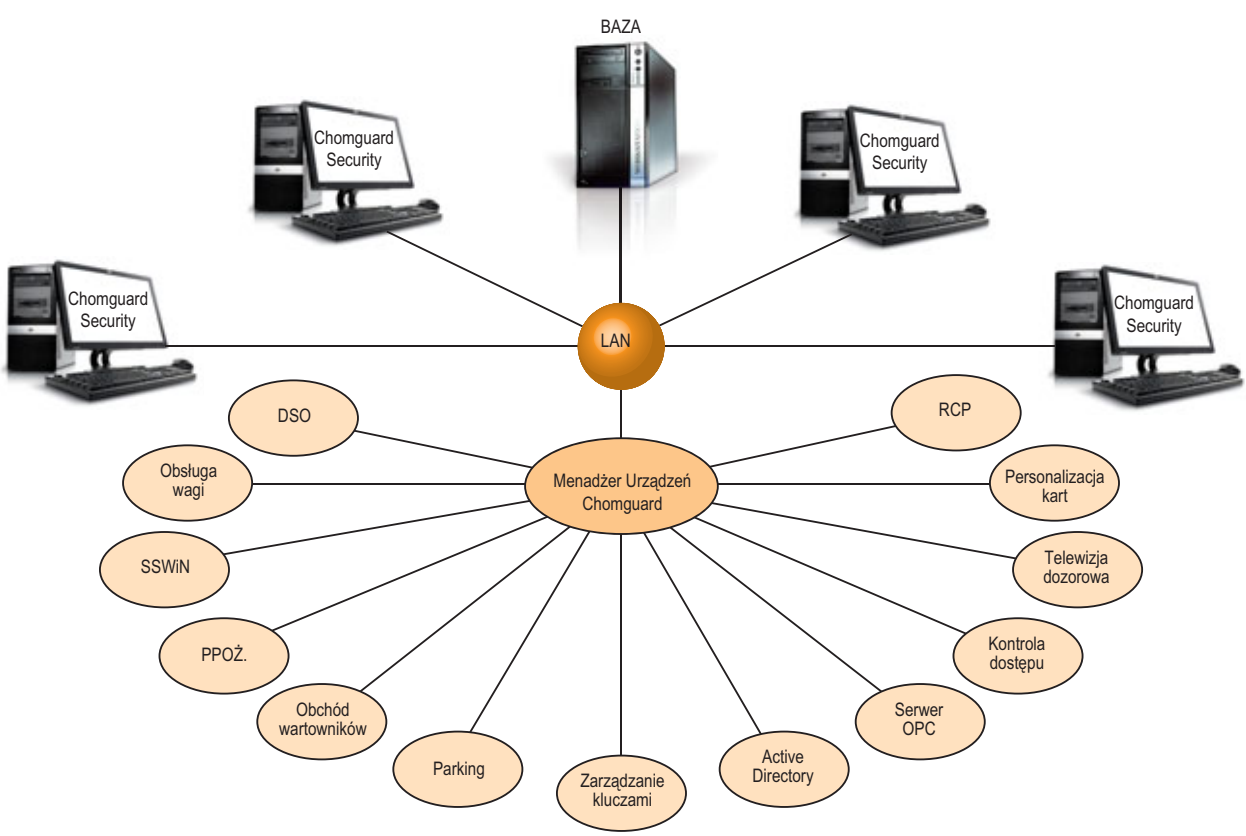
Jako tła map synoptycznych obiektów mogą być zastosowane pliki rastrowe (np. BMP, TIFF, JPG) lub wektorowe (CorelDRAW) oraz pliki CAD.

Tworzenie raportów

Pakiet Chomguard Security ma zaawansowane funkcje generowania raportów. Dane można z łatwością zamieścić w specjalnych przestawnych tabelach metodą „przeciągnij i upuść" (ang. *drag and drop*). Użytkownik może wykorzystać dowolnie utworzone przez siebie filtry. Każda tabela w raporcie może zostać wydrukowana zgodnie z ustawieniami użytkownika. Pakiet ma wbudowany generator raportów. Dzięki temu inwestor może sam, we własnym zakresie, wygenerować dowolny raport bez konieczności ustalania tego z dostawcą systemu. Użytkownicy zaawansowani, umiejący programować zapytania w SQL, mają możliwość definiowania dowolnej liczby raportów, z których mogą korzystać użytkownicy niezaawansowani.

Podstawowe funkcje pakietu:

– monitorowanie zdarzeń i alarmów w czasie rzeczywistym,
– liczba użytkowników ograniczona jedynie zasobami sprzętowymi,
– praca w kontekście wielu jednostek, jednostki głównej lub jednostek podrzędnych,



Rys.1. Schemat systemu Chomguard Security

– globalna *kontrola kolejności wejścia/wyjścia*,
– wbudowany generator raportów – kreator umożliwiający tworzenie własnych raportów z systemu z wykorzystaniem przestawnych tabel i zaawansowanego filtrowania,
– optymalizacja pracy w przypadku sieci o niskich przepustowościach (ISDN,PTSN,GSM,GPRS),
– integracja z systemem alarmowym,
– integracja z kontrolą dostępu,
– integracja z systemem przeciwpożarowym,
– integracja z telewizją dozorową,
– sterowanie kołowrotami, bramkami, furtami stadionowymi,
– sterownie bramami i szlabanami parkingowymi,
– sterowanie oświetleniem,
– tworzenie list użytkowników oraz projektowanie i drukowanie identyfikatorów,
– możliwość importu list użytkowników z innych baz danych (otwarte łącze bazy danych),
– integracja z LDAP,
– tworzenie interaktywnych map obiektów,
– pełna integracja programowa czytników biometrycznych,
– praca w sieci: LAN, WAN, Ethernet,
– silniki bazy danych: MS SQL, Oracle,
– systemy operacyjne: Windows, Linux,
– współpraca z innymi aplikacjami z grupy Chomguard (wspólna baza danych).

Dodatkowe moduły Chomgurad Security:

– moduł rozliczania czasu pracy,
– moduł liczenia ludzi w strefach,
– moduł integracji z serwerem OPC,
– moduł zarządzania parkingiem,
– moduł zarządzania windą,
– moduł zarządzania wagą,
– moduł zarządzania wydawaniem kluczy,
– moduł obsługi gości,
– moduł obsługi drukarki kart,
– moduł obsługi śluzy,
– moduł *long range*,
– moduł kontroli pracy wartowników,
– moduł narzędziowni,
– moduł obsługi konwojów i sterowania śluzami.

Chomguard Security może pracować m.in. z urządzeniami:

Axis, ACTi, Aper, Bosch, NOVUS, SANYO, HID, Indala, Mifare, Unique, POLON ALFA, Galaxy, SATEL, DSC.

Zastosowania programu Chomguard Security

Chomguard Security ma zastosowanie wszędzie tam, gdzie istnieje ryzyko i prawdopodobieństwo wystąpienia zagrożenia osób i mienia, w szczególności w obiektach przemysłowych, wojskowych i policyjnych, biurowcach, na dworcach i w portach lotniczych, w elektrowniach, galeriach handlowych, ośrodkach akademickich, szpitalach, obiektach sportowych i centrach logistycznych.

Tomasz Krawczyk
chomtech.pl

Monitorowanie systemów sygnalizacji włamania i napadu

z wykorzystaniem sieci Ethernet (część 3)

Adam Rosiński, Maciej Maszewski

W poprzednich dwóch częściach artykułu przedstawiono ogólnie różne metody komunikacji pozwalające na zaprojektowanie systemu sygnalizacji włamania i napadu (SSWiN) oraz opisano i scharakteryzowano możliwości łączności systemu do zarządzania i monitoringu z centralą alarmową poprzez sieć Ethernet. W tej części zostanie zaprezentowana aplikacja integrująca, która umożliwia zarządzanie wieloma systemami alarmowymi

1. Koncepcja systemu bezpieczeństwa z wykorzystaniem Ethernetu

Spośród wielu dostępnych na rynku systemów SSWiN wybraliśmy system wykorzystujący centrale alarmowe serii INTEGRA firmy SATEL. Wybór ten był podyktowany kilkoma względami:

– skalowalnością systemu,
– modułowością rozwiązania, dzięki której można łatwo dostosować je do konkretnego zastosowania (dostosować funkcje do potrzeb inwestora),
– otwartością protokołu komunikacyjnego (zaimplementowanego w module INT-RS), który umożliwia dodanie kolejnych funkcji dzięki zewnętrznemu oprogramowaniu oraz integracji z systemami innych producentów.

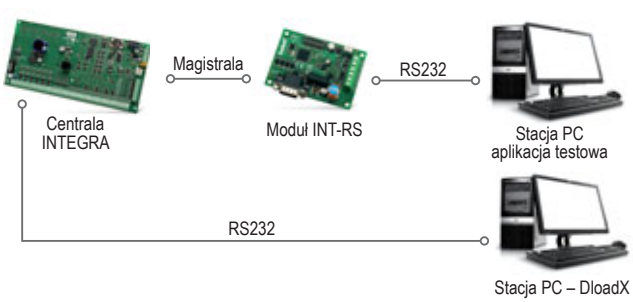
Pomimo tego, że w ofercie firmy jest moduł ETHM-1 służący do komunikacji z systemem poprzez sieć Ethernet, przedstawiona koncepcja nie zakłada jego użycia. To dlatego, że protokół komunikacyjny modułu wykorzystującego Ethernet jest zamknięty, a więc nie ma możliwości napisania oprogramowania do współpracy z modułem.

Naszym celem jest opracowanie takiego rozwiązania, które umożliwiałoby integrację systemu SSWiN z systemem klasy ERP, w którym przechowywane są informacje o użytkownikach, ich uprawnieniach, ograniczeniach czasowych itp., które powinny być dostępne dla systemu alarmowego, aby umożliwić użytkownikom korzystanie z zabezpieczonego obiektu. W przypadku dwóch odrębnych systemów (SSWiN i ERP) istnieje konieczność przesyłania danych pomiędzy nimi. Dzięki integracji dane będą przesyłane automatycznie, a ich zmiana w systemie ERP będzie automatycznie transferowana do systemu SSWiN. Opracowywana koncepcja zakłada ponadto istnienie wielu lokalizacji (np. oddziałów przedsiębiorstwa) i zarządzanie nimi poprzez Internet z poziomu jednego systemu ERP. Wszystkie funkcje związane z integracją i synchronizacją danych będą realizowane z wykorzystaniem zewnętrznej aplikacji.

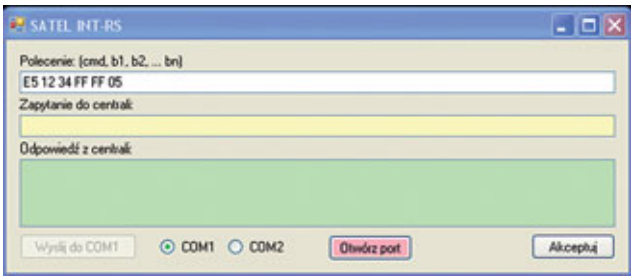
Do demonstracji, jako platformę programistyczną, wybrano środowisko ASP.NET opracowane przez firmę Microsoft i działające w systemie operacyjnym Windows. Oprogramowanie zostało napisane w języku C#.

1.1. Testowanie funkcjonalności modułu INT-RS

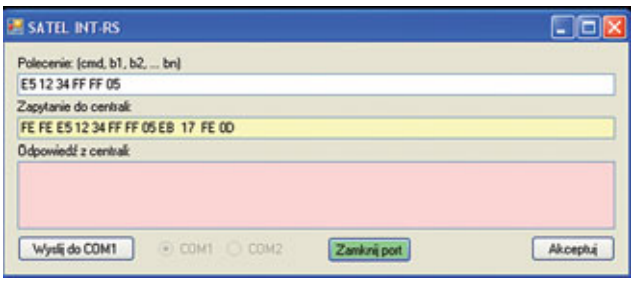
Jak wspomniano we wcześniejszym rozdziale, moduł INT-RS może pracować w trzech różnych trybach. Na potrzeby projektu wybrano tryb trzeci: „integracja z innym oprogramowaniem". W celach testowych napisano aplikację komunikującą się z modułem poprzez port RS232 oraz stworzono środowisko testowe z wykorzystaniem dwóch stacji roboczych PC, modułu INT-RS oraz centrali INTEGRA.



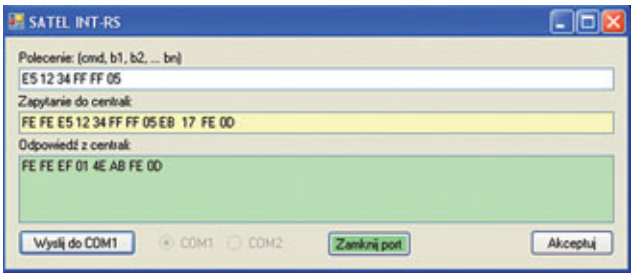
Rys. 1. Schemat połączeń między centralą a stacjami PC



Rys. 2. Aplikacja testowa – przed wykonaniem



Rys. 3. Aplikacja testowa – po przetworzeniu ramki



Rys. 4. Aplikacja testowa – po otrzymaniu odpowiedzi z centrali

Jedna ze stacji z uruchomionym oprogramowaniem DloadX monitoruje system i zachodzące w nim zmiany wprowadzane za pomocą aplikacji testowej.

Stacja PC komunikuje się z centralą za pośrednictwem modułu z zaimplementowanym protokołem komunikacyjnym. Protokół ten definiuje format ramki zawierającej polecenie do wykonania przez centralę wraz z koniecznymi parametrami. W odpowiedzi centrala przesyła ramkę zawierającą dane będące odpowiedzią na zapytanie. Aby komunikacja była prawidłowa, transmisja danych w ramkach nie może zostać zakłócona. Do weryfikacji poprawności transmisji służy suma kontrolna ramki – CRC. Jest ona wyliczana na podstawie zawartych danych i dołączana do ramki przez stronę nadawczą. Strona odbierająca dane porównuje ich sumę kontrolną z CRC danych wysłanych. Jeśli obie sumy są równe, odbiorca ma pewność, iż otrzymał ramkę z poprawnymi danymi. Jeśli suma nie jest zgodna, odrzuca ramkę.

1.1.1. Opis działania aplikacji

Zadaniem aplikacji jest wyliczenie sumy kontrolnej, przesłanie komunikatu do centrali oraz odbiór danych i prezentacja ich na ekranie. Aplikacja oczekuje na wprowadzenie danych polecenia w formie pliku z rozszerzeniem cmd, b1, b2…bn do pola *Polecenie*. Po wprowadzeniu danych należy nacisnąć przycisk *Akceptuj* (rys. 2).

Aplikacja wyliczy sumę kontrolną dla ramki oraz doda znaczniki początku (0×FE 0xFE) i końca ramki (0×FE 0×0D).Wynik tego działania zostanie umieszczony w polu *Zapytanie do centrali* (rys. 3). Jednocześnie pole *Odpowiedź z centrali* zmieni kolor, informując, że dane nie zostały jeszcze przesłane do centrali. Aby to uczynić, należy wybrać port komunikacyjny stacji PC, do którego podłączony jest moduł INT-RS, a następnie wcisnąć przycisk *Otwórz port*. Otwarcie portu jest sygnalizowane zmianą koloru przycisku. Od tej pory aktywny jest przycisk *Wyślij do COM1*. Wciśnięcie tego przycisku powoduje wysłanie ramki do centrali, po którym następuje oczekiwanie na odbiór danych.

Odebrane dane z centrali pojawią się w polu *Odpowiedź z centrali*, a kolor pola zmieni się na zielony, co będzie sygnalizować odebranie danych (rys. 4). Dane te należy zinterpretować, posługując się opisem protokołu komunikacji zamieszczonym w dalszej części publikacji.

1.2. Aplikacja integracyjna

Przy tworzeniu aplikacji integracyjnej wykorzystano doświadczenie i wiedzę zdobytą podczas tworzenia aplikacji testowej. Zadaniem aplikacji opisanej w tym rozdziale jest realizacja funkcji związanych z obsługą użytkowników SSWiN. Zadania aplikacji to:

- komunikowanie się za pośrednictwem Ethernetu z przykładową bazą systemu ERP zawierającą dane o użytkownikach,
- komunikowanie się z centralą alarmową poprzez moduł INT-RS,
- udostępnianie interfejsu WWW do realizacji zadań.

1.2.1. Konfiguracja sprzętowa systemu

Na rys. 5 przedstawiono schemat konfiguracji sprzętowej z wykorzystaniem aplikacji integracyjnej.

Otoczone fioletową linią elementy po lewej stronie rysunku są związane z SSWiN. Jako komputer z aplikacją integracyjną w środowisku produkcyjnym można wykorzystać komputer przemysłowy, który ma małe rozmiary i jest pozbawiony elementów ruchomych, co może wydłużyć okres jego bezawaryjnej pracy. Trzy elementy, o których wcześniej wspomniano, można umieścić w jednej obudowie.

Konfiguracja systemu:

- centrala INTEGRA – oprogramowanie centrali skonfigurowane do współpracy z modułem INT-RS;
- moduł INT-RS (ustawiony w integracyjny tryb pracy);
- komputer z zainstalowaną w systemie aplikacją integracyjną (komputer z zainstalowanym systemem operacyjnym Windows oraz platformą ASP.NET); port RS232 skonfigurowany do pracy z modułem INT-RS; interfejs sieciowy skonfigurowany do pracy w sieci LAN;
- serwer systemu ERP (systemu informatycznego przedsiębiorstwa, który wspomaga zarządzanie przedsiębiorstwem);
- serwer baz danych (komputer z zainstalowaną bazą danych, którą wykorzystuje system ERP);
- stacja zarządzająca (stacja PC z zainstalowaną przeglądarką internetową oraz klientem systemu ERP).

1.2.2. Implementacja aplikacji integracyjnej

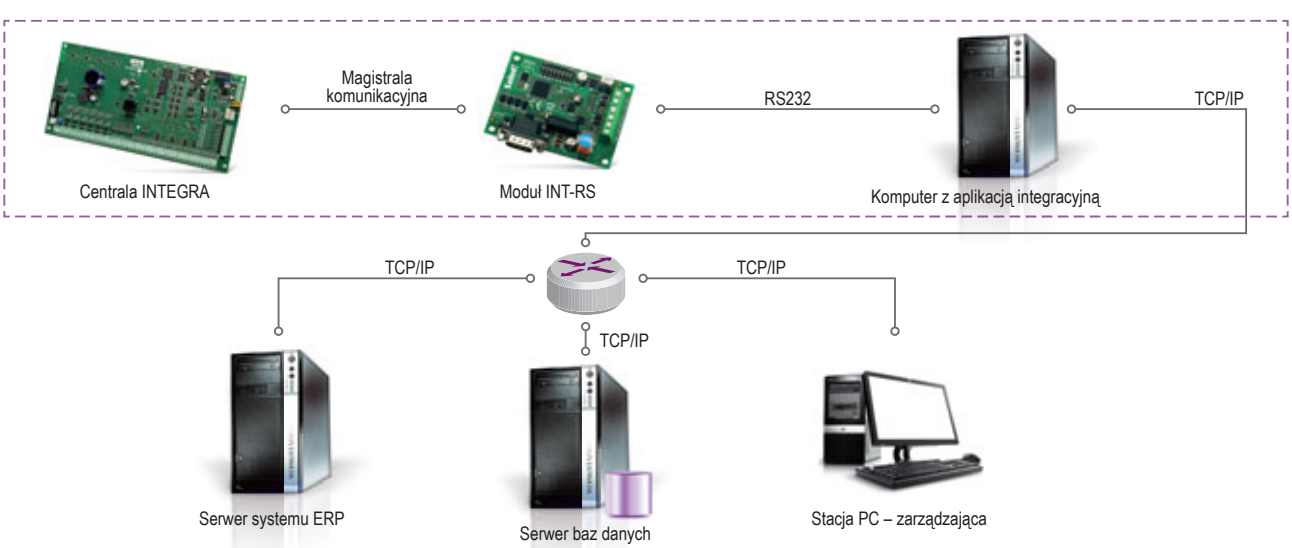
Oprogramowanie zostało napisane na platformie ASP.NET w architekturze klient-serwer. Do komunikacji z modułem INT-RS służy funkcja stworzona przy okazji tworzenia aplikacji testowej. Pośredniczy ona w wysyłaniu i odbieraniu ramek z danymi z centrali.

1.2.2.1. Struktura logiczna aplikacji

Struktura pokazana na rys. 6 przedstawia powiązania aplikacji integracyjnej z modułem INT-RS, bazą danych, w której przechowywane są informacje o użytkownikach, oraz administratorem systemu. Aplikacja integracyjna składa się z trzech modułów:

- modułu komunikacji przez RS232 z modułem INT-RS,
- modułu komunikacji z bazą danych,
- modułu interfejsu WWW z narzędziami do obsługi aplikacji.

Moduł komunikacji z modułem INT-RS jest odpowiedzialny za wysyłanie i odbieranie komunikatów z centrali. Przyjmuje on dane w postaci ciągu bajtów, w którym zawarte jest polecenie (cmd) oraz parametry (b1, b2…bn), następnie oblicza sumę kontrolną i dodaje znaczniki początku i końca ramki. Tak przygotowana ramka jest przekazywana do modułu INT-RS.



Rys. 5. Konfiguracja sprzętowa systemu

Po odebraniu odpowiedzi z centrali zwraca dane do podprogramu wywołującego.

Moduł komunikacji z bazą danych ma za zadanie łączenie aplikacji z zewnętrzną bazą danych. Wykorzystuje do tego łącze Ethernetowe i protokół TCP/IP. W zależności od polecenia pobiera odpowiednie dane z tabel.

Moduł interfejsu WWW służy do zarządzania systemem alarmowym z wykorzystaniem przygotowanych narzędzi. Do poszczególnych przycisków przypisane są funkcje, dzięki którym realizowane są określone zadania, takie jak:

– utworzenie nowego użytkownika,

– usunięcie użytkownika z systemu,

– synchronizacja użytkownika (aktualizacja jego danych zawartych w bazie danych),

– synchronizacja wszystkich użytkowników systemu alarmowego (pobranie użytkowników z bazy danych i ich zapis w pamięci centrali alarmowej).

Na rys. 6 w podstawowej strukturze aplikacji uwzględniono jeszcze „aplikację kliencką do modyfikacji bazy danych". Jest to aplikacja zewnętrzna, pomocnicza, która służy do manipulacji danymi w tabelach w bazie danych. W projekcie wykorzystano do tego celu program Microsoft Access. Za jego pomocą można dodać, usunąć lub zmienić dane użytkowników, a następnie zsynchronizować dane poprzez interfejs WWW.

W wersji rozszerzonej aplikacji integracyjnej (rys. 7), jeszcze nie zastosowanej w projekcie, uwzględniono dodatkowo system ERP wraz z bazą danych oraz zamieniono moduł interfejsu WWW na interfejs SOAP (ang. *Simple Object Access Protocol*). Protokół SOAP służy do wywoływania zdalnego dostępu do obiektów i wykorzystuje język XML (ang. *Extensible Markup Language*) do kodowania wywołań. Takie rozwiązanie umożliwia dodanie odpowiednich funkcji do samego systemu ERP, a co za tym idzie – pełną automatyzację procesu aktualizacji danych w systemie SSWiN.

1.2.2.2. Aplikacja

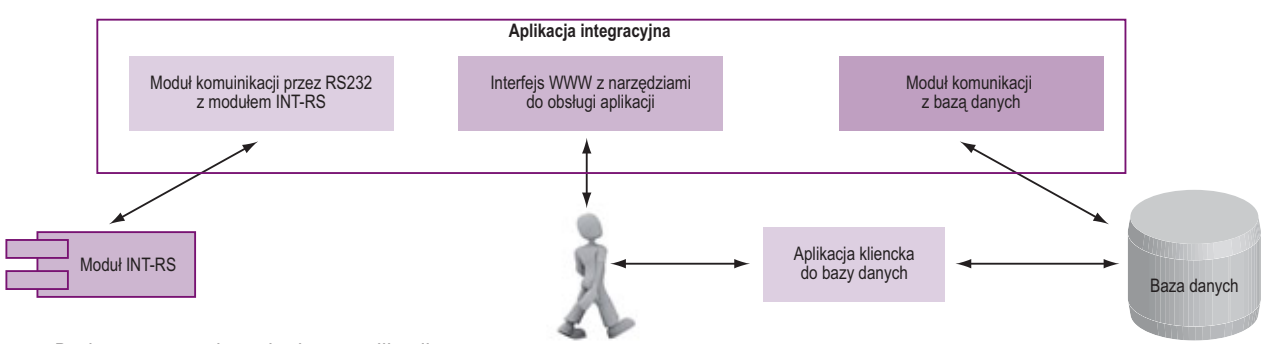
Funkcje aplikacji są udostępniane przez interfejs WWW. Pierwszą funkcją, przedstawioną na rys. 8, jest usuwanie użytkownika o danym ID z pamięci centrali alarmowej.

Przedstawiony na rys. 9 ekran ukazuje funkcje dodawania użytkownika do pamięci centrali alarmowej.

