CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 5(81)/2011

ZABEZPIECZENIA

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

W NUMERZE:

C & C solution partner

SecurityNET

Okablowanie dla systemów zabezpieczeń

SecurityNET to:

• **Kompleksowość**	możliwość połączenia wszystkich systemów bezpieczeństwa w technologii światłowodowej i miedzianej
• **Jakość**	kable zoptymalizowane pod transmisję video, pozwalające realizować usługę PoE
• **Bezpieczeństwo**	wyodrębniona, jednoznacznie identyfikowana infrastruktura kablowa
• **Prostota**	szybkie w instalacji i wygodne w eksploatacji przyłącza urządzeń
• **Unikalność**	jedyne na rynku rozwiązanie dedykowane do systemów bezpieczeństwa, spełniające międzynarodowe normy okablowania strukturalnego

C&C Partners zapewnia szkolenia z projektowania oraz instalowania rozwiązania prowadzone przez naszych doświadczonych inżynierów.

Oddział Leszno
leszno@ccpartners.pl

Oddział Gdańsk
gdansk@ccpartners.pl

Oddział Katowice
katowice@ccpartners.pl

Oddział Warszawa
warszawa@ccpartners.pl

www.ccpartners.pl

TKH GROUP

Spis treści

CZASOPISMO ZABEZPIECZENIA 5/2011

HD-SDI w systemach telewizji dozorowej – światełko w tunelu czy droga donikąd? **18**

Bezpieczeństwo dla jutrzejszego świata **26**

Czas na zmiany **42**

Oświetlenie w systemach nadzoru wizyjnego (część 1) **72**

SecurityNET – okablowanie dla bezpieczeństwa

W odpowiedzi na potrzeby rynku **C&C Partners** wprowadza spójną platformę światłowodowego i miedzianego okablowania strukturalnego, przeznaczoną do połączenia systemów bezpieczeństwa. **SecurityNET** jest dedykowaną platformą integrującą centrum zarządzania, sygnalizację włamania i napadu (SSWiN), komunikację głosową (Interkomy oraz DECT), kontrolę dostępu (KD) oraz dozór wizyjny (CCTV).

Dla centrum zarządzania oferujemy światłowodowe i miedziane gniazda przyłączeniowe, które stanowią punkty dostępu do zasobów dla administratorów systemów bezpieczeństwa. Proponujemy też 19-calowe szafy dystrybucyjne, w których – dzięki wydajnemu systemowi chłodzenia oraz kontroli dostępu – bez zakłóceń pracują urządzenia zarządzające systemami bezpieczeństwa.

System SSWiN będzie działać bez zarzutu dzięki niezakłóconemu przepływowi cyfrowych i analogowych sygnałów sterujących pomiędzy czujkami systemu bezpieczeństwa a główną centralą.

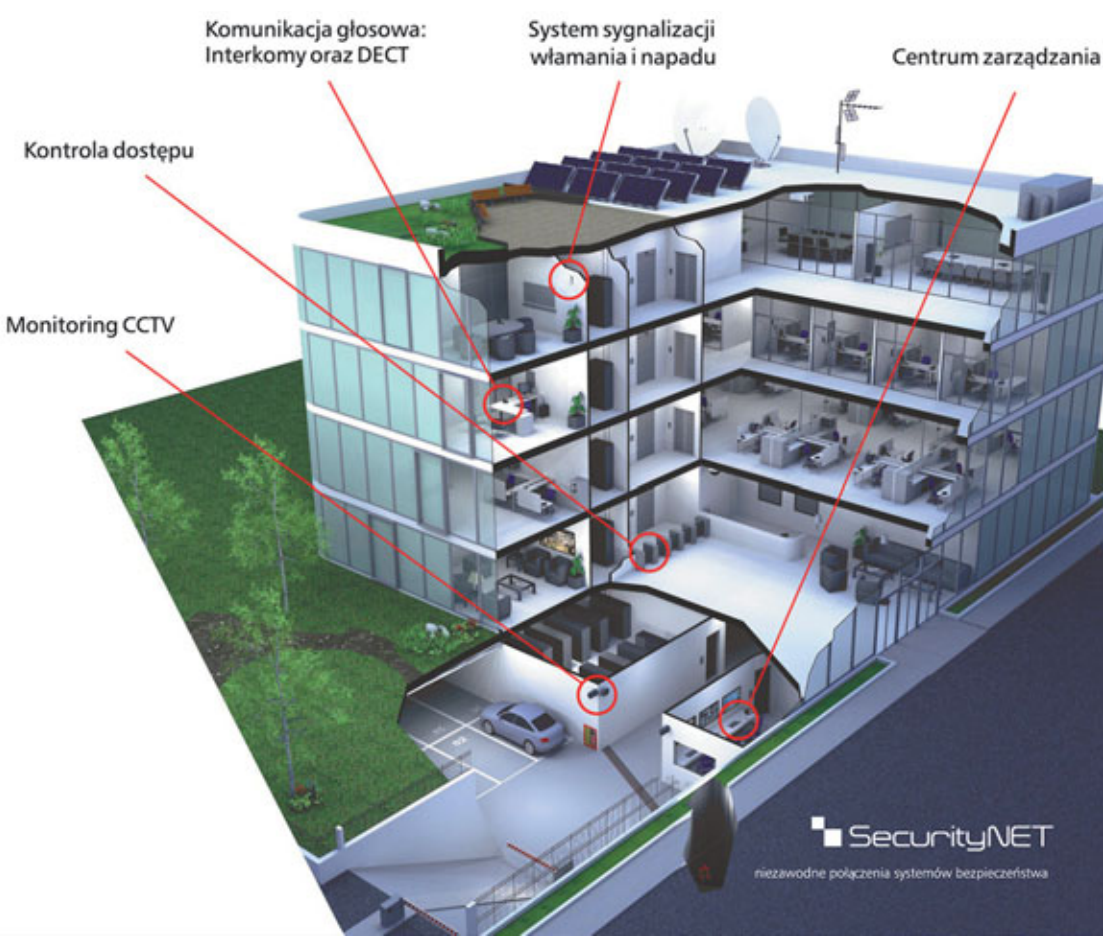
System komunikacji głosowej jest wyposażony w kable skrętkowe podwójnie ekranowane, w powłoce poliuretanowej PUR. Gwarantują one niezakłócone działanie stacji interkomowych w środowiskach, w których występują duże ilości zakłóceń elektromagnetycznych i toksyczne substancje. Hermetyczne obudowy dla stacji bazowych oraz zakończenia łączy światłowodowych i miedzianych zapewniają niezawodne działanie transmiterów DECT na zewnątrz budynku.

Zielone kable instalacyjne SecurityNET zastosowane w systemie KD wyróżniają się spośród kabli standardowej sieci LAN, co ogranicza niepowołane ingerencje w okablowanie. Zewnętrzne kable światłowodowe oraz miedziane, do bezpośredniego zakopywania w ziemi, zapewniają komunikację z terminalami w terenie.

W systemie dozorowym CCTV można wykorzystać światłowodowe kable przeznaczone do zastosowań zewnętrznych, zapewniające galwaniczne odizolowanie kamer zewnętrznych od urządzeń do rejestracji i analizy obrazu. Złącza i kable miedziane mogą być użyte do transmisji wizji z kamer CCTV IP oraz analogowych i gwarantują niezawodne zasilanie urządzeń poprzez PoE.

SecurityNET oferuje wiele dedykowanych komponentów podwyższających poziom niezawodności i zwiększających wydajność połączeń w systemach bezpieczeństwa. Najważniejsze z nich to panele rozdzielcze 19" z gniazdami umożliwiającymi wyróżnienie doprowadzonych łączy, szafy 19" z kontrolą dostępu i systemem chłodzenia, wtyki RJ45 z unikatowym kluczem oraz dedykowane kable światłowodowe i miedziane, w tym podwójnie ekranowane kable w powłoce PUR.
SecurityNET to kompleksowy system okablowania o wysokiej jakości, który dzięki unikalnym rozwiązaniom podwyższa poziom niezawodności Twojego systemu bezpieczeństwa.

Bezpośr. inf. C&C Partners



Manipulator INT-KSG finalistą konkursu *Dobry Wzór 2011*

Z przyjemnością informujemy, że manipulator sensoryczny **INT-KSG** firmy **Satel** został zakwalifikowany do finału ogólnopolskiego konkursu *Dobry Wzór 2011* na najlepiej zaprojektowany produkt i usługi na polskim rynku.

Instytut Wzornictwa Przemysłowego organizuje konkurs od 1993 roku. To jedyny w kraju niezależny monitoring wzorniczy rynku. Do konkursu *Dobry Wzór* zapraszani są producenci, dystrybutorzy i dostawcy, których produkty i usługi zostały rekomendowane przez ekspertów instytutu. Zgodnie z założeniami konkursu dobrym wzorem jest dobrze zaprojektowany produkt lub usługa, które uwzględniają zarówno uwarunkowania rynku, cele biznesowe firmy, jak i charakter marki. Konkurs promuje nowe, innowacyjne rozwiązania i technologie, które są wartościowe dla użytkowników lub usprawniają procesy produkcji.

Do tegorocznej XVIII edycji konkursu eksperci wytypowali aż 800 produktów oraz 80 usług. Jesteśmy dumni z tego, że produkt firmy Satel znalazł się w finale wśród kilkudziesięciu polskich i zagranicznych produktów i usług z różnych dziedzin.

Powody, dla których eksperci z Instytutu Wzornictwa Przemysłowego zakwalifikowali nasz manipulator do finału konkursu *Dobry Wzór*, znalazły się w specjalnej ekspertyzie. Oto jej fragment:

„**Manipulator sensoryczny INT-KSG** dla centrali alarmowej INTEGRA jest nowym produktem wprowadzonym na rynek w 2010 r. Stanowi innowacyjny produkt w swojej klasie dzięki możliwościom przystosowania do realizowania szeregu złożonych funkcji ułatwiających obsługę elektroniczną pomieszczeń przez użytkowników, w tym osoby starsze. Dzięki zaprojektowanej prostej formie, dużemu ekranowi umieszczono większą ilość informacji w porównaniu do innych rozwiązań. Podświetlenie i udźwiękowienie klawiszy ułatwia obsługę. Cztery sygnały alarmowe uruchamiane przez odrębne przyciski gwarantują bezpieczeństwo. Forma prosta, starannie opracowane detale, świetna czytelność klawiatury. Neutralny wyraz pozwala na harmonijne zastosowanie w różnego typu wnętrzach".

Jak co roku finałowe produkty i usługi zostaną wyeksponowane na pokonkursowej wystawie w Instytucie Wzornictwa Przemysłowego, która potrwa od 22 września do 22 listopada (ul. Świętojańska 5/7, Warszawa). Wystawę rozpocznie uroczysta gala konkursowa, zaplanowana na 21 września 2011 r. – również w Instytucie Wzornictwa Przemysłowego.

Bezpośr. inf. Agnieszka Pitrus
SATEL

Mobilne aplikacje iPOLiS do iPhone'a i urządzeń z systemem operacyjnym Android

Samsung opracował aplikację umożliwiającą zdalny podgląd „na żywo" obrazu z kamer sieciowych iPOLiS na ekranie iPhone'a oraz urządzeń z systemem operacyjnym Android, takich jak smartfon Samsung Galaxy S.

Bezpłatna aplikacja **iPOLiS MOBILE**, którą można pobrać na platformach iTunes i Android Market, pozwala użytkownikowi kontrolować funkcje panoramowania, wychylania i powiększania (zoom) obrazu z najnowszych kamer sieciowych marki Samsung poprzez prosty interfejs. Po zajmującym mniej niż minutę wprowadzeniu ustawień użytkownicy mogą oglądać obraz wysyłany z wybranej kamery za pośrednictwem sieci bezprzewodowej lub 3G.

Wszystkie kolejne kamery sieciowe iPOLiS marki Samsung będą kompatybilne z tą aplikacją. Wśród modeli kamer wyposażonych w najnowszy firmware, tym samym kompatybilnych, są najnowsze kamery megapikselowe HD, w tym modele wyposażone w funkcje PTZ.

Aplikacja iPOLiS MOBILE umożliwia także podgląd obrazu „na żywo" oraz sterowanie PTZ kamerami analogowymi za pośrednictwem rejestratorów analogowych z serii SRD firmy Samsung.

– Wprowadzenie aplikacji iPOLiS MOBILE to doskonały przykład na to, że nasi projektanci poszukują innowacyjnych sposobów zapewnienia klientom maksymalnych korzyści z korzystania z rozwiązań firmy Samsung z zakresu nadzoru – powiedział Peter Ainsworth, Senior Product Manager firmy Samsung Techwin Europe. – *Istnieje wiele różnych możliwości znakomitego wykorzystania tej aplikacji. Bez wątpienia będzie ona pomocna w praktyce, na przykład w pracy menedżerów ds. bezpieczeństwa, którzy nie przebywają ciągle w jednym miejscu, a są odpowiedzialni za wiele lokalizacji jednocześnie.*

Bezpośr. inf. David Solomons
DRS Marketing

Nowe stałopozycyjne, termowizyjne kamery IP firmy Bosch

Bosch wprowadza na rynek nową linię stałopozycyjnych, **termowizyjnych kamer IP** do zastosowań zewnętrznych. Kamery działają w absolutnej ciemności i są odporne na niesprzyjające warunki pogodowe. Stanowią kompleksowe rozwiązanie umożliwiające całodobowy monitoring dzięki termogramowi o wyjątkowej jakości i zaawansowanej, inteligentnej analizie obrazu IVA (*Intelligent Video Analysis*). Oferują najwyższą jakość obrazu niezależnie od warunków oświetleniowych. Działają niezawodnie także w przypadku silnego zadymienia lub niekorzystnych warunków atmosferycznych, takich jak gęsta mgła czy opady śniegu, oraz w absolutnej ciemności.

Zoptymalizowana pod kątem termowizji technologia IVA pomaga wykrywać obiekty i ostrzega pracowników ochrony o podejrzanych działaniach lub niebezpieczeństwach. Pomaga także w identyfikacji wzorców zachowań, dzięki czemu operatorzy mogą szybko ocenić, co dzieje się w obserwowanej scenie, i podjąć odpowiednie działania. Kamera jest przystosowana do nadzorowania rozległych terenów i wykrywania obiektów z dużej odległości oraz – w przeciwieństwie do kamer konwencjonalnych – pokazuje także osoby ukrywające się w cieniu lub kamuflujące się w tle.

Nowe kamery termowizyjne z IVA mają szeroki zakres funkcji, takich jak detekcja ruchu, śledzenie trajektorii i wykrywanie osób niepożądanych. Cyfrowe przetwarzanie obrazu poprawia jego jakość i daje pracownikom ochrony wydajne i skuteczne narzędzie służące do wykrywania niebezpiecznych zdarzeń oraz generowania alarmów. Zdarzenia są pokazywane natychmiast, a dane mogą być archiwizowane. Ich odszukanie ułatwia funkcja *Forensic Search* opracowana przez firmę Bosch. IVA wychwytuje wszystkie ruchome szczegóły w rejestrowanych scenach, co umożliwia operatorom wyszukanie każdego zdarzenia – nawet jeśli początkowo nie było ono zdefiniowane jako sytuacja alarmowa.

Kamery termowizyjne wykrywają różnice temperatur rzędu 50 milikelwinów lub mniejsze, dlatego łączą w sobie zalety dedykowanego przetwarzania obrazu z redukcją szumów, aby zapewnić wyraźną, bardzo dokładną konwersję obrazu termicznego na widzialny i jego wyświetlanie. Kamery są wyposażone w przetwornik VOx (tlenek wanadu) FPA o rozdzielczości 320×240 pikseli. Funkcja *Tri-streaming* umożliwia równoczesne przesyłanie dwóch strumieni z kompresją H.264 oraz jednego strumienia z kompresją JPEG. Dalsze zalety to: *multicasting, streaming* internetowy, możliwość przesyłania nagrań do macierzy iSCSI oraz możliwość obsługi kamery za pomocą bezpłatnego oprogramowania BVC.

Karta pamięci micro SD umożliwia lokalną archiwizację nagrań. Zwiększa to niezawodność systemu, ponieważ pozwala wykluczyć zakłócenia spowodowane błędami sieciowymi podczas transmisji obrazu do zewnętrznego rejestratora wizyjnego. Dzięki sterowaniu pan/tilt operator kamery może ją szybko skierować w wybranym kierunku.

Do wyboru są cztery obiektywy zapewniające wąski i szeroki kąt obserwacji. Kamery mogą mieć różne zastosowania. Mogą być wykorzystywane zwłaszcza do nadzoru portów, ruchu drogowego, terenów przygranicznych, do zadań związanych z bezpieczeństwem narodowym, do ochrony obwodowej rozległych terenów oraz do nadzoru elektrowni i obiektów przemysłowych.

Nowe kamery są zgodne ze standardem ONVIF.

Bezpośr. inf. Bosch Security Systems

GEMOS wykorzystuje *cloud computing*

Firmy **ela-compil** i **01 Partner** stworzyły rozwiązanie, które umożliwia systemowi **GEMOS** wykorzystanie architektury *cloud computing* (czyli przetwarzania w chmurze). Zaletą związaną z jego wykorzystaniem i jednocześnie ogromną korzyścią dla klienta jest zdecydowanie wyższy poziom bezpieczeństwa niż np. w przypadku zastosowania serwerów redundantnych.

Wykorzystanie przez GEMOS architektury wysokodostępnej umożliwia m.in. znaczne wydłużenie bezawaryjnego czasu pracy, utworzenie dynamicznej struktury informatycznej, usprawnienie konserwacji i uaktualniania sprzętu, ręczne i automatyczne przełączanie serwerów, konsolidację obciążeń na mniejszej liczbie serwerów, wysoki poziom automatyzacji zadań w centrum danych, a także ogranicza koszty związane z pracą, zasilaniem i konserwacją systemów.

Nowe rozwiązanie zabezpiecza użytkownika przed przerwami w pracy systemu GEMOS w przypadku awarii pojedynczego serwera lub macierzy dyskowej. Jest to niezmiernie istotne ze względu na potrzebę zapewnienia permanentnej pracy stanowisk obsługujących systemy bezpieczeństwa i automatyki budynkowej. W przypadku rozbudowy systemu, np. migracji na nowe, bardziej wydajne serwery, zastosowana technologia umożliwia dokonanie jej bez jakiejkolwiek przerwy w pracy systemu. Zmniejsza się również prawdopodobieństwo utraty danych. Zalety takiego rozwiązania są zatem znaczące. Dają użytkownikowi pewność, że wszystkie procesy są pod kontrolą, a praca systemów przebiega bez zakłóceń.

Technologia przetwarzania w chmurze znajduje zastosowanie w obiektach o szczególnym znaczeniu, takich jak np. zintegrowane centra komunikacyjne, dworce kolejowe, porty lotnicze oraz wszystkie inne obiekty wymagające podwyższonego poziomu bezpieczeństwa.

Bezpośr. inf. ela-compil

Czy jesteś spokojny o bezpieczeństwo Twojej serwerowni?

Nikogo nie trzeba przekonywać, jak ważne dla firm, instytucji i organizacji są przechowywane dane, ich niezawodne i bezprzerwowe przetwarzanie i analizowanie oraz jakim zagrożeniem dla nich jest pożar, który niszczy nośniki i urządzenia. Ale podobnym zagrożeniem dla urządzeń i nośników danych są akcje gaśnicze przeprowadzane z użyciem tradycyjnych środków, takich jak woda i piana – spowodowane przez te środki uszkodzenia zarówno nośników danych, jak i urządzeń przynoszą niepowetowane straty. Nie bez znaczenia jest także czas przerwy w działaniu tych urządzeń, będący efektem pożaru, akcji gaśniczej i konieczności naprawy urządzeń i odtworzenia strat w danych. Rozwiązaniem pozwalającym na znaczne zmniejszenie strat, a często ich całkowite uniknięcie, jest zastosowanie instalacji gaśniczych wykorzystujących gazy obojętne. Te instalacje nie tylko zapewniają skuteczne i szybkie zadziałanie w najwcześniejszej fazie pożaru, ale również, co bardzo istotne, chronią nośniki danych i urządzenia przed uszkodzeniami, jakie mogą być spowodowane przez środki gaśnicze.

Systemy gaszenia gazem stosowane są przede wszystkim tam, gdzie nie można użyć tradycyjnych środków gaśniczych ze względu na zagrożenie dla obiektów i służb zwalczających pożar (w przypadku wszelkiego rodzaju urządzeń i rozdzielni elektrycznych pod napięciem, obiektów zabytkowych itp.), a także w obiektach i pomieszczeniach, w przypadku których kluczowe znaczenie ma ochrona cennych danych i zbiorów, wartość materialna sprzętu i zapewnienie ciągłości jego działania (w serwerowniach, centrach przetwarzania danych, centralach telefonicznych i elektrycznych, a także w muzeach, archiwach czy laboratoriach).

Najczęściej stosowanymi gazowymi środkami gaśniczymi są mieszaniny gazów obojętnych, takie jak INERGEN (mieszanina azotu i argonu z niewielkim dodatkiem dwutlenku węgla), oraz gazy chemiczne FM200 i Novec 1230. Sposób działania tych gazów, szybkość wyładowania ich do gaszonego pomieszczenia, ich skuteczność gaśnicza, ale i brak szkód spowodowanych działaniem środka gaśniczego oraz brak pozostałości popożarowych umożliwiający maksymalne skrócenie czasu przywrócenia pełnej funkcjonalności pomieszczeń i urządzeń (lub niewielkie pozostałości) powoduje, że osoby zarządzające obiektami mogą być spokojne o bezpieczeństwo zarówno swoich obiektów, jak i zbiorów, a także o ochronę życia i zdrowia przebywających w danych pomieszczeniach osób. W warunkach przemysłowych do gaszenia wykorzystuje się również dwutlenek węgla.

Rodzaj zastosowanych stałych gazowych instalacji gaśniczych zależy od gaszonego obiektu. Środek gaśniczy oraz rodzaj poszczególnych komponentów instalacji powinny zostać dobrane do rodzaju pomieszczenia, jego konstrukcji i gaszonych elementów. Należy uwzględnić sposób zagospodarowania pomieszczeń, możliwe do wytrzymania wzrosty ciśnień, wytrzymałość podłóg i stropów, wymagane stężenie środka gaśniczego, czas wypełnienia i wiele innych parametrów. Stąd wniosek – nie istnieją gotowe rozwiązania, każdy z projektów musi zostać indywidualnie przygotowany. W doborze i przy wdrażaniu odpowiednich rozwiązań swoich klientów wspierają konsultanci AGIS Fire&Security, którzy dzięki wieloletniemu uczestnictwu w realizacji projektów o różnej skali w takich branżach jak IT, telekomunikacja czy przemysł posiadają unikalną wiedzę, kompetencję i *know how* dotyczące projektowania, instalowania, serwisowania i konserwacji rozwiązań w zakresie ochrony przeciwpożarowej.

Bezpośr. inf. Karolina Łokietek
AGIS Fire&Security

CD06 – zdalne sterowanie układami automatyki

Zestaw **CD06**, produkowany przez firmę **Camsat**, służy do zdalnego sterowania urządzeniami wchodzącymi w skład układów automatyki za pomocą klawiatury lub specjalnego nadajnika sterującego. System wykorzystuje dwukierunkowy interfejs transmisji szeregowej RS485, który w połączeniu z modułami radiowymi CD04 osiąga zasięg 6 km i 14 km, nawet przy niepełnej widzialności optycznej anten. Pomimo znacznych odległości sterowanie odbywa się zawsze w czasie rzeczywistym.

Odbiornikiem CD06-Rx można sterować za pomocą nadajnika znajdującego się w zestawie, ale również dowolnej klawiatury z protokołem PELCO-D. Podobnie jak w przypadku współpracy z kamerami PTZ, liczba odbiorników podłączonych do jednej magistrali szeregowej jest ograniczona wyłącznie liczbą adresów ID.

Zarówno nadajnik, jak i odbiornik są wyposażone we wskaźniki LED, które sygnalizują stany pracy oraz aktualne stany wejść i wyjść. Dodatkowo, dzięki zaawansowanym funkcjom transmisji dwukierunkowej, nadajnik otrzymuje potwierdzenie odbioru wysłanych danych i zapala wskaźniki odzwierciedlające aktualny stan odbiornika. Gwarantuje to użytkownikowi stuprocentową kontrolę nad działaniem odbiornika. Urządzenie wyposażono także w pamięć EEPROM, dlatego możliwe

jest natychmiastowe odtworzenie ostatnich ustawień. Dzięki temu praca systemu jest wysoce stabilna i przewidywalna.

Zestaw CD06 może być wykorzystywany do zdalnego załączania urządzeń oświetleniowych oraz sterowania kamerami z oświetlaczami IR, a także bramami przemysłowymi i rogatkami. Zestaw CD06 pozwala na zdalne przesyłanie sygnałów, między innymi z czujników ruchu, tablic wskaźnikowych i wyłączników krańcowych i może służyć do powiadamiania drogą radiową w systemach monitorowania stanów central alarmowych i ppoż., automatyki lub sterowania maszynami przemysłowymi. CD06 w połączeniu z modemem radiowym CD04 może pełnić funkcję pilota radiowego do zdalnego sterowania o dużym zasięgu.

CD06 jest urządzeniem bardzo wszechstronnym i umożliwia zdalne sterowanie dowolnymi urządzeniami o znacznej mocy.

Bezpośr. inf. Agnieszka Gralak
Camsat

FM Analyzer
nowy moduł ułatwiający zarządzanie bezpieczeństwem obiektów

Moduł FM Analyzer to nowy element systemu **GEMOS**, który dostarcza kompleksowych danych na temat stanu zintegrowanych systemów i urządzeń zainstalowanych w budynku. Ułatwia sprawne i skuteczne zarządzanie bezpieczeństwem.

Raporty, które generuje FM Analyzer, pozwalają na łatwe wykrycie usterek newralgicznych punktów w obiekcie, wszystkich systemów i urządzeń, które zgłaszają awarie. Szczegółowe informacje na temat rodzaju i lokalizacji wadliwie działających urządzeń umożliwiają wyeliminowanie źródeł usterek i efektywne zarządzanie bezpieczeństwem. Dzięki temu możliwe jest szybkie przywrócenie pełnego bezpieczeństwa w budynku i utrzymanie go podczas dalszego użytkowania. FM Analyzer jest przydatny zarówno na etapie rozruchu systemów w budynku, jak i w ich późniejszej eksploatacji.

FM Analyzer jest modułem systemu zarządzania budynkiem GEMOS i wykorzystuje zasoby jego bazy danych, w której zgromadzone są wszystkie informacje pochodzące ze zintegrowanych systemów technicznych budynku. Jest to ergonomiczna i łatwa w obsłudze aplikacja, dostosowywana do indywidualnych potrzeb każdego użytkownika.

FM Analyzer przedstawia informacje gromadzone w bazach systemu GEMOS w prosty i czytelny sposób, w postaci raportów zawierających łatwe do zinterpretowania wykresy kołowe i słupkowe. Raporty przedstawiają stan zintegrowanych systemów i urządzeń zainstalowanych w budynku. Moduł umożliwia również eksport danych do innych aplikacji, np. Power Point, Excel, i do formatu PDF.

FM Analyzer może być stosowany zarówno w dużych, rozległych obiektach przemysłowych, galeriach handlowych, kampusach akademickich, szpitalach, portach lotniczych, na dworcach kolejowych, stadionach, w halach widowiskowo-sportowych, obiektach bankowych, biurowcach, jak i w mniejszych budynkach o przeznaczeniu biurowym czy mieszkalnym.

Bezpośr. inf. ela-compil

Nowa generacja czujek **Blue Line**

Firma **Bosch Security Systems** wprowadziła do sprzedaży kolejną generację cieszących się niesłabnącym zainteresowaniem odbiorców czujek ruchu serii Blue Line. Serię **Blue Line Gen 2** cechuje jeszcze większa skuteczność wykrywania i odporność na fałszywe alarmy. Są też łatwiejsze do zainstalowania. Czujki dostępne są w wersji standardowej i odpornej na zwierzęta domowe (*pet-friendly*). Znakomicie sprawdzą się w budynkach mieszkalnych, obiektach handlowych i innych komercyjnych zastosowaniach dozorowych.

W skład serii Blue Line Gen 2 wchodzą pasywne czujki podczerwieni (PIR), czujki PIR Quad, a także czujki TriTech będące efektem wykorzystania technologii mikrofalowej oraz podczerwieni, która umożliwia dokładniejszą analizę wykrywanego ruchu. Wszystkie modele mają wymienną podstawę montażową, co pozwala na szybką wymianę na detektory wykorzystujące bardziej zaawansowaną technikę wykrywania w miejscach szczególnie narażonych na generowanie fałszywych alarmów. W modelach odpornych na zwierzęta domowe można wyłączyć tę funkcję, dzięki czemu jedna czujka może mieć wiele różnych zastosowań, nawet jeśli środowisko jej pracy ulegnie modyfikacji.

Dzięki zastosowaniu samoblokującej dwuczęściowej obudowy, wbudowanej dwuosiowej poziomicy pęcherzykowej oraz zespołu zacisków w podstawie montażowej instalacja czujki trwa dosłownie kilka sekund. Zespół zacisków został specjalnie zaprojektowany w taki sposób, by zapobiec ewentualnym błędom przy okablowywaniu i konieczności posiłkowania się pomocniczym przyrządem serwisowym. Czujkę można umieścić na wysokości od 2,3 do 2,7 m bez potrzeby regulacji, co zapewnia objęcie obserwacją monitorowanego obszaru na odległość do 12 m od urządzenia.

Czujki ruchu Blue Line Gen 2 zapewniają większy i pozbawiony martwych punktów obszar obserwacji (12×12 m od ściany do ściany). Dzięki przetwarzaniu sygnału FSP (*First Step Processing*) czujki inteligentnie analizują ruch celem odróżnienia poruszających się ludzi od innych źródeł ruchu i automatycznie dostosowują czułość na podstawie właściwości docierającego do nich sygnału (m.in. amplitudy, polaryzacji itp.). Tak zaawansowana technologia pozwala na zgodne wygenerowanie warunku alarmowego przez oba detektory czujki przed załączeniem przekaźnika, co zapewnia natychmiastową reakcję na włamanie bez fałszywych alarmów.