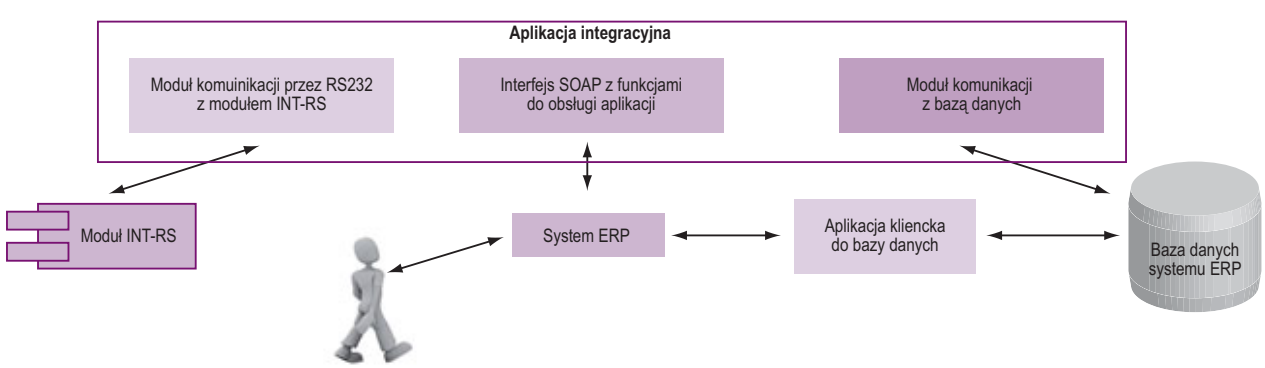
2. Podsumowanie

Integracja systemów umożliwia redukcję kosztów instalacji i obsługi systemu, a także sprawne zarządzanie. Poszczególne moduły wymieniają pomiędzy sobą informacje, dzięki czemu możliwe jest bardziej efektywne i skuteczne zabezpieczenie oraz zarządzanie obiektem. Złożoność systemów informatycznych i elektronicznych sprawia, że różne dane są często przechowywane w odrębnych bazach lub plikach. Zachowanie spójności danych wiąże się z ich aktualizacją. Podamy przykład. Informacje o pracownikach firmy są przechowywane w jednym systemie informatycznym. Obiekt, w którym znajduje się firma, jest chroniony systemem alarmowym. Pracownicy posiadają kody dostępowe umożliwiające im załączanie i wyłączanie systemu alarmowego oraz poruszanie się po terenie. W związku z obecnością dwóch odrębnych systemów – informatycznego i alarmowego – osoba zajmująca się sprawami kadrowymi bądź administrator systemu musi ręcznie aktualizować dane w systemie alarmowym tak, aby obiekt był poprawnie chroniony. Gdyby wykorzystano moduł integracyjny, aktualizacja danych mogłaby następować tylko w systemie informatycznym, a SSWiN byłby aktualizowany automatycznie, więc nie trzeba byłoby pilnować spójności danych.

W niniejszym opracowaniu wzięto pod uwagę tylko zarządzanie użytkownikami, ale aplikację integracyjną można rozbudować i zwiększyć liczbę jej funkcji – możliwości są ogromne i zależą od potrzeb oraz zaangażowanych środków. Podczas



Rys. 6. Podstawowa struktura logiczna aplikacji

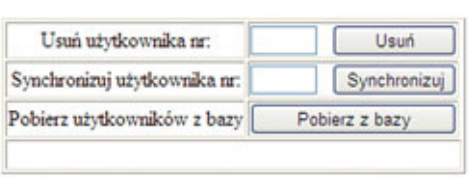


Rys. 7. Rozszerzona struktura logiczna aplikacji

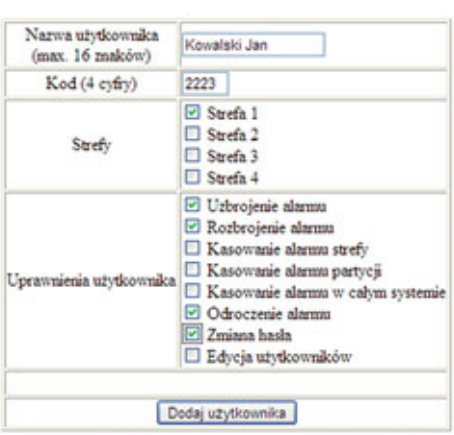
realizacji projektu należy brać pod uwagę także bezpieczeństwo transmisji w sieci Ethernet, gdyż w przypadku takich systemów jak SSWiN może mieć ono wyjątkowo duże znaczenie – skutki byłyby dalekosiężne, gdyby krytyczne dane zostały przechwycone przez nieuprawnioną osobę podczas transmisji.

Wybór centrali INTEGRA firmy SATEL był spowodowany tym, że firma ta ma w swojej ofercie moduł integracyjny oraz udostępnia dokumentację protokołu. Wielu producentów SSWiN ma zaimplementowane wyłącznie własne protokoły i nie udostępnia ich specyfikacji. W takich przypadkach jesteśmy ograniczeni do rozwiązań sprzętowo-programowych danego producenta. Wykorzystanie otwartych protokołów komunikacyjnych w systemach umożliwia integrację. Dzięki niej można zwiększyć liczbę funkcji systemu i wykorzystać go do dodatkowych celów.

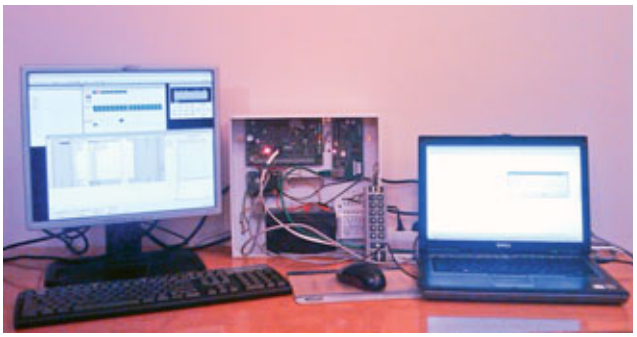
Stworzenie rozwiązania opisanego w artykule podzielono na trzy etapy. W pierwszym z nich dokonano konfiguracji sprzętowej, zestawienia wszystkich wymaganych połączeń, wyboru kabli, skonfigurowano oprogramowanie oraz przetestowano cały zestaw. Na fot. 1 pokazano wygląd stanowiska testowego. Drugi etap to opracowanie algorytmów wymiany komunikatów pomiędzy komputerem podłączonym przez port RS232 a centralą alarmową, wyliczanie sumy kontrolnej przesyłanych ramek, napisanie aplikacji będącej interfejsem dla użytkownika przeznaczonym do zapytań kierowanych do centrali i odbierania z niej komunikatów zwrotnych. Etap zakończył się testowaniem i usprawnianiem aplikacji. W trzecim etapie powstała koncepcja systemu do integracji, zbudowano i skonfigurowano testową bazę danych użytkowników, stworzono przykładową aplikację integracyjną do wymiany informacji z centralą, wykorzystując kod źródłowy aplikacji testowej. Następnie dodano do aplikacji funkcję dostępu przez WWW i funkcje związane z użytkownikami systemu alarmowego (tworzenie, modyfikacja, synchronizacja, usuwanie użytkowników). Na końcu powiązano aplikację z bazą danych w celu pobierania z niej informacji o użytkownikach, a także synchronizacji danych.



Rys. 8. Ekran narzędziowy aplikacji



Rys. 9. Ekran z funkcją dodawania użytkownika



Fot. 1. Wygląd stanowiska testowego

W opracowanym systemie synchronizacja danych jest dokonywana po ręcznym zainicjowaniu. W systemie produkcyjnym, w przypadku integracji z konkretnym systemem informatycznym, synchronizowanie może następować niezwłoczne po zmianie danych.

System integracyjny może być zainstalowany przy wielu systemach alarmowych, a część centralna będzie we wszystkich systemach alarmowych na podstawie danych z jednego systemu informatycznego

Mamy nadzieję, że zaprezentowana koncepcja i rezultaty, które osiągnęliśmy, umożliwią wielu czytelnikom (w tym właścicielom i dyrektorom firm) podjęcie racjonalnych działań podczas wdrażania systemów informatycznych zarządzających firmą i jej oddziałami z uwzględnieniem systemów bezpieczeństwa.

dr inż. Adam Rosiński
inż. Maciej Maszewski

Bibliografia

1) Centrala alarmowa INTEGRA – instrukcja instalatora, Satel.
2) Centrala alarmowa INTEGRA – instrukcja użytkownika, Satel.
3) Centrala alarmowa INTEGRA – instrukcja programowania, Satel.
4) Instrukcja modułu ETHM-1, Satel.
5) Instrukcja modułu INT-RS, Satel.
6) Instrukcja ogólna programu STAM-2, Satel.
7) Maszewski M., *Koncepcja wykorzystania sieci Ethernet w systemach bezpieczeństwa na bazie urządzeń firmy SATEL*, dyplomowa praca inżynierska, Wyższa Szkoła Menedżerska w Warszawie, Wydział Informatyki Stosowanej i Technik Bezpieczeństwa, Warszawa 2010.
8) Materiały dydaktyczne z Zespołu Laboratoriów Systemów Bezpieczeństwa Wydziału Informatyki Stosowanej i Technik Bezpieczeństwa Wyższej Szkoły Menedżerskiej w Warszawie.
9) Norma PN-EN 50131-1:2009: *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe.*
10) Rosiński A., *Programowanie systemów sygnalizacji włamania i napadu*, 13th International Conference „Computer Systems Aided Science, Industry and Transport" TRANSCOMP 2009, Zakopane 2009.
11) Szulc W., Rosiński A., *Systemy sygnalizacji włamania. Część 1 – konfiguracje central alarmowych, Zabezpieczenia* Nr 2(66)/2009

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.
- **INTERGRACJA** z innymi systemami:

RCP CCTV SSWiN

RCP Master PR602LCD

roger®

www.roger.pl

20 YEARS 1991-2011

Rozwiązania Kontroli Dostępu i Rejestracji Czasu Pracy

Wprowadzono do oferty zestawy **PR411DR-SET** oraz **PR402DR-SET.**
W skład zestawu wchodzą: kontroler, zasilacz oraz metalowa obudowa.

KD i RCP

w małych i średnich obiektach z wykorzystaniem rozwiązań firmy ROGER

Kamil Stadnicki

Firma ROGER od 20 lat projektuje i produkuje elektroniczne urządzenia do kontroli dostępu. Trzonem oferty jest system kontroli dostępu RACS4 przeznaczony do wykorzystania w małych i średnich obiektach. System RACS4 umożliwia pełną integrację z zaawansowanym programem do rejestracji czasu pracy RCP Master, tworząc w ten sposób kompleksowe rozwiązanie kontroli dostępu i rejestracji czasu pracy

Główny produkt firmy – system kontroli dostępu RACS4 – został wprowadzony do oferty prawie 10 lat temu. Od tego momentu jest on stale rozwijany w zakresie sprzętu, oprogramowania oraz funkcjonalności. Od początku istnienia systemu zachowywana jest jego pierwotna architektura, która sprawdziła się w kilku tysiącach instalacji. Obecnie system kontroli dostępu ROGER jest rozwiązaniem popularnym na rynku polskim i znanym w ponad 40 krajach, a marka ROGER jest regularnie promowana na międzynarodowych imprezach targowych.

W niniejszym artykule zawarte są podstawowe informacje na temat systemu RACS4 oraz nowości – tych wprowadzonych do sprzedaży ostatnio oraz tych, których można spodziewać się w najbliższym czasie.

Podstawowe elementy systemu RACS4

System RACS4 obejmuje:

- standardowe kontrolery dostępu serii PRxx1 (PR411, PR311, PR621, PR611),
- zaawansowane kontrolery dostępu serii PRxx2 (PR602LCD, PR402, PR302),
- centralę systemu sieciowego z funkcjami globalnymi (CPR32-SE),
- czytniki zbliżeniowe serii: PRTxxLT, PRTxxEM, PRTxxMF,
- interfejsy komunikacyjne: UT-4, UT-2USB, UT-2,
- zasilacze: PS-10, PS-20, PS-15,
- moduły rozszerzeń wejść/wyjść: XM-2, XM-8,
- program PR Master.

Kontrolery RACS4

Obie serie kontrolerów są elementami systemu RACS4 i różnią się przede wszystkim zestawem oferowanych funkcji. Główna różnica pomiędzy obydwiema seriami polega na tym, że w odróżnieniu do serii PRxx1 kontrolery serii PRxx2 mają wbudowaną pamięć zdarzeń oraz zegar czasu rzeczywistego. W przypadku kontrolerów PRxx1 funkcje bufora zdarzeń i zegara można zrealizować poprzez przyłączenie centrali CPR32-SE do systemu.

Wszystkie kontrolery w systemie RACS4 są kontrolerami jednego przejścia, które może być dozorowane jedno- lub dwustronnie. Architektura typowego systemu RACS4 została przedstawiona na rys. 1.

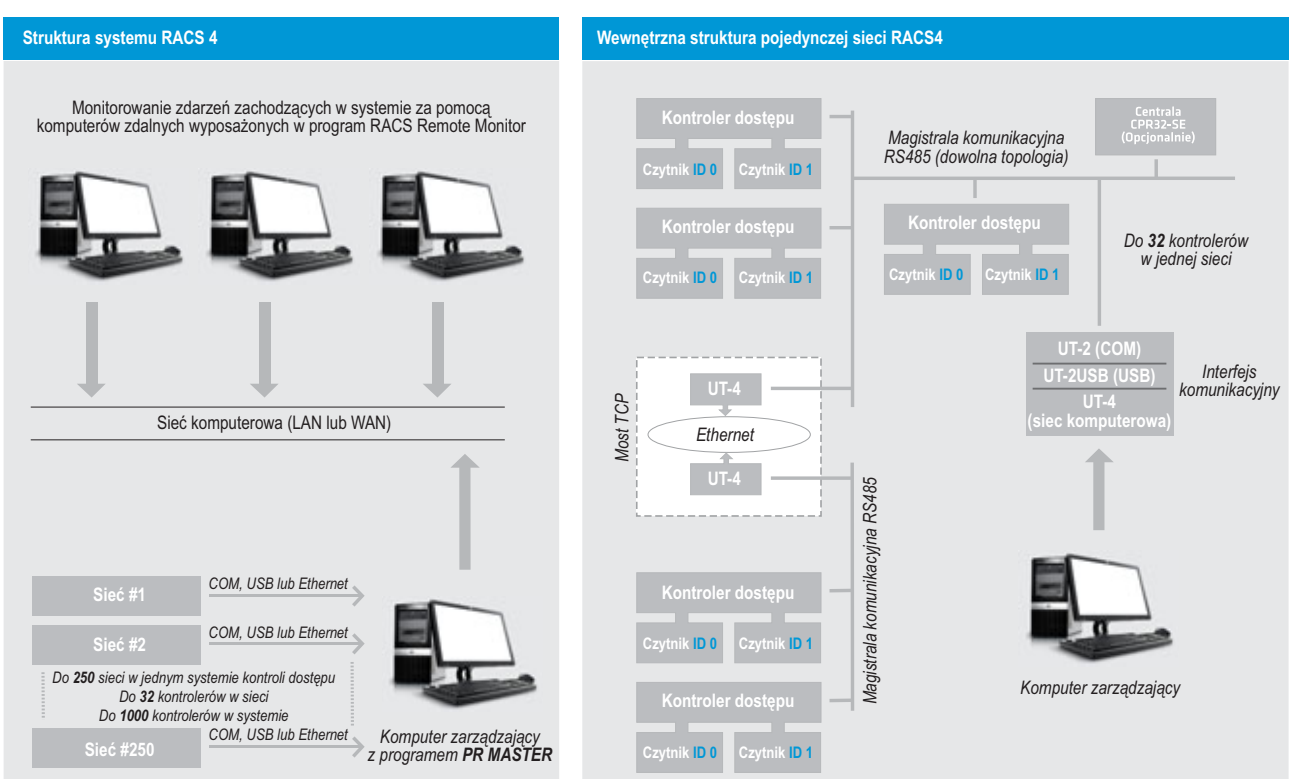
W ramach serii PRxx1 i PRxx2 dostępne są urządzenia z wbudowanymi czytnikami zbliżeniowymi (EM125 kHz) oraz kontrolery wymagające podłączenia zewnętrznych czytników (PR402 i PR411). Bez względu na typ urządzenia wszystkie kontrolery serii PRxx1 i PRxx2 oferują możliwość obsługi dwóch punktów identyfikacji.

Rozwiązanie oparte na czytniku scalonym z kontrolerem dostępu w jednej obudowie niewątpliwie upraszcza instalację i obniża jej koszty, niemniej poziom bezpieczeństwa przejścia jest niższy niż wówczas, gdy moduł elektroniczny kontrolera jest odseparowany od miejsca, w którym dokonywana jest identyfikacja.

W systemie RACS4 można stosować czytniki kart innych producentów, o ile potrafią one komunikować się za pomocą powszechnie stosowanych interfejsów Wiegand 26–66 bitów lub Magstripe. System RACS4 może składać się z maksymalnie 250 podsystemów, a każdy podsystem może obsługiwać do 32 przejść (kontrolerów) połączonych poprzez interfejs komunikacyjny z komputerem, na którym zainstalowane jest darmowe oprogramowanie zarządzające i monitorujące PR Master.

Czytniki kart

Oferta ROGER obejmuje szereg czytników zbliżeniowych przeznaczonych do obsługi standardu zbliżeniowego EM 125 kHz oraz 13.56 MHz Mifare. Większość oferowanych czytników jest



Rys. 1. Struktura systemu kontroli dostępu RACS4

dostosowana do pracy w warunkach zewnętrznych. Dostępny jest również czytnik zbliżeniowy w obudowie wandaloodpornej (PRT64EM-VP). Czytniki firmy ROGER mają duże możliwości programowe. Każdy z nich obsługuje wiele formatów transmisji (Wiegand 26–66 bitów, Magstripe, RACS4), co powoduje, że mogą one współpracować nie tylko z kontrolerami ROGER, ale również z większością dostępnych na rynku kontrolerów dostępu innych producentów.

Czytniki ROGER są podzielone według ich funkcji na trzy grupy urządzeń:

– czytniki serii PRTxxLT,
– czytniki serii PRTxxEM,
– czytniki serii PRTxxMF.

Czytniki PRTxxLT oraz PRTxxEM współpracują z kartami w standardzie EM 125 kHz, natomiast czytniki serii PRTxxMF wymagają transponderów zgodnych z ISO/IEC 14443A i Mifare. Opcjonalnie czytniki PRTxxEM oraz PRTxxMF można skonfigurować do pracy autonomicznej jako proste zbliżeniowe punkty kontroli dostępu, lecz bez możliwości łączenia ich w system sieciowy.

Dla ułatwienia pracy administratorom systemów kontroli dostępu firma ROGER opracowała rodzinę czytników USB, w skład której w chwili obecnej wchodzą czytniki RUD-2 (EM 125 kHz) oraz RUD-3 (Mifare).

Komunikacja w RACS4

Do komunikacji w systemie RACS4 wykorzystuje się przemysłowy standard RS485, który umożliwia rozmieszczenie urządzeń w maksymalnej odległości 1200 m. Do budowy magistrali komunikacyjnej systemu RACS4 można użyć dowolnej pary przewodów sygnałowych, przy czym preferowana jest skrętka nieekranowana (UTP kat. 5). Do komunikacji pomiędzy komputerem a urządzeniami potrzebny jest jeden z dostępnych interfejsów komunikacyjnych:

– UT-2USB (USB),
– UT-2 (RS232),
– UT-4 (TCP/IP).

Zastosowanie interfejsu UT-4 umożliwia komunikację z systemem za pośrednictwem sieci LAN lub WAN (Internet). Możliwość ta powoduje, że system RACS4 może obsługiwać instalacje rozmieszczone w oddalonych budynkach, miastach, a nawet krajach.

Zasilanie w RACS4

Wszystkie urządzenia do kontroli dostępu w systemie RACS4 można zasilać napięciem 12 V_{DC}. Ponadto kontrolery serii PR411, PR402 oraz centralę CPR32 można zasilać napięciem stałym 24 V_{DC} lub przemiennym 18 V_{AC}.

Fot. 1. Przykładowe elementy systemu kontroli dostępu RACS

Moduły PR411, PR402 oraz CPR32 mają wbudowany zasilacz (przetwornicę DC/DC), który służy do zasilania elementów infrastruktury systemu kontroli dostępu (czytników zewnętrznych, modułów rozszerzeń, urządzeń wykonawczych), a także do baterii rezerwowej (typowo 12 V/7 Ah).

W przypadku zasilania napięciem 12 V_{DC} zalecane jest stosowanie buforowych zasilaczy sieciowych, które są dostępne w ofercie firmy ROGER, to jest PS10 lub PS20. Zasilacze te są sprawdzonymi urządzeniami i gwarantują niezawodną pracę systemu.

Firma ROGER oferuje różne modele obudów do instalacji modułów kontroli dostępu. Nowością w tej dziedzinie jest obudowa ME-4, fabrycznie przystosowana do instalacji modułów przeznaczonych do montażu na szynie DIN. Obudowa ta jest wyposażona w transformator zasilający PS-10ACDR. Ciekawostką techniczną jest możliwość instalacji obudowy ME-4 w pozycji poziomej, co jest szczególnie ważne w obiektach z sufitami podwieszanymi.

Oprogramowanie

Do konfigurowania, zarządzania oraz monitorowania systemu kontroli dostępu służy program PR Master. Jest to program bezpłatny, który daje wiele możliwości związanych z wizualizacją raportowania pracy systemu oraz jego integracją z innymi systemami. Pakiet PR Master pozwala też na wdrożenie prostego systemu rejestracji czasu pracy z wykorzystaniem wcześniej zdefiniowanych obszarów (tzw. Obszarów Obecności). System RACS4 może również przygotowywać dane do dalszego przetwarzania w przeznaczonych do tego celu specjalistycznych programach RCP. Takim programem jest RCP Master firmy ROGER, dostępny w wersji jedno- i wielostanowiskowej.

PR Master umożliwia monitorowanie zdarzeń i alarmów w czasie rzeczywistym. Ponadto oferuje wiele funkcji narzędziowych, przydatnych podczas nadzorowania pracy systemu, takich jak lokalizacja aktualnego miejsca przebywania użytkownika, powiadamianie o wystąpieniu zdarzeń wcześniej zdefiniowanych kategorii i wyświetlanie danych tekstowych na monitorach telewizji dozorowej (dzięki generatorom tekstu). Nowością wprowadzoną do programu jest integracja z cyfrowymi rejestratorami obrazu (DVR), która umożliwia podgląd obrazów z kamer na żywo i odtwarzanie sekwencji scen zarejestrowanych przez rejestrator DVR.

Integracja z systemem alarmowym

Oprócz funkcji ściśle związanych z kontrolą dostępu kontrolery PRxx1 i PRxx2 mają możliwość integracji z systemem alarmowym. Integracja taka bazuje na logice stref alarmowych, które są definiowane w ramach systemu KD, oraz możliwości rozróżnienia trybów uzbrojony/rozbrojony w ramach każdego kontrolowanego przejścia. Fizycznie integracja polega na stworzeniu połączeń pomiędzy odpowiednio skonfigurowanymi wyjściami i wejściami sterującymi centrali alarmowej i kontrolerów. Możliwe są dwa scenariusze integracji – pierwszy polega na tym, że centrala alarmowa steruje trybami dostępu kontrolerów, w przypadku drugiego kontrolery sterują czuwaniem stref alarmowych w centrali. W najbliższym czasie firma ROGER wprowadzi do sprzedaży nową centralę systemu KD o oznaczeniu CPR32-NET, która będzie umożliwiała programową integrację systemu

Fot. 2. Rozwiązanie RCP zintegrowane z systemem RACS

alarmowego INTEGRA (SATEL) z systemem RACS4 za pośrednictwem interfejsu INT-RS (SATEL).

Program RCP Master

System RACS4 współpracuje także z płatnym, dedykowanym oprogramowaniem RCP Master do rejestracji czasu pracy (na stronie *www.roger.pl* znajduje się 60-dniowa, w pełni funkcjonalna wersja testowa). RCP Master jest oferowany wraz z różnymi licencjami, w zależności od liczby korzystających z niego pracowników oraz liczby stanowisk komputerowych, na których ma działać. Zalecane jest stosowanie tego programu wszędzie tam, gdzie prosta rejestracja czasu pracy dostępna w PR Master jest niewystarczająca. Program RCP Master działa tylko razem z systemem RACS4. Aktualnie trwają prace nad opracowaniem autonomicznego systemu RCP, który mógłby współpracować z kontrolerm PR602LCD bez udziału systemu RACS4.