Liczne funkcje dodatkowe zapewniają niezawodne działanie i funkcjonalność czujek. Hermetycznie zamknięta komora optyczna chroni czujki przed wpływem niekorzystnej cyrkulacji powietrza i owadami, a funkcja odporności na zwierzęta domowe pozwala na rozróżnienie sygnałów wywoływanych przez ludzi i zwierzęta. Funkcja dynamicznej kompensacji temperatury umożliwia dostosowanie czułości do warunków termicznych panujących w pomieszczeniu w celu precyzyjnego wykrycia włamywacza.

Bezpośr. inf. Bosch Security Systems

JVC

The Perfect Experience

Authorised Professional Dealer
euroalarm

www.euroalarm.com.pl

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,
- wprowadziliśmy sprzedaż premiowaną na wybrane modele JVC, a **nagrodą gwarantowaną** są dowolne, wybrane przez beneficjenta **NARTY.**

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

Samsung wprowadza na rynek nowe modele kamer PTZ serii **SCP** z procesorami DSP **W-V** i **SV-V**

Do linii kamer SCP z głowicą PTZ Samsung dodaje modele wzbogacone w innowacyjną, zaawansowaną technologię zastosowaną w chipsetach DSP **W-V** oraz **SV-V** marki **Samsung Techwin**.

Dziesięć nowych dzienno-nocnych modeli kamer kopułkowych mają obiektywy zmiennoogniskowe o krotnościach 27x, 33x lub 37x. Odpowiednie modele można zastosować zarówno wewnątrz, jak i na zewnątrz pomieszczeń, na parkingach, w centrach handlowych, hurtowniach, lotniskach, w portach i innych miejscach wymagających nadzoru.

Kamery z procesorem W-V generują kolorowe obrazy o znakomitej jakości i rozdzielczości dochodzącej nawet do 600 linii TV. Procesor został wyposażony także w funkcję *Super Dynamic Range* (SSDR), która automatycznie rozjaśnia zaciemnione obszary obrazu, co pozwala operatorowi dostrzec obiekty ukryte w cieniu. Inne technicznie zaawansowane funkcje to kompensacja skutków prześwietlenia pewnych obszarów (*Highlight Compensation*), która neutralizuje skutki nadmiernego oświetlenia pewnych obszarów kadru, umożliwiając operatorowi obserwację uprzednio niewidocznych fragmentów, a także cyfrowa stabilizacja obrazu (*Digital Image Stabilisation* – DIS), która może zniwelować efekty drgań kamery spowodowanych silnym wiatrem lub wibracjami konstrukcji wsporczej.

Chipset SV-V realizuje wszelkie zaawansowane funkcje procesora W-V, w tym redukcję szumów *Samsung Super Noise Reduction* (SSNRIII), a ponadto wzbogaca kamery w funkcję WDR oraz funkcję skanowania progresywnego, co umożliwia otrzymanie obrazu o niezwykłej jakości nawet w najtrudniejszych warunkach oświetleniowych. Technologia skanowania progresywnego pozwala na generowanie wysokiej jakości

obrazu obiektów ruchomych, umożliwiając – między innymi – odczyt tablic rejestracyjnych poruszających się pojazdów bez „efektu ducha". Kolejną funkcją chipsetu SV-V jest inteligentna analiza obrazu (IVA), odpowiedzialna np. za takie funkcje, jak detekcja pojawienia się/zniknięcia obiektu.

– *Istnieje duża liczba powodów skłaniających do wykorzystania kamer w nadzorze oraz równie duża liczba różnych miejsc, w których te kamery mogą zostać fizycznie zainstalowane* – mówi **Peter Ainsworth**, Senior European Product Manager w Samsung Techwin Europe. – *Mając to na uwadze, nasi projektanci wykorzystali niezwykle popularne procesory W-V i SV-V w nowych modelach kamer, z których każda spełnia specyficzną, wyjątkową funkcję, umożliwiając instalatorom oraz integratorom systemów wybór gotowej do użycia, doskonałej kamery kopułkowej.*

Dwa modele z tej linii – kamera kopułkowa SCP-3370TH (z procesorem SV-V) oraz kamera kopułkowa SCP-2370TH (z procesorem W-V) – zostały wyposażone w funkcję automatycznego śledzenia, która pozwala im wykryć poruszający się obiekt oraz automatycznie podążać za nim bez interwencji operatora, co sprawia, że nadają się do ochrony perymetrycznej oraz ochrony obiektów poza godzinami pracy.

Wszystkie dziesięć modeli z nowej linii SCP umożliwia transmisję zarówno wizyjną, jak i telemetryczną poprzez kabel koncentryczny, umożliwiając pełny dostęp do ustawień kamery oraz funkcji *pan-tilt-zoom* za pośrednictwem cyfrowych rejestratorów wizji (DVR), na przykład wybranych modeli rejestratorów Samsung z serii SRD. Technologia ta ogranicza koszty dzięki redukcji kosztów okablowania przy jednoczesnym zachowaniu elastyczności rozwiązań umożliwiającej szybką i łatwą rozbudowę istniejących systemów.

Bezpośr. inf. David Solomons
DRS Marketing

Samsung wprowadza dwa nowe, ekonomiczne modele do swojej linii kompaktowych, wandaloodpornych kamer kopułkowych

Dwa najnowsze produkty marki **Samsung**, dodane do linii wandaloodpornych kamer kopułkowych, znajdą zastosowanie wszędzie tam, gdzie kamery są narażone na akty wandalizmu lub manipulację.

Modele **SCV-2081** oraz **SCV-3081** to kamery kopułkowe do montażu powierzchniowego, dostosowane do różnorodnych zastosowań wewnętrznych i zewnętrznych, takich jak monitoring biur, sklepów, parkingów, szkół, szpitali, klatek schodowych etc. Oba modele, które wyposażono we wzmocnione obudowy aluminiowe, mają stopień szczelności IP66 i dużą odporność na próby celowego uszkodzenia.

Model SCV-2081 ma wbudowany obiektyw umożliwiający regulację ogniskowej w zakresie od 2,8 mm do 10 mm i jest wyposażony w doceniany procesor DSP Samsung Techwin W-V, dzięki czemu zapewnia doskonałej jakości kolorowy obraz w rozdzielczości dochodzącej do 600 linii TV. Zestaw zaawansowanych funkcji obejmuje redukcję szumów Samsung Super Noise Reduction trzeciej generacji (SSNRIII) oraz opcję sterowania za pośrednictwem kabla koncentrycznego, która, w przypadku zastosowania kompatybilnego rejestratora DVR (np. dowolnego rejestratora Samsung z serii SRD), umożliwia zdalną obsługę wielojęzycznego menu OSD poszczególnych kamer z poziomu pomieszczenia kontroli – bez konieczności instalowania dodatkowego okablowania do przesyłania sygnałów telemetrycznych. Warto wspomnieć także o funkcji Samsung Super Dynamic Range (SSDR), która powiększa stopień kompensacji oświetlenia tylnego i automatycznie poprawia widoczność szczegółów w zaciemnionych obszarach kadru. Umożliwia to dostrzeżenie obiektów ukrytych w cieniu.

Kamera SCV-3081 ma wbudowany obiektyw z możliwością regulacji ogniskowej w zakresie od 2,8 mm do11 mm i została wyposażona w procesor DSP Samsung Techwin SV-V, który dysponuje wszystkimi zaawansowanymi funkcjami chipsetu W-V. Najważniejszą nowością w przypadku procesora SV-V jest inteligentna analiza obrazu (IVA), realizująca na przykład funkcje detekcji pojawienia się obiektu na zaznaczonym obszarze lub jego zniknięcia z tego obszaru.

Bezpośr. inf. David Solomons
DRS Marketing

Samsung wprowadza na rynek nową 1,3-megapikselową kamerę sieciową PTZ z 20-krotnym zoomem optycznym

Nowa, zgodna ze standardami ONVIF 1,3-megapikselowa kamera sieciowa **SNP-5200** firmy Samsung jest wyposażona w obiektyw z 20-krotnym zoomem optycznym, głowicę PTZ, mechaniczny filtr podczerwieni i pracuje w trybach dzień/noc, dlatego może być dostosowana do wielu różnych zadań.

– *SNP-5200 to niezwykłe uzupełnienie naszej linii 1,3-megapikselowych kamer sieciowych iPOLiS* – powiedział **Peter Ainsworth**, Senior Product Manager Europe w Samsung Techwin Europe. – *Mimo iż cena jest bardzo atrakcyjna, kamera ma wiele funkcji i stanowi niewielkie obciążenie dla sieci IP, dlatego może być zastosowana jako część systemu nadzoru wizyjnego opartego na technologii IP wszędzie tam, gdzie potrzebny jest punkt kamerowy z opcją PTZ odznaczający się wysoką rozdzielczością.*

W kamerze SNP-5200 wykorzystany jest chipset WiseNet1 DSP marki Samsung, co pozwala użytkownikom maksymalnie wykorzystać najnowszą technologię, w tym nie wymagającą licencji inteligentną analizę obrazu (IVA) oraz dwustrumieniową kompresję H.264/MJPEG, która umożliwia równoczesną transmisję – z różnymi prędkościami – obrazów o różnej rozdzielczości do wielu odbiorców.

Przy tak dużym wyborze metod kompresji oraz rozdzielczości określona liczba uprawnionych użytkowników jest w stanie równocześnie obserwować obiekt w czasie rzeczywistym, ze stanowiska zlokalizowanego w jednym miejscu, rejestrować obrazy na urządzeniach zlokalizowanych w innym miejscu i przeglądać obrazy w czasie rzeczywistym lub już po ich zarejestrowaniu z użyciem smartfonu lub iPhone'u z zainstalowaną aplikacją iPOLiS firmy Samsung. Ponadto zdjęcia w formacie JPEG mogą zostać dołączone do alarmowej wiadomości e-mail, a pre- i postalarmowe obrazy mogą być przechowywane na karcie SD (czytnik kart jest wbudowany w kamerę). Co więcej, złącza Ethernet i BNC oraz dodatkowy port telemetryczny umożliwiają łatwe tworzenie hybrydowych systemów bezpieczeństwa. Złącze BNC zapewnia także łatwą konfigurację za pomocą standardowych monitorów instalatorskich.

Wykorzystany w kamerach system inteligentnej analizy obrazu IVA marki Samsung wykorzystuje wirtualną optyczną barierę, kierunkową detekcję wejścia na obszar i wyjścia z obszaru, jak również funkcję wykrywania pojawienia się albo zniknięcia obiektu, która analizuje jego ruch. IVA ma również funkcję monitorowania zmian pola widzenia kamery, która uruchamia alarm, gdy na przykład obiektyw kamery zostanie umyślnie zabrudzony farbą lub gdy pole widzenia kamery zostanie bez autoryzacji zmienione.

Cztery programowalne strefy detekcji ruchu, osiem programowalnych stref prywatności, dwukierunkowa transmisja dźwięku oraz wykorzystanie PoE to tylko niektóre z funkcji SNP-5200.

Model SNP-5200H, który jest wprowadzany równocześnie z SNP-5200, posiada te same funkcje, ale został wyposażony w obudowę o stopniu szczelności IP66, która jest odporna na ekstremalne warunki pogodowe i temperaturę otoczenia od –50°C do +50°C. Obydwa modele są oferowane wraz z wieloma akcesoriami oraz uchwytami umożliwiającymi montaż ścienny, słupowy, podokienny, podwieszany, narożny oraz sufitowy.

Dostępne u autoryzowanych dystrybutorów produktów Samsung kamery SNP-5200 i SNP-5200H są oferowane wraz z pełnym wsparciem serwisowym Samsung Techwin Europe, także w zakresie projektowania systemu oraz bezpłatnego wsparcia technicznego, i mają pełną, trzyletnią gwarancję.

Bezpośr. inf. David Solomons
DRS Marketing

Samsung wprowadza nowe profesjonalne monitory panoramiczne Full HD i HD

Firma **Samsung** dołączyła do swojej linii urządzeń **SMT monitory TFT LCD** o przekątnej ekranu **32"** i **40"**, które są przyjazne dla środowiska.

Podobnie jak w przypadku dotychczas istniejących modeli 17" i 19", modele 32" SMT-3223 oraz 40" SMT-4023 zostały zaprojektowane specjalnie z myślą o profesjonalnych systemach bezpieczeństwa. Z pewnością wzbudzą zainteresowanie instalatorów chcących zaoferować swoim klientom rozwiązania konkurencyjne cenowo, lecz doskonałe jakościowo oraz pobierające około 35% mniej energii w porównaniu z monitorami wcześniejszej generacji.

SMT-4023 posiada matrycę o rozdzielczości 1920×1080 (1080p Full HD), natomiast maksymalna rozdzielczość **SMT-3223** to 1366×768 (720p HD), co pozwala użytkownikom korzystać z megapikselowych kamer HD i Full HD najnowszej generacji, takich jak modele z chipsetami DSP WiseNetI oraz WiseNetII firmy Samsung.

Oba monitory mają wbudowane głośniki, posiadają wejścia BNC, DVI oraz 2 x HDMI oraz odznaczają się krótkim czasem odpowiedzi matrycy (tylko 8 ms). Wielojęzyczny interfejs ułatwia konfigurację, a zestaw uchwytów dostarczany wraz z monitorem umożliwia wiele wariantów mocowania. Do montażu ściennego, podwieszanego oraz pionowego służą uchwyty w standardzie VESA mocowane z tyłu monitorów. Dodatkowo opcjonalna podstawa SBM-320ST pozwala na wygodne ustawianie monitorów na biurku lub stole.

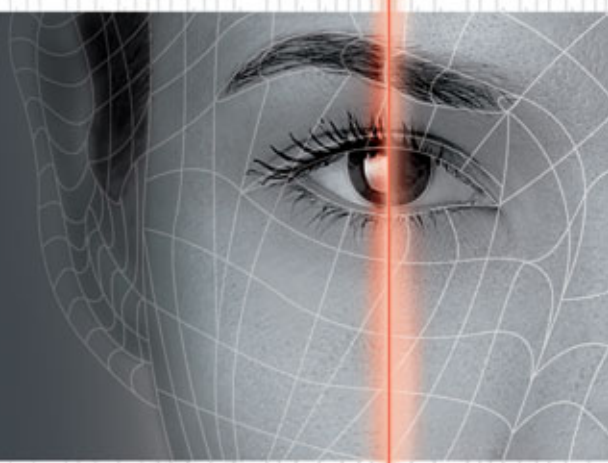
Bezpośr. inf. David Solomons
DRS Marketing

Międzynarodowe Targi Poznańskie

spotkaj przyszłość

securex 2012
POLAND

Międzynarodowe Targi Zabezpieczeń



23-26 kwietnia 2012
Poznań

zabezpiecz swój sukces

Nadesłanie zgłoszenia do **17 października**
gwarancją niższej ceny i lepszej lokalizacji

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

SAFESTAR

Nowej generacji system monitorowania

Krzysztof Ciesielski

Wielu uważa, że rozwiązania bazujące na starych, sprawdzonych architekturach działających jako aplikacje DOS i Windows to najlepsze rozwiązania w przypadku systemów monitorowania alarmów, gdyż charakteryzują się względną stabilnością i niezawodnością i są stosowane od lat. W ramach argumentacji mówi się na przykład, że w wahadłowcach kosmicznych „latają" stare i dobre rozwiązania – są sprawdzone i działają od wielu lat. Do niedawna trudno było znaleźć kontrargumenty... Era wahadłowców kosmicznych przeszła jednak do historii. Niedawno odbył się ostatni lot wahadłowca Atlantis. Czasy się zmieniają – w erze informacji stawia się na szybkość, efektywność, elastyczność i mobilność, czego stare technologie nie są w stanie zagwarantować. Naturalną drogą dalszego rozwoju informatycznego są aplikacje klasy RIA (*Rich Internet Application*), które zaspokajają nasze codzienne potrzeby w dziedzinie dostępu do usług (wykorzystuje się je np. w e-bankowości, e-administracji, e-rozrywce, e-PIT-ach, e-firmach). Mam przyjemność zaprezentować Państwu SAFESTAR – nowej generacji system do monitorowania alarmów, którego jestem głównym pomysłodawcą. Jest on dostępny przez Internet. System zbudowaliśmy całkowicie od podstaw, z zastosowaniem najnowszych technologii informatycznych, w zespole programistów DMSI Sp. z o.o. pod kierownictwem Tomasza Fąfary

SAFESTAR to nowoczesny i uniwersalny system do monitorowania sygnałów alarmowych i technicznych, który umożliwia zarazem wykorzystanie informacji o położeniu geograficznym, przeglądanie obrazów z kamer, korzystanie ze zintegrowanych połączeń telefonicznych oraz wszechstronną integrację z innymi systemami zabezpieczeń i automatyki.

Monitoring sygnałów alarmowych

SAFESTAR to kompletne środowisko do monitorowania alarmów z wykorzystaniem wszystkich najnowszych osiągnięć w dziedzinie monitoringu alarmowego, a także współczesnej telekomunikacji (w tym Internetu). Dzięki środowisku SAFESTAR można osiągnąć dotychczas nie oferowane na rynku monitoringu funkcje, takie jak wszechstronny dostęp do danych poprzez Internet, możliwość podłączenia praktycznie każdego typu nadajnika, kamer oraz pozycjonerów GPS, a co najważniejsze – możliwość udostępnienia najnowszej technologii każdej agencji ochrony, która zechce realizować usługi monitorowania bez ponoszenia kosztów zakupu specjalistycznego sprzętu.

Zaprojektowany do działania w chmurze

Jedynym warunkiem korzystania z systemu SAFESTAR jest dostęp do Internetu. System ten można uruchomić na dowolnym komputerze z dowolnym systemem operacyjnym oraz na urządzeniach mobilnych. W odróżnieniu od innych systemów i rozwiązań stosowanych w monitoringu SAFESTAR został stworzony całkowicie od podstaw w nowej technologii Jest to zbiór aplikacji uruchamianych z wykorzystaniem przeglądarek internetowych, co oznacza, że w pełni wykorzystuje wszystkie walory, jakie niesie ze sobą nowoczesna telekomunikacja, a przede wszystkim Internet.

Bezpieczeństwo i niezawodność

System został uruchomiony w środowisku Linux, które jest uważane za jedno z najbardziej bezpiecznych, wydajnych i stabilnych, a także niewprowadzających żadnych dodatkowych wymogów związanych z jego użytkowaniem, na przykład określonej przeglądarki, dodatkowych apletów, określonych wersji systemów operacyjnych, dodatkowych licencji itd. Technologia informatyczna, na której system został oparty, jest powszechnie wykorzystywana, na przykład w bankowości internetowej, co stanowi gwarancję bezpieczeństwa i operatywności. Dostęp do systemu jest chroniony dzięki zastosowaniu 1024-bitowego klucza kodującego.

Rozproszona infrastruktura

Uruchamiany w przeglądarce internetowej interfejs użytkownika (analogiczny do tego, który jest wykorzystywany w bankowości internetowej) to nie wszystko. Sercem systemu jest rozproszona infrastruktura serwerowa, która zbiera i udostępnia wszystkie sygnały, poddaje je analizie i grupowaniu, przygotowuje i generuje raporty oraz kontroluje harmonogramy. Serwery działają w środowisku Linux i wykorzystują bazy danych typu SQL. Taka architektura systemu pozwala na jego szybki rozwój, a zmiany i aktualizacje wprowadzane są w czasie rzeczywistym, bez konieczności przerywania pracy przez użytkowników.

Działanie systemu jest oparte na kilku serwerach umieszczonych w kilku centrach danych. Dzięki temu zapewniony jest najwyższy stopień niezawodności, często nieosiągalny nawet dla największych firm monitorujących. Klient nie musi się martwić o niezawodność i ciągłość działania. Dostęp do systemu jest możliwy zawsze i wszędzie, a użytkownik może zalogować się w dowolnym miejscu na świecie, używając tabletu lub laptopa z dostępem do Internetu.

Autonomiczne konektory

Oprogramowanie serwerów składa się między innymi z modułów komunikacyjnych, tzw. konektorów. Jest to nowatorskie rozwiązanie, które powstało po prawie dwóch latach badań, testów i udoskonaleń na bazie ponad 10 000 monitorowanych obiektów. Dzięki konektorom do systemu można przyłączyć każdy typ nadajnika alarmowego stosowanego w monitoringu – od najprostszych wykorzystujących PSTN i SMS-y poprzez nadajniki w pojazdach informujące o pozycji GPS, aż po nadajniki TCP/IP. W związku z tym system nie wprowadza żadnych ograniczeń w zakresie wysyłania, odbierania i gromadzenia danych. Można monitorować praktycznie wszystko – pojedyncze sygnały alarmowe, temperaturę, wilgotność (z wykorzystaniem protokołów Contact ID i SIA) czy też położenie pojazdów i osób (można sprawdzać je na mapie cyfrowej i przeglądać obrazy z kamer).

Łatwa integracja

Konektory umożliwiają praktycznie dowolną integrację z każdym systemem automatyki (także z systemami zabezpieczeń elektronicznych) oraz z każdą bazą danych umieszczoną w innym systemie monitoringu i zabezpieczeń elektronicznych. Opracowana przez nas technologia jest bardzo elastyczna. Ma zdolność „uczenia się” i można dostosować ją do różnych systemów. Dzięki temu każda integracja jest łatwa do zrealizowania, a całość uzyskana w jej wyniku jest stabilna i bezpieczna.

Lokalizacja obiektów i monitoring GPS

Integralną cechą opisywanego systemu jest wykorzystywanie informacji o położeniu geograficznym i pokazywanie go na mapach cyfrowych, a także wykorzystanie informacji

audiowizyjnych. Dzięki temu systemowi możemy monitorować obiekty stacjonarne oraz obiekty będące w ruchu, na przykład pojazdy.

Monitoring wizyjny

W zakresie audiowizyjnym system obsługuje współczesne protokoły kompresji obrazu, takie jak M-JPG, MPEG4, H264, i może współpracować z każdym urządzeniem, które wysyła obraz i dźwięk w takiej postaci. System nie wymaga instalowania dodatkowych modułów pozwalających na korzystanie z tych formatów – są one dostępne w standardzie.

Komunikacja VoIP

Łączność telefoniczna w stacji monitorowania alarmów to podstawa skutecznego działania i obsługi klienta. Jeszcze do niedawna instalowano centrale telefoniczne z liniami analogowymi i podłączano kosztowne rejestratory rozmów. Użytkownik systemu SAFESTAR nie potrzebuje centrali telefonicznej, aparatów telefonicznych ani rejestratorów rozmów. Połączenia są wykonywane bezpośrednio z aplikacji operatora i są od razu rejestrowane i przyporządkowywane do obsługiwanego zdarzenia. Numery telefonów są pobierane bezpośrednio z bazy danych i operator nie musi tracić czasu na ich wprowadzanie.

SAFESTAR całkowicie zmienia wyobrażenie o systemach monitorowania. Jest to związane przede wszystkim z dostępnością, szybkością działania i niezawodnością, a także zdolnością integracji z innymi urządzeniami. Większość obecnie spotykanych problemów dotyczących usług monitorowania praktycznie nie występuje w przypadku tego rozwiązania. Jest to efektem doboru właściwej, nowoczesnej technologii, która niejako z definicji oferuje to, co w dotychczas stosowanych rozwiązaniach osiągane jest bardzo dużym nakładem pracy.

Dla kogo jest SAFESTAR?

SAFESTAR został opracowany w taki sposób, aby sprostać oczekiwaniom jak największej grupy odbiorców. Mogą wykorzystać go zarówno małe, jak i duże firmy ochrony. Systemu można używać nawet do monitorowania pojedynczych obiektów. W każdym przypadku wszystkie jego funkcje są dostępne. Nie trzeba ponosić dodatkowych opłat za jego uruchomienie i kupować specjalistycznego sprzętu. Wystarczy mieć dostęp do Internetu i uruchomić przeglądarkę internetową, by skorzystać w pełni ze wszystkich jego zalet.

Krzysztof Ciesielski
Prezes Zarządu
DMSI

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.

RCP Master *PR602LCD*

roger®

20 YEARS 1991-2011

www.roger.pl

Rozwiązania Kontroli Dostępu i Rejestracji Czasu Pracy

Wprowadzono do oferty **czytnik administratora RUD-3** dedykowany do współpracy z transponderami zbliżeniowymi standardu 13,56MHz ISO/IEC 14443A oraz Mifare

HD-SDI

w systemach telewizji dozorowej – światełko w tunelu czy droga donikąd?

Andrzej Walczyk

Od kilkunastu miesięcy w materiałach reklamowych wielu firm zajmujących się telewizją dozorową pojawia się nowy motyw – HD CCTV lub HD-SDI. Oba te skróty niosą za sobą wiele niejasności. Określenie CCTV jest jednoznacznie utożsamiane z telewizją analogową, zaś HD oznacza telewizję o wysokiej rozdzielczości. Połączenie obu tych terminów mogłoby sugerować analogową telewizję o wysokiej rozdzielczości, gdyby nie trzeci skrót, HD-SDI, który oznacza standard cyfrowej transmisji sygnałów wizyjnych na niewielkie odległości, wykorzystywany powszechnie w technice studyjnej. W to wszystko wkrada się dość agresywny marketing, zaś przeciętny projektant czy instalator systemów dozorowych jest całkowicie zdezorientowany. Spróbujmy uporządkować te pojęcia

Podobnie jak kilkadziesiąt lat temu w przypadku telewizji dozorowej bazującej na standardzie PAL, współczesna telewizja dozorowa o wysokiej rozdzielczości także rozwinęła się dzięki udoskonalaniu sprzętu konsumenckiego. Wprowadzenie na rynek pierwszych telewizorów pracujących w standardzie HD 720, a następnie HD 1080 zwiększyło zainteresowanie producentów kamer megapikselowych tymi formatami obrazów. Zagadnienia dotyczące podobieństw oraz różnic pomiędzy kamerami megapikselowymi a kamerami HD były wielokrotnie omawiane na łamach *Zabezpieczeń* i proponuję do nich nie wracać. Przyjmijmy tylko, że symbolem HD będziemy oznaczać obraz mieszczący się w rastrze 1080×1920 pikseli.

Technologiczny rozwój kamer przemysłowych zbiegł się w czasie z rozwojem i upowszechnieniem sieci IP, w tym także Internetu. W momencie pojawienia się pierwszych kamer megapikselowych, a później kamer pracujących w standardzie HD, jedynym medium zdolnym do transmisji obrazów wytwarzanych przez te kamery była sieć IP. Co prawda standard transmisji HD-SDI już wtedy istniał, jednak jego wykorzystanie w telewizji dozorowej było zbyt kosztowne. Kamery megapikselowe i kamery pracujące w standardzie HD były wyposażone w interfejs Ethernet służący do transmisji strumienia wizyjnego o wysokiej rozdzielczości oraz do dwukierunkowej transmisji sygnałów sterujących. Ponadto większość kamer megapikselowych posiadała gniazdo BNC, przez które można było pobrać zespolony sygnał wizyjny w standardzie PAL przeznaczony do celów serwisowych. Ten stan utrzymał się do dnia dzisiejszego i standardowe wyposażenie kamer sieciowych stanowią dwa interfejsy – łącze Fast Ethernet na gnieździe RJ-45 i wyjście zespolonego sygnału wizyjnego w standardzie PAL na gnieździe BNC.

W niektórych modelach kamer gniazdo BNC jest pomijane jako mało przydatna pozostałość minionej epoki, gdyż dostępność analogowych monitorów pozwalających na regulację kamer podczas ich instalacji jest coraz mniejsza, za to udoskonalone zostały metody zdalnej regulacji kamer poprzez sieć IP. Wiele współczesnych, stacjonarnych kamer sieciowych umożliwia regulację ostrości obrazu i zmianę ogniskowej obiektywu z poziomu stacji roboczej służącej do obsługi systemu. Oczywiście tego typu funkcji nie ma w systemach wykorzystujących transmisję metodą HD-SDI.

Z upływem czasu, wraz z powiększaniem się oferty sieciowych kamer dozorowych wzrastała podaż innych urządzeń niezbędnych do budowy sieciowych systemów dozoru wizyjnego, w tym rejestratorów, monitorów, a także oprogramowania systemowego. Ze względu na chłonny rynek i masową produkcję tych urządzeń ich ceny spadły do relatywnie niskiego poziomu i tendencja spadkowa nadal się utrzymuje.

Wzrost popularności rozwiązań sieciowych i rozwój rynku telewizji IP odbił się niekorzystnie na kondycji rynku analogowych systemów dozorowych, określanych jako CCTV, który zareagował obniżką cen i zmianą strategii marketingowej, w ramach której eksponowane były zalety tych systemów, zaś korzyści wynikające z przejścia na technologię sieciową były bagatelizowane. **Wielu projektantów i instalatorów systemów dozorowych, przyzwyczajonych do dotychczasowych rozwiązań, wykazuje znaczną podatność na tego typu argumentację. Przejście na technologię sieciową wymagałoby od nich zmiany sposobu myślenia, uzupełnienia wiedzy, a nawet poczynienia pewnych inwestycji w urządzenia i oprogramowanie. Właśnie dla takich osób przeznaczone są systemy bazujące na technologii HD-SDI.**

Interfejs HD-SDI pojawił się w nielicznych modelach kamer megapikselowych dopiero w roku 2010. Jego wprowadzenie nie stanowiło przełomu technologicznego, oznaczało jedynie, że jedna z wielu metod cyfrowej transmisji sygnału wizyjnego, stosowana dotychczas w sprzęcie studyjnym, została zastosowana w sprzęcie dozorowym. Tymczasem w materiałach marketingowych datę 2010 podaje się jako punkt zwrotny w rozwoju systemów dozoru wizyjnego i dorabia się do tego jakąś pokrętną ideologię.

Między archaicznymi analogowymi systemami dozorowymi a z pozoru nowoczesnymi systemami HD-SDI zachodzą duże podobieństwa. Na przykład w obu przypadkach transmisja sygnału wizyjnego przebiega jednokierunkowo, poprzez kabel koncentryczny o impedancji falowej równej 75 Ω. Jednak oferujący rozwiązania HD-SDI nie informują swoich klientów, że wymagane jest użycie specjalnego kabla, umożliwiającego uzyskanie przepustowości toru transmisyjnego na poziomie 1,5 Gb/s, zaś klasyczne kable koncentryczne, stosowane w telewizji analogowej, nie spełniają tych wymagań. Zgodnie z danymi pochodzącymi z opisu standardu HD-SDI długość kabla koncentrycznego nie może przekraczać 200 m (pod warunkiem, że jest to kabel odpowiedniego rodzaju), zaś transmisja na większe odległości wymaga użycia światłowodów oraz specjalnych konwerterów o wysokiej przepustowości. Tymczasem w materiałach marketingowych chwalących transmisję metodą HD-SDI mówi się o możliwości wykorzystania istniejących kabli koncentrycznych, zainstalowanych wiele lat temu wraz z analogowym systemem dozorowym. W zasadzie takie

działanie należałoby nazwać świadomym wprowadzaniem klientów w błąd.