Inne zastosowania i aplikacje

Dzięki wbudowanym funkcjom system RACS4 może być stosowany w różnych aplikacjach i konfigurowany w zależności od wymagań klienta. Dzięki dostępności mechanizmu funkcji antypowrotu (ang. *antipassback*) RACS4 może być stosowany na płatnych parkingach, gdzie jeden identyfikator powinien umożliwiać dostęp jednej osobie i nie powinien być użyczany nikomu innemu, dopóki samochód nie opuści parkingu. W oparciu o tzw. Obszary Obecności w programie PR Master lub w oparciu o program RCP Master możliwe jest również rejestrowanie czasu pobytu dzieci w przedszkolach. Wykorzystując urządzenia firmy ROGER do kontroli dostępu można bez trudu zbudować śluzę bankową. System wykorzystujący kontrolery serii podstawowej może być również stosowany w hotelach, gdyż ma odpowiednie do takiej aplikacji funkcje. W przypadku zastosowania modułu rozszerzeń XM-8 można zapewnić kontrolę dostępu w windach obsługujących do 32 pięter. Tryb monitorowania oraz interaktywna mapa w PR Master umożliwiają nadzór nad działaniem systemu oraz interaktywne ingerowanie w jego działanie.

System kontroli dostępu RACS4 firmy ROGER oferuje kilkadziesiąt funkcji linii sterujących i klawiszy funkcyjnych. Potencjalnie istnieje ogromna liczba miejsc, w których można go zastosować. Ostateczny kształt systemu zależy od projektanta. Jeśli będzie prosty, jego konfiguracja będzie łatwa – nie ma potrzeby wprowadzania funkcji, które nie będą używane, a w większości przypadków można zastosować ustawienia domyślne.

Fot. 3. PR402DR - nowa wersja popularnego kontrolera dostępu serii PRxx2

Nowości

Firma ROGER sukcesywnie wprowadza do swojej oferty nowe urządzenia, z których część jest przystosowana do montażu na szynie DIN 35 mm. Oto kilka przykładów:

- PR402DR – kontroler serii zaawansowanej w obudowie przystosowanej do montażu na szynie DIN,
- PR411DR – kontroler serii podstawowej w obudowie przystosowanej do montażu na szynie DIN,
- UT-4DR – interfejs komunikacyjny RS485/Ethernet w obudowie przystosowanej do montażu na szynie DIN,
- PR411DR-SET – zestaw kontrolera PR411DR w obudowie metalowej ME-4 z transformatorem,
- PR402DR-SET – zestaw kontrolera PR402DR w obudowie metalowej ME-4 z transformatorem,
- RUD-3 – czytnik i programator USB do kart w standardzie Mifare.

Wkrótce w ofercie pojawią się kolejne urządzenia, między innymi centrala CPR32-NET wyposażona we wbudowany interfejs komunikacyjny TCP/IP, która ma możliwość integracji programowej z centralami INTEGRA (SATEL), czytnik linii papilarnych (seria RADIUS) oraz nowe wersje oprogramowania firmowego umożliwiające kontrolerom serii PR411 i PR402 obsługę dwóch niezależnych przejść. Firma ROGER pracuje również nad integracją systemu RACS4 z czytnikami Mifare montowanymi w zamkach drzwiowych serii Sallis (SALTO).

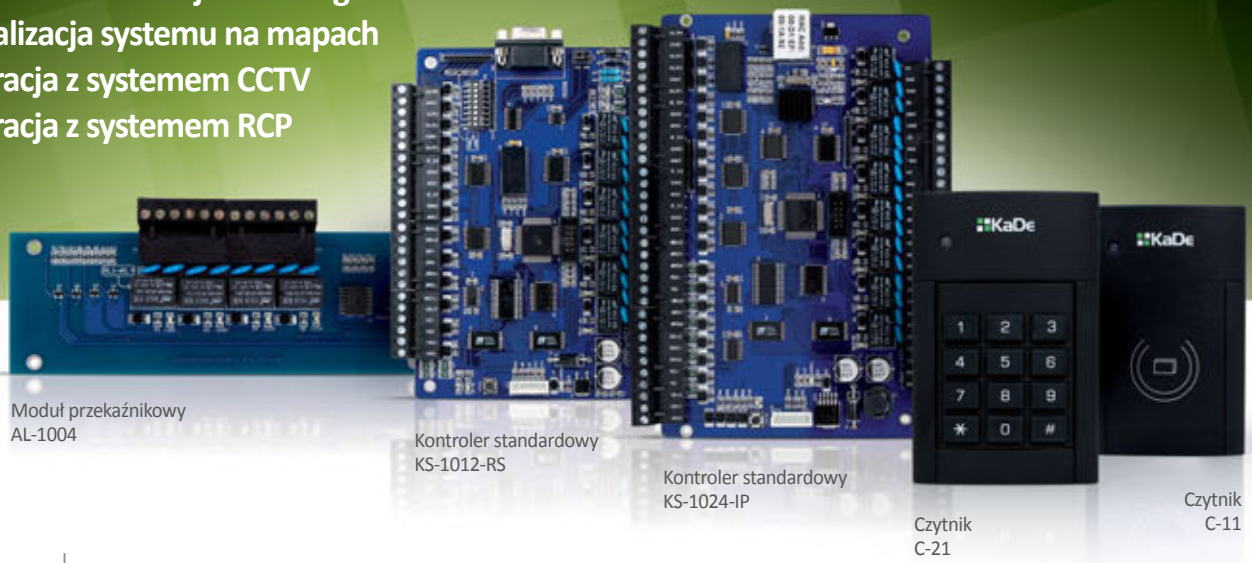
Podsumowanie

Dzięki swojej funkcjonalności i niezawodności system RACS4 jest jednym z najbardziej popularnych systemów kontroli dostępu na polskim rynku i jest dobrze przyjmowany na wielu rynkach zagranicznych. Firma ROGER oferuje profesjonalne rozwiązania od 20 lat i jest znana z nowatorstwa i dużego doświadczenia w dziedzinie systemów kontroli dostępu. Jej produkty charakteryzują się uniwersalnością i nowoczesnym wzornictwem. Ważnym elementem działalności firmy ROGER jest profesjonalne wsparcie techniczne, które można uzyskać pod stałymi numerami telefonów oraz przez Internet. Urządzenia firmy ROGER są stale rozwijane i udoskonalane. Zdobyły uznanie wielu instalatorów i użytkowników systemów kontroli dostępu zarówno w kraju, jak i za granicą.

Kamil Stadnicki
ROGER

Zaawansowany System Kontroli Dostępu Wersja PREMIUM

Kontrolery standardowe z portami RS lub IP
Czytniki w dowolnej technologii
Wizualizacja systemu na mapach
Integracja z systemem CCTV
Integracja z systemem RCP



Moduł przekaźnikowy AL-1004

Kontroler standardowy KS-1012-RS

Kontroler standardowy KS-1024-IP

Czytnik C-21

Czytnik C-11

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

Parametry systemu

4096 przejść kontrolowanych jednostronnie
20 000 użytkowników
50 000 zdarzeń w pamięci kontrolera

Oprogramowanie

KaDe wersja PREMIUM	Zaawansowana wersja programu nadzorczego dedykowana do współpracy z kontrolerami standardowymi w trybie sieciowym

Kontrolery standardowe i moduł przekaźnikowy

KS-1012-RS	Kontroler standardowy, 1 drzwi dwustronnie, 2 drzwi jednostronnie, 2 porty czytników, porty RS232 i RS485
KS-1024-RS	Kontroler standardowy, 2 drzwi dwustronnie, 4 drzwi jednostronnie, 4 porty czytników, port RS232 i RS485
KS-1012-IP	Kontroler standardowy, 1 drzwi dwustronnie, 2 drzwi jednostronnie, 2 porty czytników, port TCP
KS-1024-IP	Kontroler standardowy, 2 drzwi dwustronnie, 4 drzwi jednostronnie, 4 porty czytników, port TCP
AL-1004	Moduł przekaźnikowy przeznaczony do współpracy z kontrolerami standardowymi

Czytniki kart zbliżeniowych typu MIFARE (13,56 MHz)

C-11	Czytnik do instalacji wewnątrz i na zewnątrz pomieszczeń, format kodowania 34 bit Wiegand
C-21	Czytnik do instalacji wewnątrz i na zewnątrz pomieszczeń, format kodowania 26/34 bit Wiegand (przełączany), wyposażony w klawiaturę kodową (przełączany format 4/8 bit)
C-ADM-M	Czytnik kart administratora przeznaczony do wprowadzania dużej liczby kart MIFARE do bazy danych programu nadzorczego KaDe Premium. Istnieje możliwość wykorzystania urządzenia, np. do współpracy z dowolnym edytorem lub polami edytowalnymi w różnych aplikacjach.

System KaDe w wersji PREMIUM współpracuje z czytnikami w dowolnej technologii identyfikacji pod warunkiem, że posiadają interfejs Wieganda od 26 do 40 bit, czyli np. czytnikami kart UNIQUE, HID oraz innymi.

KaDe zintegrowane z RCP

Ryszard Sobierski

Zgodnie z obietnicą publikujemy kolejny artykuł z cyklu poświęconego systemowi KaDe. W niniejszym artykule przedstawię Państwu możliwości ewidencji i rozliczania czasu pracy z wykorzystaniem sprzętu i oprogramowania systemu KaDe oraz produktów firmy ControlSYS, która specjalizuje się w profesjonalnych rozwiązaniach RCP

Wykorzystanie elementów systemu kontroli dostępu do rejestracji wejść/wyjść związanej z ewidencją czasu pracy jest bardzo często spotykanym rozwiązaniem. Instalowanie systemu kontroli dostępu wynika jednak z potrzeby zapewnienia bezpieczeństwa, a wymóg ewidencji czasu pracy dotyczy każdej firmy, dlatego na rynku występują również samodzielne systemy RCP realizujące wyłącznie funkcje ewidencji czasu pracy.

Najczęściej spotykanym rozwiązaniem jest wykorzystanie jednej karty zbliżeniowej do systemów KD i RCP. Jeśli czytniki RCP są zainstalowane na tripodach, to również czytniki i kontrolery rejestrujące wejścia/wyjścia pracowników są elementem wspólnym systemów KD i RCP.

Jak wynika z Tab. 1 sam proces rejestracji wejścia/wyjścia oraz dane źródłowe (pozytywna weryfikacja ze znacznikiem daty i czasu) są w obu przypadkach bardzo zbliżone. Dopiero dalszy proces przetwarzania tych samych danych źródłowych na raport historii zdarzeń lub raport czasu pracy jest inny.

Podobieństwa umożliwiają dwa różne zastosowania tych samych urządzeń.

Należy nadmienić, że samodzielne systemy RCP wykorzystują najczęściej specjalistyczne terminale RCP, które zawierają czytnik, klawiaturę z przyciskami funkcyjnymi oraz wyświetlacz.

W ofercie naszej firmy posiadamy każde z powyższych rozwiązań. W dalszej części artykułu przedstawię dwa z nich.

Funkcje RCP w programie KaDe

W wersji 1.0019 programu KaDe (Lite oraz Premium) pojawiła się nowa pozycja w zakładce *System – Rejestracja czasu pracy*. Umożliwia ona wykorzystanie takich samych czytników jak w systemie kontroli dostępu (lub nawet tych samych). Jest to bardzo proste i bardzo tanie rozwiązanie, dzięki któremu można wygenerować podstawowy raport RCP.

Po wybraniu tej pozycji wyświetlany jest ekran zawierający dwie zakładki:

– *Konfiguracja RCP,*
– *Raporty RCP.*

W procesie konfiguracji administrator może wykonać następujące czynności:

– ustawić tryb pracy RCP – prosty lub zaawansowany,
– ustalić, które czytniki w systemie będą brane pod uwagę w procesie kalkulacji RCP,

Fot. 1. Zrzut z ekranu programu KaDe z zakładką RCP

– ustalić reguły działania systemu RCP,
– zdefiniować harmonogramy pracy i terminarze dla poszczególnych grup pracowników.

Tryb prosty RCP

Tryb ten opiera się na zasadzie zliczania czasu pomiędzy pierwszym wejściem i ostatnim wyjściem zarejestrowanymi w ciągu danej zmiany lub doby przez czytnik zadeklarowany jako czytnik RCP. W najprostszym przypadku może to być jeden kontroler zintegrowany KZ-1000. W tym trybie rozliczanie czasu pracy może odbywać się tylko w ramach jednej doby kalendarzowej, a więc zmiana nie może rozpoczynać się np. o godzinie 22, a kończyć o 6 rano następnego dnia. Nie ma również możliwości automatycznego rozliczania nadgodzin.

Harmonogramy pracy mogą być czasowe (nienormowany czas pracy) lub zmianowe.

Czytniki służące do rejestracji wejść/wyjść w systemie RCP mogą równocześnie pracować jako elementy systemu kontroli dostępu.

Tryb zaawansowany RCP

Tryb ten opiera się na zasadzie zliczania czasu pomiędzy wejściem i wyjściem zarejestrowanymi przez czytniki zadeklarowane jako RCP WE i RCP WY. W tym trybie potrzebne są dwa czytniki, które nie mogą być wykorzystywane w systemie kontroli dostępu, a rozliczanie czasu pracy nie musi odbywać się w ramach jednej doby kalendarzowej, czyli zmiana może rozpoczynać się np. o godzinie 22, a kończyć o 6 rano następnego dnia. Istnieje możliwość automatycznego rozliczania nadgodzin.

W obu trybach można rejestrować ręcznie nadgodziny oraz brakujące wejścia/wyjścia (np. gdy pracownik zapomniał karty). Ze względu na brak terminala z przyciskami funkcyjnymi rejestracja wyjść w czasie pracy jest dokonywana ręcznie przez administratora.

W obu trybach obowiązuje podobny proces przetwarzania danych. Po odczycie zdarzeń zarejestrowanych przez kontrolery zadeklarowane jako rejestratory RCP należy dokonać kalkulacji dotyczącej określonych

System kontroli dostępu	System rejestracji czasu pracy:
pracownik przykłada kartę do czytnika,	pracownik przykłada kartę do czytnika (przed rejestracją powinien sprawdzić status WE-N, WY-N, WY-P, WE-P i w razie potrzeby zmienić go przyciskami funkcyjnymi)
kontroler weryfikuje uprawnienia użytkownika i wydaje decyzję	kontroler weryfikuje użytkownika
w systemie generowane jest zdarzenie (ze znacznikiem daty i czasu) dotyczące pozytywnej weryfikacji, które jest zapisywane w bazie zdarzeń systemu	w systemie generowane jest zdarzenie (ze znacznikiem daty i czasu) dotyczące pozytywnej weryfikacji, które jest zapisywane w bazie zdarzeń systemu
zbiór zdarzeń umożliwia wygenerowanie raportu dotyczącego historii zdarzeń.	na podstawie ustalonych reguł RCP (harmonogramów pracy) odbywa się proces kalkulacji
	po kalkulacji czasu pracy w danym okresie możliwe jest wygenerowanie raportu, w którym zazwyczaj podane są godziny wejść/wyjść i przepracowany czas

Tab. 1. Porównanie działania systemu kontroli dostępu z systemem rejestracji czasu pracy

pracowników (wybranego działu lub wszystkich pracowników) i interesującego nas okresu. Następnie należy przejść do zakładki *Raporty RCP* i skorzystać z opcji *Szczegółowy raport RCP*. Pozwala ona na ustawienie filtrów (nazwisko, dział, okres) oraz wyświetlenie raportu na ekranie. W każdym wierszu raportu podane są między innymi wymagane wejścia/wyjścia według harmonogramu, zarejestrowane wejścia/wyjścia, przepracowany czas itp. Taki raport można następnie zapisać na dysku w postaci pliku programu Excel lub wydrukować, korzystając z opcji *Ogólne – Drukuj* w programie KaDe.

Ewidencja i rozliczanie czasu pracy w systemach firmy ControlSYS

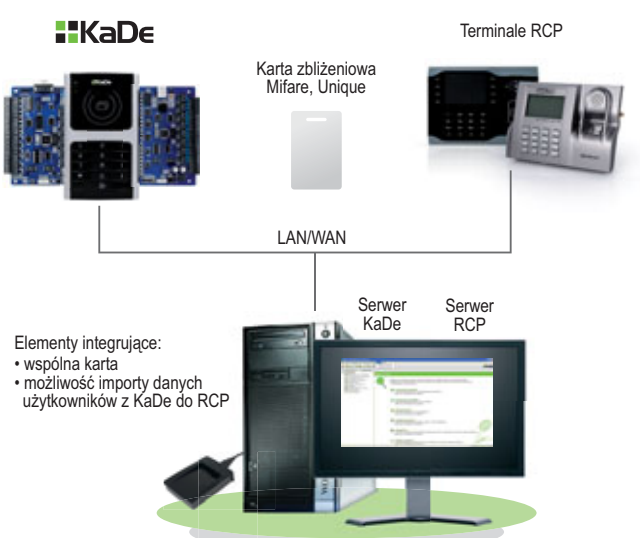
Wprowadzony do sprzedaży w naszej sieci system RCP firmy ControlSYS składa się z dwóch elementów: oprogramowania pod nazwą Punktualnik 2.0 oraz współpracujących z nim terminali RCP i KD.

Oprogramowanie Punktualnik 2.0 jest programem modułowym. Oprócz modułu RCP może zawierać opcjonalnie również moduły: KD, monitorowanie wizyjne i SMS (krótkie wiadomości są wyświetlane na terminalu RCP po rejestracji użytkownika).

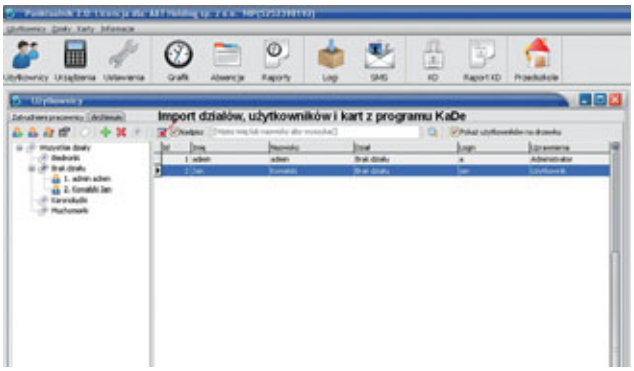
Najważniejszym modułem jest oczywiście moduł ewidencji i rozliczania czasu pracy i nieobecności. Jest to profesjonalny program wykonany zgodnie z obowiązującymi w naszym kraju przepisami i na bieżąco aktualizowany. Umożliwia definiowanie harmonogramów i terminarzy pracy dla różnych grup pracowników. Na uwagę zasługuje szata graficzna i intuicyjny interfejs dla administratora systemu.

Jedną z praktycznych opcji jest możliwość przypisania każdej osobie loginu i hasła wraz uprawnieniami. Pełny dostęp do programu ma administrator, kierownik ma dostęp do danych dotyczących podległych mu pracowników, a każdy pracownik – do swoich danych i raportów. Dzięki temu ogólnie dostępna stacja operatora umożliwia kontrolę liczby przepracowanych godzin na bieżąco.

Wśród urządzeń przeznaczonych do współpracy z programem Punktualnik 2.0 możemy wyróżnić dwie grupy terminali: tylko do systemu RCP oraz do systemów RCP i KD.



Rys. 1. Schemat integracji systemu KaDe z RCP firmy ControlSYS



Fot. 2. Zrzut z ekranu programu Punktulanik 2.0 z pokazaniem opcji importu bazy danych użytkowników z KaDe

Wszystkie terminale mają możliwość komunikowania się z programem Punktualnik 2.0 poprzez sieć LAN/WAN i protokół TCP. Każdy terminal RCP ma wyświetlacz LCD (monochromatyczny lub kolorowy, graficzny), przyciski funkcyjne (do ustawienia statusu rejestracji) oraz własne menu do konfiguracji. Ponadto w terminalach z funkcją KD znajduje się zestaw gniazd przyłączeniowych, które umożliwiają przyłączenie zamka elektrycznego i dodatkowego czytnika, a także porty RS232/485.

Dla bardziej wymagających użytkowników dostępne są również terminale z funkcjami biometrycznymi i wbudowanym komunikatorem Wi-Fi.

Systemy rejestracji czasu pracy firmy ControlSYS i kontroli dostępu KaDe firmy AAT zostały zintegrowane. Pracownik może używać jednej karty zbliżeniowej, która działa zarówno w systemie RCP z programem Punktualnik 2.0, jak i w systemie kontroli dostępu z programem KaDe. Jest to wygodne i tanie rozwiązanie. Ponadto istnieje możliwość importu danych pracowników oraz informacji o strukturze działów z programu KaDe do programu Punktualnik 2.0. Znacznie ułatwia to administratorowi zarządzanie oboma systemami i skraca czas wprowadzania danych.

Sprzęt i oprogramowanie firmy ControlSYS są znakomitym uzupełnieniem naszej dotychczasowej oferty w zakresie systemów związanych z ewidencją i rozliczaniem czasu pracy. System RCP firmy ControlSYS jest oferowany równolegle z systemem rejestracji czasu pracy BiBi firmy MicroMade.

Warto również dodać, że ostatnio obie wspomniane firmy zaoferowały niezależnie nowe moduły programowe *Przedszkole*. Moduły te umożliwiają rejestrowanie obecności i naliczanie opłat za pobyt dzieci w przedszkolu. Postaram się w rozwinąć ten temat w kolejnym numerze *Zabezpieczeń*.

Podsumowanie

Każdy klient znajdzie w naszej ofercie rozwiązanie odpowiadające jego potrzebom – zarówno proste generatory raportów RCP w bezpłatnym oprogramowaniu KaDe i współpracujące z tym oprogramowaniem jedne z najtańszych na naszym rynku kontrolery zintegrowane KZ-1000, jak i profesjonalne rozwiązania wykorzystujące sprzęt i oprogramowanie firmy ControlSYS lub MicroMade.

Ryszard Sobierski
AAT Holding

Systemy alarmowe **Satel**

micra

bezprzewodowy system alarmowy

Niezawodna ochrona
dla małych obiektów

Bezprzewodowy system alarmowy MICRA jest idealnym rozwiązaniem wszędzie tam, gdzie potrzebny jest prosty i niezawodny system z komunikatorem GSM. Dzięki wykorzystaniu bezprzewodowych czujek, jego montaż jest szybki i niekłopotliwy. Obsługa za pomocą: pilotów, bezprzewodowego manipulatora czy telefonu komórkowego, jest prosta i intuicyjna. Dzięki wejściom analogowym, moduł alarmowy MICRA może pełnić także funkcję dozoru urządzeń technicznych przekazując informację o ich stanie, jak również o przekroczeniu krytycznych parametrów, np. temperatury lub ciśnienia.

Prosty i szybki montaż, łatwa konfiguracja, intuicyjna obsługa i możliwość sterowania z telefonu komórkowego to główne zalety modułu MICRA.

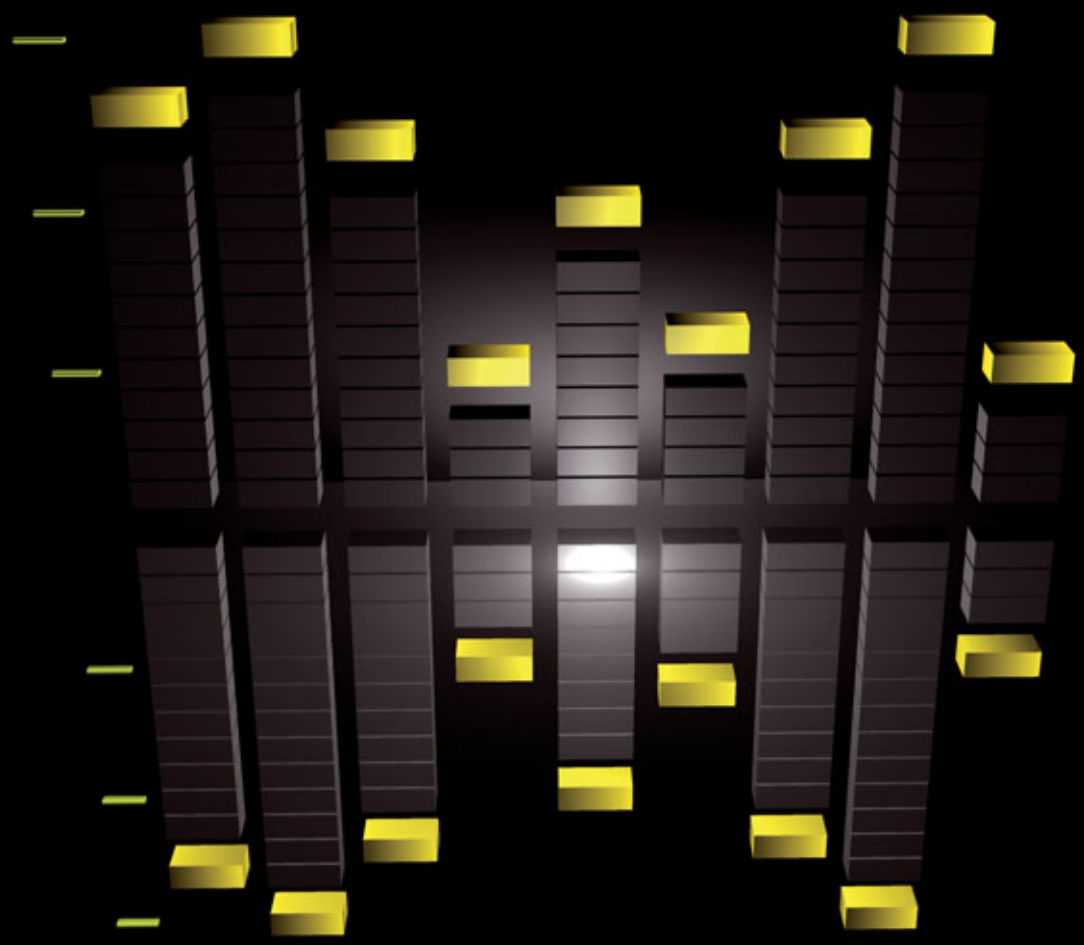
Więcej informacji na
www.satel.pl

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

Satel®

Zapomniane ultradźwięki

zastosowanie dopplerowskich czujek ruchu w systemach alarmowych w obiektach budowlanych



Marcin Buczaj

Skuteczna realizacja celów ochrony związanych z pracą systemów sygnalizacji włamania i napadu to szczelne zabezpieczenie obiektu przed możliwymi zagrożeniami i reagowanie na każdą próbę wtargnięcia intruza do jego wnętrza. Wykorzystywane do ochrony obiektów systemy sygnalizacji włamania i napadu mają za zadanie przekazać użytkownikowi danego systemu informacje o zidentyfikowaniu zagrożenia. Im dalej znajduje się miejsce zaatakowane przez intruza, tym dłuższy jest czas przeciwdziałania zaistniałemu zagrożeniu, dlatego elementy detekcyjne systemu należy dobrać w taki sposób, aby umożliwić prawidłową identyfikację zagrożenia na jak najwcześniejszym etapie jego powstania. W obiektach budowlanych można zastosować dopplerowskie czujki ultradźwiękowe. Główną część artykułu stanowi charakterystyka ultradźwięków i omówienie ich wykorzystania w dopplerowskich czujkach ruchu oraz analiza i ocena ich praktycznego zastosowania w ochronie obiektów przed włamaniem

1. Wstęp

Ze względu na długość procesu wykrywania zagrożenia ważne jest, aby system alarmowy wyposażony był w skuteczne środki detekcyjne działające zarówno wewnątrz obiektu (detekcja zaistniałej penetracji obiektu), jak i na jego peryferiach (detekcja podjęcia próby penetracji obiektu). Umożliwia to sprawny przebieg procesu wykrywania zagrożeń i ich neutralizację na wstępnym etapie powstawania [1,2].

Układami zabezpieczającymi strefy obwodowe budynku są najczęściej zabezpieczenia służące do detekcji prób wejścia do obiektu przez otwory okienne i drzwiowe. Obecnie otwory te zabezpieczane są czujkami kontaktronowymi lub stykowymi, które są podstawowymi elementami ochrony peryferyjnej obiektu. Wadą takich zabezpieczeń jest możliwość dość prostego ich obejścia, np. poprzez wybicie szyby. Czujka zabezpieczająca otwór nie działa, nie nastąpi wtedy detekcja, a zagrożenie może zostać wykryte już tylko przez elementy detekcyjne zainstalowane wewnątrz chronionego obiektu.

Wydaje się, że w przypadku zastosowania czujek ultradźwiękowych do ochrony przestrzeni między szybami chroniona będzie cała ta przestrzeń. Każdy ruch w jej obrębie będzie wywoływał sygnał alarmowy. Ze względu na znikomą przenikalność fal ultradźwiękowych przez elementy konstrukcyjne okna (szyby, ramy) zaletą opisywanego rozwiązania będzie ograniczenie chronionego obszaru tylko do przestrzeni między szybami. Ze względu na brak elementów ruchomych w tym miejscu zminimalizowane będzie również ryzyko generowania fałszywych alarmów przez czujkę. Artykuł stanowi pewnego rodzaju polemikę z panującą powszechnie opinią o nieprzydatności czujek ultradźwiękowych w systemach alarmowych. Ta zła opinia wynika z niewielkiego zasięgu czujki i możliwości wywoływania fałszywych alarmów przez liczne czynniki zewnętrzne. Z tych powodów czujki ultradźwiękowe nie znalazły szerokiego zastosowania w systemach alarmowych w budynkach, są natomiast powszechnie stosowane w alarmach samochodowych jako element umożliwiający wykrycie próby wejścia do wnętrza pojazdu.

W artykule zostanie przedstawiona koncepcja umieszczenia ultradźwiękowych czujek ruchu pomiędzy poszczególnymi warstwami okien skrzynkowych. Okna tego typu są dość powszechnie stosowane w budownictwie mieszkaniowym, a ich skuteczne zabezpieczenie umożliwi szybką identyfikację zagrożenia. Celem prowadzonych badań będzie ocena możliwości wykrywania prób sforsowania zabezpieczanej strefy (okna) oraz porównanie czujek ultradźwiękowych ze stosowanymi obecnie rozwiązaniami (czujkami kontaktronowymi i stykowymi) pod względem skuteczności.

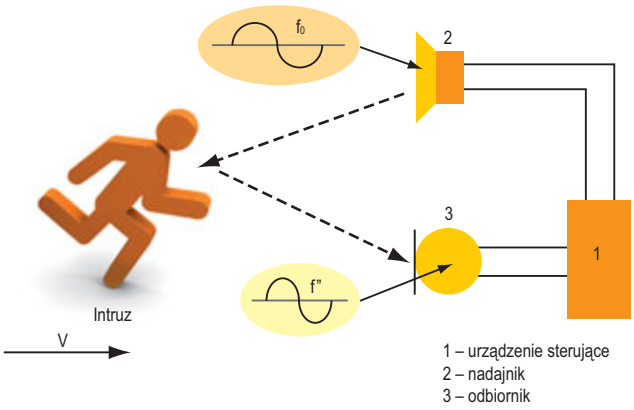
2. Charakterystyka ultradźwięków i dopplerowskich czujek ultradźwiękowych

Ultradźwiękami nazywa się drgania o częstotliwości przekraczającej górną granicę słyszalności ucha ludzkiego (od 16-20 kHz do 10 GHz). Fale ultradźwiękowe o częstotliwości do 0,6 MHz mogą rozchodzić się w ośrodkach stałych, ciekłych i gazowych [5]. Podstawowe właściwości ultradźwięków [4]:

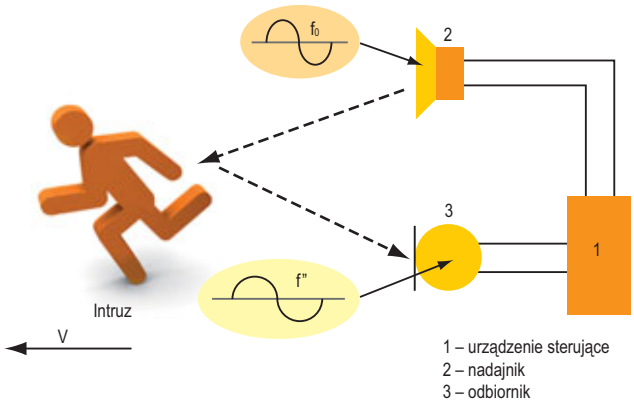
- fale ultradźwiękowe rozchodzą się promieniście od źródła wzdłuż linii propagacji;
- na granicy ośrodków rozchodzenia się część energii fali ultradźwiękowej jest rozpraszana, część pochłaniana, a część odbijana w stopniu zależnym od rodzaju granicy ośrodków;
- tłumienie fal dźwiękowych w powietrzu rośnie wraz ze wzrostem wilgotności, ciśnienia i zapylenia oraz w postępie geometrycznym wraz ze wzrostem częstotliwości fali;
- energia fali ultradźwiękowej jest odwrotnie proporcjonalna do kwadratu odległości od źródła.

Dopplerowskimi czujkami ruchu (detektorami ruchu) nazywa się elementy systemu alarmowego wykorzystujące do detekcji zagrożenia i wytworzenia sygnału alarmowego zjawisko zmiany częstotliwości fali odbieranej (w porównaniu z wzorcową częstotliwością fali emitowanej przez nadajnik), które występuje wówczas, gdy odległość między nadajnikiem a odbiornikiem, jaką musi przebyć emitowana fala, ulega zmianie (efekt Dopplera). Wszystkie rodzaje detektorów ruchu zalicza się do czujek aktywnych, ponieważ zasada ich działania opiera się na emisji fali (a więc pewnej ilości energii) do otoczenia [3,5].

W przypadku ultradźwiękowych czujek ruchu wykorzystywanych w systemach alarmowych dochodzi do sytuacji, w których nadajnik i odbiornik pozostają w spoczynku względem siebie. W takim przypadku warunkiem powstania zjawiska Dopplera jest zmiana drogi, jaką musi przebyć emitowana fala dźwiękowa odbijająca się od obiektu będącego w ruchu i znajdującego się pomiędzy nieruchomym nadajnikiem i odbiornikiem. Dla jednego sygnału wysyłanego z nadajnika i docierającego do odbiornika zachodzą w istocie bezpośrednio następujące po sobie dwa zjawiska Dopplera: pierwsze



Rys. 1. Efekt Dopplera w ultradźwiękowej czujce ruchu – ruch obiektu w kierunku układu nadajnik-odbiornik



Rys. 2. Efekt Dopplera w ultradźwiękowej czujce ruchu – ruch obiektu od układu nadajnik-odbiornik

zachodzi pomiędzy nadajnikiem a obiektem, a drugie – pomiędzy obiektem a odbiornikiem.

Jeżeli wszystkie obiekty pozostające w zasięgu czujnika będą pozostawały w spoczynku, droga, jaką musi przebyć emitowana fala, będzie stała. Nie nastąpi wtedy zmiana częstotliwości rejestrowanej przez odbiornik w porównaniu z częstotliwością emitowaną przez nadajnik (rys. 3). Jeśli w polu działania czujki wystąpi ruch obiektu, od którego emitowana fala będzie się odbijać, to droga, jaką musi przebyć fala, a w związku z tym także częstotliwość rejestrowana w odbiorniku, zacznie ulegać zmianie (rys. 4). Zależność określająca wartość częstotliwości Dopplerowskiej Δf ma postać [3,4,6]:

$$\Delta f = \frac{2V}{V_0 - V} \cdot f_0 \qquad (1)$$

przy założeniu, że:

$V_X > 0$ w przypadku przybliżania się obiektu do układu nadajnik – odbiornik;

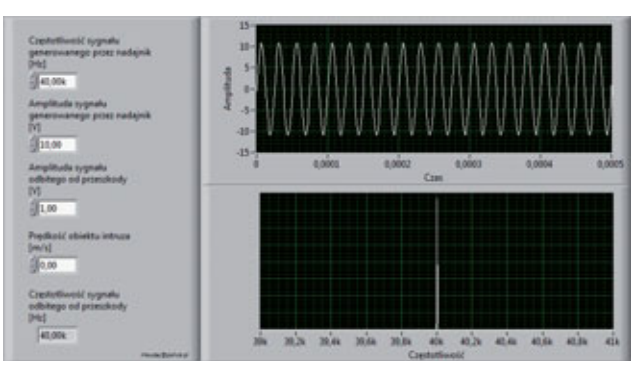
$V_X < 0$ w przypadku oddalania się obiektu od układu nadajnik – odbiornik.

3. Ocena możliwości i przydatności dopplerowskich czujek ultradźwiękowych w ochronie obwodowej obiektów

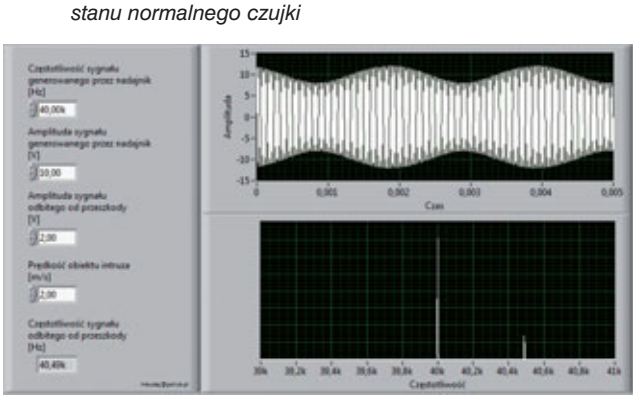
Aby potwierdzić przydatność ultradźwiękowych czujek ruchu jako rozwiązania alternatywnego względem rozwiązań, które są obecnie stosowane do zabezpieczania otworów okiennych, czyli kontaktronowych i stykowych czujek, przeprowadzono badania.

W badaniach sprawdzających możliwości wykorzystania ultradźwiękowych czujek ruchu do zabezpieczania otworów okiennych w oknach wielowarstwowych (np. typu skrzynkowego) użyto zbudowanego do tego celu modelu takiego okna (rys. 5) Konstrukcja modelu okna została opracowana w taki sposób, aby można było wykonać następujące testy:

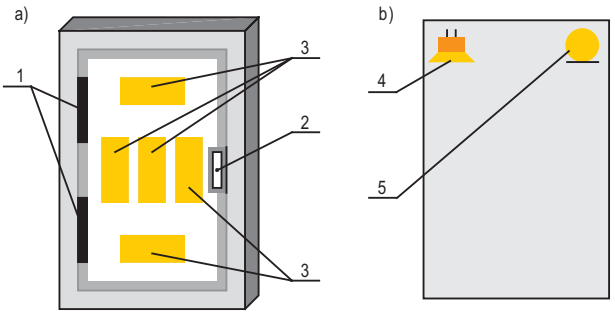
- forsowanie okna przez wyważenie jego skrzydła (zdarzenie 1),
- forsowanie okna przez otworzenie jego skrzydła (zdarzenie 2),
- forsowanie okna po wykonaniu w jego części otworu, ale bez otwierania jego skrzydła – zastosowano różne warianty umiejscowienia otworów (zdarzenie 3),
- zakłócenie pracy systemu alarmowego przez próby wywołania fałszywego alarmu – wykonywanie ruchów po zewnętrznej stronie okna (zdarzenie 4).



Rys. 3. Przebieg czasowy sygnału i widmo częstotliwości dla stanu normalnego czujki



Rys. 4. Przebieg czasowy sygnału i widmo częstotliwości w przypadku wykrycia zagrożenia



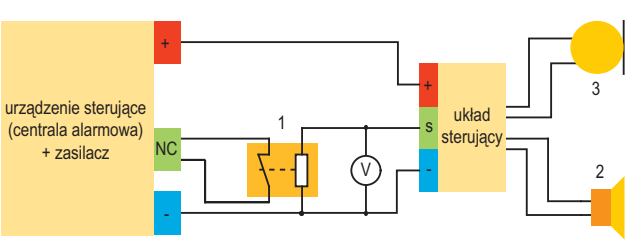
Rys. 5. Model okna skrzynkowego z umieszczoną wewnątrz niego ultradźwiękową czujką
a) rozmieszczenie elementów umożliwiających przeprowadzenie testów
b) rozmieszczenie elementów ultradźwiękowej czujki ruchu
1 – zawiasy, 2 – klamka, 3 – otwory z przesłonami, 4 – nadajnik czujki, 5 – odbiornik czujki.

Testowany model był wyposażony dodatkowo w układ pomiarowy (rys. 6). W skład układu pomiarowego wchodziły następujące elementy: ultradźwiękowa czujka ruchu typu URZ0530, centrala alarmowa, przekaźnik pośredniczący, woltomierz i zasilacz stabilizowany 12 V.

Po podłączeniu zasilania o wartości U=12 V do układu sterowania czujki URZ0530 wystąpiły następujące poziomy napięć na wyjściu sygnałowym czujki:

- U_S=6,68 V (w stanie normalnym, gdy wszystkie elementy czujki działają poprawnie i nie ma zaburzenia, które wywołałoby reakcję czujki);
- U_S=0 V (w stanie alarmowania, gdy wszystkie elementy czujki działają poprawnie i czujka jest pobudzona na skutek wykrycia zaburzenia).

Model okna typu skrzynkowego został dodatkowo wyposażony w standardową czujkę kontaktronową i standardową



Rys. 6. Schemat układu połączeń urządzeń w modelu, 1 – przekaźnik, 2 – nadajnik ultradźwiękowej czujki ruchu, 3 – odbiornik ultradźwiękowej czujki ruchu

Zdarzenie	Pobudzanie systemu alarmowego		
	Czujka ultradźwiękowa	Czujka kontaktronowa	Czujka stykowa
1	+	+	+
2	+	+	+
3	+	-	-
4	-	-	-

Tab. 1. Wyniki badań – pobudzanie systemu alarmowego

czujkę stykową. Umieszczenie tych elementów w modelu umożliwiło sprawdzenie skuteczności działania układu w różnych konfiguracjach sprzętowych. Dzięki temu możliwa jest ocena działania tych elementów w różnych przypadkach.

Skuteczność działania systemu określano na podstawie prawidłowego (oczekiwanego) zadziałania systemu w różnych wariantach zdarzeń. W przypadku pierwszych trzech zdarzeń oczekiwanym rezultatem było pobudzenie systemu alarmowego, natomiast w przypadku czwartego zdarzenia – brak pobudzenia. Wyniki przeprowadzonych doświadczeń zostały przedstawione w tabeli 1.

Testy, których wyniki znajdują się w tabeli 1, nie uwzględniały możliwości sabotowania poszczególnych układów detekcyjnych podczas próby sforsowania zabezpieczenia. W przypadku testów w bardziej urealnionych warunkach (dopuszczona ingerencja intruza w system w celu sabotowania jego działania) możliwe było sforsowanie zabezpieczeń bez wywołania alarmu (zdarzenie 2), gdy zastosowano układy wyposażone w kontaktron, a zwłaszcza w czujkę stykową. Gdy zastosowano czujkę ultradźwiękową, takie próby były nieskuteczne. Jedynie w przypadku ustawienia zbyt dużej czułości układu detekcyjnego ultradźwiękowej czujki ruchu możliwe było występowanie w układzie fałszywych alarmów powodowanych pobudzaniem się tej czujki.

4. Podsumowanie

Ważnym czynnikiem, który decyduje o skuteczności działania systemu alarmowego, jest czas wykrycia zagrożenia. Im krótszy jest czas pomiędzy chwilą wykrycia zagrożenia a reakcją użytkownika systemu, tym większa jest szansa na ograniczenie szkód. Dlatego ważne jest wyposażenie systemów nadzoru w środki techniczne, dzięki którym skuteczne wykrycie zagrożenia następuje jeszcze przed wtargnięciem intruza do wnętrza obiektu. W związku z tym ciężar procesu detekcji zagrożenia powinien być przesuwany w stronę ochrony obwodowej obiektu.

Stosowane obecnie do zabezpieczania otworów okiennych i drzwiowych rozwiązania w postaci czujek kontaktronowych i stykowych w niektórych sytuacjach są nieskuteczne (np. w przypadku wybicia szyby). Znacznie skuteczniejszym, ale też bardzo drogim rozwiązaniem może być zastosowanie do zabezpieczenia tych elementów aktywnych barier podczerwieni. Równie skuteczne jest zastosowanie ultradźwiękowych czujek ruchu, jednak ich efektywne działanie jest możliwe tylko w obrębie małych obiektów. W takim przypadku chroniona jest cała przestrzeń wewnątrz chronionego obiektu, która jest ograniczona jego elementami konstrukcyjnymi.

Ultradźwiękowe czujki ruchu nie są dużo droższe od czujek kontaktronowych i stykowych, a ich zastosowanie umożliwia znacznie większą wykrywalność zagrożeń (chroniony jest cały obszar, na który może wtargnąć intruz). Mogą zatem skutecznie zastąpić obecnie stosowane rozwiązania.

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

Literatura

1. Buczaj M., *Czas jako kryterium skuteczności przebiegu procesu neutralizacji zagrożeń w systemach nadzorujących stan chronionego obiektu, Zabezpieczenia* nr 6(70)/2009.
2. Buczaj M., *Strefowa organizacja systemów alarmowych w aspekcie realizacji założonych zadań ochrony w obiektach budowlanych, Zabezpieczenia* nr 5(81)/2011.
3. Halliday D., Resnick R., Walker J., *Podstawy fizyki*. T. 2, PWN, Warszawa 2008.
4. Nawrowski R., Skowronek K., *Systemy alarmowe pojazdów samochodowych,* Wydawnictwo Politechniki Poznańskiej, Poznań 1997.
5. Gajek A., Juda Z., *Czujniki,* Wydawnictwo WKiŁ, Warszawa 2008.
6. Resnick R., Halliday D., *Fizyka cz. 1*, PWN, Warszawa 2001.

GEO KAT

Geo-Kat jest firmą o charakterze eksperckim z wysoce wyspecjalizowaną kadrą inżynierską. Zakres działalności obejmuje kompleksowe realizacje usług w zakresie systemów bezpieczeństwa, systemów przeciwpożarowych, systemów telekomunikacyjnych oraz automatyki budynkowej BMS i HMS.

Jesteśmy dystrybutorem Systemu Sygnalizacji Pożaru **MX/ZX ZETTLER** oraz Systemu Zarządzania Ruchem i Transportem Publicznym **SCATS i RAPID**.

Oferujemy profesjonalne usługi w zakresie:
- DORADZTWA
- PROJEKTOWANIA
- ZARZĄDZANIA PROJEKTEM
- WYKONAWSTWA INSTALACJI
- INTEGRACJI I URUCHOMIEŃ
- SERWISU I KONSERWACJI

GEO-KAT Sp. z o.o.
Al. Prymasa Tysiąclecia 145/149, 01-424 Warszawa,
Tel. 22 877 08 80, Fax 22 877 08 97

www.geokat.com.pl, e-mail: info@geokat.com.pl

Aper Home Alarm

Artur Jajszczak

Niebawem w asortymencie firmy SPS Electronics Sp. z o.o. pojawi się nowa, bezprzewodowa centrala alarmowa Aper Home Alarm. Ze względu na fabryczne zaprogramowanie centrali oraz niezwykłą prostotę jej instalacji i obsługi urządzenie to stanowi innowacyjne rozwiązanie w dziedzinie bezprzewodowych central alarmowych i przeznaczonych do nich czujek

Fot. 1. Elementy zestawu SAFE HOME

W związku ze wzrastającą liczbą rozwiązań oferowanych przez szybko rozwijający się rynek systemów alarmowych zmieniają się preferencje klientów, którzy od systemów oczekują już nie tylko elastyczności i niezawodności, ale również oszczędności czasu instalacji i minimalizacji kosztów. Centrala alarmowa Aper Home Alarm w zupełności spełnia wymagania instalatorów, umożliwiając zoptymalizowanie kosztów i czasu montażu oraz wpisując się w nurt nowoczesnych i coraz bardziej popularnych rozwiązań bezprzewodowych. Urządzenie to jest wprowadzane na rynek po wielu konsultacjach z użytkownikami systemów alarmowych oraz weryfikacji szeregu pomysłów na system łączący w sobie wszystkie zalety centrali alarmowej z uniwersalnymi funkcjami, które skutecznie upraszczają jej montaż. Łatwość montażu w każdych warunkach jest zazwyczaj jednym z nadrzędnych i najbardziej pożądanych przez klientów atrybutów centrali, zwłaszcza w przypadku wykończonych mieszkań, których właściciele niechętnie i z trudnością akceptują uciążliwy proces ponownego okablowania lokalu.

Kolejną, nie mniej pożądaną zaletą centrali jest łatwość zaprogramowania jej oraz wszystkich współpracujących z nią elementów. Fabryczne zaprogramowanie centrali eliminuje konieczność wielokrotnego, czasochłonnego wprowadzania standardowych ustawień w podobnych do siebie lub niemal identycznych systemach alarmowych. Niewątpliwie ogromna oszczędność czasu zostanie doceniona przez tych instalatorów, dla których programowanie przewodowych systemów alarmowych jest najdłuższym etapem pracy. Wygoda instalacji, jaką zapewni bezprzewodowa centrala alarmowa Aper Home Alarm, jest obecnie warunkiem efektywności rozwiązań alarmowych.

Dążąc do zaspokojenia potrzeb współczesnego rynku oraz uproszczenia i optymalizacji pracy instalatorskiej firma SPS Electronics Sp. z o.o. proponuje zestaw SAFE HOME,

Fot. 3. Bezprzewodowy system alarmowy Aper Home Alarm

w skład którego, obok bezprzewodowej centrali alarmowej Aper Home Alarm, wchodzą dwie dedykowane czujki PIR odporne na zwierzęta do 38 kg, jeden kontaktron na drzwi lub okno oraz dwa piloty do załączania i wyłączania systemu. System SAFE HOME służy do nadzorowania pomieszczeń mieszkalnych. Został zaprojektowany z najwyższą starannością o bezpieczeństwo chronionych obiektów, we współpracy z czołowym izraelskim producentem bezprzewodowych systemów zabezpieczeń. SAFE HOME to najprostszy i jednocześnie niezawodny sposób na zapewnienie każdej rodzinie poczucia faktycznego bezpieczeństwa. System ten można łatwo i szybko zainstalować zarówno w dużym, wolnostojącym domu, jak i w małym mieszkaniu, gdyż nie wymaga okablowania i programowania.