Zwolennicy systemów dozorowych wykorzystujących transmisję metodą HD-SDI chętnie zwracają uwagę na to, że wiele firm zainteresowało się tą technologią i podaż urządzeń wkrótce wzrośnie. Jednak na tegorocznych targach IFSEC w Birmingham żaden z liczących się producentów nie oferował tego typu rozwiązań.

Jak dotychczas asortyment dostępnych na rynku urządzeń wykorzystujących transmisję metodą HD-SDI jest niewielki. Na przykład nie są oferowane żadne kamery szybkoobrotowe tego typu, co oznacza, że ruchome punkty kamerowe muszą być budowane z osobnych elementów. To z kolei oznacza, że kamera, obiektyw, obudowa i mechanizm napędowy muszą być zakupione oddzielnie i dopasowane do siebie przez instalatora. Takie rozwiązanie ma dość istotne wady. Po pierwsze – nie jest możliwa automatyczna regulacja ostrości, czyli auto-focus. Po drugie – podobnie jak w analogowych systemach CCTV, transmisja sygnałów w torze HD-SDI jest jednokierunkowa, przez co wysyłanie jakichkolwiek danych sterujących do kamery wymaga użycia osobnego nośnika.

W reklamach systemów dozorowych, które wykorzystują transmisję metodą HD-SDI, eksponowana jest niska cena kamer wynikająca z braku konieczności kompresji i kodowania sygnału wizyjnego w postaci umożliwiającej jego transmisję poprzez sieć TCP/IP. Tymczasem ta zaleta jest iluzoryczna, gdyż rejestratory pozwalające na zapis sygnałów wizyjnych transmitowanych metodą HD-SDI są tak drogie, że podczas zakupu kamer do ceny każdej z nich należy doliczyć kilka tysięcy złotych przeznaczonych na zakup odpowiedniego rejestratora. Koszt przykładowego systemu wykorzystującego transmisję metodą HD-SDI i zawierającego zaledwie cztery kamery przekracza kilkanaście tysięcy złotych, co czyni całą inwestycję nieopłacalną. Za podobną cenę można kupić wysokiej jakości sprzęt sieciowy o zbliżonych parametrach, oferujący wyrafinowane funkcje sterujące, niedostępne w standardzie HD-SDI.

Rozbudowa systemów dozoru wizyjnego wykorzystujących transmisję metodą HD-SDI jest utrudniona z powodu braku tanich urządzeń pozwalających na komutację sygnałów wizyjnych. W technice studyjnej takie urządzenia nazywają się ruterami wizyjnymi i stanowią odpowiednik przełączników sekwencyjnych stosowanych w dawnych systemach analogowych. Nie są dostępne żadne krosownice wizyjne, nie mówiąc już o dzielnikach obrazu. Wszystkie funkcje związane z obsługą systemów dozorowych wykorzystujących transmisję metodą HD-SDI są jak dotychczas realizowane przez rejestratory.

Promując metodę transmisji HD-SDI, często podkreśla się brak jakichkolwiek jej powiązań z sieciami IP. Jednak i to jest pozorne, bo próba transmisji obrazów na większe odległości lub próba tworzenia większych, zintegrowanych systemów obsługujących oddalone od siebie obiekty i tak kończy się przekodowaniem sygnału wizyjnego z postaci HD-SDI na postać sieciową. Tak więc tłumaczenie, że projektant czy instalator systemu nie musi dysponować wiedzą na temat sieci teleinformatycznych nie ma pokrycia w rzeczywistości.

Standard HD-SDI jest masowo stosowany przez rozgłośnie telewizyjne, do transmisji sygnałów wizyjnych w obrębie studia, wozu transmisyjnego czy obszaru, na którym zainstalowane są kamery studyjne. Jednakże w tej dziedzinie też zachodzą zmiany na lepsze i najnowsze trendy wskazują na rychłe odejście od transmisji sygnałów wizyjnych metodą HD-SDI i przejście na technologię TCP/IP z wykorzystaniem sieci Ethernet o przepustowości 1 Gb/s. Już obecnie wszystkie urządzenia studyjne przetwarzają sygnały wizyjne zamienione na postać sieciową, gdyż stwarza to możliwości łatwiejszej obróbki obrazów, ich miksowania, przełączania etc. Technologia HD-SDI służy jedynie do transmisji sygnałów wizyjnych pomiędzy urządzeniami i jest raczej przeszkodą w ich rozwoju, a nie motorem postępu.

Jedyne realne zalety systemów analogowych, na jakie powołują się oferujący rozwiązania wykorzystujące standard HD-SDI, to znaczy brak zauważalnych opóźnień w transmisji sygnałów wizyjnych, wysoka poklatkowość i ostrość obrazu wynikająca z braku kompresji, nie mogą stanowić decydującego argumentu, gdyż te same cechy wykazuje prawidłowo skonfigurowany system sieciowy. O żadnych zaletach nie może być mowy w przypadku rejestracji nieskompresowanego sygnału wizyjnego. Jak łatwo obliczyć, zaledwie kilkudniowe nagrania nieskompresowanych obrazów pochodzących z pojedynczych kamer o rozdzielczości HD prowadzą do powstania gigantycznych plików, których przechowywanie będzie wiązało się z dużymi kosztami. Poddanie tych obrazów silnej kompresji, na przykład metodą H.264, prowadzi do zrównania systemów wykorzystujących transmisję metodą HD-SDI z systemami sieciowymi, przez co całe przedsięwzięcie staje się bezcelowe.

Często podawanym przykładem zastosowania transmisji metodą HD-SDI jest wykorzystanie jej w systemach obserwacyjnych zainstalowanych w kasynach gry, gdzie ostrość i płynność obrazu telewizyjnego ma kluczowe znaczenie. Omawiane rozwiązanie mogłoby być opłacalne, gdyby chodziło jedynie o obserwację stołów gier, gdyż możliwe byłoby zastosowanie tanich kamer o rozdzielczości HD. Jednak w kasynach wymagana jest rejestracja obrazów ze wszystkich kamer i przechowywanie nagrań przez długie miesiące w celach operacyjnych, co w przypadku transmisji metodą HD-SDI wiąże się z budową potężnych macierzy dyskowych. Dużo skuteczniejszym i tańszym rozwiązaniem jest zastosowanie dobrze zaprojektowanego systemu sieciowego, w którym nie wystąpią żadne problemy ani z doborem sprzętu, ani z przechowywaniem plików z zakodowanymi obrazami.

Tak więc pomysł wykorzystania standardu HD-SDI w telewizyjnych systemach dozorowych należy uznać za nietrafiony. To droga donikąd. Ocenę metod marketingu odwołujących się do emocji i przyzwyczajeń projektantów i instalatorów systemów dozorowych, a nie do argumentów o charakterze merytorycznym, pozostawiam czytelnikom.

Andrzej Walczyk

CBC GROUP

GANZ

WWW.CBCPOLAND.PL

NOWA RODZINA HD W CBC

OBIEKTYWY MARKI computar

Profesjonalne obiektywy mega pikselowe COMPUTAR charakteryzują się wysoką jakością wykonania oraz innowacyjnością, pozwalającą na maksymalne wykorzystanie możliwości kamer megapikselowych.
Prezentowane obiektywy są dedykowane do zastosowań z kamerami CCTV wysokiej rozdzielczości 3Mpix. Japońska precyzja i jakość wykonania gwarantują idealne odwzorowanie obrazu w jak najwyższej jakości.

REJESTRATORY MARKI GANZ

Rejestratory DRH-LITE H.264 to nowoczesne modele z serii DIGIMASTER umożliwiające nagrywanie obrazu video z 4, 8 lub 16 kamer oraz rejestrację dźwięku z 4 źródeł audio.
Modele DRH-LITE zapewniają nagrywanie obrazu z szybkością do 400 klatek/sek. Wewnątrz urządzenia znajduje się miejsce na zamontowanie jednego dysku twardego SATA.

MONITORY MARKI ORION TECHNOLOGY A/S

Zastosowanie technologii LED w monitorach marki ORION pozwoliło na uzyskanie bardzo kompaktowej obudowy oraz obrazu o wyjątkowo równomiernej jasności i wysokim kontraście.
Te profesjonalne monitory o dużej przekątnej matrycy 18.5" oraz 21.5" i rozdzielczości Full HD (1920x1080 pikseli) charakteryzują się wyjątkowo niewielką obudową oraz małą wagą.
W całej gamie monitorów ORION są dostępne różne modele w zależności od rodzaju wejść i wyjść: HDMI, DVI, VGA, BNC, Audio oraz wejścia przekaźnikowe do przełączania źródła sygnału.

CBC (Poland) Sp. z o.o. ul. Krasińskiego 41A, 01-755 Warszawa, tel. 22 633 90 90, fax. 22 633 90 60 www.cbcpoland.pl
W chwili obecnej dostępne są trzy promocje: Computar, Ganz, Orion.

Autonomiczne systemy IP firmy Panasonic

Karol Fietkiewicz

W dziedzinie monitoringu wizyjnego od kilku lat można zaobserwować wypieranie tradycyjnych analogowych systemów dozorowych przez systemy IP. Na rynku od dłuższego czasu funkcjonują kamery z przetwornikami o liczbie pikseli przekraczającej 10 000 000. To ponad 20 razy więcej niż w przypadku obrazu w standardzie 4CIF. Systemy dozorowe wykorzystujące technologię sieciową mogą przekroczyć technologiczną barierę narzucaną przez standard PAL, umożliwiają analizę obrazu i można je łatwo rozbudować (dodatkowe urządzenia rejestrujące, centra monitorowania)

Podobnie jak przypadku starszych rozwiązań, systemy rejestracji obrazu można budować dwojako.

Pierwsze rozwiązanie polega na zastosowaniu urządzeń skonstruowanych na bazie komputerów PC z odpowiednim oprogramowaniem przeznaczonym do zapisu obrazu oraz, ewentualnie, do jego analizy. System taki posiada niewątpliwe zalety, do których należy elastyczność w doborze oprogramowania i sprzętu, szybkość aktualizacji do nowszej wersji czy elementy obsługi dobrze znane ze standardowych komputerów. Możliwość doboru oprogramowania i sprzętu może stanowić jednocześnie duże utrudnienie. Podzespoły komputera, nawet jeśli będą przeznaczone do zastosowań serwerowych, mogą działać nieprawidłowo w przypadku rejestracji obrazów z kamer IP. Skuteczny w przypadku standardowych zastosowań system operacyjny nie jest skonfigurowany i przetestowany w sposób odpowiadający tym konkretnym rozwiązaniom. Wykorzystane oprogramowanie może nie być w stu procentach kompatybilne z podzespołami komputera. Wszystko to powoduje trudności w stworzeniu platformy IP o dużej bezawaryjności i niezawodności działania.

Drugim rozwiązaniem jest zastosowanie urządzeń współpracujących z dedykowanym sprzętem producenta i dedykowanym systemem operacyjnym będącym jednocześnie oprogramowaniem rejestrującym. Pozwala to producentowi na optymalny dobór wszystkich komponentów na podstawie ich wydajności i stabilności. Autonomiczność takiego rozwiązania w wielu przypadkach uniemożliwia lub utrudnia niepowołaną lub nieodpowiedzialną ingerencję, która może spowodować awarię systemu. Łatwość instalacji dodatkowych urządzeń peryferyjnych, obsługa popularnych kamer IP (implementacja ONVIF) oraz opcja aktualizacji oprogramowania powoduje, że owa pozorna „zamkniętość" nie stanowi żadnych przeszkód. Takie urządzenia nazywane są sieciowymi rejestratorami wizyjnymi (ang. *Network Video Recorder*). W tym zakresie jednym z wiodących producentów jest firma Panasonic, posiadająca w ofercie zarówno różne modele rejestratorów sieciowych, jak również dużą liczbę kamer IP.

Najnowszym i najbardziej zaawansowanym rejestratorem jest model WJ-NV200. Jest to całkowicie autonomiczne urządzenie pozwalające na obsługę poprzez monitor HD, mysz i klawiaturę bez konieczności instalowania osobnego oprogramowania dostępowego na komputerze PC.

Jako jedno z nielicznych urządzeń dostępnych na rynku model WJ-NV200 potrafi zapisywać obraz z kamer IP kompresowany trzema różnymi kodekami – MPEG4, MJPEG oraz H.264. Do najbardziej innowacyjnych funkcji, dostępnych w przypadku współpracy z kamerami IP firmy Panasonic, należy zaliczyć detekcję twarzy (i rozpoznawanie na podstawie wzorca znalezionego w bazie danych) oraz możliwość zapisywania obrazów na karcie SD umieszczonej wewnątrz kamery, dzięki czemu zapewniony jest dostęp do nagrań alarmowych w przypadku awarii sieci czy nawet samego rejestratora. Funkcją bardzo przydatną w trakcie instalacji jest automatyczne wyszukiwanie kamer w sieci. Oczywiście rejestrator wyposażony jest również w szereg bardziej standardowych funkcji, takich jak wyszukiwanie odpowiednich fragmentów materiału wizyjnego, wyświetlanie obrazów związanych z alarmami, wiele trybów pracy na podstawie wcześniej ustalonego harmonogramu oraz możliwość wykorzystania wejść i wyjść alarmowych.

Fot. 2. Rejestrator sieciowy WJ-ND400

Urządzeniem przeznaczonym do zapisu obrazu, które nie ma rozbudowanych funkcji służących do obsługi lokalnej, jest WJ-ND400. Podobnie jak WJ-NV200, model ND400 dysponuje trzema różnymi rodzajami kodeków – MPEG4, MJPEG oraz H.264 – i umożliwia obsługę aż 64 kamer IP. Przechowywanie obrazów z tak wielu kamer wymaga zastosowania nośników o dużej pojemności. Przykładowo – jeśli pojemność, jaką dysponuje dziewięć dysków twardych montowanych w urządzeniu WJ-ND400, okaże się niewystarczająca, można dołączyć dodatkowo pięć macierzy dyskowych typu WJ-HDE400 pracujących w systemie RAID5 lub RAID6. Zarówno dyski wykorzystywane w urządzeniu WJ-ND400, jak i dyski pracujące w macierzach WJ-HDE400 mogą być wyjmowane lub wkładane w trybie *HotPlug*, czyli bez konieczności wyłączania rejestratora i przerywania zapisu. Trzydzieści dwa wejścia alarmowe zamontowane na tylnym panelu obudowy pełnią taką samą rolę jak odpowiednie wejścia alarmowe umieszczone w kamerach. Uzupełnienie stanowią wejścia/wyjścia specjalnego przeznaczenia, które sygnalizują awarie (w tym awarie kamery, dysków twardych, sieci) lub uruchamiają specjalne tryby rejestracji i inne funkcje.

Fot. 1. Rejestrator sieciowy WJ-NV200

Do komunikacji ze światem zewnętrznym służą dwa złącza LAN o prędkości 1 Gb/s. Jedno z nich jest domyślnie przeznaczone do pobierania strumieni danych z kamer IP, drugie służy do podłączenia rejestratora do sieci lokalnej, w której pracują stacje robocze z oprogramowaniem zarządzającym WV-ASM100/WV-ASM10. Rejestrator umożliwia dostęp 16 użytkowników jednocześnie oraz zdefiniowanie różnych praw dostępu. Oprócz identyfikacji użytkownika na podstawie identyfikatora i hasła istnieje także opcja filtrowania adresów IP klientów.

Pozostałe dwa modele, WJ-ND300A i WJ-ND200, są mniej rozbudowane niż WJ-ND400. Model WJ-ND300A obsługuje 32 kamery IP, a także pozwala na powiększenie pamięci dyskowej o macierz RAID5. Model WJ-ND200 obsługuje 16 kamer IP i umożliwia zdublowany zapis danych (RAID1).

W razie potrzeby wszystkie elementy składające się na cały system mogą zostać połączone i zarządzane przez oprogramowanie VW-ASM10, którego możliwości są znaczne. Oprogramowanie potrafi obsłużyć do 3200 kamer w 100 rejestratorach i 256 kamer podłączonych do koderów IP. Model kamery i rejestratora jest rozpoznawany automatycznie. System pozwala na utworzenie do 400 grup kamer konfigurowanych przez użytkownika i na wyświetlanie obrazów pochodzących z tych kamer na wielu monitorach. Oprogramowanie umożliwia elastyczny dobór rodzaju i rozdzielczości pobieranego strumienia wizyjnego w zależności od trybu podziału ekranów monitorów. Mapy synoptyczne z aktywnymi ikonami ułatwiają podejmowanie właściwych działań związanych z zaobserwowanymi sytuacjami i odebranymi sygnałami alarmowymi. Są na nich umieszczone ikony symbolizujące poszczególne kamery – po ich kliknięciu wyświetlany jest obraz z danej kamery z opcją aktywacji wyjść alarmowych (AUX). Pulpit WV-CU950 ułatwia sterowanie samym programem i ruchami kamer (PTZ). Program oferuje rozbudowane zarządzanie prawami użytkowników, w tym autoryzację użytkowników za pomocą hasła (aktualną przez określony okres), wiele poziomów dostępu i różne możliwości podglądu i sterowania kamerami.

Bogaty asortyment autonomicznych rejestratorów sieciowych obejmuje zarówno proste urządzenia, będące cyfrowymi odpowiednikami małych rejestratorów analogowych, jak również rozbudowane „kombajny" obsługujące 64 kamery IP, z możliwością rozszerzenia pamięci dyskowej do 54 napędów w technologii RAID5/6 oraz uruchomienia funkcji rozpoznawania twarzy i innych zaawansowanych funkcji analizy obrazu.

Wszystko to jest uzupełnione przez duży wybór kamer IP – obrotowych z opcją dzień/noc, w tym kamer megapikselowych. W przypadku starszych, analogowych modeli należy zastosować koder przetwarzający sygnał analogowy i zapisujący go w formacie MJPEG, MPEG lub H.264, dzięki czemu nie ma konieczności przebudowy całego systemu. Rodzaje i możliwości poszczególnych modeli kamer zostaną szczegółowo zaprezentowane w odrębnym artykule.

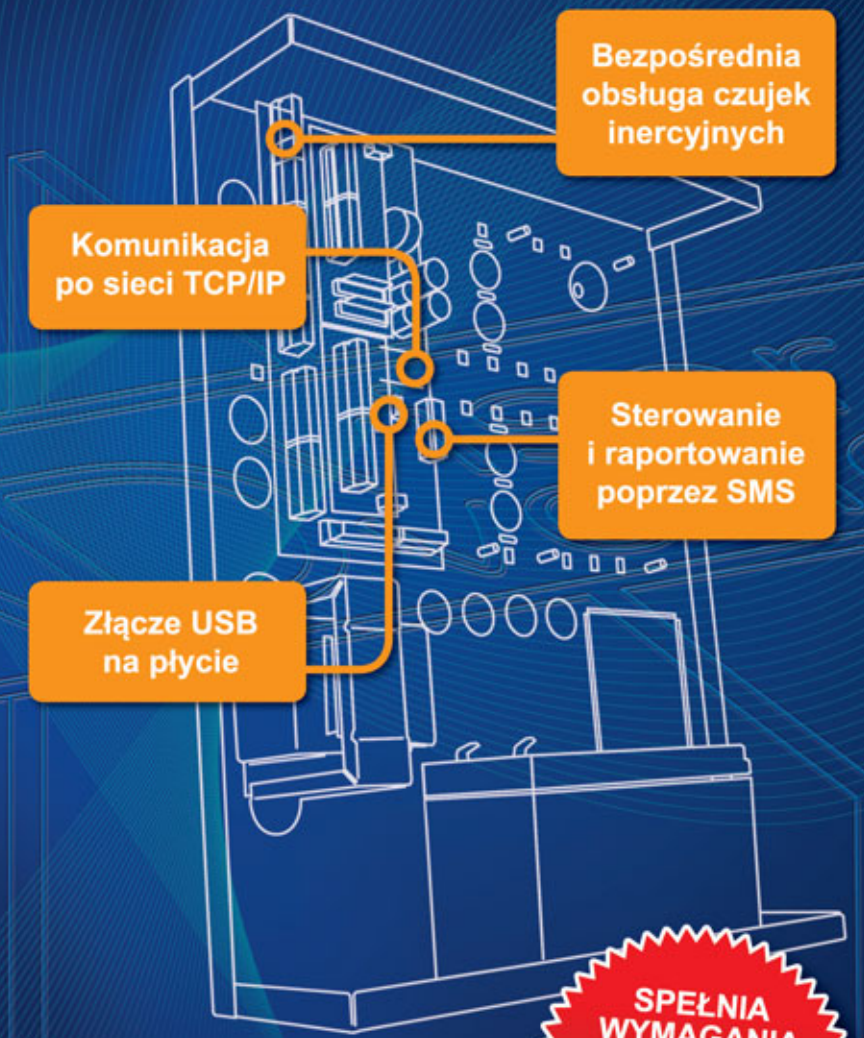
Karol Fietkiewicz
SPS Electronics

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

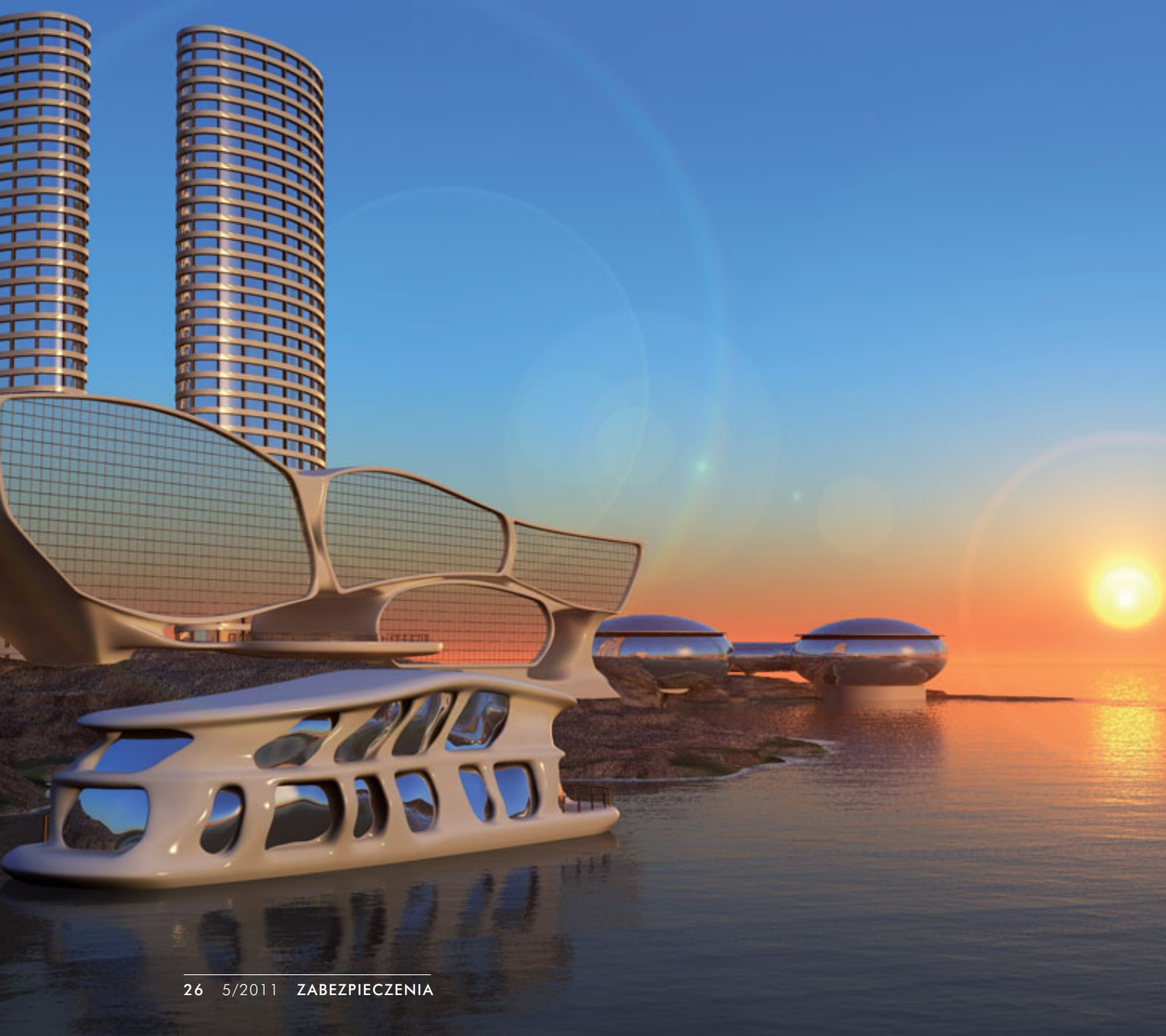
Oddział w Warszawie
Al. Stanów Zjednoczonych 59
04-028 WARSZAWA
tel.: (22) 810 00 03
fax: (22) 810 10 55

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

Bezpieczeństwo dla jutrzejszego świata

James Smith

James Smith jest menedżerem odpowiedzialnym za marketing firmy Samsung Techwin na terenie Europy. W niniejszym artykule James przedstawia w zarysie to, co już udało się osiągnąć w dziedzinie elektronicznych systemów zabezpieczających, i mówi o planach na przyszłość



Czym dziś dysponujemy?

W dzisiejszym świecie systemów zabezpieczeń elektronicznych kamery i urządzenia służące do rejestracji obrazów przechodzą metamorfozy, dzięki którym można tworzyć rozwiązania tanie i wykorzystywać je w projektach, na które przeznaczono bardzo skromny budżet. Skomplikowane funkcje, takie jak na przykład inteligentna analiza treści obrazów, niegdyś realizowana z użyciem specjalistycznego oprogramowania i oddzielnych urządzeń wartych wiele tysięcy funtów, obecnie mogą być bezpłatnie realizowane przez kamery najnowszej generacji. Współczesne systemy kontroli dostępu także oferują wiele użytecznych funkcji. Można je wykorzystać w niskobudżetowych projektach związanych z obsługą tysięcy przejść. Na rynku dostępnych jest wiele czytników, które wykorzystują różne technologie. Mogą umożliwiać analizę kształtu linii papilarnych czy realizować funkcje związane z kontrolą czasu pracy, współpracować z klasycznymi kartami zbliżeniowymi lub zaawansowanymi technologicznie kartami wymagającymi potwierdzenia za pomocą kodu PIN. Biometryczna technologia pozwalająca na analizę kształtu linii papilarnych rozwinęła się na tyle, że w czytnikach pracujących samodzielnie mogą być wzory tysięcy odcisków palców, zaś proces analizy przebiega błyskawicznie.

CCTV znaczy telewizja w obwodzie zamkniętym i przez wiele lat znaczenie to było rzeczywiście adekwatne do realizowanych przez ten system funkcji, jednakże obecnie możliwe jest łączenie poszczególnych systemów ze sobą i tworzenie prywatnych sieci lub wykorzystanie Internetu do zdalnej obserwacji obrazów, odtwarzania nagrań i sterowania urządzeniami wchodzącymi w skład systemów. Wszędzie da się zauważyć wpływ postępu technologicznego na działanie sprzętu elektronicznego powszechnego użytku. Trudno się dziwić, że w związku z tym postępem oczekujemy udoskonalania także urządzeń specjalistycznych. W warunkach domowych można automatycznie nagrywać wybrane audycje telewizyjne za pomocą domowych rejestratorów cyfrowych, możliwy jest odbiór strumieni wizyjnych pochodzących z domowych systemów dozorowych lub z Internetu za pomocą laptopów, można pobierać i zapisywać obrazy w systemach sieciowych, nie mówiąc już o oglądaniu telewizji w standardzie HD. Nikogo to nie dziwi. Nie powinno więc dziwić, że w zakładach pracy i organizacjach publicznych pojawiają się oczekiwania dotyczące wprowadzenia podobnych innowacji do profesjonalnych systemów bezpieczeństwa, tak by udaremniały one działania przestępców.

Dokąd prowadzi postęp technologiczny?

W chwili obecnej kamery dozorowe oraz inne urządzenia stosowane w elektronicznych systemach zabezpieczających realizują funkcje, których zaledwie kilka lat temu nawet nie można było sobie wyobrazić. Jakość obrazu oraz funkcjonowanie systemów uległy znacznej poprawie, jednakże poszczególne urządzenia nadal wykazują pewne ograniczenia. Od tego i od sposobu, w jaki urządzenia te zostaną wykorzystane, zależeć będą przyszłe realne korzyści dla użytkowników końcowych w dziedzinie prewencji, wykrywania i zwalczania rozwijających się, coraz bardziej wyrafinowanych działań związanych z przestępczością zorganizowaną i terroryzmem.

Rewolucja sieciowa

W życiu codziennym jesteśmy coraz bardziej uzależnieni od technologii sieciowych. W zastosowaniach przemysłowych urządzenia i systemy wykorzystujące sieci IP stają się standardowym wyposażeniem ze względu na ich realną zdolność do współpracy i integracji z hostami wykorzystującymi w swym działaniu inne technologie. Właśnie ta elastyczność przejawiająca się w możliwości integracji oraz inteligencja systemów zapewniają realne korzyści w przyszłości.

W świecie jutra użytkownicy będą czerpać korzyści wynikające z licznych zalet systemów bezpieczeństwa opierających swoje działanie na wykorzystaniu sieci IP, przy czym jedne z istotniejszych zalet to możliwość sterowania sprzętem i uzyskiwania dostępu do materiałów wizyjnych z dowolnego punktu w sieci oraz możliwość wykorzystania do tego celu smartfonów lub tabletów. Wielu liczących się producentów, takich jak Samsung, ma istotny udział w programie rozwoju sprzętu sieciowego stanowiącym odpowiedź na zapotrzebowanie rynku zgłaszane w postaci informacji zwrotnej od instalatorów i integratorów systemów. Zważywszy na to, że w przeszłości zmiany na rynku konsumenckim miały istotny wpływ na rozwój technologiczny sprzętu wykorzystywanego w elektronicznych systemach zabezpieczających, obecnie należy skupić się na wprowadzaniu funkcji zaspokajających potrzeby osób odpowiedzialnych za bezpieczeństwo pracowników, majątku oraz dorobku firm, a także osób przebywających na ulicach naszych miast.

Integracja stanowi także czynnik umożliwiający spełnienie tych wymagań użytkowników, które dotyczą możliwie szybkiego zwrotu kosztów inwestycji poniesionych podczas wdrażania rozwiązań podwyższających poziom bezpieczeństwa. W przyszłości możliwa będzie integracja wszystkich części składających się na system bezpieczeństwa, włącznie z zabezpieczeniami antywłamaniowymi, sygnalizacją przeciwpożarową, systemami kontroli dostępu, zabezpieczeniami peryferyjnymi i obwodowymi oraz systemami CCTV, a także współdziałanie tego systemu z systemami automatyki budynkowej, a w dalszej konsekwencji możliwość swobodnego doboru najlepszych produktów pełniących określone role w systemach.

Rozwój systemów wykorzystujących sieć IP i pojawianie się nowych firm oferujących otwarte platformy programowe, integrujące zarówno sprzęt, jak i systemy pochodzące od różnych producentów, zapewni łatwą integrację na poziomie systemowym. Z historycznego punktu widzenia problem stanowiła różnorodność indywidualnych rozwiązań oferowanych przez różnych producentów, opracowujących swoje unikatowe rozwiązania sprzętowe, protokoły i interfejsy graficzne. Z biegiem czasu sytuacja poprawiała się dzięki takim organizacjom jak ONVIF, obligującym producentów do stosowania otwartej filozofii przy podejmowaniu decyzji dotyczących strategii rozwoju.

Dodatkowa wartość wynikająca z możliwości współużytkowania systemów

Możliwość sterowania i monitorowania z dowolnego miejsca w sieci z użyciem zintegrowanych systemów zabezpieczających pozwoli różnym działom organizacji biznesowych na współużytkowanie systemów. Mimo iż bezpieczeństwo nadal pozostanie

podstawowym celem, który będzie skłaniał firmy do inwestowania w systemy zabezpieczające, będziemy mieli do czynienia także z innymi korzyściami, wynikającymi z wdrażania najnowszych rozwiązań. Przykładowo – zastosowanie systemów liczących ludzi może mieć pozytywny wpływ na działanie systemów zabezpieczających. Systemy zabezpieczające mogą służyć nie tylko do ochrony przed przestępczością, ale także do stwierdzania zgodności zachowań pracowników z zasadami bezpieczeństwa i higieny pracy, a także do analizy tras, po jakich poruszają się klienci robiący zakupy w obiektach handlowych. W takich momentach przychodzi na myśl znany film „Raport mniejszości" Stevena Spielberga, należący do gatunku fantastyki naukowej, którego akcja rozgrywa się w 2054 roku. Gdy bohater kreowany przez Toma Cruise'a przechadza się po sklepie z odzieżą męską, jest rozpoznawany przez oprogramowanie analizujące wygląd twarzy ludzkich, sprzężone z systemem CCTV stanowiącym wyposażenie sklepu, i witany przez komunikaty słowne, które zachęcają do przymierzenia marynarek pasujących do spodni, które kupił podczas poprzedniej wizyty w tym sklepie.

Obrazy stanowiące niezbite dowody

Dzięki znakomitej jakości obrazy z kamer megapikselowych pracujących w standardzie HD mają dużą wartość dowodową dla policji. Co więcej, jakość ta sprawia, że można wykorzystać systemy zabezpieczające w innych celach. Zdolność do tworzenia obrazów o rozdzielczości wielokrotnie wyższej niż w przypadku kamer stosowanych dotychczas w systemach CCTV bez wątpienia spowoduje, że kamery megapikselowe pracujące w standardzie HD staną się w najbliższych latach standardowym wyposażeniem systemów zabezpieczających. Podstawowym ograniczeniem są wymagania związane z pasmem sieciowym, niezbędnym podczas transmisji obrazów o rozdzielczości HD poprzez sieć IP. Pojemność urządzeń rejestrujących także musi być zwiększona. Jeśli jednak potrzeba jest matką wynalazków, niewątpliwie w najbliższych latach pojawią się nowe metody kompresji obrazów, które rozwiążą powyższe problemy. Gdy to wreszcie nastąpi, będziemy zastanawiać się, jak to było możliwe, że kiedyś wystarczały nam obrazy pozbawione klarowności typowej dla standardu HD. Alternatywnym rozwiązaniem jest technologia HD-SDI, która umożliwia użytkownikom systemów CCTV wypróbowanie kamer megapikselowych. Ze względu na to, że przed transmisją sygnały wizyjne w standardzie HD-SDI nie są kompresowane i pakietowane, nie występują żadne zniekształcenia obrazu ani przerwy w transmisji. Szczególnie istotny jest fakt, że technologia HD-SDI pozwala na transmisję i rejestrację obrazów w standardzie Full HD (1080p) z wykorzystaniem fragmentów istniejącego okablowania, co może stanowić dodatkowe ułatwienie.

Skalowalne rozwiązania

W najbliższym czasie skuteczność działania wszystkich wspomnianych systemów wzrośnie na tyle, że będzie możliwa realizacja nawet najtrudniejszych zadań związanych z bezpieczeństwem, przez co nasz świat stanie się również bardziej bezpieczny.

Dzięki przechwytywaniu i analizie obrazów pochodzących z kamer zainstalowanych wzdłuż głównych dróg, na obszarach podmiejskich, w parkach i obiektach związanych z transportem publicznym nastąpi podwyższenie poziomu bezpieczeństwa centralnych części dużych aglomeracji miejskich. Zdolność do jednoczesnej detekcji wielu wydarzeń zachodzących równolegle oraz zastosowanie inteligentnej analizy treści obrazów (IVA) pozwala na informowanie operatorów systemów oraz służb ratowniczych o gromadzeniu się tłumu, podejrzanych zachowaniach osób, niewłaściwie zaparkowanych samochodach itp. Prawidłowo zaprogramowany system inteligentnej analizy treści obrazów (IVA) umożliwia automatyczną inicjację serii z góry przygotowanych działań i procesów pozwalających na możliwie szybkie reagowanie na incydenty lub zagrożenia. IVA może być wykorzystana np. do wykrywania wypadków drogowych i automatycznego włączania sygnalizacji ostrzegawczej wzdłuż określonego odcinka drogi, informującej kierowców o zbliżającym się niebezpieczeństwie.

Można już spotkać się z projektami zastosowania automatycznych, zrobotyzowanych strażników patrolujących obszary wymagające wysokiego poziomu bezpieczeństwa lub obszary szczególnie podatne na działania przestępcze. Te roboty, mogące wykrywać i śledzić poruszające się obiekty, są wyposażone w kamery termowizyjne oraz wysokoczułe kamery o dużej rozdzielczości, zdolne do obserwacji obiektów znajdujących się w odległości dochodzącej do trzech kilometrów. Zastosowanie tego typu rozwiązań na obszarach, gdzie poziom zabezpieczenia może być niższy, jest tylko kwestią czasu, zaś użycie kamer megapikselowych pozwoli osobom zarządzającym systemami zabezpieczającymi na bardziej wiarygodne wykorzystanie robotów i wykorzystanie ich do czynności, które dotychczas były realizowane wyłącznie przez ludzi, co pozwoli na redukcję kosztów związanych z zapewnieniem bezpieczeństwa.

Na koniec mamy „Chmurkę", czyli Internet. Wygląda na to, że w przyszłości nie będzie dało się uniknąć wykorzystania tej światowej sieci w kontekście bezpieczeństwa, gdyż umożliwia ona zastosowanie uzasadnionych ekonomicznie i skutecznych metod dostępu, sterowania i monitorowania z użyciem systemów zabezpieczających za pośrednictwem niezależnie działających serwerów, na których mogą być wirtualnie przechowywane zarówno obrazy, jak i dane operacyjne. Oczywiście będzie to wymagało całkowitego zabezpieczenia samej „Chmurki", jednakże użytkownicy płacący jedynie za te usługi, z których korzystają, zauważą wyraźne korzyści finansowe, usprawiedliwiające konieczność poniesienia nakładów inwestycyjnych związanych zarówno ze sprzętem, jak i oprogramowaniem, a nie tylko z urządzeniami krańcowymi, takimi jak kamery.

Niezależnie od tego, czy jesteś właścicielem firmy zajmującej się ochroną małego miasteczka, czy odpowiadasz za bezpieczeństwo w znacznie większej skali, w „jutrzejszym świecie" z pewnością odnotujesz udział takich firm jak Samsung, które konsekwentnie rozwijają technologie i rozwiązania dające Ci stałą przewagę w wyścigu z osobami usiłującymi Cię zaatakować lub okraść.

James Smith
Samsung Techwin Europe
Tłumaczenie: Redakcja

Dual vision, Real time.

ULISSE COMPACT THERMAL

Urządzenie pozycjonujące jest zintegrowanym rozwiązaniem do zastosowania w warunkach ciemności, mgły, deszczu i dymu.

VIDEOTEC

CCTV PRODUCTS

www.videotec.com

Aper IP

długo oczekiwane systemy cyfrowej telewizji dozorowej

Rafał Zieliński

Produkty marki APER pojawiły się na rynku telewizji dozorowej niemal 8 lat temu. W tym czasie zdobyły zaufanie instalatorów i uplasowały się w czołówce najchętniej wybieranych urządzeń do monitoringu wizyjnego. Od początku istnienia tych produktów rozwój technologiczny przyczyniał się do ciągłego ich udoskonalania. Rozdzielczość kamer została zwiększona niemal dwukrotnie, a rejestratory, które początkowo miały bardzo prostą konstrukcję, stały się wielozadaniowymi jednostkami pracującymi w sieci. Nadszedł więc czas na kolejny krok, jakim niewątpliwie są systemy IP

Przez wiele miesięcy uzyskanie pełnej kompatybilności kamer IP marki APER z istniejącymi już na rynku oprogramowaniami rejestrującymi było wyzwaniem. Ponadto producenci oprogramowania dużo chętniej integrowali urządzenia znanych marek światowych, np. SANYO, gdyż zapewniało to potencjalne zyski ze sprzedaży na całym świecie. Integracja małej grupy modeli kamer marki APER wymagała od programistów takiego samego nakładu pracy, a więc była mniej opłacalna. Rozwiązaniem problemu miało być ujednolicenie obsługi kamer przez wprowadzenie standardowego protokołu ONVIF. Dzięki niemu programiści mieli przeprowadzić żmudną integrację tylko raz, a dodawanie kolejnych kamer zgodnych z tym standardem sprowadzałoby się tylko do dopisania ich na liście obsługiwanych urządzeń i aktywowania obsługiwanych funkcji. W praktyce okazało się jednak, że nie sposób objąć jednym standardem tak szeroki zakres funkcji, jakimi dysponują obecnie kamery IP. Należy bowiem pamiętać, że oprócz obrazu i dźwięku standard musi uwzględniać zmianę ustawień kamery, takich jak regulacja przysłony czy określenie czasu ekspozycji, umożliwiać konfigurację dodatkowych funkcji, takich jak BLC, WDR, HLC (które w różnych kamerach są realizowane w inny sposób), zapis obrazów na kartach pamięci, obsługę wejść i wyjść alarmowych, uwzględniać wbudowane opcje detekcji ruchu i wiele innych. Opisane trudności sprawiły, że integracja kamer pochodzących od różnych producentów z oprogramowaniem znanych dostawców stała się problematyczna. Z tego powodu trwają właśnie prace nad wersją 2.0 tego standardu.

APER IP ma umożliwić wyjście z patowej sytuacji. Dzięki bliskiej współpracy m.in. z firmą Alnet udało się uzyskać pełną integrację wszystkich funkcji kamer bez oczekiwania na ukończenie specyfikacji ONVIF 2.0. Dzięki atrakcyjnej cenie urządzeń i darmowemu oprogramowaniu klienckiemu NetStation instalatorzy i projektanci będą mogli tworzyć duże i średnie systemy IP za stosunkowo nieduże pieniądze.

Kamery APER IP podzielone są na dwie grupy. Modele z serii 41xx mają rozdzielczość 1,3 Mpx (1280×1024), natomiast modele serii 42xx uzyskują maksymalną rozdzielczość 2 Mpx (Full HD). W każdej z grup można znaleźć trzy podstawowe typy obudów: klasyczną kompaktową, wandaloodporną kopułkową i tulejową z promiennikiem podczerwieni. Wszystkie modele są zbudowane w oparciu o ten sam 5-megapikselowy przetwornik CMOS w formacie 1/2,5". Dzięki zwiększonej powierzchni światłoczułej przetwornika obrazowego i funkcji dzień/noc z mechanicznie przesuwanym filtrem podczerwieni każda z kamer, pomimo wysokiej rozdzielczości, odznacza się dobrą czułością i dzięki temu bardzo dobrze funkcjonuje w trudnych warunkach oświetleniowych. Z kolei modele z wbudowanym promiennikiem podczerwieni mogą pracować przy całkowitym braku zewnętrznych źródeł światła i nawet w nocy zapewnią wysokiej jakości obraz o rozdzielczości megapikselowej, pozbawiony szumów.

Fot. 1. Oprogramowanie Alnet NetStation

Fot. 2. Mobilna wersja oprogramowania NetStation umożliwia podgląd obrazów z kamer APER IP na dowolnym telefonie komórkowym

Podstawową metodą kompresji w przypadku kamer z serii APER IP jest H.264. W tym trybie oferowane jest 25 kl./s we wszystkich dostępnych rozdzielczościach. Klienci bardzo często wymagają właśnie jak najwyższej rozdzielczości i jak największej płynności obrazu, zapominając o fizycznych ograniczeniach dzisiejszego sprzętu komputerowego. Wyświetlenie 16 obrazów o rozdzielczości Full HD z prędkością 25 kl./s jest dziś niemal niemożliwe i to nawet w przypadku najpotężniejszych stacji serwerowych. Każda z kamer generuje jednak dodatkowo drugi strumień wizyjny o niższej rozdzielczości, który może być kompresowany metodą H.264 lub MJPEG. Dzięki oprogramowaniu Alnet NetStation można w bardzo wygodny sposób przełączać się z jednego strumienia na drugi. Wystarczy jednym kliknięciem wskazać daną kamerę, a oprogramowanie automatycznie wyświetli obraz o najlepszej możliwej do uzyskania jakości. Pozostałe obrazy będą wyświetlane w niższej rozdzielczości, dzięki czemu nawet w dużym systemie, złożonym z kilkudziesięciu kamer, będzie możliwy podgląd 16, 25 czy nawet 32 obrazów jednocześnie, na ekranie podzielonym na części, bez znacznego obciążania stacji klienckiej.

Obecnie obraz to nie wszystko, dlatego każdy model kamery wyposażono w kilka dodatkowych funkcji, które powiększają zakres zastosowań. Z uwagi na ustawę o sposobie rejestracji przebiegu imprez masowych i konieczność rejestracji dźwięku do dyspozycji jest wejście foniczne służące do podłączenia zewnętrznych mikrofonów. Dostępne jest także wyjście foniczne przeznaczone do podłączenia niewielkich głośników, dzięki czemu można zapewnić dwukierunkową komunikację głosową w obiekcie. Jeśli konieczna jest rejestracja pojedynczych obrazów w miejscach, gdzie nie ma rozbudowanej infrastruktury sieciowej, można wykorzystać gniazdo kart microSD i prowadzić lokalną rejestrację obrazów w kamerze.

Dane mogą być później w prosty sposób odczytane na komputerze (są zapisywane w formacie JPEG) po włożeniu karty do czytnika lub połączeniu się z kamerą z wykorzystaniem protokołu FTP – identycznie jak w przypadku połączenia z serwerami plików w internecie. Dzięki temu można przekopiować dane z karty

Fot. 3. Panel zdalnego sterowania obiektywem

na dysk komputera. Połączenie z systemem alarmowym umożliwiają wejścia i wyjścia alarmowe, za pomocą których można wysterować dodatkowe urządzenia podłączone do kamery.

Dzięki dodatkowym przyciskom, dostępnym w oprogramowaniu NetStation, można zdalnie włączyć oświetlenie obiektu, otworzyć drzwi czy załączyć syreny alarmowe.

Znacznym udogodnieniem dla instalatorów jest możliwość zdalnego sterowania obiektywami kamer kopułowych i tulejowych. Funkcja automatycznego ustawiania ostrości, którą mają kamery APER IP, jest taka sama jak w kamerach marki SANYO. Pierścienie obiektywów są połączone z miniaturowymi silniczkami, dzięki czemu cały proces ustawiania optyki może odbywać się zdalnie z poziomu komputera. Co więcej, oprócz sterowania ostrością możliwa jest także regulacja ogniskowej. Jeżeli w trakcie pracy systemu okaże się, że kąt, pod jakim obserwowane jest dane miejsce, jest zbyt szeroki, możliwa będzie zmiana parametrów optycznych obiektywu bez konieczności wchodzenia na drabinę czy nawet wizyty w obiekcie. Po zmianie ogniskowej wystarczy tylko ponownie uruchomić proces automatycznej regulacji ostrości, a kamera sama dobierze optymalne ustawienie obiektywu. Ponadto do dyspozycji instalatora pozostaje serwisowe wyjście BNC z możliwością podłączenia dowolnego monitora pracującego w standardzie PAL.

Kolejnym ułatwieniem oferowanym przez APER IP jest uniwersalny sposób zasilania kamer, który pozwala na wykorzystanie napięć 12 V_{DC}, 24 V_{AC} lub zasilania po skrętce komputerowej metodą PoE.

Projektantów ucieszy fakt, że strumień danych wychodzący z kamer można precyzyjne regulować, przy czym maksymalna wartość wynosi 8 megabitów na sekundę. Można zatem bardzo łatwo oszacować obciążenie sieci oraz wymaganą pojemność dysków potrzebną do osiągnięcia zakładanego czasu rejestracji. W sytuacji odwrotnej, gdy wielkość przestrzeni dyskowej jest już określona, można łatwo ustalić odpowiednią wielkość strumienia wyjściowego z kamer, aby dyski nie uległy przepełnieniu szybciej niż wymaga tego inwestor.

Informatykom przypadnie do gustu obsługa protokołu RTSP i współpraca z takimi odtwarzaczami jak VLC Media Player. W przypadku konferencji można w bardzo prosty sposób zapewnić wyświetlanie obrazu na wielu monitorach, a dzięki obsłudze multicastu wykluczona zostanie konieczność inwestowania w bardzo szybką sieć LAN.

Wysokiej jakości kamery znanej na polskim rynku marki APER w połączeniu z profesjonalnym oprogramowaniem NetStation, które w pełni wykorzystuje ich możliwości, powinny przyczynić się do dalszej ekspansji systemów IP na rynku telewizji dozorowej.

Rafał Zieliński
SPS Electronics

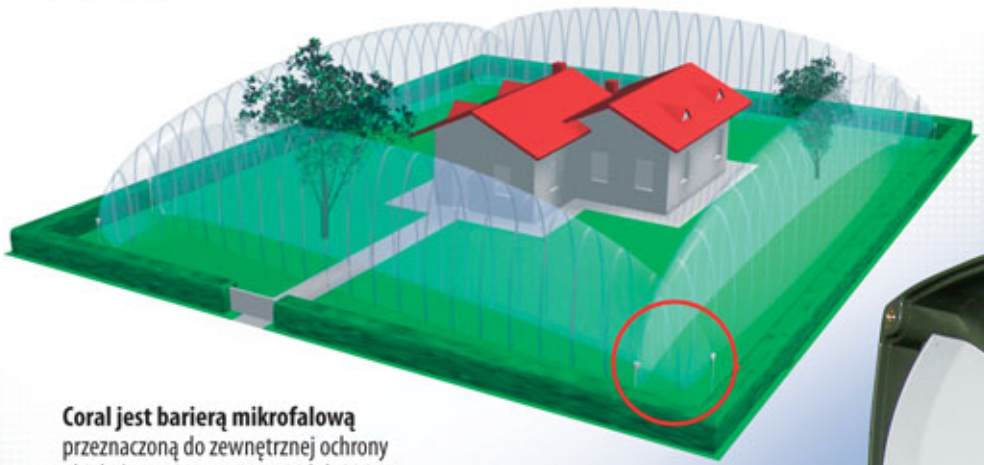
firma ATLine®

www.atline.pl

ZSJZ

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

Wpływ firm ochrony na rozwój systemów alarmowych

Daniel Kamiński

Polski rynek zabezpieczeń zaczyna osiągać dojrzałość. Wprawdzie nadal rozwija się, ale zmieniają się mechanizmy na nim panujące. Zauważyć można działania wcześniej w Polsce mało znane, takie jak: akwizycje funduszy inwestycyjnych, wejścia firm ochrony na giełdę, konsolidacje rynku poprzez przejęcia dużych i średnich firm. W efekcie tych działań główni gracze z każdym miesiącem zwiększają udziały w rynku, a usługi monitorowania osiągają najniższy w historii pułap cenowy. To powoduje pojawienie się nowych wyzwań związanych z redukcją kosztów, takich jak: zmniejszanie kosztów serwisu i instalacji, skrócenie czasu reakcji serwisowej, eliminacja interwencji spowodowanych fałszywymi alarmami. Jednocześnie firmy uświadamiają sobie, że muszą zwiększać swój udział w rynku, oferować usługi dodane i podnosić abonamenty. Jak to osiągnąć? Czy rynek jest na to gotowy? Jakie doświadczenia miały firmy z innych krajów, w których podobne mechanizmy rynkowe pojawiły się wcześniej? Czy na rynku są dostępne narzędzia pozwalające na zmianę podejścia?

Fot. 1. Przykład stanowiska do zdalnego wsparcia technicznego (fot. Visonic)

Wprowadzenie

Dla wielu osób może to być zaskakujące, ale sposób działania systemu alarmowego nie zmienił się od ponad 130 lat. Głównymi składowymi systemu są nadal centrala alarmowa, elementy wykrywające intruza, elementy sterujące systemem oraz elementy sygnalizujące stany alarmowe.

Mimo tak długiej tradycji jest mało informacji o nich w prasie branżowej i trudno napotkać je na targach. Możliwe, że powodem mniejszego zainteresowania systemami alarmowymi są inne systemy bezpieczeństwa, które, spełniając swoje zadania, mogą być jednocześnie substytutem systemu alarmowego. Wszak sieciowe systemy kontroli dostępu, wykorzystujące do identyfikacji np. biometryczne cechy osób, są dużo bardziej funkcjonalne i zapewniają wyższy poziom bezpieczeństwa, podobnie jak systemy telewizji dozorowej, które wykorzystują analizę obrazu do kontroli obszarów za pomocą wirtualnych płotów czy też kontrolowania obecności przedmiotów (np. obrazów w muzeum). Są one bardziej elastyczne w zastosowaniu od najbardziej zaawansowanych systemów alarmowych.

Systemy alarmowe są natomiast bardzo popularne wśród inwestorów. Trudno dziś znaleźć nowo budowany obiekt handlowy, biuro czy dom, których projekty nie obejmowałyby instalacji alarmowej – obok instalacji elektrycznej, telefonicznej czy domofonowej. Systemy alarmowe stały się standardem dzięki prostocie oraz temu, że przez lata zostały tak udoskonalone, iż w zapomnienie odchodzą „wyjące" alarmy sprzed lat. Ponadto bardzo ważną cechą systemów alarmowych jest ich niski koszt. Są po prostu dużo tańsze od innych systemów bezpieczeństwa.

Dodatkowym bodźcem powodującym wzrost popularności systemów alarmowych wśród inwestorów są działania firm ochrony, które oferują klientom systemy z kredytowaniem. W takim przypadku inwestor nie musi od razu ponosić całego kosztu systemu alarmowego, gdyż jest on rozkładany na 36 rat i dodawany do abonamentu za usługi monitorowania. Rozwiązanie jest atrakcyjne dla obu stron – inwestor bez nakładów finansowych wchodzi w posiadanie systemu alarmowego wraz z usługą reakcji, a firma świadcząca usługi monitorowania ma lojalnego klienta i stały przychód przez kilka kolejnych lat.

Możliwe, że ten ostatni aspekt spowodował, iż systemy alarmowe stały się synonimem monitorowania oferowanego przez agencje ochrony (podobnie jak kiedyś cekolowanie stało się synonimem nakładania gładzi szpachlowych) i praktycznie są przez nie obecnie reklamowane. Stało się tak, ponieważ agencje ochrony wyspecjalizowały się w oferowaniu „popularnych" systemów alarmowych i proponują je masowo wraz z usługami. Dzięki dużym obrotom agencje ochrony uzyskują preferencyjne ceny u producentów zabezpieczeń, a specjalizacja i duży wolumen zleceń obniżają koszty realizacji usług. W efekcie mogą oferować swoje rozwiązania po cenach nieosiągalnych dla innych firm.

Wielkość rynku monitorowania systemów alarmowych

Rynek usług monitorowania alarmów ulega nieustannym przeobrażeniom. Dziesięć lat temu usługa monitorowania dotyczyła tylko obiektów stałych; nie można było jednoznacznie wskazać lidera. Pięć lat temu monitorowanych było około 500 tys. obiektów, z czego około 200 tys. przez dwudziestu głównych graczy*.

W ciągu ostatnich 5–7 lat liczba głównych graczy zmniejszyła się do dziesięciu. Było to związane z konsolidacją rynku oraz efektem skali. Jako ciekawostkę należy uznać fakt, że do czołówki weszły firmy wyspecjalizowane w monitorowaniu obiektów ruchomych.

Dziś na rynku usług monitorowania alarmów wyróżnić można trzy grupy graczy**:

– dwie firmy posiadające ponad 50 tys. przyłączeń (razem około 300 tys. przyłączeń),
– osiem firm posiadających ponad 10 tys. przyłączeń (razem ok. 150 tys. przyłączeń),
– pozostałe firmy (razem ok. 200 tys. przyłączeń).

Łatwo zauważyć, że wśród głównych graczy wyróżnia się pierwsza dwójka, która posiada tak dużą liczbę obsługiwanych przyłączeń, że można tę grupę porównać do alternatywnych/wirtualnych operatorów telekomunikacyjnych. Przy takim porównaniu można zastosować niektóre mechanizmy występujące w segmentach obsługujących klienta masowego do prognozowania rozwoju rynku w kolejnych pięciu latach.

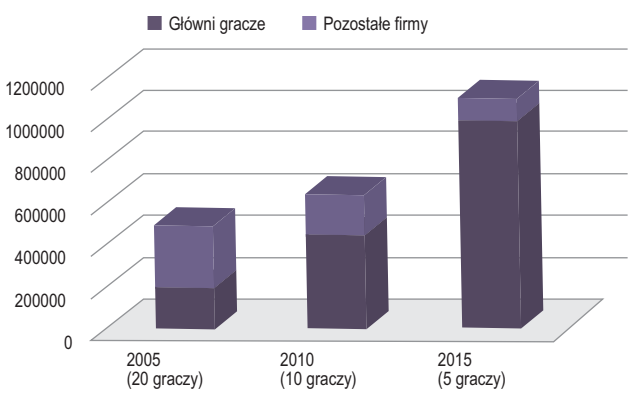
W ostatnich latach rynek monitorowania wzrastał o 7% rocznie. Główną siłą napędową były firmy z pierwszej dziesiątki, w przypadku których przyrost przyłączeń wynosił około 18%, częściowo kosztem pozostałych graczy. Firmy te stosowały dwa modele sprzedaży usług – sprzedaż własną (tzw. wzrost organiczny) i akwizycję kontraktów, czyli skupowanie firm w celu zdobycia jak największej liczby umów.

Na podstawie obserwacji rynków monitorowania w Europie oraz wspomnianego rynku usług telekomunikacyjnych można założyć, że w kolejnych pięciu latach liczba głównych graczy zmniejszy się do pięciu, a liczba monitorowanych przez nich obiektów może wzrosnąć do 1 000 000 i będzie stanowić nawet 90-procentowy udział całego rynku monitorowania alarmów***. Bardzo prawdopodobne jest to, że wśród modeli sprzedaży dużą rolę odegra sprzedaż elektroniczna.

**) Szacunki autora*

***) Założenia autora*

****) Prognozy autora*



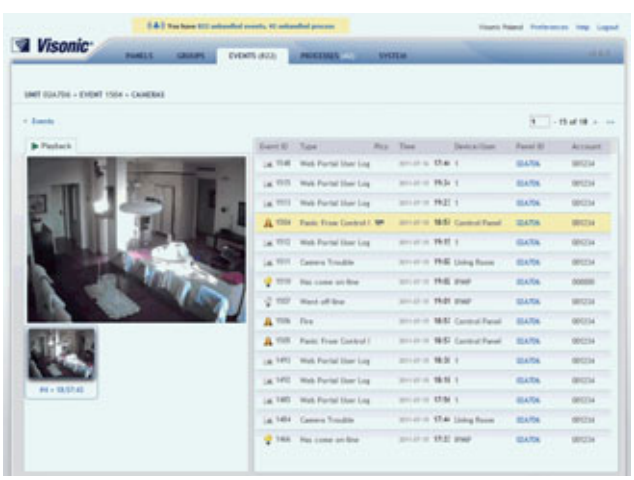
Rys. 1. Prognoza wielkości rynku monitorowania alarmów

Dziś nie wiadomo, kto będzie liderem na rynku za 5–10 lat. Można spodziewać się kolejnych niespodzianek, np. nowych graczy z zagranicy, nowych firm wyspecjalizowanych w monitorowaniu usług, które są dziś mniej popularne (monitoring wizyjny, opieka nad starszymi, odczyty stanów liczników itp.). Wiadomo natomiast, że rynek ochrony jest dojrzały, stabilny i nadal ma tendencję do wzrostu.

Czy firmy powielające obecne metody rozwoju oraz pielęgnujące standardowe usługi pozostaną w grze? Obserwując rynek europejski, na którym branża ochrony jest obecna od ponad 100 lat, można zauważyć, że mimo podobieństw głównych kierunków rozwoju świadczone usługi znacznie się różnią. Poza granicami Polski przy pozyskiwaniu klientów akcentuje się usługi dodane, a podczas realizacji usług stawia się na automatyzację i zdalny dostęp, czyli na narzędzia pozwalające zredukować koszty. Podobne trendy widoczne są na naszym rynku usług telekomunikacyjnych. Na tej podstawie można założyć, że również w naszym kraju odniosą sukces firmy, które poprzez obniżenie kosztów oraz uatrakcyjnienie usług zwiększą efektywność tak, aby osiągnąć efekt skali.