Dzięki standardowej linii telefonicznej oraz komunikatorowi GSM/GPRS centrala Aper Home Alarm oferuje znacznie więcej możliwości oraz maksymalną wszechstronność przesyłania informacji (np. do centrum monitorowania alarmów) niż wiele innych porównywalnych systemów. Ponadto możliwość

Fot. 2. Przykładowe rozmieszczenie elementów systemu Aper Home Alarm w mieszkaniu

CNB TECHNOLOGY Inc.
HD XNET
łatwa konfiguracja
proste użytkowanie
darmowy software
ROZWIĄZANIA IP
KOMFORT & BEZPIECZEŃSTWO

XNET - Kamery XNET HD firmy CNB mogą pracować z rozdzielczością full HD (2Mpx) przy 25kl/s – „full real time" – oraz generują obraz panoramiczny 16:9 (taki jak w telewizji wysokiej rozdzielczości). Wybieranie progresywne wraz prędkością 25 kl/s gwarantuje płynność ruchu bez smużeń czy urywanych krawędzi.
ONVIF - XNET HD obsługuje protokół ONVIF który jest standardem pozwalającym na bezproblemowe łączenie kamer i oprogramowania różnych producentów w jeden system.
SDK - Do wszystkich kamery IP dostępne są pakiety SDK i API co pozwala na integrację z własnym oprogramowaniem np. w systemach kontroli dostępu.

DARMOWE OPROGRAMOWANIE

IP Installer - Dzięki funkcji Plug & Easy Play over IP (protokoły Bonjour oraz UPnP możliwe jest wyszukanie kamer w sieci, połączenie za nimi za pomocą przeglądarki a także ma możliwość zmiany adresu IP kamery „w locie". Takie rozwiązanie pozwala na bardzo wygodne ustawienie adresów kamer IP przed ich konfiguracją.

CMS - Głównym zadaniem tego programu jest zarządzanie i administracja małymi i średnimi sieciami IP CCTV, podgląd on-line, przeglądanie nagrań na rejestratorach (nagrań na dysku lokalnych rejestratora) oraz praca jako prosty NVR. CMS obsługuje do 128 kamer, w tym 64 kamery IP, tryb Dual Monitor oraz wielopoziomowa E-Mapę.

XNET MOBILE VIEWER pozwala na zdalny podgląd, sterowanie kamerami obrotowymi czy przeglądanie nagrań, a SSL zapewnia poufność transmisji. Mobile Viewer występuje w wersji na iPhone oraz na urządzenia z system Android.

NVR umożliwia rejestrację obrazów z maks. 32 kamer IP. Jest bardzo prosty w konfiguracji i użytkowaniu, niezbyt wymagające sprzętowo a dodatkową zaletą jest brak ograniczeń bazy danych, czyli czasu zapisu.

Axxon SMART - w wersji dla CNB - pozwala na pracę wielu klientów równocześnie, posiada detekcję ruchu, przekroczenia linii, zbyt długiego przebywania w danym miejscu, porzucenia przedmiotu a także zabrania przedmiotu. Możliwe jest klasyfikowanie zdarzeń i ich późniejsze przeszukiwanie według stopnia ważności. Maksymalnie możemy podłączyć 16 kamer, limit bazy danych wynosi 2TB co pozwala na ok 7 dni zapisu 6 kamer FullHD z detekcją ruchu.

&GDE POLSKA
Włosań, ul. Świątnicka 88, 32-031 Mogilany
tel. 12 256 50 25, 12 256 50 35
fax 12 270 56 96
biuro@gde.pl
www.gde.pl
GWARANCJA &GDE POLSKA DOOR-2-DOOR
Infolinia techniczna 693 631 403
Pomoc techniczna techniczny@gde.pl
JOTAKABEL | CNB | SCOT | LonBon | tti | COMMAX | ABAXO

zastosowania uniwersalnych wyjść PGM-5 pozwala na połączenie systemu z dowolnymi urządzeniami automatyki domowej lub nadajnikiem systemu przesyłania alarmów.

Prostotę instalacji i użytkowania bezprzewodowego systemu zabezpieczeń dopełnia wizualny walor zestawu. Elegancka, nowoczesna i uniwersalna obudowa centrali Aper Home Alarm doskonale komponuje się z wyposażeniem każdego wnętrza. Niewielkich rozmiarów panel wyposażony w wyświetlacz LCD, który umożliwia wizualizację komunikatów alarmowych, stanowi dyskretny i nieinwazyjny element pomieszczenia.

Centrala Aper Home Alarm pracuje w kodzie zmiennym na częstotliwości 868 MHz. Należy zaznaczyć, że częstotliwość 868 MHz jest bardziej odporna na zakłócenia radiowe od powszechnej częstotliwości 433 MHz wykorzystywanej przez rozmaite urządzenia stosowane w gospodarstwie domowym, np. słuchawki bezprzewodowe, piloty sterujące pracą wielu urządzeń czy systemy transmisji wizyjnej. Ze względu na stale wzrastającą liczbę urządzeń pracujących na częstotliwości 433 MHz pożądane stało się użytkowanie innej, bardziej odpornej na zakłócenia częstotliwości radiowej. Wykorzystanie częstotliwości 868 MHz znacznie ułatwia instalację, niezakłóconą i bezproblemową pracę oraz użytkowanie systemów bezprzewodowych.

Należy docenić również nowy sposób montażu centrali Aper Home Alarm. Od panelu przedniego całkowicie oddzielono panel tylny centrali, który jest przymocowywany do ściany. Zawiera on wszystkie przyłącza od panelu głównego łączonego za pomocą taśm szyny danych. Jednocześnie wprowadzony został wewnętrzny montaż modułu dodatkowych przekaźników i modułu transmisji GSM. Kolejnym udogodnieniem są cztery niezależne partycje w centrali, z których każda może być załączana całkowicie lub częściowo, co znacznie zwiększa elastyczność bezprzewodowego systemu alarmowego. Centrala umożliwia zbudowanie systemu, który może składać się z czterech wirtualnych, niezależnych podsystemów w obrębie jednego mieszkania.

Wszystkie nadajniki radiowe, które wchodzą w skład zestawu, tj. dwie czujki PIR (odporność na zwierzęta do 38 kg), kontaktron oraz dwa piloty, wyposażone są w baterie umożliwiające, bez konieczności ich wymiany, długoletnią pracę urządzeń. To zasługa specjalnie opracowanego systemu oszczędzania baterii oraz przemyślanej konstrukcji czujek, które wykorzystują energooszczędne sensory. Centrala Aper Home Alarm zasygnalizuje konieczność wymiany baterii w urządzeniach z odpowiednim wyprzedzeniem, zapewniając użytkownikowi potrzebną ilość czasu na ich wymianę oraz gwarantując ciągłość pracy systemu.

Proponowany przez firmę SPS Electronics Sp. z o.o. zestaw do zabezpieczenia mieszkania SAFE HOME można rozbudować, aby jeszcze bardziej podwyższyć poziom bezpieczeństwa i komfort mieszkańców, dodając takie akcesoria jak wskaźniki dymu, czadu czy gazu, dwukierunkowe piloty sygnalizujące uzbrojenie systemu, różnego rodzaju i wielkości czujki ruchu, w tym również zewnętrzne i kurtynowe, dodatkowe bezprzewodowe klawiatury oraz sygnalizatory radiowe. Uzupełniony o powyższe elementy zestaw znacznie zwiększy efektywność całego systemu alarmowego oraz rozszerzy zakres jego funkcjonalności zgodnie z preferencjami użytkowników końcowych.

Artur Jajszczak
SPS Electronics

Jeden dzień. 124 incydenty.
124 słuszne decyzje.

Kiedy ponosi się odpowiedzialność za bezpieczeństwo systemu miejskiego transportu publicznego obejmującego tysiące autobusów, ilość incydentów,które należy codziennie wykryć, ocenić i rozwiązać jest ogromna.

Czy nie chcielibyście Państwo posiadać centralnego systemu nadzoru wizyjnego wyposażonego w inteligentne narzędzia, umożliwiające podejmowanie szybkich, i słusznych decyzji w celu zminimalizowania aktów wandalizmu i zakłóceń w dostarczaniu usług a także by przyciągnąć większą ilość pasażerów? Narzędzia takie jak automatyczne powiadamianie i udostępnianie materiału wizyjnego na żywo ze wszystkich części systemu tranzytowego-dworców, zajezdni, infrastruktury a nawet bezprzewodowo z taboru kolejowego –ze szczegółowością HDTV?

Pomyśleliśmy, że chcielibyście. Dlatego zadbaliśmy o to by nasze rozwiązania z zakresu sieciowego nadzoru wizyjnego mogły poradzić sobie ze wszystkim. Tak więc możesz podjąć właściwą decyzję. W przypadku każdego zdarzenia..

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

Axis oferuje dedykowane rozwiązania nadzoru wizyjnego dla wszystkich środowisk związanych z transportem. • Odporne na wibracje kamery i rejestratory mobilne • Wandaloodporne kamery wewnętrzne i do pracy na zewnątrz • Kamery termowizyjne i pracujące przy słabych warunkach oświetleniowych dla skutecznego nadzoru nocą.

AXIS COMMUNICATIONS

Oświetlenie
w systemach nadzoru wizyjnego
(część 2)

Agata Majkucińska

O tym, że dobór właściwego oświetlenia ma kluczowe znaczenie w przypadku dozoru wizyjnego, starałam się Państwa przekonać w poprzednim artykule, opublikowanym w numerze 5/2011 *Zabezpieczeń*. W niniejszym artykule chciałabym zwrócić uwagę na pozostałe kwestie związane z doborem oświetlenia i dostosowaniem go do wymogów systemów monitoringu, a także omówić sprawę wyboru kamery w zależności od warunków panujących w pomieszczeniach lub na zewnątrz budynku

Wiązki świetlne

Aby zapewnić poprawne oświetlenie w telewizyjnych systemach nadzoru, kąt promieniowania powinien być tak dobrany, by cała obserwowana scena była odpowiednio oświetlona. Nowoczesne oświetlacze typu *Adaptive Illumination* pozwalają na dostosowanie kąta promieniowania do specyficznych wymogów obserwowanej sceny. Zbyt wąska wiązka światła wytwarza tzw. *white out*, czyli rozjaśnienie w środku sceny z jednoczesnym nieprawidłowym oświetleniem pozostałych obszarów. Z kolei oświetlenie zbyt szeroką wiązką oznacza stratę światła i zmniejszenie odległości skutecznej obserwacji.

W wielu instalacjach wykorzystywane są obiektywy o zmiennej ogniskowej i byłoby idealnie, gdyby dało się osiągnąć taki sam poziom elastyczności w zakresie oświetlenia, aby maksymalnie zwiększyć skuteczność działania systemu. Oświetlacze przeznaczone do pracy w systemach nadzoru wizyjnego, takie jak oferowane przez Axis, mają szeroki zakres kątów promieniowania, dlatego można wybrać kąt, który jest dokładnie dopasowany do pola widzenia kamer i zapewni przez to najlepszy obraz. Regulacja jest szybka i wygodna, a wymagany kąt promieniowania można łatwo uzyskać.

Prawo odwrotnych kwadratów

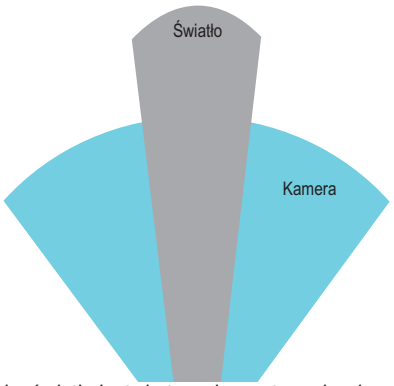
Natężenie oświetlenia w określonej lokalizacji jest odwrotnie proporcjonalne do kwadratu odległości od źródła światła. Zwróćmy uwagę na to, jakie są praktyczne konsekwencje tej zasady. Światło wypromieniowane przez odległe, punktowe źródło rozprzestrzenia się we wszystkich kierunkach. W praktyce oznacza to, że jeśli oświetlany obiekt zostanie przeniesiony z danego punktu do innego, leżącego dwa razy dalej od źródła światła, to ilość docierającego do niego światła będzie czterokrotnie mniejsza. Jeśli oświetlenie obiektu położonego 10 m od źródła światła wynosi 100 lx, odsunięcie tego obiektu na odległość 40 m od źródła światła spowoduje szesnastokrotny spadek poziomu oświetlenia, w wyniku czego oświetlenie tego obiektu zmniejszy się do 6,25 lx. Prawo odwrotnych kwadratów dotyczy zarówno światła białego, jak i podczerwonego.

Odległości robocze dla produktów Axis

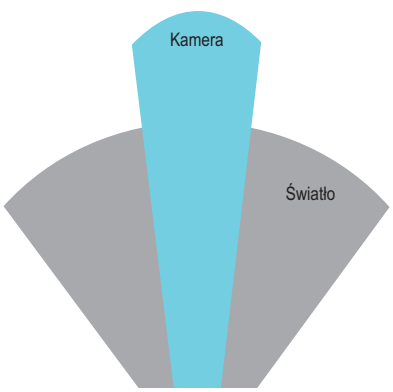
Wykres (rys. 5) ułatwia dobór odpowiedniego oświetlacza Axis pracującego w podczerwieni w zależności od kąta widzenia kamer i odległości obiektu od oświetlacza. Zauważmy, że pole wyróżnione kolorem odpowiada optymalnie wykorzystanemu obszarowi obserwacji, zaś pole zacienione oznacza obszar gorzej oświetlony.

Korzystanie z wielu oświetlaczy

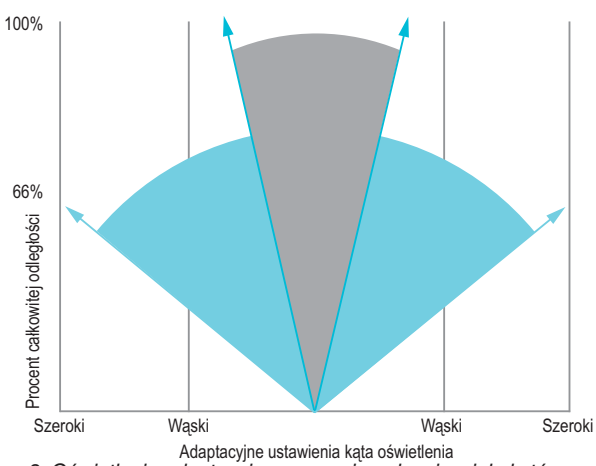
Prawo odwrotnych kwadratów pozwala określić ilość światła padającego na obszar znajdujący się w pewnej odległości od pojedynczego źródła światła, ale może być wykorzystane również do obliczania liczby dodatkowych oświetlaczy niezbędnych do osiągnięcia wymaganego zasięgu. Jeżeli podwoimy odległość od jednego oświetlacza, ilość padającego światła spadnie do poziomu 25%. A więc do oświetlenia jakiegoś obszaru z dwukrotnie większej odległości konieczne jest użycie czterech oświetlaczy o tej samej mocy ($2^2 = 4$). By osiągnąć



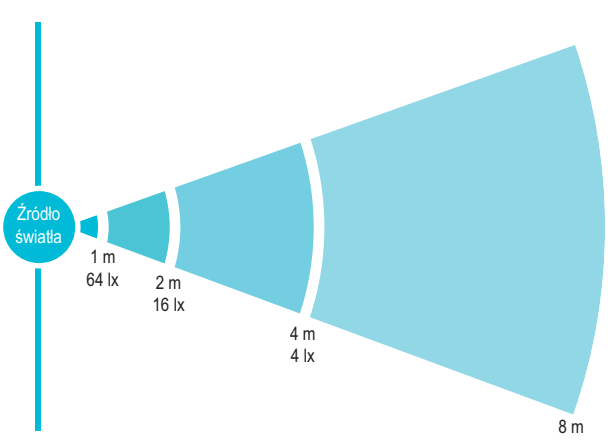
Rys. 1. Wiązka światła jest zbyt wąska w stosunku do pola widzenia kamery



Rys. 2. Wiązka światła jest zbyt szeroka w stosunku do pola widzenia kamery



Rys. 3. Oświetlenie adaptacyjne zapewnia pokrycie wielu kątów widzenia



Rys. 4. Prawo odwrotnych kwadratów

trzykrotnie większy zasięg oświetlenia, należy użyć dziewięciu oświetlaczy o tej samej mocy ($3^2 = 9$).

Prawo odwróconych kwadratów może być wykorzystane także do obliczenia wpływu liczby zastosowanych oświetlaczy na ich wypadkowy zasięg. W takim przypadku współczynnikiem korygującym zasięg jest pierwiastek kwadratowy z liczby użytych oświetlaczy. Na przykład wykorzystując cztery oświetlacze, uzyskamy dwukrotny wzrost zasięgu ($\sqrt{4} = 2$), a wykorzystując dwadzieścia pięć oświetlaczy, uzyskamy pięciokrotny wzrost zasięgu ($\sqrt{25} = 5$).

WSKAZÓWKA 1

Nie zawsze trzeba zastosować wiele oświetlaczy, by osiągnąć wzrost zasięgu. Oświetlacze z węższymi kątami promieniowania lub odznaczające się większą mocą mogą zapewnić wymagany dodatkowy wzrost zasięgu.

WSKAZÓWKA 2

Jeżeli konieczne jest oświetlenie pewnego obiektu znajdującego się w określonej odległości od źródła światła, a w systemie telewizyjnym wykorzystywane są obiektywy zmiennoogniskowe, możliwe jest umieszczenie oświetlacza o małej mocy w pobliżu obserwowanego obiektu. Przykładem takiego zastosowania może być brama oddalona od budynków i innych elementów infrastruktury.

WSKAZÓWKA 3

Podwojenie zasięgu oświetlenia wymaga czterokrotnie większej mocy.

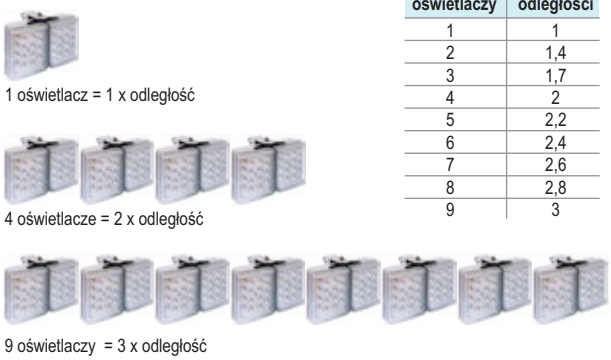
WSKAZÓWKA 4

Podwojenie liczby oświetlaczy zapewnia wzrost zasięgu o około 41%

Pomiar oświetlenia

Światło białe

Oświetlenie światłem białym jest mierzone w luksach. Luks jest jednostką oświetlenia w układzie SI, która nie charakteryzuje źródła światła, lecz jasność oświetlenia powierzchni, na którą pada światło. 1 lx = 1 lumen na metr kwadratowy.



Liczba oświetlaczy	Krotność odległości
1	1
2	1,4
3	1,7
4	2
5	2,2
6	2,4
7	2,6
8	2,8
9	3

Rys. 6. Korelacja liczby oświetlaczy z oświetlanym dystansem

Oświetlenie obserwowanej sceny światłem białym może być mierzone z użyciem luksomierza. Typowe poziomy natężenia światła w luksach są zilustrowane na rysunku nr 6.

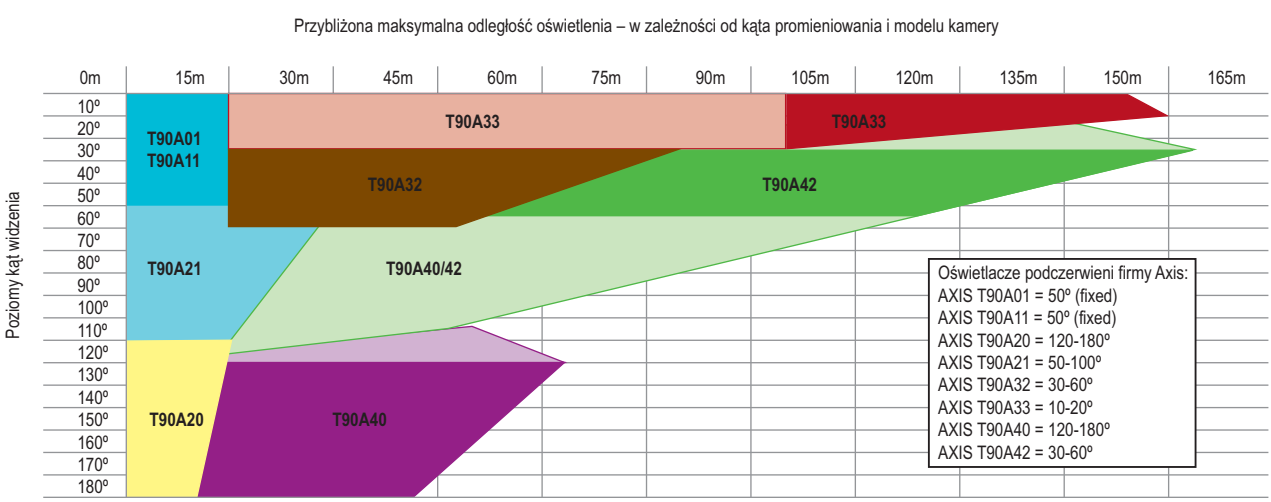
Światło podczerwone

Luks jest miarą oświetlenia światłem widzialnym, tymczasem światło podczerwone nie jest widzialne dla oka ludzkiego. Dlatego luks nie może być miarą oświetlenia światłem podczerwonym. Najpopularniejszym sposobem pomiaru intensywności oświetlenia światłem podczerwonym jest określenie mocy światła mierzonej w watach, przypadającej na metr kwadratowy oświetlanej powierzchni.

Potrzeba równomiernego oświetlenia

Podczas projektowania jakiegokolwiek systemu oświetlenia najważniejsze jest osiągnięcie równomiernego oświetlenia. Zarówno ludzkie oko, jak i kamera telewizyjna i jej obiektyw muszą dostosowywać się do znacznych różnic w poziomie oświetlenia w obrębie pola widzenia.

Prowadząc samochód w nocy, widzimy drogę, po której jedziemy, dzięki przednim światłom, jednakże gdy inny samochód zbliża się z przeciwka, nasza zdolność do obserwacji drogi ulega ograniczeniu, mimo iż poziom oświetlenia znacznie wzrasta. Dzieje się tak, ponieważ w centralnej części obserwowanej sceny umieszczone jest silne źródło światła, co powoduje zamykanie źrenicy w tęczówce oka. Takie same procesy zachodzą w kamerach pracujących w systemach dozorowych



Rys. 5. Wykres ułatwiający dobór oświetlaczy. Zależność maksymalnej odległości od kąta widzenia kamery i modelu użytego oświetlacza.

– jasna plama w obrębie obrazu spowoduje zamykanie się przesłony obiektywu i pogorszy zdolność urządzenia do obserwacji obszarów słabo oświetlonych. Aby uzyskać możliwie najlepszy obraz w nocy, oświetlenie musi być równomiernie rozprowadzone przy wykorzystaniu oświetlaczy zaprojektowanych do tych celów.

Wybór właściwej kamery

Czułość

Czułość jest parametrem określającym wrażliwość kamery na światło i zasadniczo oznacza minimalny poziom oświetlenia koniecznego do wytworzenia obrazu o akceptowalnej jakości, aczkolwiek określanie tej akceptowalnej jakości jest bardzo subiektywne. Dana jakość obrazu dla jednych może być akceptowalna, a dla innych nie do przyjęcia. Czułość kamer jest zazwyczaj mierzona w luksach, jednakże często nie wiadomo, czy wartości podawane przez producentów dotyczą minimalnego poziomu oświetlenia obserwowanej sceny, czy odnoszą się do poziomu oświetlenia przetwornika kamery światłem przechodzącym przez obiektyw. W przypadku kamer Axis wartość ta odnosi się do poziomu oświetlenia obserwowanej sceny. Chociaż podawane wartości liczbowe wydają się zawyżone i dotyczą jedynie światła widzialnego, wyrażanie czułości kamery w luksach jest powszechnie stosowane ze względu na łatwość i dostępność tej metody pomiaru.

WSKAZÓWKA 1

Nie istnieją kamery zdolne do pracy w zupełnej ciemności – każda kamera potrzebuje światła, by wytworzyć obraz o wysokiej jakości. Nawet najczulsze kamery działają lepiej w dobrych warunkach oświetleniowych, co przekłada się na wzrost amplitudy sygnału wyjściowego oraz poprawę stosunku sygnału do szumu.

Wyjątkiem są kamery termowizyjne, które tworzą obrazy z wykorzystaniem promieniowania cieplnego emitowanego przez pojazdy czy organizmy żywe, co pozwala na prowadzenie obserwacji także w kompletnych ciemnościach. Ciekawym rozwiązaniem jest również technologia Lightfinder firmy Axis, która została opisana w 4(80) numerze *Zabezpieczeń*.

WSKAZÓWKA 2

Aby dowiedzieć się więcej na temat światłoczułości kamer, można zapoznać się z naszymi dokumentami technicznymi „W najlepszym świetle" pod adresem: *www.axis.com/corporate/corp/tech_papers.htm*.