Wyzwania dla firm ochrony związane z systemami alarmowymi

Konsekwencją wyspecjalizowania się firm ochrony w dostarczaniu systemów alarmowych jest spora konkurencja. Wprawdzie zarejestrowano kilka tysięcy firm ochrony, ale tylko kilkadziesiąt z nich aktywnie uczestniczy w zmaganiach na rynku usług związanych z systemami alarmowymi. Mają one rozbudowane działy techniczne, w których pracują instalatorzy realizujący usługi na terenie całego kraju, całodobowy serwis oraz całodobowe telefoniczne wsparcie techniczne. Są to spore inwestycje wymagane do tego, aby obsłużyć obecną pulę klientów. Niestety przy obecnym modelu biznesowym to nie wystarcza, by realizować usługi na oczekiwanym poziomie, gdyż często zdarza się, że klienci czekają na realizację zamówionych usług. Biorąc pod uwagę potrzebę wzrostu sprzedaży, należy zastanowić się nad zmianą modelu biznesowego i rozpocząć stosowanie systemów wspierających zdalną diagnostykę i administrowanie.



Fot. 2. Przykład oprogramowania serwera komunikacyjnego (fot. Visonic)

Instalacje

Obecnie czas instalacji prostego systemu alarmowego zajmuje około dwóch dni. Instalacja realizowana jest w dwóch etapach – jeden dzień na instalację okablowania (przed tynkowaniem) oraz drugi dzień (po zakończeniu prac budowlanych) na weryfikację okablowania po pracach budowlanych, montaż urządzeń, programowanie centrali, sprawdzenie działania systemu, podłączenie i weryfikację monitorowania oraz szkolenie użytkowników. W obecnym modelu biznesowym zwiększenie sprzedaży skutkuje wydłużeniem się czasu oczekiwania na instalację lub zwiększeniem zatrudnienia w dziale technicznym.

W Anglii, Belgii czy Holandii zakłada się, że instalator zamontuje dziennie min. pięć systemów alarmowych. Praktycznie jest to dziesięciokrotnie większa wydajność niż u nas, niemożliwa do osiągnięcia przy standardowym podejściu. Stosuje się tam systemy bezprzewodowe zamiast przewodowych. W ten sposób eliminuje się problem związany z etapowością instalacji i rezygnuje się z okablowania, co daje oszczędność ze względu na mniejsze zużycie materiałów i niższe koszty instalacji. W efekcie różnica kosztów systemów bezprzewodowych i przewodowych jest niwelowana. Koszt poniesiony przez klienta jest taki sam, ale dla firmy monitorującej różnica jest znacząca. Stosuje się zestawy wstępnie zaprogramowane. Rolą instalatora jest zamontowanie urządzeń i przeszkolenie klienta. Uruchomienie i weryfikacja monitorowania są realizowane z poziomu stacji monitorowania. Wpływa to znacznie na czas instalacji oraz jakość usługi. Likwiduje się w ten sposób wiele późniejszych problemów serwisowych związanych z jakością montażu (więcej o tym w podrozdziale *Wsparcie techniczne*). Stosowane bezprzewodowe systemy alarmowe mają łączność ze stacją monitorowania za pośrednictwem serwera komunikacyjnego. Pozwala to na automatyczne zdalne zapisywanie ustawień oraz informacji o zainstalowanych elementach systemu. W efekcie zwalnia się czas instalatora, dotychczas poświęcany na przekazywanie stacji monitorowania opisów linii oraz na archiwizację konfiguracji systemu.

Serwis

Przyjęcie zgłoszenia serwisowego stanowi niekiedy trudne zadanie. Dzwoniący klient z reguły nie pamięta, jaki system ma zainstalowany. Na ogół nie umie zdefiniować usterki i mówi tylko, że system nie działa. Część firm stosuje w takim przypadku skrypty (zestawy pytań), które pozwalają przybliżyć istotę problemu na tyle, by właściwie przygotować zlecenie dla serwisanta w celu wykonania przez niego odpowiedniego zadania (restart systemu, wymiana akumulatora, przeniesienie czujnika, zmiana kodów itp.). Następnie serwisant udaje się do obiektu, aby zdiagnozować usterkę i usunąć jej przyczynę. Niestety często okazuje się, że reklamowany przez klienta element działa, a uszkodzeniu uległ moduł, który nie był objęty zgłoszeniem, i serwisant nie posiada przy sobie potrzebnego elementu. Konieczny jest powrót do magazynu i pobranie właściwego modułu na wymianę. Taka sytuacja generuje dodatkowe koszty, przedłuża okres niesprawności systemu i podważa zaufanie do firmy świadczącej usługi serwisowe.

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

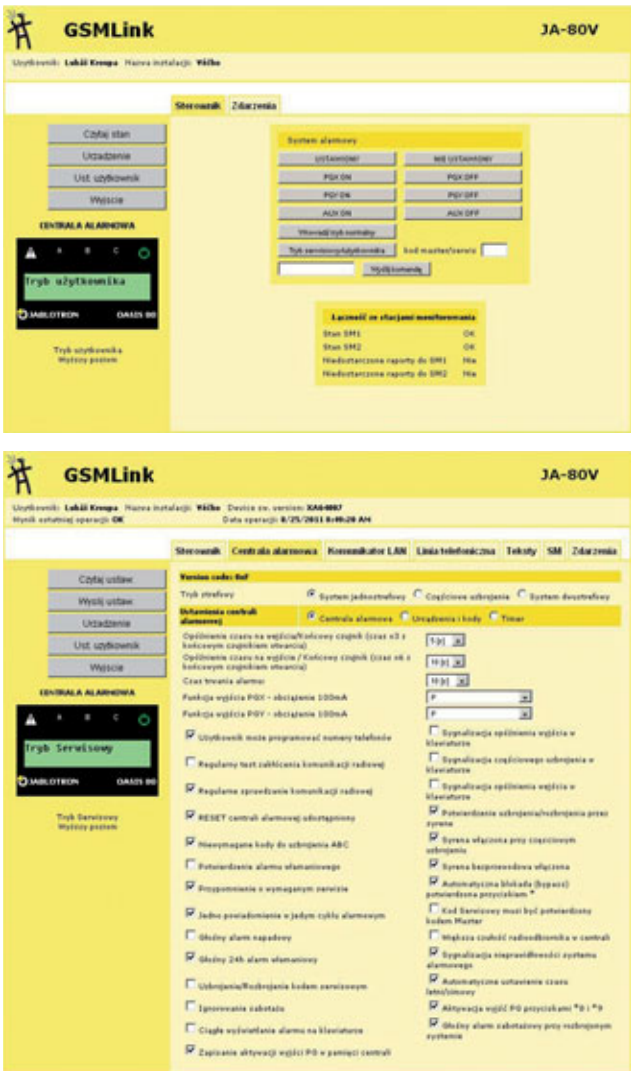
NVIP-DN6137SD

- 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



Fot. 3. Przykład aplikacji do zdalnej konfiguracji systemów alarmowych (fot. Jablotron)

Korzystanie z narzędzi oferowanych wraz ze współczesnymi systemami alarmowymi pozwala wyeliminować większość z wymienionych problemów. Osoba przyjmująca zgłoszenie serwisowe może w trakcie rozmowy z klientem połączyć się zdalnie z monitorowanym obiektem i wykonać diagnostykę systemu. W ten sposób sprawdzi, które elementy systemu są uruchomione i jakie zdarzenia są w historii. Może sprawdzić stan baterii oraz poziomy sygnałów radiowych w urządzeniach bezprzewodowych i w efekcie ustalić rodzaj i przyczynę usterki bez wizyty serwisanta w obiekcie. Zlecenie serwisowe wygenerowane po takim połączeniu będzie zawierało opis zainstalowanego systemu oraz wskazywało rodzaj usterki. Serwisant będzie mógł usunąć usterkę w trakcie jednej wizyty, firma zaoszczędzi czas serwisanta i zmniejszy koszty dojazdu, a klient będzie zadowolony z profesjonalnej obsługi.

Może być jeszcze korzystniej, gdy zadanie dotyczy czynności administracyjnych związanych z wydłużeniem czasu na wejście (np. w okresie zimowym), zablokowaniem uszkodzonej linii dozorowej generującej fałszywe alarmy czy z awaryjną zmianą kodów. W takim przypadku czas oczekiwania na serwisanta można ograniczyć do minimum, gdyż wymienione czynności mogą być wykonane zdalnie w trakcie rozmowy z klientem po zweryfikowaniu jego tożsamości.

Wykorzystywanie zdalnego dostępu znacząco wpływa na efektywność serwisu. Dzięki niemu można wyeliminować niepotrzebne wyjazdy i uniknąć związanej z nimi frustracji pracowników, skraca się czas reakcji, a serwisanci koncentrują się tylko na przypadkach wymagających fizycznej obecności.

Wsparcie techniczne

W związku z tym, że systemy alarmowe muszą być sprawne całą dobę, w firmach ochrony powstają komórki wsparcia technicznego. Z reguły znajdują się one przy stacjach monitorowania i ich rola polega na analizie informacji technicznych z obiektów (problemy z zasilaniem i komunikacją, błędy opisu wejść central i nadajników) oraz obsłudze instalatorów i serwisantów. Dotyczy to działań związanych z uruchomieniami systemów alarmowych, serwisów oraz konserwacji.

Zdalny dostęp do urządzeń umożliwia personelowi zajmującemu się wsparciem technicznym sprawdzenie poprawności pracy systemu alarmowego i dokonanie niezbędnych działań w celu przywrócenia mu sprawności. Jeśli te działania nie dają dobrego rezultatu, generowane jest zlecenie serwisowe, o którym klient jest informowany. Proaktywne działania są szczególnie popularne wśród tych klientów (przede wszystkim z grupy tzw. VIP), którzy przykładają dużą wagę do sprawności systemu alarmowego. Informacja od firmy ochrony o tym, że wkrótce rozładuje się akumulator, i propozycja jego wymiany jest potwierdzeniem tego, że system alarmowy jest pod stałą kontrolą – w przeciwieństwie do sytuacji, gdy klient zauważa awarię akumulatora w momencie załączania systemu w dozór tuż przed wyjazdem na urlop.

Funkcja zdalnego dostępu pozwala też zmienić sposób uruchomień, realizacji usług serwisowych i konserwacji. Dziś firmy ochrony nie zawsze potrafią przeprowadzić weryfikację realizacji zleceń wykonywanych przez służby techniczne. Obowiązek sprawdzenia poprawności działania systemu spoczywa na barkach instalatora i serwisanta. Po sprawdzeniu sporządzany jest protokół, który jest podpisywany przez klienta. Jeśli firma ma słabiej wyszkolonych pracowników technicznych lub korzysta z podwykonawców, którzy nie przejmują się „papierkowymi" sprawami, zaczynają się problemy. W takim przypadku personel wsparcia technicznego może zdalnie sprawdzić, czy wszystkie elementy systemu są sprawne, czy opisy linii są zgodne z kartą zgłoszenia, czy w systemie zostały naruszone wszystkie linie w celu wygenerowania alarmów itp. Po całej weryfikacji można zmienić kod instalatora, aby mieć pewność, że nikt nieuprawniony nie będzie miał dostępu do systemu.

Oczekiwania klientów wobec systemów alarmowych

Głównym zagrożeniem dla firm świadczących usługi jest strach klientów przed obsługą systemów alarmowych. Klienci obawiają się, że nie dadzą sobie rady, bo system jest zbyt skomplikowany, lub boją się konsekwencji błędnej obsługi, czyli zadziałania alarmu oraz kosztów interwencji firm ochrony. W efekcie tacy klienci przestają używać systemu, a w skrajnych przypadkach rozwiązują umowy dotyczące świadczenia usług ochrony. Firmy ochrony operujące poza

Polską określają nawet współczynnik procentowy liczby rozwiązań umów DISCO mówiący o poziomie realizacji usługi. Zakłada się tam, że standardowy poziom rotacji nie przekracza 7% rocznie. Dodatkowo firmy te wypracowały mechanizmy kontroli polegające między innymi na weryfikowaniu, czy klienci korzystają z systemów, gdyż dodatkowa sprzedaż (rozbudowy) stanowi tam nawet 40% wartości sprzedaży nowych umów.

Kolejnym zagrożeniem dla firm ochrony są klienci, którzy akceptują tylko najniższe abonamenty. Okazuje się, że nie można liczyć na ich lojalność. Wśród tych klientów jest największy odsetek rozwiązań umów oraz największe problemy z windykacją, gdyż zwykle owi klienci nie płacą.

W odpowiedzi na te zagrożenia firmy ochrony rozpoczęły poszukiwania systemów na tyle prostych i atrakcyjnych, aby klienci nie bali się ich. Zaczęły też tworzyć usługi, które uatrakcyjniały te systemy, a klientów przywiązywały do konkretnej firmy. Poniżej zostaną omówione współczesne możliwości systemów alarmowych, dzięki którym można uruchomić usługi pozwalające na zwiększenie zainteresowania klientów, a tym samym na uzyskanie wzrostu sprzedaży oraz ograniczenie kosztów realizacji usług.

Sterowanie systemem alarmowym

Obecnie głównym narzędziem służącym do sterowania systemem alarmowym jest klawiatura. Mimo swej pozornej prostoty jest ona często udręką dla klientów. Wymaga zapamiętania kodu, znajomości opisów klawiszy funkcyjnych oraz skrótów klawiszowych, a często także obsługi menu pojawiającego się na wyświetlaczu. Duża część klientów rezygnuje z korzystania z klawiatury, wybierając piloty radiowe lub karty zbliżeniowe czy tagi RFID.

Dzisiejsze piloty do sterowania systemami wykorzystują szyfrowaną komunikację i modulacje ze „skaczącymi" częstotliwościami. Nie da się ich w prosty sposób odczytać, więc odpada wiele zastrzeżeń i obaw, które były istotnym zagrożeniem kilka lat temu. Są małe i poręczne, więc można je mieć przy sobie. Jeśli są dwukierunkowe, pokazują również informację o stanie systemu (uzbrojony/rozbrojony). Ponadto umożliwiają sterowanie innymi systemami, np. bramą garażową czy zewnętrznym oświetleniem.

Fot. 4. Przykład sterowania systemem przez internet (fot. Juwentus)

Młodsze osoby upodobały sobie korzystanie z kart dostępu. Karty te, często wykorzystywane w firmach do kontroli czasu pracy czy dostępu do pomieszczeń, mogą służyć również do sterowania systemem alarmowym po przypisaniu ich do niego. Podobnie jest z dostępnymi na rynku tagami RFID. Oferowane są w wielu kształtach i kolorach, a dzięki niewielkiemu rozmiarowi stanowią atrakcyjne breloczki do kluczy. Mogą być zawsze pod ręką, gdy trzeba załączyć lub wyłączyć system z dozoru. Zaletą tagu jest to, że osoba postronna nie podejrzy kodu dostępu, a w przypadku jego utraty można go łatwo dezaktywować i usunąć z pamięci systemu.

Kolejną grupą osób, która ma indywidualne potrzeby, są osoby lubiące zaawansowane technologie. W ich przypadku sterowanie systemem musi być realizowane z poziomu telefonu komórkowego, smartfona oraz strony internetowej. Wymaga to podłączenia systemu alarmowego do Internetu (zwykle poprzez wbudowany nadajnik GPRS). W przypadku telefonu użytkownik może załączać/wyłączać system na trzy sposoby: dzwoniąc do systemu i sterując nim z klawiatury, wysyłając do systemu odpowiedni SMS lub korzystając z aplikacji zainstalowanej w telefonie. Ta ostatnia opcja jest najbardziej rozwojowa, szczególnie w przypadku smartfonów z systemem Android i iOS (Apple).

Strona internetowa jest odpowiednikiem aplikacji na smartfona i umożliwia zdalny dostęp do systemu. Jest to szczególnie ważne w sytuacjach awaryjnych, gdy chcemy wyłączyć alarm, zmienić kod lub nadać nowy dla sprzątaczki czy opiekunki dla dziecka, i bardzo przydatne, gdy chcemy zablokować czujnik generujący fałszywe alarmy lub przejrzeć historię.

Dwukierunkowa komunikacja

Współczesny system alarmowy potwierdza komendy głosowo, jest wyposażony w elektroniczną sekretarkę, ma wbudowane interkomy i w razie problemów umożliwia połączenie się z serwisantem lub ze stacją monitorowania. Dodatkowo wyposażony jest w mikrofon i kamerę, które pozwalają na zdalną obserwację obiektu i komunikację z domownikami.

Komendy głosowe mają za zadanie odrobinę „uczłowieczyć" system. Dla osób ze słabszym wzrokiem oraz dzieci, które nie umieją czytać, jest to duże ułatwienie obsługi systemu eliminujące wiele fałszywych alarmów. Opcja nagrywania wiadomości ma natomiast zachęcić domowników do pozostawiania sobie ważnych wiadomości, które są automatycznie odtwarzane po wyłączeniu systemu z dozoru, więc nie można ich przeoczyć.

Opcją zachęcającą klienta do korzystania z usług danej firmy jest możliwość błyskawicznego i bezpłatnego połączenia się ze stacją monitorowania za pośrednictwem wbudowanego modułu GSM. Firmie ochrony system umożliwia dodatkowo połączenie się z obiektem w przypadku alarmu. Obie opcje

Fot. 5. Przykład komunikacji z systemem przez telefon (fot. EL)

mają na celu zmniejszenie liczby fałszywych alarmów. System może też mieć przypisany numer telefonu do opiekującego się nim serwisanta. W wielu dużych domach interkomy będą wykorzystywane również do komunikowania się z domownikami oraz sterowania domofonem.

Systemy alarmowe są coraz częściej wyposażane w aparaty fotograficzne wbudowane w czujki (PIR Camera). Głównym zadaniem takich rozwiązań jest weryfikacja wizyjna alarmów. Na jej podstawie zarówno stacja monitorowania, jak i klient mogą klasyfikować zdarzenie jako alarm prawdziwy albo fałszywy. Ponadto, w razie potrzeby, klient może zdalnie sprawdzić, czy w chronionym obiekcie wszystko jest w porządku.

Powiadomienia

Kolejną ważną dla klientów funkcją są powiadomienia dotyczące chronionego obiektu. System alarmowy może wysyłać bezpośrednio lub przez współpracujący serwer informacje o alarmach, usterkach oraz zdarzeniach zdefiniowanych przez klienta. Powiadomienia mogą być głosowe albo w formie SMS-a lub e-maila. Rolą tych powiadomień jest automatyczne dostarczenie aktualnych informacji o stanie obiektu. Dzięki nim jest mniej połączeń telefonicznych z klientami zadającymi pytania typu: „Czy mój system się uzbroił?”, „Czy moje dziecko wróciło do domu?”. Wprowadzenie usługi powiadomień pozwala firmom ochrony obsługiwać więcej klientów bez potrzeby zwiększenia liczby pracowników.

Nowe spojrzenie na usługi związane z systemami alarmowymi

W firmach ochrony oferujących systemy alarmowe dużą część obrotu stanowią przychody jednorazowe, uzyskiwane ze sprzedaży urządzeń wchodzących w skład systemu alarmowego oraz instalacji. Dużo istotniejsze są jednak obroty związane z przychodami odnawialnymi, które w Polsce są uzyskiwane głównie dzięki monitorowaniu z interwencjami, serwisowi oraz konserwacji.

Przychody jednorazowe są zawsze mile widziane, ale to dzięki przychodom odnawialnym uzyskiwana jest stabilizacja pozwalająca na bezpieczne inwestycje. Warto więc włożyć trochę więcej wysiłku i pozyskać jak najwięcej kilkuletnich umów terminowych. Dobrym wzorcem do naśladowania są w tym zakresie firmy telekomunikacyjne oraz dostawcy telewizji satelitarnej.

Mając to na uwadze, należy zastanowić się, jakie rodzaje usług można wykorzystać w ochronie. Pomocne może być zapoznanie się z ofertami firm ochrony z innych krajów. Główna różnica w stosunku do obecnie stosowanego modelu polega na tym, że zarówno firmy telekomunikacyjne, jak i zagraniczne firmy ochrony wprowadziły podział na usługi podstawowe oraz usługi dodane. Usługi podstawowe mają zachęcić klienta do podpisania umowy. Usługa podstawowa jest tania, ale jej zakres jest minimalny, dlatego klient jest zachęcany do skorzystania z usług dodanych, których koszt jest uzasadniony dodatkową, unikalną funkcjonalnością.

W przypadku systemów alarmowych do podstawowych usług odnawialnych można zaliczyć wymienione wcześniej monitorowanie i konserwacje, natomiast do dodanych usług odnawialnych zaliczamy takie funkcje, jak automatyczne powiadomienia e-mail i SMS, weryfikacje akustyczne i wizyjne, zdalny dostęp do systemu poprzez smartfony i strony WWW, zdalna diagnostyka.

Podsumowanie

Pomimo tego, że sposób pracy systemu alarmowego nie zmienił się od ponad wieku, w ostatnich latach dużym zmianom uległ sposób jego wykorzystania. Obecnie uwzględnia się nie tylko potrzeby klientów, ale również interesy firm ochrony świadczących usługi związane z monitorowaniem systemów alarmowych.

Czy opisane usługi mogą stać się standardem w Polsce? Trudno odruchowo odpowiedzieć, że tak, wszak wszystkie opisane funkcje są dostępne od kilku lat, a mimo to nie były wykorzystywane. Jednak biorąc pod uwagę potencjał rynku oraz korzyści wypływające z tych usług, mogę śmiało prognozować, że firmy, które zainwestują w nowe usługi dodane, w krótkim czasie osiągną znaczącą przewagę.

Daniel Kamiński
OCHRONA JUWENTUS

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Megapikselowe kamery IP dzień/noc

Doskonała jakość obrazu, duża funkcjonalność!

Kamera standardowa

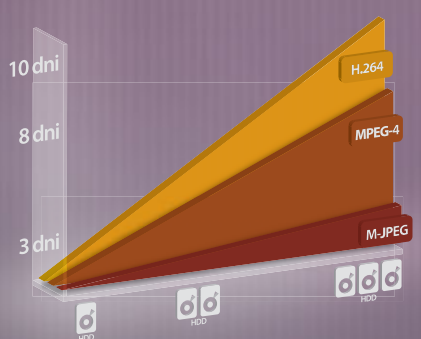
Megapikselowe kamery IP marki NOVUS

Rozdzielczość megapikselowa 2.0Mpx

Pozwala na zapis nagrania w bardzo dobrej jakości, co umożliwia przybliżanie fragmentów obrazu i odczytanie najmniejszych szczegółów. Kamery o rozdzielczości 2.0Mpx mogą obserwować obszar do 4.6x większy niż kamery o standardowej rozdzielczości 720x576. Można zatem przyjąć, że w niektórych sytuacjach, jedna kamera z przetwornikiem 2.0Mpx odpowiada pięciu kamerom standardowym.

Praca w trybie trójstrumieniowym

Pozwala dopasować jakość i objętość transmitowanych danych do indywidualnych potrzeb użytkownika. Przykładowa konfiguracja strumieni wideo: ▪ pierwszy strumień wysokiej jakości i rozdzielczości do lokalnego monitoringu i rejestracji ▪ drugi strumień do podglądu obrazu przez internet ▪ trzeci strumień do transmisji przez sieć telefonii komórkowej (podgląd obrazu na telefonach i innych urządzeniach przenośnych).



Kompresja H.264

Zastosowanie najnowszej wydajniejszej kompresji H.264 pozwala, bez utraty jakości, zmniejszyć wielkość zapisywanego obrazu nawet o 80% w stosunku do kompresji M-JPEG i o ok. 20% w stosunku do MPEG-4. Dzięki temu, na dyskach o tej samej pojemności, można archiwizować znacznie większą ilość materiału.

T SERIA

NMS Compatible

ALNET Compatible

Oprogramowanie NMS do monitoringu wizyjnego IP w komplecie!

▪ Mechaniczny filtr podczerwieni ▪ Maks. rozdzielczość przetwarzania wideo 1600 x 1200 (UXGA) ▪ 3 strefy prywatności ▪ Detekcja ruchu ▪ 1 wejście i 1 wyjście alarmowe ▪ Kontrola połączenia sieciowego oraz funkcja sprawdzania adresu IP ▪ Wparcie dla urządzeń mobilnych - strumień 3GPP ▪ Możliwość nagrywania na karty SD i serwery FTP ▪ Zasilanie: PoE (Power over Ethernet) lub 12 VDC (zasilacz sieciowy w zestawie)

NVIP-TDN5401C/MPX2.0
- Czułość: 0.5 lx/F=1.4
- Montaż obiektywu: CS

NVIP-TDN4401V/IR/MPX2.0
- Oświetlacz IR - 18 diod LED
- Wbudowany obiektyw f=2.7 ~ 9 mm
- Obudowa wandaloodporna, IP 66

NVIP-TDN3401H/IR/MPX2.0
- Oświetlacz IR - 35 diod LED
- Wbudowany obiektyw f=3.6 ~16 mm
- Klasa szczelności IP 66
- Uchwyt w komplecie z kamerą

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

Czas na zmiany

Jan Rybczyński

Zgodnie z ustawą z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych, jeżeli liczba zmian w ustawie jest znaczna lub gdy ustawa była uprzednio wielokrotnie nowelizowana i posługiwanie się nią może być istotnie utrudnione, Marszałek Sejmu ogłasza tekst jednolity ustawy. Opublikowanie w dniu 4 sierpnia 2005 r. jednolitego tekstu ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. Nr 145, poz. 1221) było poprzedzone ośmioma zmianami tekstu pierwotnego. Obecnie wprowadzono kolejnych dziewięć zmian tekstu jednolitego z 2005 roku, w tym największą i najnowszą, wynikającą z ustawy z dnia 25 marca 2011 r. o ograniczaniu barier administracyjnych dla obywateli i przedsiębiorców. Można więc znów mówić o trudnościach w posługiwaniu ustawą, o wyławianiu z niej zmian. Warto więc przedstawić ważniejsze zmiany tekstu jednolitego

Od początku 2006 roku Minister Spraw Wewnętrznych i Administracji może upoważnić Komendanta Głównego Straży Granicznej do kontroli działalności gospodarczej w zakresie usług ochrony osób i mienia, która dotyczy prawidłowości dokonywania kontroli bezpieczeństwa przeprowadzanej w krajowych portach lotniczych. Komendant Główny SG może powierzyć przeprowadzenie kontroli komendantom oddziałów SG. Przedsiębiorców branży ochrony wykonujących tego rodzaju usługi nie może więc zdziwić wysłane z organu SG zawiadomienie o zamiarze przeprowadzenia kontroli lub wizyta funkcjonariusza SG w celu kontroli w przypadkach braku obowiązku zawiadamiania (przypadki te są określone w ustawie z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej). Ponadto w 2006 roku dołączono szefa CBA do listy organów, wobec których ustawa nie narusza przepisów dotyczących ochrony obszarów, obiektów i urządzeń jednostek organizacyjnych podległych, podporządkowanych lub nadzorowanych przez te organy.

W roku 2008 zmiany wprowadziła *notabene* ustawa z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich. Rozszerzono (art. 43 ust. 3) zakres obowiązków dotyczących usuwania naruszeń przepisów prawa i nieprawidłowości stwierdzonych w ramach nadzoru policji sprawowanego nad specjalistycznymi uzbrojonymi formacjami ochronnymi (SUFO). Obowiązki te dotyczą – odpowiednio do stwierdzonych uchybień – kierowników jednostek, w skład których wchodzą obszary, obiekty i urządzenia podlegające obowiązkowej ochronie, osób działających w imieniu lub interesie przedsiębiorcy, który uzyskał koncesję na działalność gospodarczą w zakresie ochrony osób i mienia i który ma pozwolenie na broń na okaziciela, a także kierowników jednostek, w których utworzono wewnętrzną służbę ochrony. Ponadto dodano przepis penalizujący zaniechanie usunięcia stwierdzonych w ramach sprawowanego przez Komendanta Głównego Policji nadzoru naruszeń przepisów prawa lub nieprawidłowości w terminie określonym w zaleceniu, wprowadzając karę grzywny, karę ograniczenia wolności albo pozbawienia wolności do lat dwóch.

W tymże roku dano również prawo ubiegania się o licencję pracownika ochrony fizycznej pierwszego lub drugiego stopnia osobom posiadającym obywatelstwo Konfederacji Szwajcarskiej.

W dniu 10 lipca 2009 roku weszła w życie oczekiwana przez firmy ochrony zmieniona delegacja do wydania rozporządzenia, które zostało opublikowane dopiero po przeszło roku w Dzienniku Ustaw z 2010 r. Nr 166, poz. 1128. Chodzi mianowicie o rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 września 2010 r. w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne.

W kolejnym, 2010 roku dodano przepis o formie dokumentów dołączanych do wniosku o wydanie koncesji (oryginał, poświadczona kopia lub poświadczone tłumaczenie). W tej samej ustawie zmieniającej wyłączono stosowanie korzystniejszych dla przedsiębiorców prowadzących niereglamentowaną działalność gospodarczą przepisów art. 11 ust. 3–9 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej w sprawach udzielenia koncesji, odmowy udzielenia koncesji, jej zmiany, cofnięcia, ograniczenia jej zakresu oraz kontroli działalności gospodarczej w zakresie usług ochrony.

W nowej ustawie o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r., która obowiązuje od 2 stycznia 2011 r., powtarza się przepis mówiący o tym, że pracownik ochrony, któremu mają być powierzone zadania pełnomocnika ochrony lub pracownika pionu ochrony informacji niejawnych, musi dodatkowo spełnić wymagania określone w tej ustawie. Warto zwrócić uwagę na przepis przejściowy (art. 187), mówiący o tym, że przedsiębiorcy realizujący postanowienia umów zawierających klauzulę „poufne", związanych z dostępem do informacji niejawnych, którzy nie posiadają ważnego świadectwa bezpieczeństwa przemysłowego w dniu wejścia w życie ustawy, powinni uzyskać takie świadectwo w terminie 12 miesięcy od dnia wejścia w życie ustawy.

Inna ustawa (z dnia 29 października 2010 r., o rezerwach strategicznych) skorygowała określenie jednego z rodzajów obiektów podlegających obligatoryjnej ochronie. Do tej pory takie obiekty nazywane były magazynami rezerw państwowych. Obecnie ustawa posługuje się pojęciem magazynów rezerw strategicznych, zdefiniowanym w art. 15 ustawy o rezerwach strategicznych.

Przejdźmy do najnowszej i najobszerniejszej zmiany w ustawie o ochronie osób i mienia, zawartej w ustawie z dnia 25 marca 2011 r. o ograniczaniu barier administracyjnych dla obywateli i przedsiębiorców (Dz. U. z 2011 r. Nr 106, poz. 622 z późn. zm.), która weszła w życie z dniem 1 lipca br. Najobszerniejszej, gdyż w zmienionym art. 17 przeniesiono wymagania dotyczące danych, które muszą być zawarte w treści wniosku o udzielenie koncesji, oraz dokumentów dołączanych do takiego wniosku, zawarte do tej pory w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 27 maja 1998 r. w sprawie rodzajów dokumentów wymaganych przy składaniu wniosku o udzielenie koncesji na prowadzenie działalności gospodarczej w zakresie usług ochrony osób i mienia. Nowe rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 czerwca 2011 r. w sprawie wzoru wniosku o udzielenie lub zmianę koncesji na wykonywanie działalności gospodarczej w zakresie usług ochrony osób i mienia zostało opublikowane w Dz. U. z 2011 r. Nr 136, poz. 802 i weszło w życie z dniem 1 lipca 2011 r.

Najistotniejsze w tych zmianach jest dopuszczenie wyboru, jaki ma wnioskodawca – może złożyć zaświadczenie albo oświadczenie o niezaleganiu z wpłatami należności budżetowych oraz o niekaralności. W przypadku składania oświadczenia składający jest zobowiązany do zawarcia w nim klauzuli o świadomości odpowiedzialności karnej za złożenie fałszywego oświadczenia. Klauzula ta zastępuje pouczenie organu o odpowiedzialności karnej za składanie fałszywych zeznań.

Do ustawy z dnia 25 marca 2011 r. o ograniczaniu barier administracyjnych dla obywateli i przedsiębiorców wprowadzono dwie zmiany, które weszły w życie w dniach 30 czerwca i lipca br. Ważniejsza dla nas wynika z ustawy z dnia 13 maja 2011 r. o zmianie ustawy o swobodzie działalności gospodarczej oraz niektórych innych ustaw. Tutaj można jedynie ogólnie wskazać, że odnoszą się one do stopniowej zmiany organu ewidencyjnego, którym – jedynie w przypadku wpisów nieprzeniesionych do Centralnej Ewidencji i Informacji o Działalności Gospodarczej

i tylko do końca br. – pozostanie wójt, burmistrz albo prezydent miasta, a także do rozszerzenia zasad zawieszania działalności gospodarczej (art. 14a).

Po długim, sześciomiesięcznym *vacatio legis*, w dniu 11 lipca weszła w życie ustawa z dnia 26 listopada 2010 r. o zmianie ustawy o usługach detektywistycznych (Dz. U. z 2011 r. Nr 6, poz. 17). Zawiera ona dużo zmian odnoszących się zarówno do praw i obowiązków detektywa, zasad działalności gospodarczej w zakresie usług detektywistycznych, jak i wymagań kwalifikacyjnych wobec detektywów. Prześledźmy ważniejsze z nich.

Doprecyzowaniu uległy zasady postępowania detektywa ze zgromadzonymi w toku postępowania danymi osobowymi (art. 8 ust. 3). Obecnie detektyw, po zaprzestaniu prowadzenia sprawy lub na polecenie zatrudniającego przedsiębiorcy, ma obowiązek przekazać przetwarzane dane osobowe bezpośrednio zleceniodawcy albo innemu detektywowi, wyznaczonemu przez przedsiębiorcę, albo zniszczyć te dane w przypadku rezygnacji zleceniodawcy z ich odbioru lub nieodebrania ich w wyznaczonym terminie. Wykonując takie polecenie, detektyw sporządza notatkę o określonej w ustawie treści, którą dołącza się do księgi realizacji umowy.

W zakresie postępowania o wpis do rejestru doprecyzowano, jakie dane osobowe przedsiębiorcy – osoby fizycznej, pełnomocnika, członków zarządu czy prokurentów – obejmuje wpis, zapewniając zgodność z ustawą o ochronie danych osobowych (obecnie to wyłącznie imię i nazwisko, data urodzenia, adres zamieszkania oraz – w przypadku posiadania licencji – numer licencji).

W przepisach dotyczących organów uprawnionych do kontroli zamiast określenia „inny organ państwowy wyspecjalizowany w kontroli danego rodzaju działalności" wymieniono Komendanta Głównego Policji oraz komendantów wojewódzkich policji, co konkretyzuje, kto, oprócz organu prowadzącego rejestr, może kontrolować przedsiębiorcę świadczącego usługi detektywistyczne.

W art. 29 pkt 9 ograniczono wymagania zdrowotne wobec osób ubiegających się o licencję detektywa wyłącznie do zdolności psychicznej do wykonywania zawodu. Dotychczasowy wymóg odpowiedniego stanu zdrowia fizycznego zamykał drogę do wykonywania tego zawodu osobom posiadającym doświadczenie i wiedzę, ale należącym do jakiegokolwiek rodzaju grupy inwalidzkiej.

Ponadto ustawa zmieniająca dopuszcza oświadczenia w miejsce zaświadczeń odnoszących się do zdolności do czynności prawnych, skazania czy prowadzonych postępowań karnych lub karno-skarbowych.

Zmodyfikowano również liczne przepisy dotyczące egzaminu na licencję detektywa (art. 30–34).

Oddzielono procedurę przeprowadzania egzaminu od procedury postępowania administracyjnego związanej z wydawaniem licencji detektywa. Wydawanie licencji pozostaje nadal w gestii KWP, a procedura organizacji i przeprowadzenia egzaminu znalazła się w kompetencji Komendanta Głównego Policji. Przygotowywaniem pytań i zadań praktycznych na egzamin będzie zajmował się trzyosobowy zespół powoływany przez Komendanta Głównego Policji.

Zmniejszeniu do sześciu osób ulega skład komisji egzaminacyjnej. Do składu komisji wprowadzono przedstawiciela organizacji zawodowych zrzeszających detektywów.

Ograniczony został zakres tematów obowiązujących na egzaminie poprzez wyłączenie wiktymologii i psychologii sądowej. Włączono natomiast przepisy regulujące zasady wykonywania działalności gospodarczej w zakresie usług detektywistycznych.

Egzamin będzie odbywał się nie rzadziej niż raz na kwartał (a nie, jak do tej pory, raz na sześć miesięcy).

Pierwszy egzamin na licencję detektywa na zasadach określonych w przepisach ustawy zmieniającej zostanie przeprowadzony najpóźniej w terminie trzech miesięcy od dnia jej wejścia w życie.

Nowa delegacja ustawowa i wydanie rozporządzenia określającego szczegółowy zakres tematów egzaminacyjnych, tryb wyznaczania członków komisji i zespołu, sposób i tryb pracy komisji i zespołu oraz organizację egzaminu zlikwiduje możliwość zaliczania niektórych tematów policjantom i funkcjonariuszom niektórych organów, która wynikała z dotychczas obowiązującego w tym zakresie rozporządzenia.

Jan Rybczyński
radca prawny

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

Strefowa organizacja systemów alarmowych

w aspekcie realizacji założonych zadań ochrony w obiektach budowlanych

Marcin Buczaj

Ochrona i nadzór nad obiektem, zapewniane przez systemy zabezpieczenia mienia, powinny być realizowane w sposób uniemożliwiający potencjalnemu intruzowi dostęp do newralgicznych stref obiektu i osiągnięcie przez niego zamierzonych celów ataku. Systemy sygnalizacji włamania i napadu (SSWiN) wykorzystywane do ochrony obiektów mają za zadanie przekazać użytkownikowi systemu informacje o zidentyfikowaniu zagrożenia. Celowe staje się takie zabezpieczenie obiektu, aby informacja o wykryciu zagrożenia nastąpiła w możliwie najwcześniejszym etapie jego powstawania, jeszcze przed osiągnięciem przez intruza zamierzonych celów ataku. Taka organizacja systemu alarmowego umożliwia przedsięwzięcie skutecznych środków ochrony mających na celu neutralizację zagrożenia. Artykuł pokazuje, na czym polega strefowa organizacja systemów alarmowych na przykładzie obiektów budowlanych, w szczególności o charakterze mieszkalnym. Przedstawione są główne zadania poszczególnych stref stanowiących strukturę organizacyjną SSWiN w obiektach. Główną częścią artykułu jest analiza roli elementów detekcyjnych w poszczególnych strefach ochrony oraz ocena skuteczności systemu alarmowego realizującego zadania systemu sygnalizacji włamania i systemu sygnalizacji napadu

1. Wprowadzenie

Technika zabezpieczenia mienia to dziedzina techniki, która wykorzystuje osiągnięcia wielu dziedzin nauki i techniki do ochrony mienia, życia i zdrowia lub informacji. W technikach zabezpieczenia mienia najczęściej wykorzystuje się osiągnięcia mechaniki, elektroniki i informatyki. Podstawowymi grupami, jakie można wyodrębnić w szeroko pojmowanej dziedzinie technik zabezpieczenia mienia, są:

– systemy kontroli dostępu,
– systemy alarmowe,
– systemy dozorowe (monitorowanie).

Każda z tych grup charakteryzuje się specyficznymi, wyróżniającymi się czynnikami. Różny jest zakres ich działania oraz związanych z nim funkcji i procedur.

System kontroli dostępu to system obejmujący wszystkie składniki konstrukcyjne i organizacyjne oraz te, które odnoszą się do urządzeń, niezbędne do sterowania dostępem [3]. Z definicji wynika, że systemy kontroli dostępu odpowiadają za fizyczne uniemożliwienie dostępu intruza do zabezpieczanego mienia. Środki zabezpieczające z tej grupy są oparte na zdobyczach z zakresu mechaniki, mechatroniki i automatyki, wspomaganej jedynie telekomunikacją i przesyłem sygnału.

System alarmowy to instalacja do wykrywania i sygnalizowania obecności, wejścia lub usiłowania wejścia intruza do chronionego obiektu [1]. Środki z tej grupy odpowiadają za identyfikowanie zagrożenia oraz przekazanie informacji o wykrytym zagrożeniu użytkownikowi systemu odpowiedzialnemu za neutralizację zagrożenia. Rozwój tej grupy zabezpieczeń jest możliwy dzięki zaadaptowaniu osiągnięć z zakresu elektroniki, metrologii i cyfrowego przetwarzania sygnałów.

System dozorowy to system służący do obserwacji, wykrywania, rejestrowania i sygnalizowania warunków wskazujących na zaistnienie niebezpieczeństwa powstania szkód lub zagrożenia osób lub mienia [5]. Zadania tej części systemów zabezpieczeń to kontrolowanie stanu chronionego obiektu oraz monitorowanie zachodzących w nim zmian.

W dalszej części artykułu zostaną przedstawione warunki skuteczności działania systemów ochrony oparte na analizie czasów poszczególnych działań potencjalnego intruza w chronionym obiekcie oraz działaniami użytkownika systemu. Poziom skuteczności zastosowanego systemu ochrony będzie wynikiem zależności czasowych pomiędzy występującymi w obiekcie zdarzeniami. Główną częścią artykułu jest prezentacja koncepcji strefowej organizacji systemu ochrony. W ramach tego zostanie scharakteryzowane zostaną poszczególne strefy ochrony i ich usytuowanie na terenie chronionego obiektu.

2. Pojęcie skutecznego działania systemów ochrony

Mechanizm zabezpieczenia posiadanego dobra (życia, zdrowia, mienia, informacji, wartości intelektualnej) polega na informowaniu o wystąpieniu potencjalnego zagrożenia i sygnalizowaniu możliwości utraty posiadanego dobra oraz przeciwdziałaniu utracie posiadanego dobra. Działania mające na celu przywłaszczenie sobie cudzej własności są niezmienne i polegają na zebraniu informacji o posiadanym przez inne osoby i stanowiącym realną wartość mieniu oraz dokonaniu zaboru tego mienia.

Chociaż sam mechanizm działania systemów zabezpieczeń nie zmienił się od lat, stosowane w nich techniki ewoluowały wraz z rozwojem i postępem technologicznym. Obecnie w systemach, które mają za zadanie ograniczenie lub uniemożliwienie intruzowi fizycznego dostępu do chronionego dobra, coraz częściej wykorzystuje się techniki komputerowe i teleinformatyczne. Systemy te umożliwiają już nie tylko fizyczne zabezpieczenie dóbr przez kontrolowanie dostępu do nich, ale także ich obserwację oraz działania alarmowe w przypadku wykrycia zagrożenia.

Systemy alarmowe nie służą do powstrzymania intruza przed wejściem do obiektu; ich zadaniem jest wykrycie zagrożenia oraz powiadomienie o nim użytkownika. Parametrem określającym skuteczność systemu alarmowego jest czas jego reakcji na wykryte zagrożenie [4]. Samo poinformowanie użytkownika o wykryciu intruza może być działaniem spóźnionym, ponieważ użytkownik nie będzie miał dostatecznie dużo czasu na skuteczną reakcję. System zabezpieczeń powinien umożliwiać wykrycie próby wtargnięcia intruza do obiektu jeszcze przed sforsowaniem przez niego zabezpieczeń fizycznych. Z kolei efektywność systemu alarmowego (prawidłowa realizacja jego zadań) zależy nie tylko od wyposażenia systemu zabezpieczeń w skuteczne i liczne elementy detekcyjne, ale również od ich prawidłowego rozmieszczenia na terenie chronionego obiektu.

Podczas projektowania systemu dąży się do tego, by jak najskuteczniej wykrywał on zagrożenia, a jego reakcja na nie była jak najszybsza.

Każdy z zastosowanych elementów systemu ochrony obiektu ma istotny wpływ na dobór środków mających na celu powstrzymanie intruza oraz skuteczność zmierzających do tego działań. Dlatego przy projektowaniu systemu zabezpieczeń powinno kierować się następującą zasadą – przewidywany czas reakcji użytkownika systemu na zaistniałe zagrożenie powinien być krótszy od czasu, jaki jest potrzebny intruzowi na działania prowadzące do przejęcia kontroli nad chronionym dobrem. Można opisać to następującymi zależnościami:

$$t_r < t_a \tag{1}$$

$$t_r = t_b + t_d + t_i + t_n \tag{2}$$

$$t_a = t_{we} + t_{rca} + t_{wy} \tag{3}$$

gdzie:

t_r – czas reakcji systemu ochrony na zaistniałe zagrożenie;
t_a – czas realizacji ataku na chroniony obiekt;
t_b – czas bezwładności systemu nadzoru;
t_d – czas detekcji zagrożenia przez elementy detekcyjne systemu alarmowego;
t_i – czas potrzebny na przekazanie informacji o zaistniałym zagrożeniu przez komórki systemu nadzoru;
t_n – czas fizycznej neutralizacji zagrożenia lub podjęcia kroków mających na celu przeciwdziałanie zaistniałemu zagrożeniu;
t_{we} – czas związany z koniecznością forsowania fizycznych zabezpieczeń systemu ochrony przez intruza podczas atakowania chronionego obiektu (etap wstępny);
t_{rca} – czas związany z realizacją konkretnych, zaplanowanych celów ataku na chroniony obiekt (etap zasadniczy);
t_{wy} – czas potrzebny intruzowi na sforsowanie fizycznych zabezpieczeń systemu ochrony podczas opuszczania chronionego obiektu (etap końcowy).

Dla przykładowego zdarzenia (rys. 1) przedstawiono charakterystykę czasową przebiegu procesu ataku na chroniony obiekt oraz procesu reakcji systemu nadzoru na zaistniałe w chronionym obiekcie zagrożenie. W tabeli 1 przedstawiono wyniki analizy skuteczności działania systemów nadzoru związanej z reakcją systemu nadzoru na różne potencjalne zagrożenia, jakie mogą się urzeczywistnić w chronionym obiekcie.

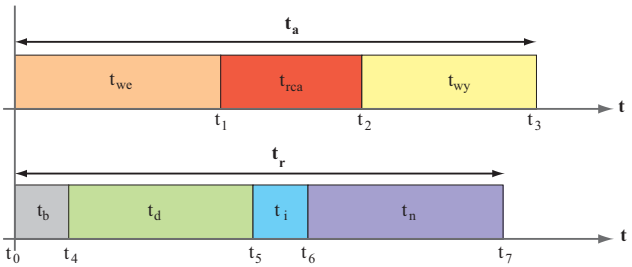
Założonym celem ochrony jest uniemożliwienie intruzowi dostania się do newralgicznych obszarów chronionego obiektu. Dlatego przy projektowaniu systemów alarmowych należy zwrócić uwagę na ograniczenie do minimum czasu bezwładności systemu t_b, a więc czasu, jaki upłynie od momentu podjęcia przez intruza próby sforsowania zabezpieczeń do momentu wykrycia zagrożenia przez elementy detekcyjne. Z drugiej strony należy pamiętać, że równie skutecznym rozwiązaniem jest dążenie do wydłużenia czasu $t_{we} - t_b$, a właściwie wydłużenia przedziału czasowego . Dzięki temu użytkownicy systemu mają więcej czasu na stosowne procedury przeciwdziałające zagrożeniu. Dlatego element detekcyjny powinien być zainstalowany na samym początku drogi prowadzącej do newralgicznej strefy, najlepiej przed głównymi elementami fizycznego zabezpieczenia obiektu (mechanicznymi i architektonicznymi).

Kolejną istotną rzeczą wynikającą z przedstawionej analizy czasów reakcji i działań jest określenie zadań i funkcji systemu zabezpieczeń, np. przez dokonanie analizy potencjalnych zagrożeń, jakie mogą się urzeczywistnić w danym obiekcie. Inne są zadania systemu sygnalizacji włamania, a inne systemu sygnalizacji napadu. Określenie tych zadań uwarunkowuje późniejsze wytyczne dla projektowanego systemu alarmowego.

3. Strefowa struktura organizacji systemu nadzoru

Ze względu na arbitralnie założony przez projektanta poziom prawdopodobieństwa wystąpienia zdarzeń danego typu w chronionym obiekcie istnieje skończona liczba zagrożeń, na które system reaguje. Liczba wykrywanych zdarzeń jest ściśle związana z liczbą elementów detekcyjnych w systemie, która z kolei ma związek z kosztem instalacji systemu. Zminimalizowanie czasu reakcji systemu na wystąpienie zagrożenia ma związek z określeniem zarówno wpływu parametrów technicznych elementu detekcyjnego, jak i miejsca, w którym dany element detekcyjny został zamontowany [4].

Ze względu na długość procesu wykrywania zagrożenia ważne jest, aby system był wyposażony w skuteczne środki detekcyjne, działające zarówno wewnątrz obiektu (detekcja zaistniałej penetracji obiektu), jak i na jego peryferiach (detekcja podjęcia próby penetracji terenu obiektu).



Rys. 1. Przebieg procesu ataku i procesu reakcji systemu nadzoru na zagrożenie występujące w chronionym obiekcie t_0 – rozpoczęcie próby wtargnięcia do chronionego obiektu, t_1 – zakończenie etapu forsowania zabezpieczeń, niezbędnego do wejścia do chronionego obiektu, i przejście do etapu mającego na celu osiągnięcie głównego celu ataku na chroniony obiekt, t_2 – osiągnięcie celu ataku i rozpoczęcie wycofywania się z chronionego obiektu, t_3 – zakończenie działań związanych z atakiem na chroniony obiekt, t_4 – wykrycie wtargnięcia na teren chronionego obiektu, t_5 – zakończenie analizowania czynników zewnętrznych przez detektory i rozpoczęcie przekazywania informacji w systemie nadzoru, t_6 – zakończenie przekazywania informacji o wykrytym zagrożeniu i rozpoczęcie neutralizacji zagrożenia lub przeciwdziałania zagrożeniu, t_7 – zakończenie neutralizacji zagrożenia i osiągniecie założonych celów ochrony

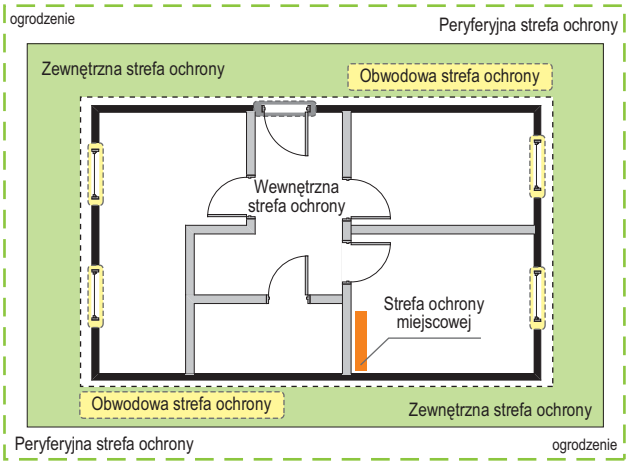
W celu sprecyzowania zasad działania systemu nadzoru i określenia szczegółowych celów ochrony wprowadzone zostało pojęcie stref ochrony. Strefy ochrony to obszary, na których na których muszą być realizowane pewne specyficzne zadania. W chronionym obiekcie można wyróżnić następujące strefy ochrony: wewnętrzną, obwodową, zewnętrzną i peryferyjną oraz dodatkową strefę ochrony miejscowej. Na rys. 2 przedstawiono typowe rozmieszczenie stref ochrony w przykładowym obiekcie budowlanym. Każda z wymienionych stref spełnia inne funkcje w systemie.

Peryferyjna strefa ochrony to strefa terenowa, która obejmuje granicę chronionego obszaru (najczęściej są to różnego rodzaju ogrodzenia działek). Jest najdalej wysuniętą strefą, do której dostęp jest najłatwiejszy i do której można legalnie się zbliżyć.

Zewnętrzna strefa ochrony to również strefa terenowa. Obejmuje ona obszar pomiędzy ogrodzeniem a budynkami. Jest

Zależność	Określenie poziomu skuteczności systemu nadzoru	Uwagi
$t_7 < t_1$	optymalny	• system nadzoru neutralizuje zagrożenie jeszcze przed osiągnięciem przez intruza celów ataku • zminimalizowany poziom zagrożenia
$t_1 < t_7 < t_2$	warunkowo akceptowalny	• system nadzoru nie jest w stanie zupełnie udaremnić osiągnięcia celu ataku • poziom wystarczający w przypadku systemów realizujących funkcje antywłamaniowe IAS, niewystarczający w przypadku systemów realizujących funkcje sygnalizacji napadu HAS
$t_2 < t_7 < t_3$	warunkowo dopuszczalny	• system nadzoru nie jest w stanie udaremnić osiągnięcia celu ataku • poziom akceptowalny w przypadku systemów realizujących funkcje antywłamaniowe IAS, niewystarczający w przypadku systemów realizujących funkcje sygnalizacji napadu HAS
$t_7 > t_3$	nieskuteczny	system nadzoru reaguje na występujące zagrożenie, ale ze względu na zbyt długie czasy reakcji system ochrony nie jest w stanie skutecznie przeprowadzić procesu neutralizacji zagrożenia
$t_6 > t_3$	niedopuszczalny	system nadzoru nie jest w stanie podjąć próby neutralizacji zagrożenia i przeciwdziałać występującym w chronionym obiekcie zagrożeniom
$t_4 > t_3$	brak ochrony	system nadzoru nie reaguje na zaistniałe w chronionym obiekcie zagrożenia

Tab. 1. Skuteczność systemów nadzoru w chronionym obiekcie



Rys. 2. Rozmieszczenie stref ochrony w chronionym przez system alarmowy obiekcie

pierwszą strefą ochrony, w której nieuprawniony dostęp osób postronnych nie powinien zostać niezauważony przez system nadzoru. Dostęp do zewnętrznej strefy ochrony jest możliwy po sforsowaniu zabezpieczeń terenowych strefy peryferyjnej.

Obwodowa strefa ochrony jest pierwszą strefą wyznaczoną przez elementy architektoniczne chronionego obiektu budowlanego. Szczególnymi elementami obwodowej strefy ochrony są otwory okienne i drzwiowe, przez które można dostać się do wnętrza chronionego budynku. Dostęp do obwodowej strefy ochrony jest możliwy po przejściu zewnętrznej strefy ochrony. W przypadku przylegania chronionego budynku bezpośrednio do obszarów ogólnie dostępnych (np. ulicy) obwodowa strefa ochrony jest pierwszą strefą ochrony obiektu. Obecnie w obiektach budowlanych, zwłaszcza w obiektach mieszkalnych, otwory okienne i drzwiowe zabezpieczane są najczęściej przez czujki kontaktronowe, które są podstawowymi elementami ochrony obwodowej obiektu. Wadą takiego rozwiązania jest możliwość dość prostego obejścia tego zabezpieczenia, np. poprzez wybicie szyby, które spowoduje, że system ochrony przestanie być szczelny i wrażliwy na pewne działania. Elementy zabezpieczające strefy obwodowe budynku służą najczęściej do detekcji podjętych prób wejścia do obiektu przez otwory okienne i drzwiowe.

Wewnętrzna strefa ochrony to obszar wewnątrz chronionego obiektu, w którym umiejscowione są główne cele ochrony. Dostęp do niej jest możliwy po uprzednim sforsowaniu obwodowej strefy ochrony. Wewnętrzną strefę ochrony zabezpiecza się za pomocą elementów detekcyjnych o charakterze obszarowym (np. pasywnych czujek podczerwieni, czujek mikrofalowych) w przypadku systemów realizujących zadania związane z sygnalizacją włamania lub za pomocą miejscowych elementów detekcyjnych (np. przycisków napadowych) w przypadku systemów realizujących zadania związane z sygnalizacją napadu.

Strefa ochrony miejscowej to szczególna, wyróżniona strefa w wewnętrznej strefie ochrony. W niej umiejscowione są przedmioty będące najbardziej prawdopodobnymi celami potencjalnych ataków. Wyposażona jest w dodatkowe elementy detekcyjne, które zabezpieczają tylko te przedmioty.

W przypadku systemów alarmowych realizujących zadania związane z sygnalizacją napadu obwodowa strefa ochrony może być jedynym obwodem skutecznej ochrony, a w przypadku systemów realizujących zadania związane z sygnalizacją włamania może stanowić ważny element umożliwiający skuteczną eliminację zagrożenia. Dlatego ważne jest wyposażenie obwodowej strefy ochrony w elementy detekcyjne umożliwiające skuteczne wykrywanie potencjalnych prób sforsowania dróg dostępu do wnętrza chronionego obiektu.

4. Podsumowanie

Na etapie projektowania systemu zabezpieczeń strefowa organizacja systemów alarmowych umożliwia precyzyjne określenie zadań realizowanych w poszczególnych strefach chronionego obiektu. Dzięki temu możliwe jest odpowiednie zastosowanie elementów detekcyjnych umożliwiających wykrycie zagrożenia danego typu oraz odpowiednie umiejscowienie zabezpieczeń fizycznych mających na celu powstrzymanie intruza lub spowolnienie jego działań. Informacja o wykryciu zagrożenia lub wtargnięcia do wyznaczonej strefy nadzoru może mieć charakter prewencyjny (odstraszający), zachowawczy lub reakcyjny.

Ważnym czynnikiem decydującym 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 wywołanych tym zagrożeniem. Istotne staje się zatem wyposażenie systemów nadzoru w środki techniczne, dzięki którym skuteczne wykrycie zagrożenia następuje jeszcze przed wtargnięciem intruza do wnętrza chronionego obiektu. W związku z tym ciężar procesu detekcji zagrożenia powinien być przesuwany – w zależności od typu chronionego obiektu –w stronę ochrony peryferyjnej lub obwodowej.

Przy projektowaniu należy również pamiętać, że nawet najlepszy, najczulszy i najskuteczniejszy system alarmowy nie powoduje fizycznego powstrzymania intruza. Może jedynie zniechęcić go do dalszych działań. Aby zwiększyć skuteczność systemu nadzoru, należy wydłużyć (poprzez utrudnienia) niezbędny dla intruza czas na dotarcie do chronionych stref lub skrócić czas reakcji użytkownika systemu na zaistniałe zagrożenie. Skuteczność systemu nadzoru polega na udaremnieniu planów intruza, a nie tylko na wykryciu zagrożenia.

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

Literatura

1. PN-EN 50131-1:2009 – *Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 1: Wymagania systemowe*, PKN, Warszawa 2009.
2. PN-EN 50136-1-1:2001 – *Systemy alarmowe. Systemy i urządzenia transmisji alarmu. Wymagania ogólne dotyczące systemów transmisji alarmu*, PKN, Warszawa 2001.
3. PN-EN50133-1:2002 – *Systemy alarmowe. Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia. Część 1: Wymagania systemowe*, PKN, Warszawa 2002.
4. Buczaj M., *Czas jako kryterium skuteczności przebiegu procesu neutralizacji zagrożeń w systemach nadzorujących stan chronionego obiektu, Zabezpieczenia* nr 6(70)/2009.
5. Kałużny P., *Telewizyjne systemy dozorowe*, WKiŁ, Warszawa 2008.

aperio™

Nowatorskie rozwiązanie

W dzisiejszych czasach trudno sobie wyobrazić nowy obiekt biurowy czy handlowy bez kontroli dostępu. Już w fazie projektu planujemy zabezpieczenie wejścia głównego do firmy, gabinetów, serwerowni czy magazynu. Producenci systemów kontroli dostępu prześcigają się w stosowanych technologiach i innowacyjnych rozwiązaniach. Dzięki tym innowacjom technicznym możemy zdalnie logować się do systemu kontroli dostępu, zintegrować go z systemem alarmowym i systemem monitorowania, otwierać i zamykać drzwi, dowolnie nadawać uprawnienia. Wiemy, kto i kiedy wszedł do pomieszczenia i ile osób przebywa w danej strefie, co umożliwia szybką lokalizację osób lub kontrolę stanu w przypadku konieczności ewakuacji

ASSA ABLOY Poland

Omawiane systemy są ulepszane, dodaje się do nich nowe, coraz bardziej zaawansowane funkcje. Mogą spełnić najwyższe wymagania dotyczące procedur bezpieczeństwa, ponieważ w fazie projektowania możemy dokonać dowolnej konfiguracji. Problemy mogą pojawić się dopiero w gotowych instalacjach, po rozpoczęciu ich użytkowania. Co zrobić, kiedy musimy zmienić przeznaczenie pomieszczeń? Czy zabezpieczyć dodatkowy pokój, gdy chcemy mieć szklane drzwi? Co zrobić, jeśli chcemy załatwić to szybko, tanio i uniknąć konieczności remontu po wykonaniu dodatkowych instalacji?

Dotychczas mieliśmy dwie możliwości:

1) Wezwać instalatora, który zamontuje elektrozaczep lub inny zamek elektryczny w drzwiach, czytnik kart zbliżeniowych, doprowadzi zasilanie i wszystko połączy z kontrolerem drzwiowym.
2) Zainstalować punkt kontroli dostępu pracujący w trybie autonomicznym.