Dobór właściwego obiektywu

F-stop

Wartość F-stop (apertura) określa zdolność obiektywu do przepuszczania światła z obserwowanej sceny do przetwornika kamery. Mówiąc prosto – im niższa wartość F-stop, tym więcej światła przechodzi przez obiektyw. Tabela nr 1 ilustruje zależność poziomu oświetlenia od apertury obiektywu.

WSKAZÓWKA

Im niższa wartość F-stop obiektywu, tym więcej światła przechodzi na przetwornik. W przypadku obiektywów zmiennoogniskowych najmniejsza wartość F-stop jest osiągana przy ustawieniu „szerokokątnym", gdyż wartość F-stop jest wprost proporcjonalna do ogniskowej obiektywu.

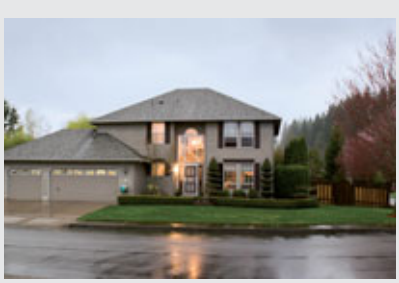
Transmisja

Zdolność do transmisji światła przez obiektyw określa wartość użytkową tego obiektywu. Część światła przechodzącego przez obiektyw zostaje utracona – zależnie od jakości materiałów, z jakich został on wykonany. Wartość F-stop obiektywu nie jest miarą jego zdolności do przepuszczania światła.

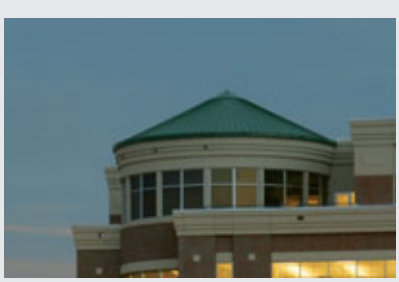
WSKAZÓWKA

Zdolność do przepuszczania światła przez obiektyw zmienia się wraz z długością fali. Na przykład – jeden obiektyw

Jasny słoneczny dzień = 10 000 - 100 000 lx



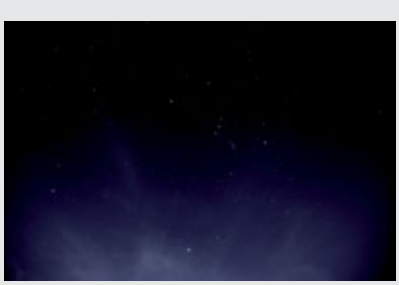
Pochmurny dzień = 1 000 - 10 000 lx



Zmierzch = 1 - 100 lx

Oświetlenie uliczne = 5 lx

Pełnia księżyca = 0,1 lx



Bezchmurna, gwieździsta noc = 0,0001 lx

Fot. 1. Natężenie światła w różnych typowych sytuacjach

Liczba przysłon	Przechodzące światło [%]	Ilość światła potrzebna do osiągnięcia oświetlenia przetwornika na poziomie 1 luksa
f/1	20	5 lx
f/1,2	15	7,5 lx
f/1,4	10	10 lx
f/1,6	7,5	13,3 lx
f/1,8	6,25	16 lx
f/2	5	20 lx
f/2,4	3,75	30 lx
f/2,8	2,5	40 lx
f/4	1,25	80 lx

Tab. 1. Zależność poziomu oświetlenia od apertury obiektywu

może przepuścić 95% widzialnego światła i 80% światła podczerwonego o długości fali równej 850 nm, podczas gdy inny obiektyw może przekazać 95% widzialnego światła i 50% światła podczerwonego o długości fali równej 850 nm. Dobierając obiektyw, należy wziąć pod uwagę zakres widmowy, w jakim będzie on wykorzystywany. Należy również pamiętać, że ilość utraconego światła jest mniejsza w przypadku soczewek szklanych niż w przypadku soczewek plastikowych.

Obiektywy przystosowane do pracy w podczerwieni

Obiektywy przystosowane do pracy w podczerwieni są zaprojektowane tak, by wyeliminować problem utraty ostrości podczas przechodzenia z trybu dziennego pracy do trybu nocnego. W tym celu aberracja chromatyczna obiektywu musi być skorygowana w znacznie szerszym zakresie widmowym, zaś zastosowane warstwy przeciwodblaskowe muszą mieć lepsze właściwości.

Obiektywy przeznaczone do pracy w świetle widzialnym

Zakres widmowy światła emitowanego przez naturalne źródła, na przykład przez słońce, pokrywa się z zakresem, w którym oko ludzkie reaguje na światło. Tego typu promieniowanie jest określane jako światło białe. W efekcie obiektyw przenoszący światło z obserwowanej sceny na przetwornik w kamerze musi poprawnie działać w szerokim zakresie widmowym. Wiele tanich obiektywów nieskutecznie odwzorowuje kolory mieszczące się w widmie widzialnym, co w rezultacie powoduje niedokładne odwzorowanie barw w materiale wizyjnym. Obiektywy przeznaczone do pracy w świetle białym przepuszczają tylko światło widzialne i mają skorygowaną aberrację chromatyczną jedynie w zakresie widzialnym. Ze względu na to większość obiektywów przeznaczonych do pracy w świetle białym nie jest odpowiednia do stosowania w świetle podczerwonym, chociaż istnieją pewne wyjątki.

Opracowała ***Agata Majkucińska***
Axis Communications

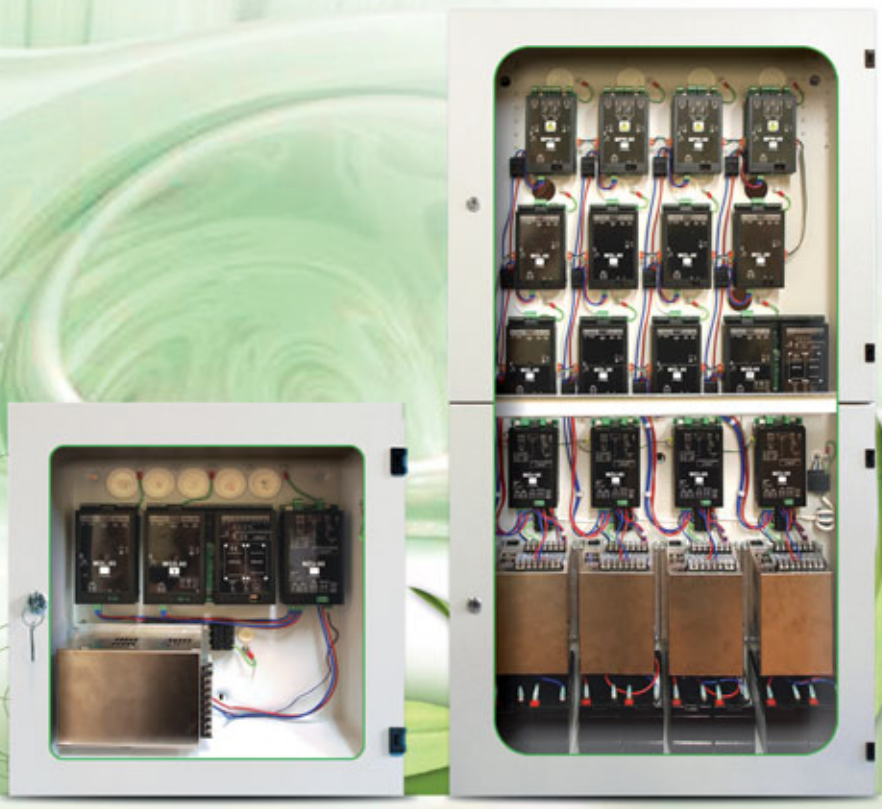
POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

BEZPIECZNY ZAKUP

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k. (dawniej „POLON-ALFA" Zakład Urządzeń Dozymetrycznych sp. z o.o.)

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

UCS 6000
Oddymianie pod kontrolą
(część 2)



Fot. 1. UCS 6000 – widok wnętrza (z lewej wersja 16 A, z prawej 64 A)

Mariusz Sowiński

Według najnowszych badań największe zagrożenie dla przebywających w czasie pożaru w budynku osób jest spowodowane przez dym i toksyczne gazy będące efektem spalania. 90% ofiar pożarów w obiektach ginie wskutek zatrucia gazami. Dzięki specjalnym urządzeniom można odprowadzać trujące produkty spalania ze stref objętych pożarem lub zmniejszać ich stężenie. W pierwszej części artykułu przedstawiono funkcje i parametry techniczne central systemu UCS 6000 służących do sterowania oddymianiem. W niniejszej części zostaną przedstawione funkcje umożliwiające sterowanie oddymianiem i kontrolę procesu oddymiania, które są realizowane przez poszczególne moduły uniwersalnej centrali sterującej

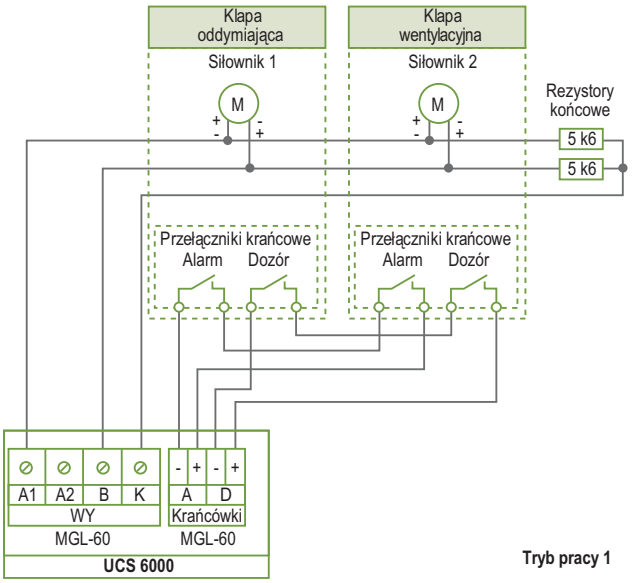
Wprowadzenie

Do oddymiania budynków wykorzystuje się elektryczny lub pneumatyczny system sterowania klapami dymowymi. Oba są równie skuteczne, jednakże system elektryczny ma szereg zalet, które sprawiają, że jest bardziej uniwersalny i funkcjonalny. Podstawowe zalety to możliwość wykorzystania klap dymowych do celów wentylacyjnych (bez ponoszenia dodatkowych kosztów), stała kontrola stanu systemu oraz możliwość optymalnego zintegrowania z innymi systemami bezpieczeństwa obiektu. W pneumatycznym systemie sterowania klapami możliwości wentylacji są ograniczone praktycznie tylko do chwili wystąpienia pożaru. Sterowanie pneumatyczne znacznie zwiększa koszty eksploatacji całego systemu ze względu na wysoki koszt próbnych uruchomień systemu oddymiania podczas konserwacji. Modułowa uniwersalna centrala sterująca UCS 6000 (rys. 1) ma zastosowanie w elektrycznym systemie sterowania oddymianiem.

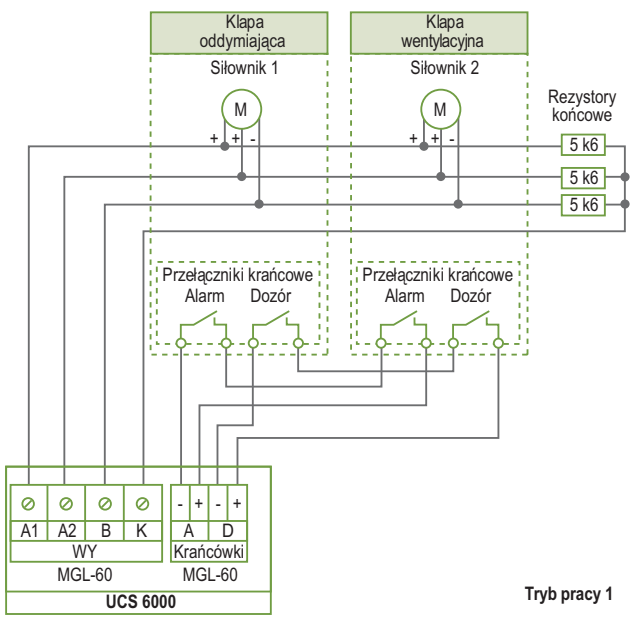
Sterowanie oddymiającymi i odcinającymi klapami przeciwpożarowymi

Obecnie na rynku istnieje wiele rozwiązań służących do sterowania klapami przeciwpożarowymi. W przypadku klap oddymiających elementem wykonawczym jest napęd elektryczny. Może to być siłownik wrzecionowy, siłownik łańcuchowy, siłownik zębatkowy. Do sterowania wykorzystuje się zazwyczaj dwa przewody (rys. 2). Ruch siłownika, lewo – prawo (góra – dół), odbywa się po podaniu napięcia stałego 24 V na silnik elektryczny, przy czym polaryzacja tego napięcia określa kierunek ruchu. Siłowniki ze sterowaniem trzyprzewodowym są stosowane rzadziej. Sterowanie trzyprzewodowe oznacza sterowanie (zmianę kierunku obrotu) siłownikiem i napędem za pomocą trzech przewodów, poprzez przełączanie napięcia między przewodami (rys. 3).

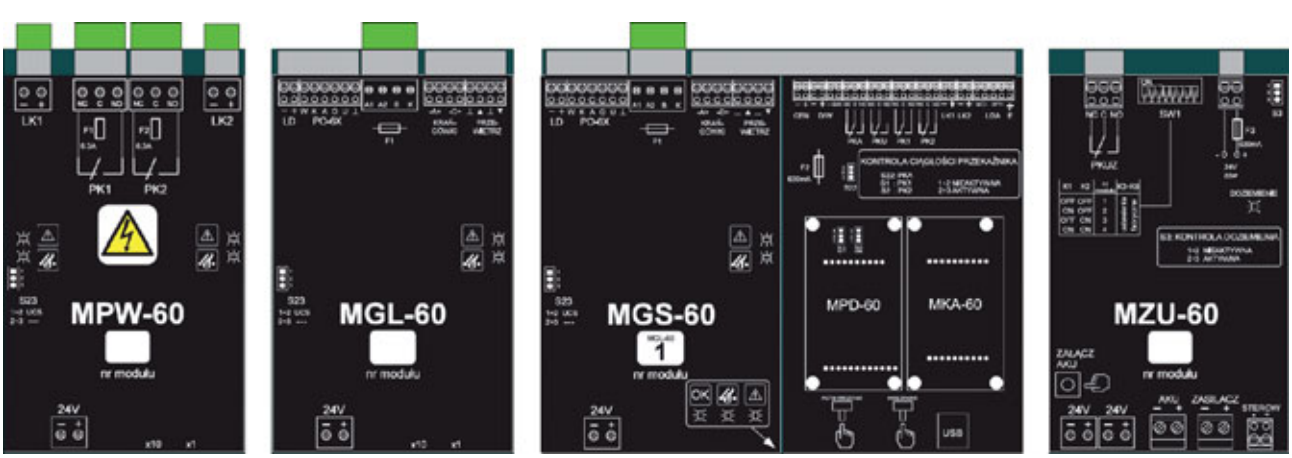
W przypadku klap odcinających elementem wykonawczym jest siłownik ze sprężyną powrotną. W obiektach użyteczności publicznej często wymagane jest sterowanie drzwiami przeciwpożarowymi, które w normalnym stanie są otwarte (albo odwrotnie – zamknięte) i przytrzymywane elektromagnesem. W przypadku zagrożenia następuje automatyczne zamknięcie (albo odwrotnie – otwarcie) tych drzwi – zwolnienie elektromagnesu poprzez sterowanie przerwą lub impulsem prądowym. Centrala UCS 6000 jest przygotowana do pracy z takimi urządzeniami niezależnie od tego, czy musi wysterować siłownik dwuprzewodowy, trzyprzewodowy czy elektromagnes sterowany przerwą lub impulsem prądowym. Do sterowania tymi urządzeniami i zasilania ich przeznaczone jest dedykowane wyjście przekaźnika głównego, który jest umieszczony na module MGL-60 (rys. 1). Maksymalna liczba modułów MGL-60 w centrali to 7 + 1 w MGS-60. Adres



Rys. 2. Sposób podłączenia siłowników sterowanych dwuprzewodowo



Rys. 3. Sposób podłączenia siłowników sterowanych trzyprzewodowo



Rys. 1. Moduły funkcjonalne systemu UCS 6000

Prąd obciążenia		1 A	2 A	3 A	4 A	5 A	6 A	7 A	8 A
Siłownik 0,5A – liczba		2 szt.	4 szt.	6 szt.	8 szt.	10 szt.	12 szt.	14 szt.	16 szt.
Przekrój/długość	1,5 mm²	100 m	50 m	33 m	25 m	20 m	17 m	14 m	13 m
Przekrój/długość	2,5 mm²	167 m	83 m	56 m	42 m	33 m	28 m	24 m	21 m
Przekrój/długość	4 mm²	267 m	133 m	89 m	67 m	53 m	44 m	38 m	33 m

Tab. 1. Maksymalne długości przewodów w zależności od poboru prądu przez siłowniki i przekroju przewodu

modułu ustawia się za pomocą przełączników obrotowych. Wyjście przekaźnika głównego jest wyjściem uniwersalnym i może być zaprogramowane w trzech trybach pracy (co zostało przedstawione w pierwszej części artykułu) – z odpowiednimi parametrami czasowymi. Ponadto można zaprogramować kontrolę ciągłości zasilania (rezystory końcowe 5,6 kΩ) oraz kontrolę stanu przełączników krańcowych urządzeń przeciwpożarowych sterowanych i zasilanych za pomocą wyjścia głównego.

Przy niekorzystnych warunkach atmosferycznych zewnętrzne klapy lub okna mogą przymarznąć. Moduł MGL-60 centrali UCS 6000 umożliwia zaprogramowanie funkcji *deadlock*, czyli funkcji forsowania klap. W przypadku zadeklarowania funkcji forsowania po uruchomieniu wyjścia głównego w stanie alarmu pożarowego następuje cykliczne, chwilowe przestawianie kierunku pracy siłowników (napędów) w odstępach dwuminutowych przez 30 minut. W przypadku zastosowania siłowników lub napędów samohamownych (z wyłącznikami przeciążeniowymi) możliwe jest zaprogramowanie wyłączania zasilania i sterowania siłownikiem po osiągnięciu pozycji krańcowej, co ogranicza zużycie energii elektrycznej.

Krańcówki

Aby wymagania scenariusza pożarowego dla obiektu były spełnione, stan urządzeń wykonawczych (klap) powinien być monitorowany. W przypadku UCS 6000 możliwa jest kontrola stanu (położenia) tych urządzeń poprzez kontrolę stanu dedykowanych wejść modułów MGL-60, do których podłączone są styki przełączników krańcowych sterowanych urządzeń. Możliwe jest sprawdzanie tylko stanu przełączników krańcowych (czy są zwarte, czy rozwarte). Ponadto można nadzorować ciągłość linii przełączników krańcowych (zwarcie albo przerwa). W przypadku zaprogramowania nadzoru nad ciągłością linii przełączników krańcowych należy również zaprogramować kontrolę stanu. W przeciwnym razie centrala zgłasza nieprawidłową konfigurację jako uszkodzenie systemu.

Podłączenie siłowników

Centrala UCS 6000 umożliwia podłączenie przewodów siłowników o maksymalnym przekroju 4 mm² (żyła w postaci drutu miedzianego). Ze względu na znaczny pobór prądu (spadek napięcia na linii) przez siłowniki klap należy dobrać odpowiedni przekrój przewodów łączących siłowniki z centralą. Wymagany przekrój przewodu z żyłami miedzianymi można wyznaczyć, posługując się zależnością:

$$S = 0{,}015 \times I \times L \qquad (1)$$

gdzie: S – przekrój przewodu [mm²]
I – przewidywany prąd obciążenia [A]
L – długość przewodu [m]

Dzienna wentylacja – przyciski przewietrzania

Centrala UCS 6000 umożliwia dzienne przewietrzanie. Do sterowania oknem lub klapą wentylacyjną (do otwierania i zamykania) służą przyciski przewietrzania, które są podłączane do dedykowanych zacisków modułu MGL-60.

Przewietrzanie jest realizowane przez każdy moduł MGL-60 niezależnie (indywidualnie). Wspólny jest tylko czujnik deszczu/wiatru podłączany do modułu MGS-60.

W **trybie 1** przewietrzania okna lub klapy są otwierane (albo zamykane), dopóki wciśnięty jest przycisk *OTWÓRZ* (albo *ZAMKNIJ*). Tym samym można uchylić (ustawić) okno lub klapę w dowolnej pozycji. Dodatkowo można ustawić czas automatycznego zamknięcia **Tp2** okien lub klap wentylacyjnych. W **trybie 2** przewietrzania jednokrotne wciśnięcie przycisku *OTWÓRZ* (albo *ZAMKNIJ*) powoduje otwarcie (albo zamknięcie) okien lub klap wentylacyjnych.

W tym trybie można dodatkowo ustawić parametry czasowe przewietrzania:

– czas otwarcia okien lub klap wentylacyjnych (**Tp1**),
– czas automatycznego zamknięcia okien lub klap wentylacyjnych (**Tp2**).

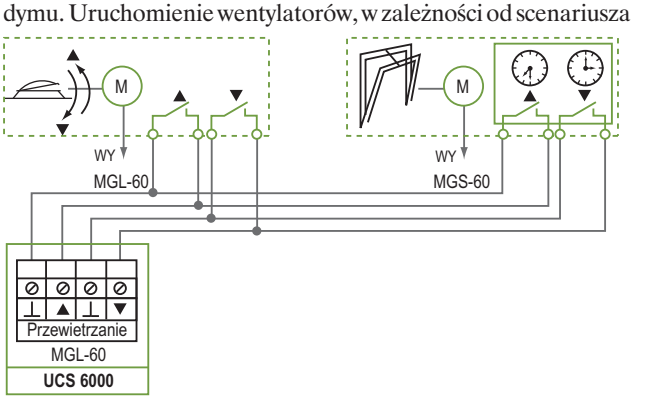
W **trybie 2** do modułu MGL-60 można przyłączyć – zamiast przycisków przewietrzających – zewnętrzny programowany zegar sterujący z dwoma stykami *OTWÓRZ* i *ZAMKNIJ* (rys. 4). W ten sposób można niezależnie sterować przewietrzaniem i dodatkowo wykorzystać w tym celu urządzenia automatyki pogodowej – czujnik deszczu i (lub) wiatru.

W przypadku alarmu pożarowego działanie przycisków przewietrzających jest zablokowane.

W centrali UCS 6000 w wersji wielostrefowej w przypadku alarmu w jednej strefie otwarte wcześniej w pozostałych strefach klapy do dziennej wentylacji zostaną niezwłocznie zamknięte.

Sterowanie wentylatorami oddymiającymi

W systemach sterowania oddymianiem stosowane są wentylatory wyciągowe i nawiewne w celu utrzymania stref wolnych od dymu. Uruchomienie wentylatorów, w zależności od scenariusza



Rys. 4. Dzienna wentylacja

pożarowego obiektu, może nastąpić albo w wyniku opóźnienia sygnału sterującego wentylatorami względem sygnału sterującego klapami, albo po otrzymaniu sygnału zwrotnego potwierdzającego otwarcie (lub zamknięcie) klap w strefie objętej pożarem. Zastosowanie blokady uruchomienia wentylatorów do czasu potwierdzenia przejścia klap w pozycje bezpieczeństwa może, w przypadku uszkodzenia łączników krańcowych, doprowadzić do unieruchomienia systemu oddymiania. Centrale systemu UCS 6000 mogą sterować wentylatorami na oba sposoby. Projektant systemu może zdecydować, jaki sposób sterowania będzie najbardziej odpowiedni, tym bardziej, że centrala UCS nadzoruje stan (położenie) klap przeciwpożarowych.

Moduł przekaźników wysokonapięciowych MPW-60 (rys. 1) umożliwia sterowanie urządzeniami przeciwpożarowymi zasilanymi z sieci napięcia przemiennego 230 V poprzez przekaźniki PK1 i PK2. Ponadto możliwe jest monitorowanie stanu urządzeń przeciwpożarowych sterowanych przekaźnikami PK1 i PK2 za pomocą wejść linii kontrolnych. W centrali mogą znaleźć się maksymalnie cztery moduły MPW-60. Adres modułu ustawia się za pomocą przełączników obrotowych. Programowalne przekaźniki ze stykami bezpotencjałowymi PK1 i PK2 można wykorzystać do sterowania urządzeniami wykonawczymi instalacji oddymiania (do ich załączania i wyłączania), między innymi do sterowania wentylatorami nawiewnymi lub wywiewnymi (w zależności od potrzeb), kurtynami i roletami dymowymi, oddzieleniami przeciwpożarowymi. Przykład wykorzystania przekaźnika PK2 wraz z potwierdzeniem zadziałania za pomocą linii kontrolnej LK2 przedstawiono na rys 5. Linie wyjściowe przekaźników PK1 i PK2 są dodatkowo zabezpieczone bezpiecznikiem topikowym o nominale 6,3 A/250 V.

Ponadto można zaprogramować uzależnienia czasowe przekaźników PK1 i PK2.

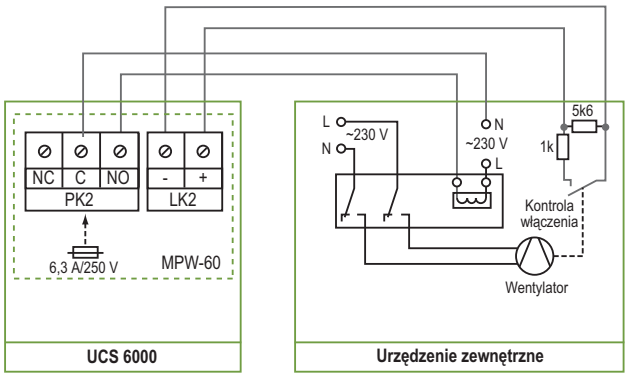
Programując kontrolę (potwierdzenie) zadziałania przekaźników, można ustawić dodatkowo czas na potwierdzenie zadziałania. W przypadku braku potwierdzenia w zaprogramowanym czasie centrala UCS 6000 zgłasza uszkodzenie. Jeżeli centrala UCS 6000 współpracuje z centralą systemu POLON 4000, ta ostatnia będzie dodatkowo sygnalizować odpowiednie komunikaty alarmów technicznych (w dozorowaniu i alarmie) lub uszkodzeń niemaskowalnych (w alarmie). W przypadku modułu przekaźników dodatkowych MPD-60 mamy do dyspozycji dwa przekaźniki niskonapięciowe o obciążalności 1 A/24 V.

Nadzór i kontrola nad systemem oddymiania

Centrala systemu UCS 6000 zawiera jeden moduł głównego sterownika MGS-60 (rys. 1), który kontroluje cały system oddymiania poprzez sprawowanie funkcji nadzoru i sterowania pozostałymi modułami funkcjonalnymi systemu UCS 6000 oraz posiada dedykowane wejścia i wyjścia do podłączenia tych elementów systemu, które są wspólne dla wszystkich modułów, niezależnie od wersji prądowej systemu (4A, 8A, 16A, 32A, 48A, 64A).

Połączenie kablowe	Wymaganie dotyczące kabla
Linie sterujące oddzieleniami i zamknięciami ogniowymi i dymoszczelnymi	
kable do sterowania oddzieleniami pożarowymi i zasilania oddzieleń pożarowych działających na zasadzie przerwy prądowej (np. klap odcinających w kanałach wentylacji ogólnej)	Nie ma wymogu niepalności i nadzorowania tych linii sterujących. Wynika to z zasady działania tych napędów (są zamykane uprzednio zmagazynowaną energią mechaniczną).
kable stosowane do sterowania oddzieleniami pożarowymi działającymi po dostarczeniu energii elektrycznej (np. bramami otwieranymi i zamykanymi w trakcie pożaru)	kabel klasy PH zgodnie z rozporządzeniem [1] (dotyczy to wszystkich kabli, także do przycisków sterowania ręcznego, zasilania i sygnalizacji działania) nadzorowane przez centralę sterującą
linie z CSP działające na zasadzie przerwy prądowej, które odłączają np. maszynownie wentylacji ogólnej, schody ruchome, taśmociągi	brak wymogu niepalności i nadzorowania linii
linie działające na zasadzie przerwy prądowej, które odłączają windy przeznaczenia ogólnego	Nie ma wymogu niepalności i nadzorowania linii. Przepalenie kabla powinno sprowadzać windę na poziom ewakuacji lub przystanek alternatywny.
sterowane impulsem prądowym linie sterujące klapami w kanałach wentylacji ogólnej	kabel klasy PH
Linie systemów zabezpieczających przed zadymieniem oraz odprowadzających dym i ciepło	
zasilanie sieciowe central sterujących UCS	kabel klasy PH, zgodnie z rozporządzeniem [1], prowadzony sprzed wyłącznika przeciwpożarowego prądu z oddzielnym zabezpieczeniem w rozdzielni głównej
zasilanie wentylatorów oddymiania pożarowego	kabel klasy PH
zasilanie napędów klap oddymiania grawitacyjnego	kabel klasy PH 30, linie nadzorowane
linie kablowe krańcówek, potwierdzające wykonanie funkcji (położenie klap) w instalacjach oddymiania grawitacyjnego	kabel klasy PH 30, linie nienadzorowane (w UCS są nadzorowane)
zasilanie napędu klap i sterowanie napędem klap w instalacjach kontroli rozprzestrzeniania się dymu i ciepła poprzez różnicowanie ciśnień mechanicznej wentylacji oddymiającej	kabel klasy PH 90, linie nadzorowane
linie kablowe do urządzeń potwierdzających wykonanie funkcji (położenie klap) w instalacjach oddymiania mechanicznego	kabel klasy PH, linie nienadzorowane
zasilanie klap otworów oddymiających i doprowadzających powietrze i sterowanie klapami otworów oddymiających i doprowadzających powietrze w instalacji oddymiania	kabel klasy PH uszkodzenie kabla nie powinno powodować uruchomienia klapy otworu dolotowego linie nienadzorowane
kable sterujące urządzeniami do oddymiania pożarowego, przeznaczone do ręcznego sterowania przez uprawniony personel	kabel klasy PH zgodnie z PN-EN 12101-6, linie nadzorowane
kable sterujące i sygnałowe pomiędzy CSP, UCS i tablicami ręcznego sterowania wentylatorami i klapami do oddymiania	kabel klasy PH zgodnie z PN-EN 12101-6, linie nadzorowane

Tab. 2. Okablowanie w systemach oddymiania



Rys. 5. Przykładowy sposób wykorzystania przekaźnika PK2 z kontrolą zadziałania

Do modułu głównego sterownika można przyłączyć:
- zewnętrzny, nadrzędny SSP (centrale systemu POLON 4000),
- zewnętrzny, nadrzędny SSP (konwencjonalny, np. centrale systemu IGNIS 1000),
- zewnętrzny system monitorowania lub sygnalizacji,
- czujnik deszczu/wiatru do sterowania pogodowego.

Zasilanie systemu oddymiania

Podstawowym źródłem zasilania systemu oddymiania, sterowanego i kontrolowanego przez centralę systemu UCS 6000, jest sieć elektroenergetyczna 230 V/50 Hz. Zmiana napięcia o +10% i –15% nie ma wpływu na poprawną pracę centrali. Jednoczesne zasilanie centrali oraz buforowanie lub ładowanie baterii akumulatorów dołączonej do modułów MZU-60 (rys. 1) zapewniają wewnętrzne zasilacze, które wytwarzają napięcie o wartości regulowanej przez moduły MZU-60 w zależności od stopnia naładowania baterii rezerwowych. Zasilacze centrali umożliwiają pobór prądu:
- do 5 A w sposób ciągły, przez moduł zasilacza SP-150-27.5PLA,
- do 10 A w sposób ciągły, przez moduł zasilacza SP-240-27.5PLA,
- do 20 A w sposób ciągły, przez moduł zasilacza SP-500-27.5PLA.

Na etapie projektowania instalacji należy sprawdzić, czy całkowity prąd, który będzie pobierany z zasilaczy centrali, nie przekroczy wyżej podanych wartości.

Podczas sprawdzania należy wziąć pod uwagę sumę wszystkich prądów pobieranych jednocześnie z zacisków centrali, łącznie z prądem zasilania samej centrali. Należy również zwrócić uwagę na dopuszczalne wartości prądów poszczególnych wyjść.

W przypadku zaniku napięcia w sieci, rezerwowym zasilaniem centrali jest bateria akumulatorów o napięciu znamionowym 24 V (2×12 V, 4×12 V, 6×12 V lub 8×12 V w zależności od konfiguracji sprzętowej centrali) i pojemności od 7,2 do 9 Ah. Przełączenie z zasilania zasadniczego na rezerwowe następuje samoczynnie, bez powodowania przerwy w zasilaniu. Podczas dozorowania, bez zasilania zasadniczego, z kompletem ostrzegaczy na linii dozorowej i podłączonym jednym ręcznym przyciskiem oddymiania PO-6X, lecz bez zasilania urządzeń dodatkowych, prąd pobierany przez centralę nie przekracza 120 mA.

Bateria akumulatorów jest ładowana samoczynnie przez urządzenie ładujące, które jest zintegrowane z modułem MZU-60 centrali. Prąd ładowania jest ograniczony do około 2,1 A. W stanie pełnego naładowania wartość prądu ładowania jest bliska zera, a napięcie buforowania powinno wynosić 27,3 V.

Ogólna sprawność baterii i urządzenia ładującego jest stale kontrolowana, a uszkodzenia są sygnalizowane przez centralę.

Moduł MZU-60 jest wyposażony w przekaźnik sygnalizacji uszkodzenia zasilania PKUZ (styki bezpotencjałowe). Jakiekolwiek uszkodzenie urządzeń zasilających moduł MZU-60 (np. akumulatora, zasilacza) powoduje przełączenie styków przekaźnika.

Moduł MZU-60 jest wyposażony dodatkowo w nadzorowane wyjście do zasilania zewnętrznych urządzeń. Wyjście umożliwia pobór prądu o natężeniu do 0,5 A i jest zabezpieczone bezpiecznikiem 630 mA.

Okablowanie w systemach sterowania oddymianiem

Wszystkie podłączenia elektryczne należy wykonać zgodnie z obowiązującymi przepisami odnoszącymi się do wytrzymałości ogniowej i mechanicznej oraz z zachowaniem parametrów określonych w dokumentacji techniczno-ruchowej central UCS 6000 (odpowiedniej rezystancji). Połączenia elektryczne można wykonać przewodami nieekranowanymi, za wyjątkiem przewodu łączącego centralę UCS 6000 z centralą systemu POLON 4000 (zalecany jest przewód instalacyjny YnTKSYekw 1×2×0,8 mm). W tab. 2 zestawiono obwody systemów oddymiania wraz z wymaganiami dotyczącymi niepalności i wytrzymałości ogniowej przewodów.

Zgodnie z rozporządzeniem [1] należy dobierać takiej klasy kable PH bez podanego wyróżnika liczbowego (odpowiadającego czasowi odporności ogniowej), która gwarantuje ciągłość dostawy energii i sygnału przez wymagany czas. Zgodnie ze stosowaną klasyfikacją mogą to być kable PH30, PH60 lub PH90.

Podsumowanie

W zależności od opracowanego scenariusza pożarowego dla danego obiektu może zaistnieć potrzeba sterowania wieloma urządzeniami pożarowymi różnego typu: klapami oddymiającymi, klapami odcinającymi, kurtynami powietrznymi, drzwiami przeciwpożarowymi, wentylatorami wentylacji nawiewnej i wyciągowej. Może też być potrzebna kontrola ich stanu czy położenia. Ze względu na swoją modułowość i uniwersalność centrale systemu UCS 6000 umożliwiają praktycznie każde sterowanie za pomocą wyjść sterujących i wejść kontrolnych modułów MGS-60, MGL-60, MPW-60 i MPD-60.

Mariusz Sowiński
POLON-ALFA

Bibliografia

1) Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U. z 2002 r., nr 75, poz. 690 z późniejszymi zmianami; Dz. U. z 2003 r., nr 33, poz. 270; Dz. U. z 2004 r., nr 109, poz. 1156; Dz. U. z 2008 r., nr 201, poz. 1238; Dz. U. z 2008 r., nr 228, poz. 1514; Dz. U. z 2009 r., nr 56, poz. 4510)

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)

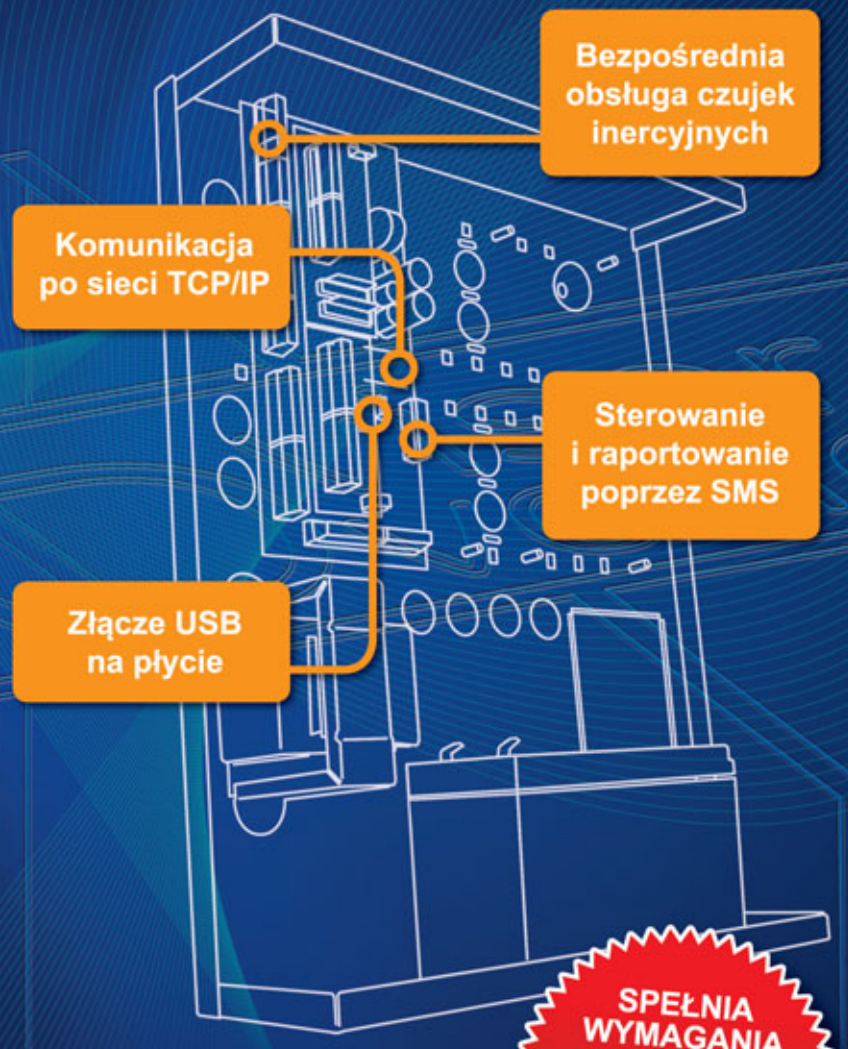
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

UTC Fire & Security

Nowa Platforma
Advisor Advanced

Prosty wybór bogatych możliwości!

- Różne tryby zazbrajania i rozbrajania przy pomocy karty i/lub kodu PIN
- Zazbrajanie po 3-krotnym użyciu karty
- Parametryzowane linie dozorowe do obsługi czujek z układem wykrywania maskowania (Anti-masking) i czujek inercyjnych
- Podział na niezależne obszary (4/8) z możliwością stosowania zazbrajania częściowego w każdym z nich.
- Bogaty wybór interfejsów komunikacyjnych i możliwość sterowania oraz raportowania przez komunikaty SMS
- Dostępne wersje z interfejsem IP (Ethernet) na płycie
- Szeroki wybór czujek przewodowych i bezprzewodowych oraz innych urządzeń peryferyjnych



SPEŁNIA WYMAGANIA NORMY EN50131: 2009

UTC Fire & Security
A United Technologies Company

Centrala UTC Fire & Security Polska Sp. z o.o.
ul. Sadowa 8
80-771 GDAŃSK
tel.: (58) 301 38 31, (58) 760 64 80
fax: (58) 301 14 36

Oddział w Warszawie
Al. Stanów Zjednoczonych 59
04-028 WARSZAWA
tel.: (22) 810 00 03
fax: (22) 810 10 55

Oddział w Poznaniu
Oś. Na Murawie 11/2
61-655 POZNAŃ
tel.: (61) 821 35 66
tel./fax: (61) 821 31 94

Puszki instalacyjne serii PI, PU

Puszki serii PI-T

Puszki instalacyjne serii PI-T przeznaczone są do stosowania w systemach telekomunikacyjnych. Umożliwiają łączenie lub krosowanie przewodów o maksymalnym przekroju 0,75 mm^2 (PI-T10) lub 2,5 mm^2. W zależności od wersji puszki użytkownik może połączyć 7, 10 lub 150 par przewodów. Otwory montażowe w puszce umożliwiają wprowadzenie przewodu o maksymalnej średnicy 7 mm lub 10 mm (PI-T150). Puszka PI-T150 posiada dodatkowo zamek w pokrywie, który umożliwia ograniczenie dostępu osobom trzecim do wnętrza puszki.

Puszki serii PU-T

Puszki instalacyjne serii PU-T przeznaczone są do stosowania w systemach telekomunikacyjnych. Umożliwiają łączenie lub krosowanie przewodów o maksymalnym przekroju 2,5 mm^2. Użytkownik może połączyć 20 par (PU-T20) lub 30 par (PU-T30) przewodów. Otwory montażowe w puszce umożliwiają wprowadzenie przewodu o maksymalnej średnicy 14 mm. Obudowa puszki jest dodatkowo uszczelniona, co ogranicza przedostawanie się do wnętrza puszki zanieczyszczeń w postaci pyłu, kurzu.

Puszki serii PI-W

Puszki instalacyjne serii PI-W przeznaczone są do stosowania w systemach włamaniowych. Konstrukcja puszki jest analogiczna do konstrukcji puszki PI-T, dodatkowo posiadają element antysabotażowy, który umożliwia rozpoznanie: otwarcia pokrywy puszki, oderwania puszki od podłoża (ściany).

Puszki serii PU-W

Puszki instalacyjne serii PU-W przeznaczone są do stosowania w systemach włamaniowych. Konstrukcja puszki jest analogiczna do konstrukcji puszki PU-T, dodatkowo posiadają element antysabotażowy, który umożliwia rozpoznanie: otwarcia pokrywy puszki, oderwania puszki od podłoża (ściany).

	PI-W6, PI-W9	PI-T7, PI-T10	PU-T18, PU-T20, U-T30	PU-W18, PU-W30	PI-T150
Wymiary [mm]	104×60×29 104×60×29	104×60×29 104×60×29	235×103×32 176×103×32 235×103×32	235×103×32 235×103×32	630×280×45
Materiał obudowy	ABS		Blacha ocynkowana malowana proszkowo		
Maks. średnica przewodu (wejście puszki)	7 mm	7 mm	14 mm	14 mm	10 mm
Maks. przekrój przewodu	2,5 mm^2 0,75 mm^2	2,5 mm^2 0,75 mm^2	2,5 mm^2 2,5 mm^2 2,5 mm^2	2,5 mm^2 2,5 mm^2	2,5 mm^2
Liczba przewodów	6 par + sabotaż 9 par + sabotaż	7 par 10 par	18 par 20 par 30 par	18 par + sabotaż 30 par + sabotaż	150 par
Szczelność obudowy	IP 40D	IP40D	IP30C	IP30C	IP30C
Rodzaj środowiska pracy	Przeznaczone do stosowania wewnątrz budynków				

Producent:

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

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

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

Pronto – Drukarka do kart identyfikacyjnych

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

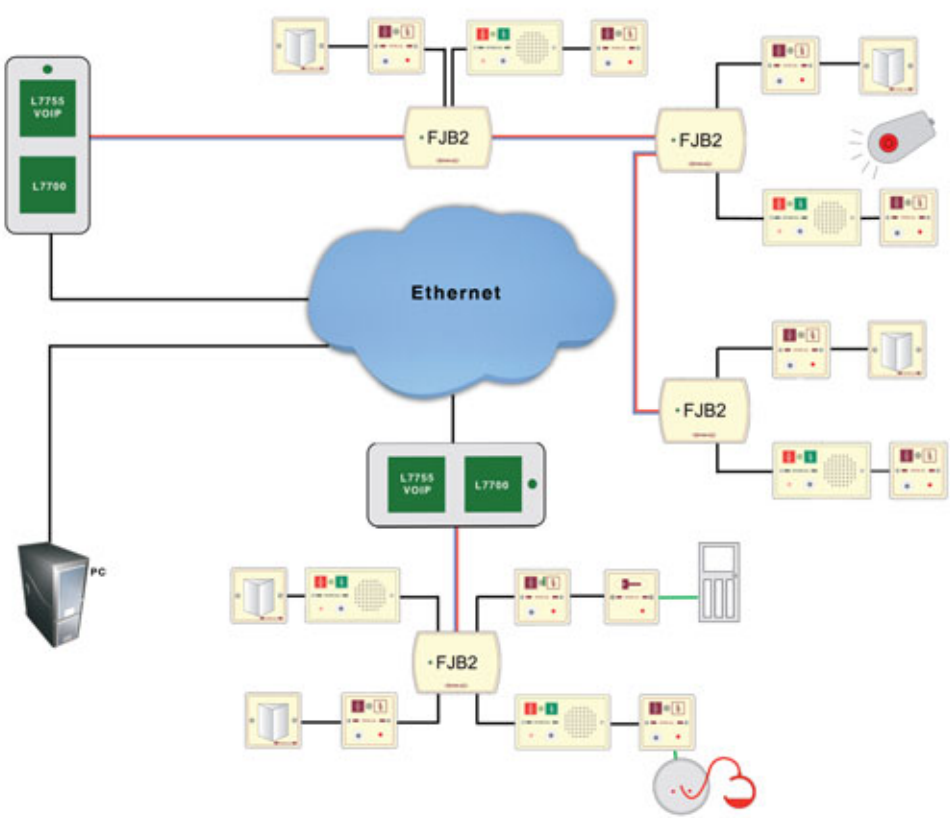
Intercall – szpitalny system przywoławczy

Prosty w instalacji – pomocny dla obsługi – zapewniający bezpieczeństwo pacjenta

Intercall jest najwyższej jakości systemem przywoławczym przeznaczonym dla specjalistycznych placówek opieki zdrowotnej (szpitale, domy opieki, hospicja itp.). Prosty w obsłudze i łatwy w rozbudowie, oferuje wyjątkowe funkcje: komunikację głosową (Intercall 700), rejestrację przywołań, przywołania o różnych priorytetach, czytelną i dokładną informację o rodzaju alarmu oraz miejscu wywołania.

Intercall zapewnia również maksymalnie uproszczony proces instalacji systemu, a dzięki 2-żyłowej magistrali (Intercall 600) pozwala na zastąpienie systemów starszej generacji, bez konieczności wymiany okablowania.

- Nieograniczone możliwości rozbudowy zarówno w zakresie punktów przywoławczych, jak i urządzeń sygnalizacyjnych
- Buforowanie oraz bieżący podgląd zdarzeń
- Dwukierunkowa komunikacja w trybie głośnomówiącym bez użycia słuchawek (Intercall 700)
- Definicja priorytetów zdarzeń alarmowych
- Możliwość bezpośrednich wydruków oraz powiadomienia na pager
- Szeroka gama punktów przywoławczych, w tym maty ciśnieniowe, czujniki moczenia, czujki ruchu, ręczne aktywatory ściskowe, ustne podmuchowe, łazienkowe oraz zdalne nadajniki podczerwieni
- Instalacja czterożyłowa (dwużyłowa przy systemie bez komunikacji głosowej)
- Bezpośrednie i zdalne konfigurowanie urządzeń za pomocą komputea PC

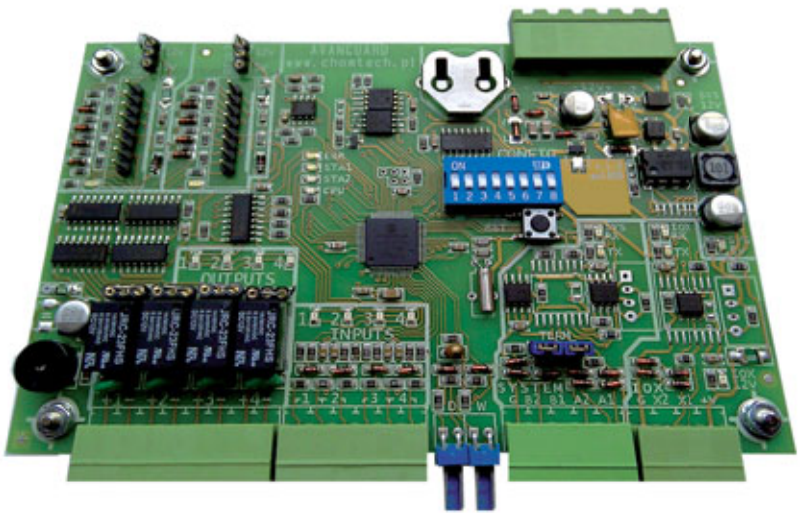


Dystrybucja:

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

Avanguard+
Kontroler lokalny systemu bezpieczeństwa obiektu



Kontroler Avanguard+ jest specjalistycznym urządzeniem mikroprocesorowym stosowanym w systemach bezpieczeństwa technicznego i automatycznej identyfikacji, ze szczególnym uwzględnieniem kontroli dostępu, obsługi szafek basenowych, śluzy, kamer IP.
Innowacją jest zastosowanie w kontrolerze funkcji pozwalającej na łączenie sterowników z nadrzędnym kontrolerem Avanguard Professional, uzyskując dzięki temu wszystkie zaawansowane możliwości tego kontrolera. Wystarczy zainstalować w miejscu dowolnego kontrolera Avanguard+ wersję Avanguard Professional. Kontroler Avanguard Professional przejmuje wówczas zarządzanie globalne, a Avanguard+ pracuje jako sterownik lokalny.