W przypadku wyboru pierwszego rozwiązania musimy pamiętać, że poprawny i estetyczny montaż elektrozaczepu czy zamka elektrycznego jest skomplikowany i czasochłonny. Instalator musi wykazać się doświadczeniem i wysoką kulturą pracy. Powinniśmy liczyć się z naprawą i malowaniem ścian, co znacznie zwiększa koszty instalacji.

Drugie rozwiązanie jest prostsze, lecz wymaga niezależnego zarządzania drzwiami objętymi autonomiczną kontrolą. Tracimy możliwość rejestracji zdarzeń, dodawania użytkowników czy generowania raportów w jednym spójnym systemie. System kontroli dostępu zawierający zarówno urządzenia pracujące w trybie sieciowym, jak i autonomicznym, jest mniej wygodny w zarządzaniu.

Rozwiązaniem tych problemów jest Aperio – nowatorskie rozwiązanie firmy ASSA ABLOY, które nagrodzono złotym medalem na targach IFSEC 2011.

Aperio to najnowsza bezprzewodowa technologia, która efektywnie integruje drzwi wyposażone w zamki mechaniczne z istniejącym systemem kontroli dostępu. Technologia ta została stworzona w celu umożliwienia łatwej rozbudowy istniejących systemów elektronicznej kontroli dostępu i równocześnie zapewnienia prostego i wygodnego sposobu zwiększenia poziomu bezpieczeństwa obiektów. Jest w stanie zapełnić dotychczasową lukę pomiędzy mechanicznymi i elektronicznymi systemami zamknięć. To jedyne tego typu rozwiązanie na świecie.

Nazwa „Aperio" nie jest przypadkowa. To łacińskie słowo, które znaczy „otwórz".

Zasilanie bateryjne, a przez to brak okablowania, istotnie wpływa na czas i koszt instalacji. Instalację możemy wykonać na niemal wszystkich rodzajach drzwi. Do dyspozycji mamy dwa rodzaje elementów wykonawczych:

1) Czytnik kart zbliżeniowych zintegrowany z szyldem podłużnym i z bezprzewodowym odbiornikiem (HUB). Szyld, przeznaczony do drzwi pełnych i profilowych, jest zgodny ze wszystkimi zamkami wpuszczanymi zgodnymi z normą DIN (dostępna jest również wersja przeznaczona do zamków w standardzie skandynawskim).
2) Czytnik kart zbliżeniowych zintegrowany z wkładką cylindryczną i z bezprzewodowym odbiornikiem (HUB). Jest on kompatybilny ze wszystkimi zamkami wpuszczanymi zgodnymi z DIN oraz zamkami do drzwi szklanych (w których można zamontować wkładkę).

Czytniki są wyposażone w wielokolorowe diody LED sygnalizujące stan zamka, poprawną autoryzację karty i niski poziom naładowania baterii. Na dzień dzisiejszy obsługiwane są dwie technologie RFID – Mifare i iClass. Każdy element wykonawczy potrzebuje odbiornika do komunikacji z systemem kontroli dostępu. Odbiornik (HUB) jest instalowany w odległości do pięciu metrów od zamka i zasilany napięciem stałym w zakresie od 9 V do 30 V. Jest on wyposażony w port komunikacyjny i współpracuje z systemem kontroli dostępu. Przesyła informacje z szyldu zamka do kontrolera i komendy zwrotne do szyldu (szyfrowanie AES 128-bitowe). Wykorzystanie portu RS485 wymaga zintegrowania go z istniejącym systemem przez integratora systemu kontroli dostępu. Dzięki temu uzyskuje się dwustronną komunikację z urządzeniem i można sprawdzić stan baterii, stan urządzenia i jakość połączenia z HUB-em. W przyszłości możliwe będą nowe komendy. Obecnie trwają badania nad dodatkowymi funkcjami, np. monitorowaniem stanu drzwi czy możliwością zdalnego otwarcia.

Dodany ostatnio interfejs Wieganda znacznie zwiększył możliwości integracji. Oznacza to, że można połączyć Aperio z większością systemów kontroli dostępu dostępnych na rynku. W przypadku takiego połączenia tracimy możliwość bezpośredniej komunikacji z urządzeniem i tym samym sprawdzania stanu połączenia czy stanu baterii, ale uzyskujemy za to możliwość sterowania istniejącym zamkiem. Komunikacja jest wtedy uproszczona, po odczycie karty następuje zainicjowanie połączenia z HUB-em. Czytnik przesyła numer karty do odbiornika, który komunikuje się z kontrolerem kontroli dostępu. Po otrzymaniu odpowiedzi z systemu przesyła polecenie otwarcia do zamka. Zamek przez określony czas czeka na odpowiedź odbiornika. Brak odpowiedzi interpretuje jako odmowę dostępu.

ASSA ABLOY, jako lider na rynku zabezpieczeń, przykłada dużą wagę do bezpieczeństwa. Cała elektronika oraz śruby mocujące znajdują się po wewnętrznej, bezpiecznej stronie szyldu, uniemożliwiając nieautoryzowane otwarcie drzwi poprzez demontaż czytnika czy całego zamka. Urządzenie zostało również zabezpieczone na wypadek utraty łączności odbiornika z kontrolerem lub uszkodzenia kontrolera. Do każdego zestawu Aperio możemy wprowadzić dziesięć kart bezpieczeństwa. Karty te są zawsze akceptowane przez urządzenie, niezależnie od stanu komunikacji z kontrolerem. W sytuacjach awaryjnych możemy również otworzyć drzwi kluczem.

Aperio można stosować do wszystkich rodzajów drzwi o grubości skrzydła do 100 mm w przypadku szyldu podłużnego i 140 mm w przypadku wkładki cylindrycznej (70 mm/70 mm). Możemy go stosować w hotelach, szkołach, szpitalach i we wszystkich innych miejscach, gdzie ważne są bezpieczeństwo, wygoda i potrzeba łatwego i szybkiego włączenia istniejących drzwi z zamkiem mechanicznym do systemu kontroli dostępu.v

Opracowanie:
ASSA ABLOY Poland

Monitorowanie systemów sygnalizacji włamania i napadu

z wykorzystaniem sieci Ethernet (część 2)

Adam Rosiński, Maciej Maszewski

1. Wstęp

W pierwszej części artykułu przedstawiono ogólnie różne metody komunikacji pozwalające na zaprojektowanie systemu sygnalizacji włamania i napadu. Pokazano je na przykładzie zarówno łączności lokalnej pomiędzy składnikami systemu, jak i zdalnego monitoringu i zarządzania SSWiN. W tej części zostaną przedstawione różne możliwości łączności systemu do zarządzania i monitoringu z centralą alarmową poprzez sieć Ethernet.

2. Możliwości łączności systemu do zarządzania i monitoringu z centralą INTEGRA firmy SATEL poprzez sieć Ethernet

System sygnalizacji włamania i napadu wykorzystujący centralę alarmową INTEGRA umożliwia, za pomocą dodatkowych modułów, przyłączenie do sieci Ethernet [1,2,3]. Jest możliwość skorzystania z gotowych rozwiązań sprzętowych przeznaczonych do tego celu (modułów ETHM-1 i ETHM-2) lub stworzenia własnego rozwiązania [7] wykorzystującego port RS232 lub moduł INT-RS [5].

2.1. Połączenie z wykorzystaniem modułu ETHM-1

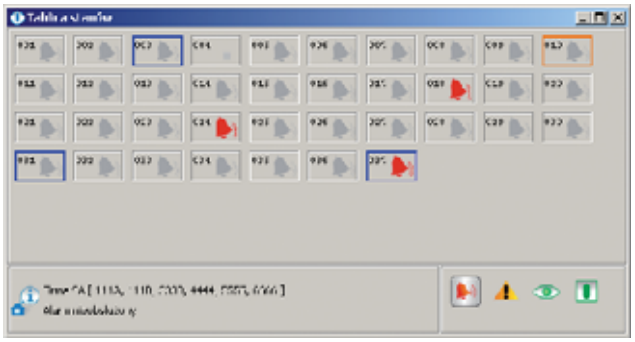
W przypadku wykorzystania modułu ETHM-1 podłączonego do centrali do zarządzania/monitoringu można wykorzystać następujące rozwiązania:

– stację PC z zainstalowanym oprogramowaniem STAM-2,
– stację PC z zainstalowanym oprogramowaniem GuardX i (lub) DloadX,
– stację PC z przeglądarką WWW,
– terminal GSM z napisaną w JAVA aplikacją do komunikacji z modułem ETHM-1.

Na rys. 1 pokazano schemat połączeń poszczególnych rozwiązań. Trzy rozwiązania spośród czterech tutaj omawianych wykorzystują transmisję przewodową, natomiast jedno, z terminalem GSM, korzysta z transmisji TCP/IP poprzez sieć pakietową GPRS/UMTS.

2.1.1. Stacja PC z zainstalowanym oprogramowaniem STAM-2

Rozwiązanie wykorzystujące aplikację STAM-2 ma zastosowanie w monitorowaniu wielu systemów alarmowych i jest przeznaczone do użycia w centrum monitorowania. Stacja monitorująca składa się z zainstalowanych w komputerze kart oraz oprogramowania, które umożliwia zarządzanie sygnałami przez moduły. Stacja taka może monitorować poprzez sieć Ethernet i otrzymywać sygnały drogą telefoniczną, a także poprzez sieć GSM (SMS i CLIP). Aplikacja ma możliwość detekcji uszkodzenia medium transmisyjnego. Dzięki strukturze klient-serwer program pozwala kilku operatorom na kilku stanowiskach na obsługę przychodzących zdarzeń. Oprogramowanie pracuje pod kontrolą systemu operacyjnego Windows. Operatorzy śledzący sytuację za pośrednictwem tej aplikacji mogą na bieżąco reagować na zaistniałe zdarzenia.

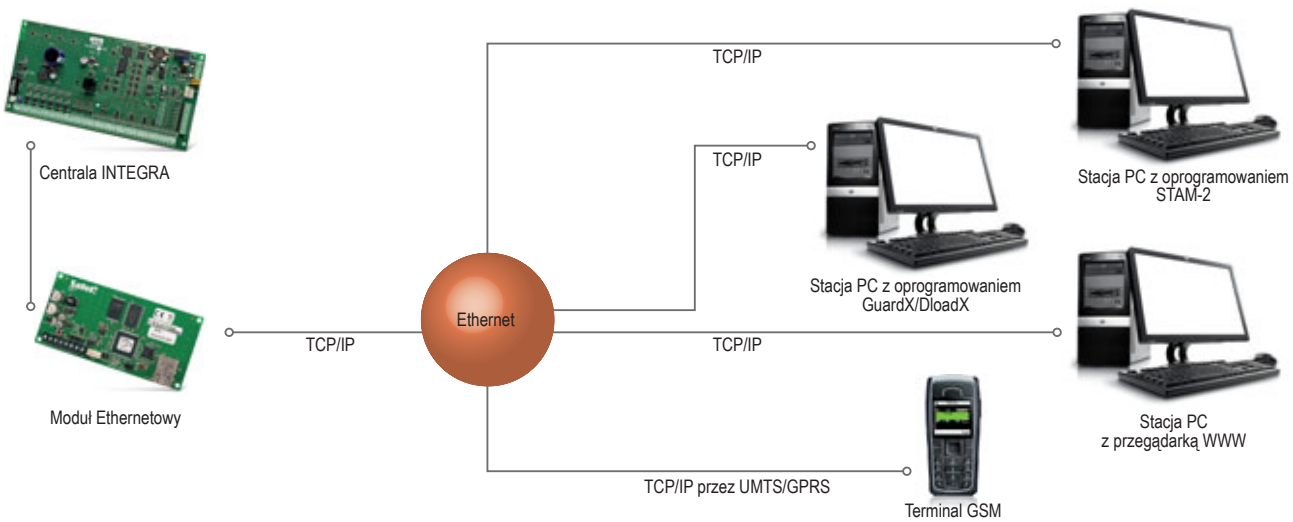


Rys. 2. Okno stanów z aplikacji STAM-2 [6]

Bezpieczeństwo danych jest zapewnione dzięki szyfrowanej komunikacji klient-serwer, przechowywaniu danych w zaszyfrowanym pliku bazy danych oraz definiowaniu uprawnień użytkowników programu. Na rys. 2 pokazano przykładowe okno stanów w aplikacji STAM2. Każda centrala przyłączona do systemu przedstawiona jest w postaci pola z jej numerem porządkowym i z odpowiednią ikoną, która w sposób graficzny ilustruje stan centrali. Klikając jedną z ikon na dole okna, użytkownik może określić, jakie informacje mają być aktualnie dostępne za pośrednictwem ikon.

2.1.2. Stacja PC z zainstalowanym oprogramowaniem GuardX/DloadX

GuardX to program do nadzoru i administrowania centralami INTEGRA. Aplikacja GuardX służy do podglądania



Rys. 1. Schemat połączenia centrali z PC/terminalem GSM [opracowanie własne]

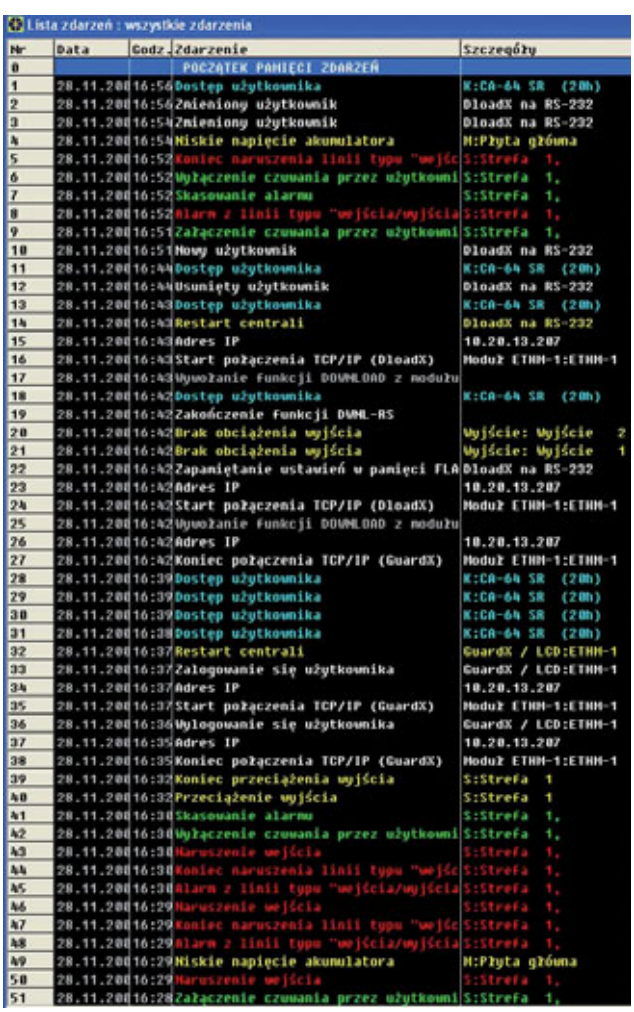
stanu pojedynczego systemu alarmowego i umożliwia wizualizację stanu chronionego obiektu na monitorze komputera, informowanie o bieżących sytuacjach alarmowych, odczyt pamięci zdarzeń centrali alarmowej, sygnalizowanie alarmu dźwiękiem i na ekranie monitora, tworzenie i edycję użytkowników systemu i ich uprawnień. Program jest przeznaczony dla operatora systemu. Na rys. 3 przedstawiono okno podglądu zdarzeń.

Program DloadX służy do programowania i zarządzania systemem SSWiN. Za jego pomocą administrator lub serwisant systemu może zmieniać parametry centrali i przyłączonych modułów dodatkowych. To funkcja podstawowa. Oprócz niej dostępne są inne: podglądanie zdarzeń, odczyt pamięci zdarzeń, wizualizacja stanu systemu alarmowego na monitorze komputera.

Aplikacja składa się z wielu niezależnych okien. Wygodną funkcją programu jest okno z widokiem manipulatora z wyświetlaczem, na którym możemy zobaczyć, jaki jest bieżący stan systemu. Wygląd kilku okien wchodzących w skład całej aplikacji pokazano na rys. 4.

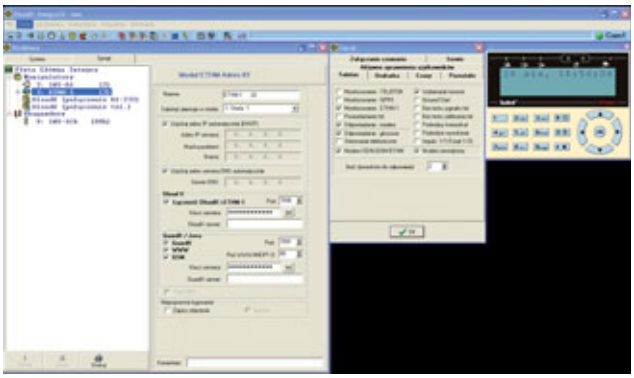
2.1.3. Stacja PC z przeglądarką WWW

Połączenie ze stacją PC z przeglądarką WWW jest wygodne dlatego, że nie wymaga od klienta zainstalowania żadnego dodatkowego oprogramowania – wystarcza przeglądarka WWW. W przeglądarce generowany jest wygląd manipulatora, a za jego pośrednictwem możliwa jest interakcja z systemem alarmowym. Wadą rozwiązania jest to, że ma wyłącznie takie funkcje jak zwykły manipulator, a także konieczność korzystania z wirtualnej klawiatury numerycznej oraz emulatora dwuwierszowego wyświetlacza.


Lista zdarzeń : wszystkie zdarzenia

Nr	Data	Godz.	Zdarzenie	Szczegóły
0			POCZĄTEK PAMIĘCI ZDARZEŃ	
1	28.11.200	16:56	Dostęp użytkownika	K:CA-64 SR (20h)
2	28.11.200	16:56	Zmieniony użytkownik	DloadX na RS-232
3	28.11.200	16:54	Zmieniony użytkownik	DloadX na RS-232
4	28.11.200	16:54	Niskie napięcie akumulatora	M:Płyta główna
5	28.11.200	16:52	Koniec naruszenia linii typu "wejśc	S:Strefa 1,
6	28.11.200	16:52	Wyłączenie czuwania przez użytkowni	S:Strefa 1,
7	28.11.200	16:52	Skasowanie alarmu	S:Strefa 1,
8	28.11.200	16:52	Alarm z linii typu "wejścia/wyjścia	S:Strefa 1,
9	28.11.200	16:51	Załączenie czuwania przez użytkowni	S:Strefa 1,
10	28.11.200	16:51	Nowy użytkownik	DloadX na RS-232
11	28.11.200	16:44	Dostęp użytkownika	K:CA-64 SR (20h)
12	28.11.200	16:44	Usunięty użytkownik	DloadX na RS-232
13	28.11.200	16:43	Dostęp użytkownika	K:CA-64 SR (20h)
14	28.11.200	16:43	Restart centrali	DloadX na RS-232
15	28.11.200	16:43	Adres IP	10.20.13.207
16	28.11.200	16:43	Start połączenia TCP/IP (DloadX)	Moduł ETHM-1:ETHM-1
17	28.11.200	16:43	Wywołanie funkcji DOWNLOAD z modułu	
18	28.11.200	16:42	Dostęp użytkownika	K:CA-64 SR (20h)
19	28.11.200	16:42	Zakończenie funkcji DWNL-RS	
20	28.11.200	16:42	Brak obciążenia wyjścia	Wyjście: Wyjście 2
21	28.11.200	16:42	Brak obciążenia wyjścia	Wyjście: Wyjście 1
22	28.11.200	16:42	Zapamiętanie ustawień w pamięci FLA	DloadX na RS-232
23	28.11.200	16:42	Adres IP	10.20.13.207
24	28.11.200	16:42	Start połączenia TCP/IP (DloadX)	Moduł ETHM-1:ETHM-1
25	28.11.200	16:42	Wywołanie funkcji DOWNLOAD z modułu	
26	28.11.200	16:42	Adres IP	10.20.13.207
27	28.11.200	16:42	Koniec połączenia TCP/IP (GuardX)	Moduł ETHM-1:ETHM-1
28	28.11.200	16:39	Dostęp użytkownika	K:CA-64 SR (20h)
29	28.11.200	16:39	Dostęp użytkownika	K:CA-64 SR (20h)
30	28.11.200	16:39	Dostęp użytkownika	K:CA-64 SR (20h)
31	28.11.200	16:38	Dostęp użytkownika	K:CA-64 SR (20h)
32	28.11.200	16:37	Restart centrali	GuardX / LCD:ETHM-1
33	28.11.200	16:37	Zalogowanie się użytkownika	GuardX / LCD:ETHM-1
34	28.11.200	16:37	Adres IP	10.20.13.207
35	28.11.200	16:37	Start połączenia TCP/IP (GuardX)	Moduł ETHM-1:ETHM-1
36	28.11.200	16:36	Wylogowanie się użytkownika	GuardX / LCD:ETHM-1
37	28.11.200	16:35	Adres IP	10.20.13.207
38	28.11.200	16:35	Koniec połączenia TCP/IP (GuardX)	Moduł ETHM-1:ETHM-1
39	28.11.200	16:32	Koniec przeciążenia wyjścia	S:Strefa 1
40	28.11.200	16:32	Przeciążenie wyjścia	S:Strefa 1
41	28.11.200	16:30	Skasowanie alarmu	S:Strefa 1,
42	28.11.200	16:30	Wyłączenie czuwania przez użytkowni	S:Strefa 1,
43	28.11.200	16:30	Naruszenie wejścia	S:Strefa 1,
44	28.11.200	16:30	Koniec naruszenia linii typu "wejśc	S:Strefa 1,
45	28.11.200	16:30	Alarm z linii typu "wejścia/wyjścia	S:Strefa 1,
46	28.11.200	16:29	Naruszenie wejścia	S:Strefa 1,
47	28.11.200	16:29	Koniec naruszenia linii typu "wejśc	S:Strefa 1,
48	28.11.200	16:29	Alarm z linii typu "wejścia/wyjścia	S:Strefa 1,
49	28.11.200	16:29	Niskie napięcie akumulatora	M:Płyta główna
50	28.11.200	16:27	Naruszenie wejścia	S:Strefa 1,
51	28.11.200	16:28	Załączenie czuwania przez użytkowni	S:Strefa 1,

Rys. 3. Lista zdarzeń w programie GuardX [8]

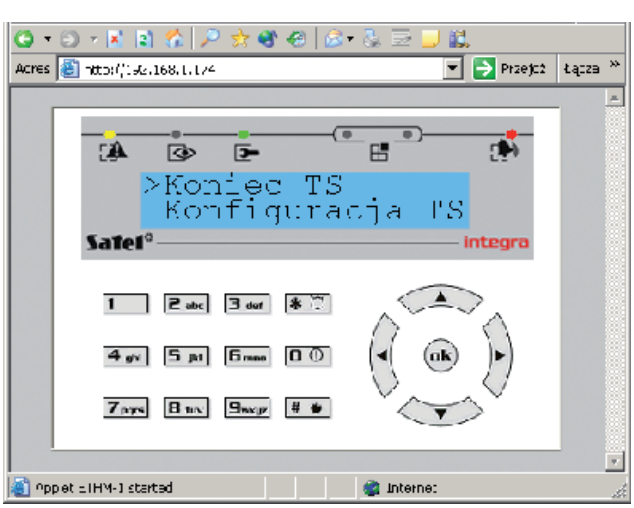

Rys. 4. Okna programu DloadX [opracowanie własne]

Aplikacja, której wygląd pokazano na rys. 5, jest napisana w formie apletu w kodzie JAVA. Rozwiązanie takie nadaje się do monitorowania i administrowania pojedynczym systemem alarmowym i nie ma zbyt wielu możliwości. Bezpieczeństwo przesyłania danych przez sieć Ethernet jest zapewnione dzięki kodowaniu transmisji przez moduł ETHM-1 z wykorzystaniem zaawansowanego algorytmu ze 192-bitowym kluczem.

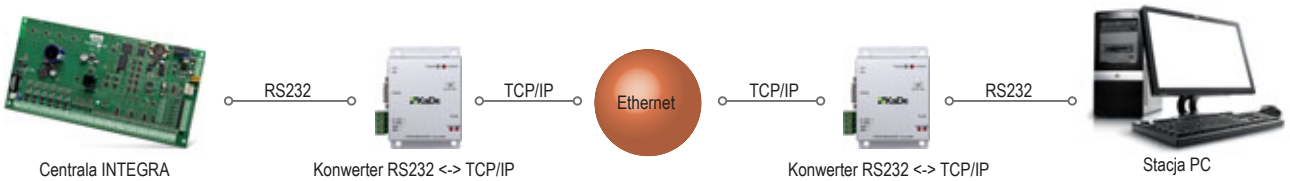
2.1.4. Terminal GSM z aplikacją do komunikacji z modułem ETHM-1

Połączenie z centralą monitorującą jest realizowane z wykorzystaniem transmisji TCP/IP przez Ethernet oraz przez sieć komórkową. Terminal GSM musi zapewniać obsługę aplikacji JAVA. Wygoda korzystania z programu zależy od modelu terminalu i rozdzielczości jego wyświetlacza. Takie rozwiązanie jest przydatne wtedy, gdy nie ma możliwości skorzystania z aplikacji napisanej na platformę PC lub gdy trzeba odbierać komunikaty przy jednoczesnej prostej interakcji z systemem. Zaawansowana konfiguracja sprawiłaby dość dużo kłopotu ze względu na klawiaturę numeryczną terminalu oraz ograniczone możliwości wyświetlacza.

Podobnie jak w poprzednim przypadku bezpieczeństwo transmisji jest chronione dzięki szyfrowaniu za pomocą 192-bitowego klucza.



Rys. 5. Emulacja manipulatora w przeglądarce WWW [4]



Rys. 6. Schemat połączenia przy użyci konwerterów RS232 <-> TCP/IP [opracowanie własne]

2.2. Połączenie z wykorzystaniem konwertera RS232 – TCP/IP

Do zarządzania systemem SSWiN przez sieć Ethernet można wykorzystać parę konwerterów RS232 – TCP/IP. W takiej konfiguracji jeden z konwerterów zostaje przyłączony poprzez interfejs RS232 bezpośrednio do płyty głównej systemu alarmowego oraz poprzez łącze sieciowe do sieci komputerowej. Drugi z konwerterów zostaje przyłączony do sieci Ethernet w miejscu, w którym będzie odbywać się monitorowanie systemu, a jego wyjście RS232 – do stacji monitorującej.

Konwertery te pozwalają przyłączyć urządzenia z interfejsem RS232 do sieci Ethernetowej. Tworzą one przezroczysty kanał pomiędzy portem szeregowym RS232 a protokołem TCP/IP. Dzięki temu urządzenie przyłączone do portu szeregowego jest widoczne w sieci lokalnej. Konwertery mogą pracować w sieci TCP/IP, wykorzystując transmisję poprzez protokół TCP lub UDP. W trybie TCP konwerter po jednej stronie łącza pracuje w trybie serwera, natomiast konwerter po drugiej stronie – w trybie klienta. W trybie UDP obydwa konwertery są równorzędne.

Konwertery zazwyczaj nie mają wbudowanych mechanizmów zabezpieczających transmisję danych poprzez sieć Ethernet. Gdy konwertery komunikują się ze sobą przez Internet, konieczne jest zastosowanie dodatkowych środków bezpieczeństwa, takich jak szyfrowanie danych.

Urządzenia szyfrujące transmisję TCP/IP mogą być komputerami z zainstalowanym odpowiednim oprogramowaniem. Mogą to być również inne urządzenia z zaimplementowaną funkcją szyfrowania transmisji.

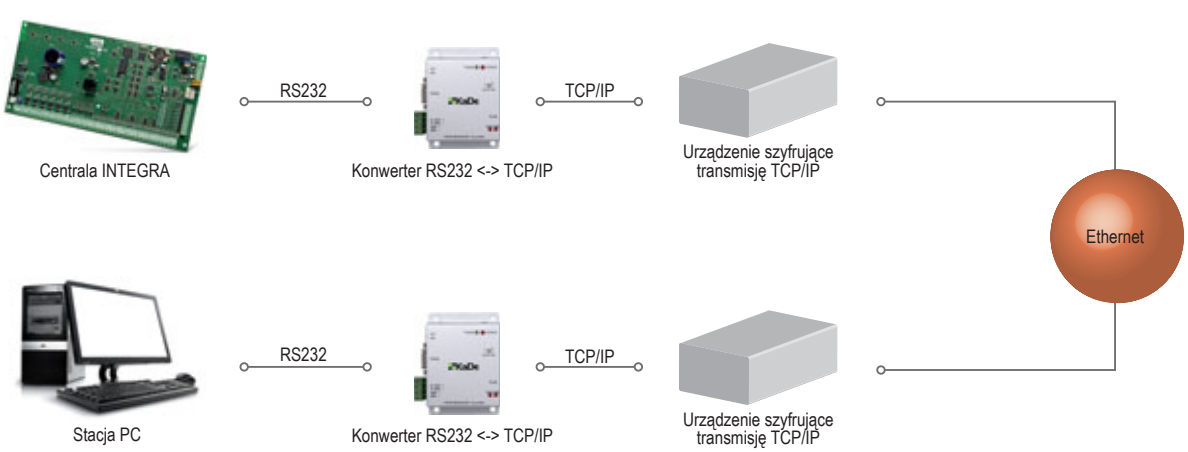
2.3. Połączenie z wykorzystaniem modułu INT-RS

Połączenie z wykorzystaniem modułu INT-RS daje dużo większe możliwości niż te przedstawione dotychczas. To dlatego, że moduł ten został stworzony z myślą o rozbudowie systemu SSWiN oraz jego integracji z innymi systemami. Wcześniej pokazane rozwiązania służące do łączności są ograniczone do konkretnego sprzętu oraz dedykowanego oprogramowania. Moduł INT-RS konwertuje dane przesyłane magistralą manipulatorów na standard magistrali szeregowej RS232 i może być wykorzystany do następujących zastosowań:

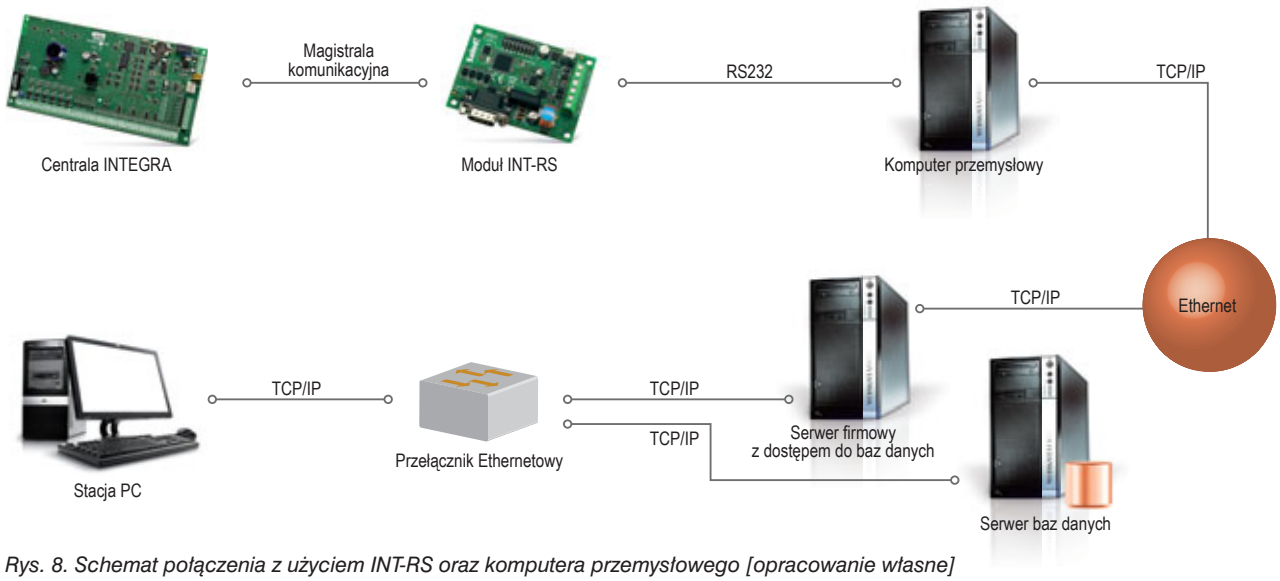
– podłączenie komputera z zainstalowanym programem GuardX,
– monitorowanie zdarzeń za pośrednictwem specjalistycznych modułów zewnętrznych innych producentów (moduł wysyła komunikaty o zaistniałych zdarzeniach),
– obsługa centrali alarmowej za pomocą oprogramowania innego niż oferowane przez firmę SATEL (to zastosowanie jest przeznaczone dla firm zajmujących się integracją systemów obiektowych).