Kontroler Avanguard+ steruje pracą czytników zapewniając pełną identyfikację i rejestrację zdarzeń. Kontroler monitoruje i rejestruje sygnały z różnych urządzeń dodatkowych takich jak: czujnik otwarcia drzwi, przycisk, antysabotaż czytnika kontroli dostępu, itp. Kontroler pozwala dla każdego z urządzeń zdefiniować wiele typów reakcji, które są zapisywane w pamięci wewnętrznej kontrolera.

Niezależnie od sekwencji sterujących Avanguard+ może sterować czytnikami i ustawiać je w tryb pracy oparty o harmonogramy. Kontroler posiada możliwość konfiguracji z programu nadzorczego na komputerze lub autonomiczny tryb pracy (stand-alone). Rozwiązanie takie daje dużą elastyczność, szczególnie w systemach, gdzie stała komunikacja z komputerem nadrzędnym nie jest możliwa.

Podstawowe funkcje:

- wbudowany moduł wykonawczy
- strefy czasowe
- kod dostępu z klawiatury (PIN KOD)
- tygodniowy harmonogram trybów czytnika
- tygodniowy harmonogram przełączeń rygla
- komunikaty dla karty identyfikacyjnej
- karta wirtualna
- kod napadowy
- strefy czasowe
- data ważności karty
- licznik karty
- aktywna punktacja czytnika

Podstawowe cechy:

- rejestracja zdarzeń w czasie rzeczywistym
- pamięć do 60000 zdarzeń
- liczba użytkowników systemu do 40000
- komunikacja z PC poprzez RS485
- praca w trybie off-line lub on-line
- współpraca z kontrolerem Avanguard Professional

chomtech.pl®
systemy bezpieczeństwa i autoidentyfikacji

chomtech.pl sp. z o.o.
ul. Mieszczańska 5
30-313 Kraków

tel. 12 421 43 83, 428 12 00
faks 12 350 40 69
http://www.chomtech.pl

Czytnik kart zbliżeniowych Mifare AV-G25 Helios

Doskonała jakość, bardzo wytrzymała konstrukcja, praca w każdych warunkach klimatycznych. Najwyższy poziom niezawodności w technologii zbliżeniowej.

Czytnik kart zbliżeniowych Mifare AV-G25 jest czytnikiem inteligentnych kart zbliżeniowych, pracującym w częstotliwości 13,56 MHz. Przeznaczony jest do stosowania w systemach kontroli dostępu, rejestracji czasu pracy, stołówkach i wszędzie tam, gdzie zachodzi potrzeba wykorzystania kart zbliżeniowych.

Czytnik Mifare AV-G25 charakteryzuje się ciekawym wzornictwem i kolorystyką (9 wersji kolorystycznych). Czytniki odczytują każdy rodzaj kart i tagów Mifare (standard, ultralight). Dzięki temu mogą stanowić alternatywę dla obecnie występujących produktów Mifare na naszym rynku.

Czytniki dostępne są w wykonaniu wewnętrznym lub zewnętrznym. Posiadają klawiaturę mechaniczną lub dotykową. Dostępna jest również opcja bez klawiatury. Dodatkowo każdy czytnik posiada wbudowany antysabotaż. Opcjonalnie urządzenia mogą być również wyposażone w kontroler, dzięki czemu mogą pracować jako pełny autonomiczny punkt dostępowy. Sygnalizacja stanów alarmowych odbywa się akustycznie i za pomocą kolorowych piktogramów.

Podstawowe cechy drukarki	
Napięcie zasilania	od 9 do 16 V_{DC}
Zasięg odczytu	do 10 cm
Częstotliwość pracy	13,56 MHz
Temperatura pracy	od –35°C do 75°C
Format wyjściowy	Wiegand 26/34, ABATRACK2, ASYNC 9600, N, 8,1
Obudowa (materiał)	poliwęglan UL94
Wymiary	12,50×8,9×3,0 cm
Kolor	czarny, szary, srebrny, niebieski, czerwony, pomarańczowy, biały, zielony, żółty
Instalacja	na każdym podłożu
Sygnalizacja	dioda trójkolorowa i brzęczyk
Transmisja	szyfrowana, klucz 64 bity
Kontrolery	Avanguard, SD-108, IKR, IKR108, SD-660, SD-560
Masa	249,5 g
Wilgotność	5% – 95% bez kondensacji
Pobór prądu	50 / 75 mA przy zasilaniu 12 V_{DC}
Wodoodporny	IP 54

chomtech.pl®
systemy bezpieczeństwa i autoidentyfikacji

chomtech.pl sp. z o.o.
ul. Mieszczańska 5
30-313 Kraków

tel. 12 421 43 83, 428 12 00
faks 12 350 40 69
http://www.chomtech.pl

Kamera WCM-21VF

Kamera WCM-21VF to zewnętrzna kamera kompaktowa o bardzo wysokiej czułości i wysokiej rozdzielczości 600 TVL/650 TVL (B/W), wyróżniająca się estetyczną obudową.
Podobnie jak w innych kamerach firmy CNB zastosowano procesor Monalisa oraz technologię Intelligent IR, eliminującą efekt przejaskrawienia i rozmycia obrazu gdy obserwowany obiekt zbliża się do kamery. W standardowym oświetlaczu jasność świecenia jest stała, dlatego bliskie obiekty są oświetlone tak samo intensywnym światłem jak dalekie, co w praktyce może spowodować prześwietlenie obrazu. Funkcja Intelligent IR umożliwia sterowanie jasnością oświetlenia w zależności od odległości obserwowanego obiektu od kamery. Możliwe są dwa tryby pracy, pierwszy określany jest jako *Wide* – gdzie kamera próbuje oświetlić scenę jak najintensywniej, licząc się z możliwością wystąpienia lokalnych przejaskrawień i drugi określany jako *Smart* – gdzie kamera nie dopuszcza do najmniejszych prześwietleń.

Zalety:

- wbudowany obiektyw o zmiennej ogniskowej 3,8-9,5 mm z automatyczną przysłoną DC
- możliwość pracy w dzień i w nocy
- odsuwany mechanicznie filtr TDN(ICR), zapewniający wierne odwzorowanie kolorów w dzień
- oświetlacz pracujący w podczerwieni o zasięgu 20 m
- Intelligent IR – adaptacyjne oświetlenie w podczerwieni
- dodatkowe wyjście wizyjne dla instalatora

Innymi kamerami kompaktowymi z wbudowanymi oświetlaczami Intelligent IR są WCL-21S i WCL-11S (obiektyw 6 mm) oraz XCM-25VF (większy zasięg oświetlenia, nowy wygląd obudowy, obiektyw 3,8-9,5 mm).

Właściwości:

- przetwornik 1/3" Sony Super HAD II
- wysoka rozdzielczość 600 TVL (kolor), 650 TVL (B/W)
- przełącza się w tryb B/W
- czułość 0,05 lx (kolor), 0,005 lx (B/W), 0,00 lx (IR LED włączone)
- AGC, SBLC, AWB, DNR, Flickerless, D/N – regulacja przez OSD
- detekcja ruchu, strefy prywatności, funkcja mirror, wyostrzanie obrazu
- obudowa przystosowana do montażu do ściany albo pod sufitem

Model	WCM-21VF
Standard sygnału wizyjnego	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
Rozmiary matrycy	752(H) x 582(V) 440K
Rozdzielczość	600 TVL (kolor), 650 TVL (B/W)
Wyjście wizyjne	1,0V p-p, 75 Ohm
Odstęp sygnał/szum	>50 dB (wył. AGC)
Obiektyw	f=3,8~9,5 mm, F1,2
Tryb dzień/noc	mechaniczny filtr IR
Czułość	0,05 lx (kolor) 0,005 lx (BW) 0,00 lx (IR LED włączone)
Menu OSD	angielski, chiński
Oświetlacz pracujący w podczerwieni	Intelligent IR LED 18EA (850 nm, 30°)
Zasięg oświetlenia	maks. 20 m
Cyfrowa redukcja szumu	DNR, 3 poziomy
Balans bieli	automatyczny, PUSH, ręczny
Automatyczna regulacja wzmocnienia (AGC)	wł./wył.
Kompensacja tylnego oświetlenia	SBLC /3 poziomy
Redukcja migotania	wł./wył.
Strefy prywatne	4 programowalne strefy
Detekcja ruchu	4 programowalne strefy
Odbicie lustrzane obrazu	w pionie
Elektroniczna migawka	1/50~1/120 000 sek.
Stopień ochrony IP	IP66
Zasilanie	12 V_{DC}
Pobór prądu	maks. 0,5A /6 W
Wymiary (szer. x wys.)	78,0 x 150,0 mm
Temperatura pracy/wilgotność	-10°C~50°C/30%~80% RH
Masa	800 g

Dystrybucja:

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 BBM-21F

Modele BBM-21F oraz DFL-21S to najpopularniejsze kamery firmy CNB. Bardzo wysoka czułość, mechanicznie odsuwany filtr IR zapewniający bardzo dobre i wierne odwzorowanie kolorów w dzień oraz zastosowanie procesora Monalisa to najważniejsze zalety tych kamer. Port RS-485 pozwala na zdalne programowanie kamery przez menu OSD co ułatwia pracę instalatora i pozwala na zdalną diagnostykę systemu.
W przypadku wykorzystania podświetlenia w podczerwieni należy pamiętać by zastosować obiektyw z korekcją w IR, gdyż w przeciwnym razie obraz będzie rozmyty.

Zalety:

- odsuwany mechanicznie filtr podczerwieni, dzięki czemu kamera wyróżnia się bardzo dobrym, wiernym odwzorowaniem kolorów w dzień
- możliwość pracy w dzień i w nocy, praca z reflektorami podczerwieni
- SBLC – ulepszona odmiana BLC, czyli kompensacji tylnego oświetlenia
- sterowanie przez port RS485 – protokół Pelco-D

Właściwości:

- kolorowa kamera dzień/noc
- przetwornik 1/3" Super HAD II
- bardzo wysoka rozdzielczość 600 TVL oraz w trybie czarno-białym 650 TVL
- przełącza się w tryb B/W
- wyposażona w mechanicznie odsuwany filtr IR - TDN(ICR)
- czułość 0,1 lx (kolor), 0,01 lx (B/W)
- regulacja jasności oraz koloru
- AGC, SBLC, AWB, DNR, Flickerless, D/N – regulacja przez OSD
- detekcja ruchu, strefy prywatności, funkcja mirror
- zasilanie 12 V_{DC}

Kamera w wersji BBM-25F ma zasilanie dualne 12 V_{DC}/24 V_{AC} zaś kamera w wersji BBM-27F ma zasilanie 230 V_{AC}. Kamera w wersji BBM-21 ma nieruchomy filtr IR. Opcjonalnie dostępne są także uchwyty ścienne WDB65 oraz WDB80 w kolorze srebrnym.

CNB TECHNOLOGY Inc.

Model	BBM-21F
Standard sygnału wizyjnego	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
Wielkość matrycy	752(H) x 582(V) 440K
Rozdzielczość	600 TVL (B/W 650TVL)
Wyjście wizyjne	1,0V p-p, 75 Ohm
Odstęp sygnał/szum	>50 dB
Obiektyw	mocowanie C/CS
Tryb dzień/noc	tak, mechanicznie odsuwany filtr IR
Czułość	0,1 lx (kolor) 0,01 lx (B/W) F1.2, 30IRE
Menu OSD	polski, hiszpański, portugalski, niemiecki, angielski, chiński i inne
Cyfrowa redukcja szumu	DNR, 3 poziomy
Balans bieli	ATW, Manual, Push
Automatyczna regulacja wzmocnienia (AGC)	wł./wył.
Kompensacja światła tylnego	SBLC, 3 poziomy
Redukcja migotania	wł./wył.
Strefy prywatne	4 programowalne strefy
Detekcja ruchu	4 programowalne strefy
Odbicie lustrzane obrazu	w poziomie
Elektroniczna migawka	1/50~1/120 000 s
Ręczna migawka	1/50~1/120 000 s
Zasilanie	12 V_{DC}
Pobór prądu	maks. 2,2 W/150 mA
Wymiary (Ø×wys.)	64×57,6×124,66 mm
Temperatura pracy/Wilgotność	-10°C~50°C/30%~80% RH
Masa	ok. 335 g

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

CDV-1020AE - monitor wideodomofonowy dla wymagających

Ofertę monitorów dla systemów przeznaczonych dla jednego abonenta uzupełnia najnowszy model – CDV-1020AE, który jest skierowany do wymagającego użytkownika, ceniącego sobie niebanalną stylistykę oraz jakość i niezawodność działania. Przeznaczony jest do użytku w domach jedno- lub kilkurodzinnych. Monitor posiada największy w swojej klasie ekran o przekątnej 10,2" z dotykową matrycą. Intuicyjne menu (także w języku polskim) obsługiwane przez ekran dotykowy pozwoliło wyeliminować przyciski na obudowie, dzięki czemu metalowy panel przedni jest całkowicie płaski. Monitor obsługuje dwa panele wejściowe dzięki czemu możliwy jest kontakt audiowizualny np. z osobami znajdującymi się w pobliżu dwóch furtek (wraz z funkcją otwarcia obu wejść) oraz dodatkowo obsługuje dwie zewnętrzne kamery CCTV - umożliwiające np. obserwację większego obszaru podczas rozmowy z odwiedzającym (funkcja PIP – picture-in-picture). Zestaw wideodomofonu może być rozbudowany o dodatkowe monitory z serii CDV-xxx oraz unifony DP-4VH (dostępne w pięciu wersjach kolorystycznych) z funkcją interkomu wewnątrz budynku. Monitor wyposażony jest w moduł pamięci umożliwiający zapis do 128 obrazów (inicjowany automatycznie lub ręcznie) z zaznaczeniem daty i godziny. Umożliwia to dodatkową kontrolę odwiedzających (np. podczas nieobecności domowników). Monitor współpracuje z dowolnym panelem wejściowym w systemie 4-żyłowym, dzięki czemu można skonfigurować odpowiedni zestaw dla własnych wymagań. Ponad 40-letnie doświadczenie firmy COMMAX w projektowaniu elementów systemów wideodomofonowych pozwala cieszyć się użytkownikowi doskonałą jakością i bezawaryjną pracą przez długi czas.

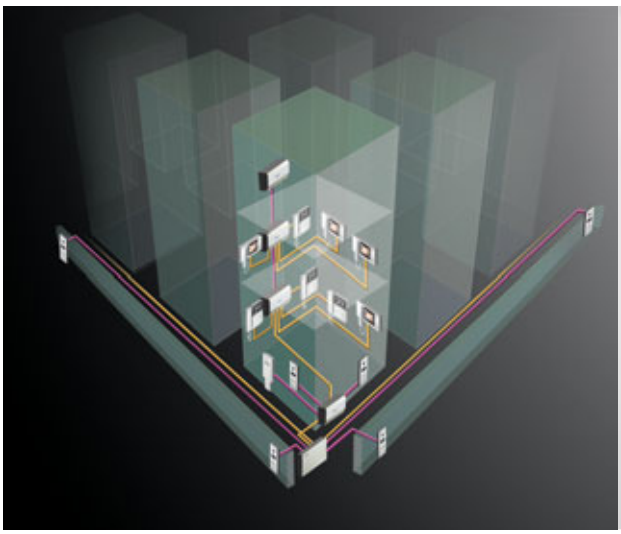
Właściwości:

- monitor kolorowy
- wyświetlacz 10,2" Color TFT-LCD 16:9
- standard sygnału wizyjnego PAL/NTSC
- obsługuje dwa wejścia (dwa panele wejściowe)
- obsługa kamer CCTV (wyświetlanie PIP – picture-in-picture)
- wbudowany moduł pamięci 128 obrazów
- możliwość podłączenia dodatkowego monitora
- współpraca z unifonami DP-4VR, DP-4VH
- komunikacja pomiędzy stacjami
- instalacja czteroprzewodowa + obwód elektrozamka
- współpracuje z kamerami analogowymi czteroprzewodowymi
- zasilanie 230 V
- wymiary: 317×213×34 mm

Dystrybucja:

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

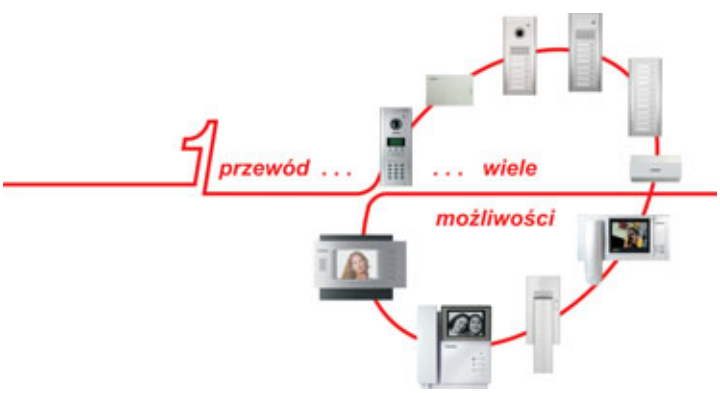
System wieloabonentowy serii 2400

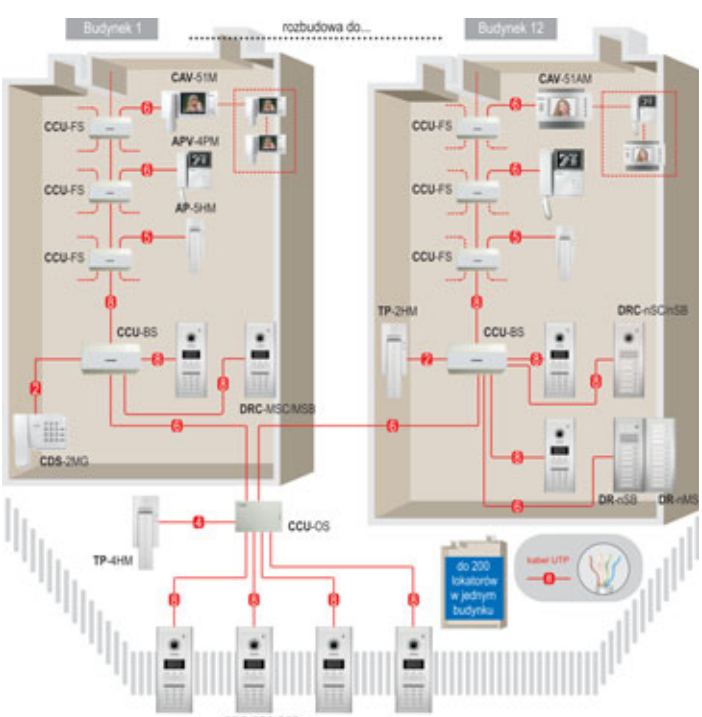


System wieloabonentowy serii 2400 przeznaczony jest do instalacji zarówno w prostych, jak i w bardzo rozbudowanych aplikacjach - maksymalna liczba obsługiwanych przez system abonentów wynosi 2400. U każdego lokatora może być zainstalowane do 3 urządzeń (jedno urządzenie typu Master i dwa urządzenia typu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

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

System umożliwia zastosowanie zarówno paneli zewnętrznych audio, jak wideo - wyposażonych w moduł kamery (czarno-biały lub kolorowy). Panele zewnętrzne występują w wersji przyciskowej lub z klawiaturą numeryczną (umożliwiającą dodatkowo wybór lokatora za pomocą spisu lokatorów oraz otwieranie zamka elektrycznego przy użyciu indywidualnych kodów). System może być wyposażony w unifon lub stację portierską instalowaną w portierni, przez co lokatorzy oraz osoby ich odwiedzające mogą mieć kontakt z osobą dozorującą (portierem). Dzięki dużej elastyczności możliwe jest skonfigurowanie systemu dla małych, pojedynczych bloków, jak i całych osiedli zamkniętych, gdzie ogrodzonych może być klikanaście budynków, a całość nadzorowana przez kilku portierów.





Dystrybucja:

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

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

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

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

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 **Radom**
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 49 79, 411 57 47
faks 12 411 94 74
e-mail: insap@insap.pl
www.insap.pl

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

JANEX INTERNATIONAL Sp. z o.o.
ul. Płomyka 2
02-490 Warszawa
tel. 22 863 63 53
faks 22 863 74 23
e-mail: janex@janexint.com.pl
www.janexint.com.pl

KABE Systemy Alarmowe Sp. z o.o.
ul. Waryńskiego 63
43-190 Mikołów
tel. 32 324 89 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

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

SATIE
ul. Łączyny 3
02-820 Warszawa
tel. 22 462 30 86
faks 22 462 30 87
e-mail: info@satie.pl
www.satie.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 BUILDINGS POLSKA Sp. z o.o.
ul. Rzymowskiego 53
02-697 Warszawa
tel. 22 313 24 10
faks 22 313 24 11
e-mail:
SEPLBuildings.Poland@buildings.schneider-electric.com
www.schneider-electric.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

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	–	–
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

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
ISM EuroCenter	–	–	TAK	–	TAK
Janex International	–	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	–	–
Satel	TAK	–	–	–	–
SATIE	–	–	TAK	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

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	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	TAK	TAK	–
GEO-KAT	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
HSA	TAK	TAK	TAK	TAK	–	–	–	–	–
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
ISM EuroCenter	–	TAK	–	–	–	TAK	TAK	–	–
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	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
SATIE	–	–	TAK	–	–	TAK	TAK	–	–
Sawel	TAK	TAK	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	–	–	–	–	–

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
Ryszard Sobierski
Waldemar Szulc
Adam Wojcinowicz

Współpraca
Marcin Buczaj
Adam Bułaciński
Piotr Czernoch
Marcin Pyclik
Adam Rosiński
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

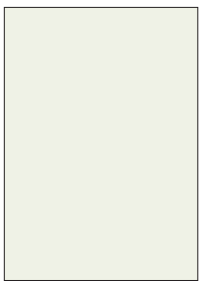
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

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

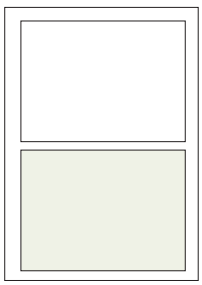
Cennik reklam

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)

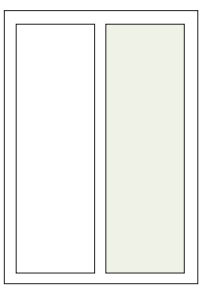


1/2 strony
(170 x 125 mm)

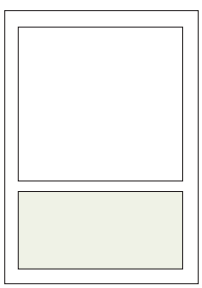
Artykuł sponsorowany:
indywidualne negocjacje (forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)

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)



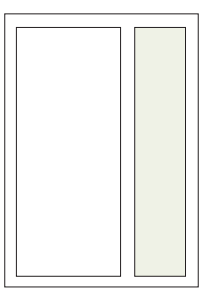
1/3 strony
(170 x 80 mm)

Spis teleadresowy:
jednorazowy wpis 70 zł

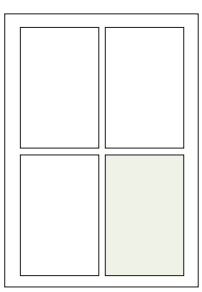
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Podane ceny nie uwzględniają podatku VAT (23%)

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



1/3 strony
(54 x 260 mm)



1/4 strony
(83 x 125 mm)

Spis reklam

AAT Holding	47, 62, 87
Alnet Systems	111
ATline	29
Axis Communications	75
Bosch Security Systems	1
Camsat	31
chomtech.pl	51
Euroalarm	2, 11
GDE Polska	74
GEO-KAT	71
Gunnebo	80
HID	112
Linc Polska	42
MTP	21
Polon-Alfa	81
Roger	57
Samsung Techwin Europe	35
Satel	67
Schrack Seconet Polska	25
Techom	34
UTC Fire & Security	88
Videotec	43

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

profesjonalne rozwiązania
do cyfrowej rejestracji obrazu

ponad 60 000 instalacji
pracujących na całym świecie

www.alnetsystems.com

ALNET SYSTEMS

sieciowe oprogramowanie do cyfrowej rejestracji obrazu — NS NETSTATION

hybrydowy system do cyfrowej rejestracji obrazu — NET HYBRID

hybrydowy system do cyfrowej rejestracji obrazu HD-SDI — NET HYBRID HD

profesjonalne oprogramowanie klienckie — CMS PROFESSIONAL

oprogramowanie klienckie dla urządzeń mobilnych — CMS MOBILE

blisko 1000 kamer zintegrowanych
z oprogramowaniem Alnet Systems

wybór należy do Ciebie!

ACTi · Arecont Vision · AXIS · BASLER · CRYPTOTELECOM · ETROVISION · GANZ
HIKVISION · iCANTEK · IQinVision · JVC · LILIN · Lumenera · PELCO · MESSOA
Panasonic · SANYO · SAMSUNG · SONY · STARDOT · TOA · VIVOTEK · ZAVIO

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.