Dzięki otwartemu protokołowi wymiany danych możliwe jest napisanie oprogramowania realizującego niemalże każdą funkcję. Przykład wykorzystania modułu do rozbudowy systemu pokazany jest na rys. 8. Do portu RS232 modułu został podłączony komputer przemysłowy z oprogramowaniem, którego głównym zadaniem jest interpretacja informacji przychodzących z modułu, a także zwrotne wysyłanie odpowiednio przygotowanych komunikatów. Drugim medium konfiguracyjnym komputera jest port sieci Ethernet, z którego otrzymuje on informacje przekazywane systemowi alarmowemu. Zainstalowane oprogramowanie może:

– wyłącznie pośredniczyć między portem RS232 a siecią Ethernet, ograniczając się do translacji komunikatów wymienianych między tymi mediami,
– zarządzać systemem SSWiN oraz monitorować go i przekazywać informacje dalej, innemu systemowi, a w razie potrzeby pobierać dane z zewnątrz w celu zaktualizowania ich w systemie alarmowym.



Rys. 7. Schemat szyfrowanego połączenia przy użyciu konwerterów RS232 <-> TCP/IP [opracowanie własne]



Rys. 8. Schemat połączenia z użyciem INT-RS oraz komputera przemysłowego [opracowanie własne]

Komputer na rysunku, nazwany serwerem firmowym z dostępem do baz danych, może na przykład zawierać zainstalowany system klasy ERP z informacjami o użytkownikach mających prawo do dostępu do wybranych pomieszczeń. Dzięki temu dane mogą być pobierane bezpośrednio z tego systemu i aktualizowane za pomocą wcześniej omówionego komputera przemysłowego. Dużą zaletą takiego rozwiązania jest brak konieczności „ręcznego" aktualizowania informacji dotyczących bieżących uprawnień użytkowników w systemie alarmowym. W serwerze baz danych zainstalowana jest baza danych wykorzystywanych przez system ERP. Stacja PC jest w tym rozwiązaniu komputerem monitorującym i zarządzającym, za pośrednictwem którego można wydać polecenie natychmiastowego zsynchronizowania informacji pobieranych z systemu ERP do systemu SSWiN.

Przy projektowaniu integracji systemów należy zwrócić szczególną uwagę na poziom bezpieczeństwa. W powyższym przykładzie system SSWiN został zintegrowany z systemem ERP. Systemy te mają całkowicie odmienne funkcje oraz wymagania związane z bezpieczeństwem. W przypadku systemu alarmowego zaklasyfikowanie go według norm będzie zależało od jego najniżej sklasyfikowanego elementu.

Dzięki zastosowaniu komputerów po obu stronach łącza mamy możliwość instalacji oprogramowania szyfrującego, które posłuży do zestawienia bezpiecznego kanału transmisyjnego poprzez sieć Ethernet.

3. Podsumowanie

W niniejszej części przedstawiono różne możliwości łączności systemu do zarządzania i monitoringu z centralą alarmową poprzez sieć Ethernet. Zwrócono przy tym szczególną uwagę na aspekty bezpieczeństwa transmisji danych poprzez tę sieć. Analiza przedstawionych rozwiązań umożliwiła podjęcie decyzji o wykorzystaniu urządzeń SSWiN, które można zintegrować z innymi systemami i które mają otwarty protokół wymiany danych, do dalszych badań.

W części trzeciej zostaną przedstawione kolejne etapy tworzenia aplikacji integrującej, umożliwiającej zarządzanie wieloma systemami alarmowymi. Jej praktyczne zastosowanie w systemach ERP pozwoli na integrację zarządzania zasobami firmy z zarządzaniem wykorzystywanymi systemami 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

Systemy alarmowe **Satel**

czujka temperatury
TD-1

TD-1
czujka temperatury

Zadaniem TD-1 jest wykrywanie różnych zagrożeń związanych z temperaturą

– przekroczenia ustalonych progów temperatury lub szybkości jej zmiany. Dzięki możliwości programowania jej parametrów i czytelnemu wyświetlaczowi **idealnie nadaje się do nadzorowania temperatury w szerokim zakresie w obiektach o różnym przeznaczeniu.**

Czujka TD-1 zapewnia skuteczną sygnalizację awarii urządzeń chłodniczych, lub grzewczych.

Więcej informacji na
www.satel.pl
www.mieszkajbezpiecznie.pl

Satel®

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

Historia z przyszłością

Opowiadanie nie-*science-fiction*

(część 4)

Grzegorz Ćwiek

Po prawie dwu lunargodzinach przerwy zebranie sił prewencyjnych międzygałaktycznej straży pożarnej rozpoczyna ostatnią sesję dyskusji. W powietrzu czuć napięcie i atmosferę wyczekiwania na decyzje. Na krok naprzód. Wszyscy zgromadzeni wiedzą, że już dłużej nie można zwlekać, a działania zaradcze muszą zostać podjęte natychmiast. Problemy istnieją przecież już od dawna, a straty są coraz większe. Kłopoty z komunikacją, utrata sprzętu i utrudnienia w akcjach ratowniczych – wszystko to może zakończyć się katastrofą. Myśli zgromadzonych na sali skupione są wokół pytania: „Czy tym razem znajdziemy rozwiązanie?”

Z głośników rozległ się głos generała: – *Wszyscy daliśmy się uśpić, panowie! Poddaliśmy się wszechogarniającej bierności i marnej jakości naszych przemyśleń i decyzji. Dopiero ten młody kapitan otworzył nam oczy i pokazał naszą próżność. Zapomnieliśmy o regułach, które kierowały poczynaniami ludzkości od prawieków. Odrzuciliśmy zasadę „dobrej roboty”, odrzuciliśmy wszystko, co dobre w tradycyjnym podejściu do problemów. Uznaliśmy, że skoro nasi dziadowie popełnili wiele błędów, które doprowadziły do katastrofy, my będziemy działali wyłącznie według nowych reguł. To był błąd! Zapominając o naszym dziedzictwie, wiedzy naszych przodków, historii i fundamentach naszej kultury technicznej i sztuki inżynierskiej, wpadliśmy w wielką pułapkę, z której – mam nadzieję – uda nam się wydostać. Jeszcze dzisiaj wystąpię do Rady Mędrców o pomoc w wyjściu z naszej tragicznej sytuacji. Za chwilę będziemy głosowali w tej sprawie i proszę wszystkich o poparcie.*

Zamierzam wystąpić o zwiększenie środków na wzmocnienie i rozbudowę infrastruktury bezpieczeństwa. Owe środki przeznaczymy natychmiast na rozbudowę naszych kanałów teleportacyjnych i wzorem naszych przodków, twórców Integrala IP, zdublujemy wszystkie nasze kanały komunikacyjne. Wybudujemy nowe bazy serwisowe i techniczne, a nowe stacje ratunkowe zdecentralizujemy wzorem sieci kratowych Schracka. Sporą część środków przeznaczymy na reedukację naszych specjalistów i wprowadzimy częstsze, cykliczne szkolenia dla wszystkich naszych podopiecznych. To oczywiście działania długofalowe, które nie rozwiążą naszych bieżących problemów, ale, moi drodzy, dość już łatania dziur i pozostawiania prawdziwych problemów kolejnym pokoleniom. Nie będziemy postępować jak nasi przodkowie w 2011 roku, którzy budowali pękające po tygodniu autostrady i niesprawne instalacje, aby zaoszczędzić groszy!

Właśnie dlatego najpierw mówię o planach strategicznych, długofalowych i zamierzam wdrożyć je od razu – równolegle z działaniami doraźnymi, bieżącymi.

Głos z sali: – *A te bieżące, panie generale? Jakie będą te bieżące działania? Przecież ponosimy coraz większe straty…*

– Rozmawiałem z wieloma z was podczas przerwy i wiem, że przedstawiona przez kapitana koncepcja dawnego systemu Integral IP pobudziła waszą wyobraźnię i przez wielu – choć dotyczy konkretnego rozwiązania technicznego sprzed 200 lat – została przyjęta z nadzieją jako podstawa do dalszych rozważań o naszych problemach. Wiem, że wielu z was sądzi – podobnie jak ja – że to doskonały i unikatowy przykład do naśladowania. Powołamy zatem natychmiast rezerwowe grupy techniczno-logistyczne, których zadaniem będzie lepsze zarządzanie dostawami środków ratowniczych. Duże dostawy będziemy dzielić na mniejsze kontyngenty i – tak jak w Integralu – będziemy używać zdublowanych portali przesyłowych. Dziś wykorzystamy istniejące tory transmisji, a kiedy zbudujemy nowe, wykorzystamy je w następnych akcjach ratowniczych. Dzięki temu ryzyko dużych, jednorazowych strat zostanie wyeliminowane.

Nasze roboty gaśnicze SUG-REX 10 będziemy dostarczać w modułach. Przyszło mi to do głowy, kiedy dowiedziałem się o topologii Integrala IP. Budowa modułowa naszych maszyn, podobnie jak w centralach Schracka, umożliwi ich szybki montaż i demontaż – nawet na miejscu akcji ratowniczej. Elementy składowe przesyłać będziemy z różnych baz tak, by uniknąć ryzyka strat w przypadku anomalii elektromagnetycznych. Zamierzam zarządzić utworzenie większej liczby baz i magazynów lokalnych – na wzór sieci partnerów Schracka w XXI wieku. Będziemy mogli wysyłać części naszych droidów z dowolnego miejsca Nowego Świata! Składaniem naszych droidów zajmą się na miejscu nasi międzygalaktyczni strażacy, którzy i tak już teraz czasem zmuszeni są do takich czynności. Doszkolimy ich i poprawimy ich sprawność. Podzielimy kompetencje. Będziemy naśladować dobrą starą szkołę inżynierską rodem z XXI wieku. Czy są jakieś pytania, uwagi?

Głos z sali: *– Napędy plazmotronowo-refrakcyjne naszych robotów montowane są jako oddzielne, wymienne moduły. Można je szybko wymieniać i zastępować innymi. Działania te będą błyskawiczne i nie utrudnią żadnych akcji. To świetny pomysł!*

Głos z sali: *– Przesyłanie elementów robotów i droidów czy zaopatrzenia to świetny pomysł. Ale co z przypadkami specjalnymi, gdy akcja będzie wymagać specjalnie zaprogramowanych algorytmów działania maszyn? Jeśli będziemy programować system ratunkowy na miejscu, szansa na sukces będzie większa. Jeśli natomiast elementy będą pochodziły z różnych baz, programowanie będzie wymagało specjalistycznej wiedzy. Teleportowanie specjalistów w przypadku każdej akcji będzie niemożliwe! Jak zamierzamy temu zaradzić?*

– Generale, proszę pozwolić mi odpowiedzieć na to pytanie.

– Udzielam panu głosu, kapitanie.

– W tym przypadku posłużymy się znowu logiką Integrala IP. Jak już powiedziałem wcześniej, inżynierowie mogli programować ten system z dowolnego miejsca na ziemi, posługując się bardzo bezpiecznym protokołem i oprogramowaniem przeznaczonym do tego celu. Jako jedyni na ówczesnym rynku mieli nawet stosowne certyfikaty. Przecież my także mamy możliwość wysyłania informacji na odległość.

Głos z sali: *– To bez sensu! Przecież nasza komunikacja jest właśnie zakłócana i nie da się tego zrobić.*

– Co pan na to, kapitanie?

– Oczywiście możemy temu zaradzić. Będziemy ładować zdalne oprogramowanie za pomocą hiperimpulsów! To także jest bezpieczne rozwiązanie, choć faktycznie jeszcze nie było używane w tym celu. Musimy je przetestować. W Schracku można było stosować wiele różnych łącz komunikacyjnych – od przewodów miedzianych poprzez światłowody, Internet i Intranet do połączeń radiowych. My wykorzystamy hiperimpulsy. Jeżeli pan generał pozwoli, jeszcze dzisiaj zlecę próby wykorzystania takiego rozwiązania.

– Oczywiście, kapitanie. Proszę działać szybko. Szkoda czasu.

Głos z sali: *– A co ze strefami skażonymi, kapitanie? Tam nikt nie posklada droidów, a analizatory widmowe muszą być dostarczone i uruchomione.*

– Zastosujemy inną metodę rodem z Integrala. Ówczesny system zasysający Schrack ASD535 działał w taki sposób, że we wnętrzu zagrożonego pomieszczenia instalowano zestaw rurek, przez które powietrze było zasysane i wydostawane z pomieszczenia. Skład powietrza był analizowany już poza pomieszczeniem. Rozwiązanie to było niezwykle skuteczne i było w stanie wykryć nawet promile zanieczyszczeń! Nasze analizatory widmowe są bardzo drogie i ponosimy z ich powodu ogromne straty. Mamy jednak ich starsze wersje i w wielu jednostkach lokalnych są one dostępne. W przeciwieństwie do analizatorów widmowych mają one budowę modułową i są mniejsze. Z pewnością przebiją się przez śmieci z ogona komety Novarion G-0 czy burze elektromagnetyczne. Mogą one pobrać próbki powietrza i przetransportować je na zewnątrz w bezpieczne miejsce. Dopiero w nim użyjemy analizatorów widmowych! Możemy wybrać dowolne bezpieczne miejsce na gwiazdostradzie.

Głos z sali: *– Zatem mamy rozwiązania najbardziej palących problemów. Aż dziw bierze, że do tej pory nikt z nas na to nie wpadł. Ale to tylko działania bieżące. Ważne dla naszego bezpieczeństwa, ale bieżące. Jeżeli jednak nie uda nam się otrzymać więcej środków i wdrożyć planu generała – czyli rozbudować infrastruktury, zbudować więcej baz serwisowych i poprawić jakości naszych działań – nie damy sobie rady w przyszłości!*

– Panowie, usiądźmy i przygotujmy się do głosowania. Daje wam moje słowo, słowo generała międzygalaktycznej straży pożarnej, że jeżeli poprzecie moje propozycje w dzisiejszym głosowaniu, zrobię wszystko, co w mojej mocy, żeby zdobyć środki na nasze cele.

– Yyy… Panie generale…

– Dlaczego pan szepcze, kapitanie?

– Nie wspomniał pan jednak o korporacjach z XXI wieku. O tym, o czym rozmawialiśmy w przerwie zebrania… O firmie Schrack Seconet, o tym co stało się z innymi systemami w roku…

– Przemyślałem to. Uważam, że niepotrzebne są dodatkowe informacje i mówienie o całym tym zamieszaniu. Pan wie, jak ludzie mogliby zareagować. Są tu przeciwnicy i zwolennicy różnych metod działania. Na co dzień w naszej branży za dużo jest polityki, a za mało porządnej i uczciwej pracy. I tak jestem zaskoczony, że wszyscy tak spokojnie, a nawet entuzjastycznie przyjęli wiadomość, że nasz plan ratunkowy oprzemy na logice systemu z XXI wieku. Dostatecznie wiele razy padła tu nazwa Integral IP i ci, którzy mogli mieć coś przeciwko niemu, już dawno zaprotestowaliby. Trudno jednak protestować, bo dla nas jest to naprawdę idealne rozwiązanie. To ciekawe, ale i oczywiste, że dobrze przemyślany pomysł potrafi przetrwać burze i zarówno polityczne, jak i elektromagnetyczne zawirowania… Teraz cieszmy się, że ta wiedza przetrwała tak długo, że nawet dzisiaj jest przydatna i aktualna, a przede wszystkim nadal ratuje życie i zdrowie ludzkie. Inne rasy i galaktyki też z tego skorzystają. To kwestia czasu…

Grzegorz Ćwiek
Schrack Seconet Polska

UCS 6000
Oddymianie pod kontrolą
(część 1)

Mariusz Sowiński

Trudno dziś wyobrazić sobie kompletną ofertę dotyczącą systemów przeciwpożarowych bez systemu odprowadzania ciepła i dymu (potocznie zwanego oddymianiem). Skuteczny system oddymiania powinien: przeciwdziałać przedostawaniu się dymu i gorących gazów pożarowych poza strefę objętą pożarem, umożliwiać ewakuację ludzi z zagrożonej strefy, ułatwiać przeprowadzenie skutecznej akcji ratowniczo-gaśniczej poprzez zapewnienie odpowiedniej widzialności oraz zmniejszać straty materialne spowodowane działaniem dymu i wysokiej temperatury. Zrealizowanie powyższych postulatów jest możliwe w przypadku zastosowania nowej centrali sterującej UCS 6000 (UCS – Uniwersalna Centrala Sterująca) firmy Polon-Alfa. W pierwszej części artykułu zostaną przedstawione funkcje i parametry techniczne central systemu 6000, w drugiej natomiast przykładowe opcje sterowania oddymianiem realizowane przez UCS

Wprowadzenie

Uniwersalna centrala sterująca UCS 6000 jest modułowym urządzeniem mikroprocesorowym, które łączy w sobie funkcje centrali sygnalizacji pożarowej i uniwersalnego sterownika oddymiania z funkcją dziennego przewietrzania. Centrala jest przeznaczona do uruchamiania urządzeń przeciwpożarowych służących do oddymiania grawitacyjnego i mechanicznego (klapy oddymiające, klapy odcinające) i umożliwia:

– wykrywanie pożaru (zadymienia),
– uruchamianie automatyczne lub ręczne urządzeń przeciwpożarowych instalowanych w systemach oddymiania,
– akustyczne i optyczne sygnalizowanie stanów pracy zewnętrznych urządzeń sterowanych (alarm, uszkodzenie),
– automatyczną kontrolę zadziałania urządzeń przeciwpożarowych i wykonawczych (siłowniki, elektromagnesy, wentylatory itp.) systemu oddymiania,
– automatyczną kontrolę własnych układów i obwodów centrali,
– przekazywanie podstawowych informacji o alarmie, uszkodzeniu, stanie urządzeń przeciwpożarowych i wykonawczych systemom nadrzędnym (np. systemowi POLON 4000, systemowi IGNIS 1000 lub innym).

Centrala UCS 6000 może pracować indywidualnie jako jedno- lub wielostrefowy uniwersalny sterownik oddymiania lub w adresowalnych liniach/pętlach dozorowych central sygnalizacji pożarowej systemu POLON 4000.

Modułowość – dopasowanie do potrzeb

Ze względu na budowę modułową uniwersalna centrala sterująca UCS 6000 może występować w wielu konfiguracjach (tabele 1 i 2), tworząc system central UCS 6000 o wydajności prądowej wyjść sterujących od 4 A do 64 A (osiem niezależnych stref oddymiania po 8 A).

W zależności od potrzeb dotyczących sterowania i zasilania urządzeń przeciwpożarowych centrala może być wyposażona w następujące moduły funkcjonalne i akumulatory (rys. 1):

– **MGS-60 4A, 8A** (moduł głównego sterownika zawierający jeden moduł MGL 4 A lub 8 A):
  » nadzorowana linia wejściowa przyjmująca sygnał alarmu z zewnętrznej centrali sygnalizacji pożarowej,
  » linia zasilająca czujnik deszczu i (lub) wiatru (0,5 A/24 V),
  » linia przyjmująca sygnał z czujnika deszczu i (lub) wiatru,
  » przekaźnik alarmu PKA – nadzorowana ciągłość toru (1 A/24 V),
  » przekaźnik uszkodzenia PKU (1 A/24 V);
– **MZU-60** (moduł zasilania uniwersalnego 16 A/24 V):
  » przekaźnik uszkodzenia zasilania PKUZ (1 A/24 V),
  » nadzorowane wyjście do zasilania urządzeń zewnętrznych (0,5 A/24 V);
– **MGL-60 4 A, 8 A** (moduł grupowo-liniowy, wersja 4 A lub 8 A):
  » konwencjonalna linia dozorowa (czujki szeregu 40),
  » konwencjonalna linia ręcznych przycisków oddymiania (przyciski szeregu PO-6X),
  » nadzorowane wyjście główne uniwersalnego zastosowania do sterowania urządzeniami przeciwpożarowymi i zasilania ich (siłowniki i napędy klap przeciwpożarowych, elektromagnesy oddzieleń przeciwpożarowych itp.) – 4 A/24 V lub 8 A/24 V,
  » linie kontrolne stanu przełączników krańcowych urządzeń przeciwpożarowych sterowanych i zasilanych przez wyjście główne,
  » linie przyjmujące sygnały z przycisków przewietrzających (OTWÓRZ, ZAMKNIJ).
– **MPW-60** (moduł przekaźników wysokonapięciowych):
  » 2 programowalne przekaźniki wysokonapięciowe PK1 i PK2 (5 A/230 V),
  » 2 nadzorowane, programowalne linie kontrolne LK1 i LK2 (24 V);
– **MKA-60** (moduł komunikacji adresowalnej) – do włączenia do adresowalnej linii dozorowej systemu POLON 4000;
– **MPD-60** (moduł przekaźników dodatkowych):
  » 2 nadzorowane, programowalne przekaźniki PK1 i PK2 (1 A/24 V),
  » 2 nadzorowane, programowalne linie kontrolne LK1 i LK2 (24 V);
– **SP-150-27.5PLA** – moduł zasilacza 150 W (5 A);
– **SP-240-27.5PLA** – moduł zasilacza 240 W (10 A);
– **SP-500-27.5PLA** – moduł zasilacza 500 W (20 A) w dwóch wykonaniach: SP1 i SP2;
– akumulator 7,2–9 Ah (dwie sztuki przypadające na każdy moduł zasilania uniwersalnego).

Powyższe wyposażenie centrali, łącznie z akumulatorami, mieści się w obudowie małej – o wymiarach 400×400×160 dla łącznej obciążalności wyjść do 16 A – oraz dużej – o wymiarach 1150×630×190 dla łącznej obciążalności wyjść od 32 A do 64 A.

Wyzwalanie – detekcja zagrożeń

Do detekcji pożaru służy konwencjonalna linia dozorowa z czujkami szeregu 40. Można zaprogramować wariant

Wer.	MGS 60		MGL 60		MZU 60	MPW 60	Zasilacz			AKU	MPD 60	MKA 60	Prąd
	4 A	8 A	4 A	8 A	16 A	szt.	SP 150	SP 240	SP1 500	szt.	szt.	szt.	
1	1	-	-	-	1	-	1	-	-	2	1 *	1 *	4 A (1x4 A)
2	-	1	-	-	1	-	-	1	-	2	1 *	1 *	8 A (1x8 A)
3	-	1	-	1	1	-	-	-	1	2	1 *	1 *	16 A (2x8 A)
4	1	-	-	-	1	1 *	1	-	-	2	1 *	1 *	4 A (1x4 A)
5	-	1	-	-	1	1 *	-	1	-	2	1 *	1 *	8 A (1x8 A)
6	1	-	1	-	1	-	-	1	-	2	1 *	1 *	8 A (2x4 A)

Tab. 1. Obudowa do 16 A (– opcja dodatkowa)*

alarmowania ze wstępnym kasowaniem (60 s) w celu eliminacji przypadkowych zadziałań.

W sekcji sterowania oddymianiem uruchomienie urządzeń przeciwpożarowych jest możliwe w wyniku:

– zadziałania czujki na konwencjonalnej linii dozorowej,
– zadziałania ręcznego przycisku oddymiania,
– pojawienia się sygnału alarmu z zewnętrznej centrali sygnalizacji pożarowej, np. IGNIS 1000,
– otrzymania rozkazu z centrali systemu POLON 4000.

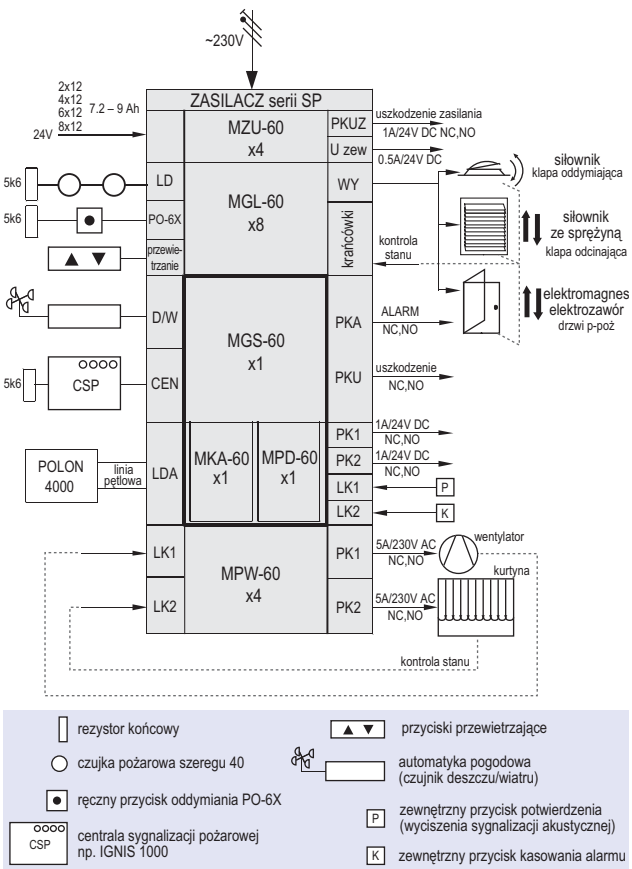
W przypadku otrzymania sygnału inicjującego następuje uruchomienie procedury oddymiania zgodnie z zaprogramowanym scenariuszem pożarowym danego obiektu. Blokowane są przyciski przewietrzania, ignorowane są sygnały z czujnika deszczu i (lub) wiatru.

Funkcjonalne i elastyczne sterowanie

Ze względu na swoją uniwersalność centrale UCS 6000 umożliwiają praktycznie każdy rodzaj sterowania za pomocą wyjść sterujących (moduł MGL-60), które można zaprogramować do pracy w trzech trybach.

TRYB PRACY 1 jest przeznaczony dla urządzeń przeciwpożarowych wyposażonych w dwukierunkowe, sterowane dwulub trzyprzewodowo i zasilane napięciem stałym 24 V siłowniki (napędy) elektryczne.

TRYB PRACY 2 jest przeznaczony dla urządzeń przeciwpożarowych wyposażonych w siłowniki (napędy) elektryczne (24 V) ze sprężyną. Siłowniki tego rodzaju są stosowane



Rys. 1. Schemat blokowo-funkcjonalny systemu oddymiania z centralą UCS 6000

Wer.	MGS 60		MGL 60		MZU 60	MPW 60	Zasilacz			AKU	MPD 60	MKA 60	Prąd
	4 A	8 A	4 A	8 A	16 A	szt.			SP2 500	szt.	szt.	szt.	
7	-	1	-	3	2	-	-	-	2	4	1 *	1 *	32 A (4x8 A)
8	-	1	-	5	3	-	-	-	3	6	1 *	1 *	48 A (6x8 A)
9	-	1	-	7	4	-	-	-	4	8	1 *	1 *	64 A (8x8 A)
10	-	1	-	4	3	3 *	-	-	3	6	1 *	1 *	40 A (5x8 A)
11	-	1	-	6	4	4 *	-	-	4	8	1 *	1 *	56 A (7x8 A)
12	-	1	-	3	2	1	-	-	2	4	1 *	1 *	32 A (4x8 A)
13	-	1	-	3	2	2	-	-	2	4	1 *	1 *	32 A (4x8 A)
14	-	1	-	5	3	1	-	-	3	6	1 *	1 *	48 A (6x8 A)
15	-	1	-	5	3	2	-	-	3	6	1 *	1 *	48 A (6x8 A)
16	-	1	-	5	3	3	-	-	3	6	1 *	1 *	48 A (6x8 A)
17	-	1	-	7	4	1	-	-	4	8	1 *	1 *	64 A (8x8 A)
18	-	1	-	7	4	2	-	-	4	8	1 *	1 *	64 A (8x8 A)
19	-	1	-	7	4	3	-	-	4	8	1 *	1 *	64 A (8x8 A)
20	-	1	-	7	4	4	-	-	4	8	1 *	1 *	64 A (8x8 A)

Tab. 2. Obudowa od 32 A do 64 A (– opcja dodatkowa)*

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

w odcinających klapach przeciwpożarowych. Siłownik ze sprężyną powrotną ustawia klapę w położenie pracy (pozycja *DOZÓR*), napinając w tym samym czasie sprężynę powrotną. Po zatrzymaniu siłownik jest cały czas pod napięciem do chwili, gdy zostanie przerwane zasilanie (w wyniku alarmu lub uszkodzenia). Energia zmagazynowana w naciągniętej sprężynie automatycznie ustawia klapę w położeniu bezpiecznym, czyli *ALARM*.

TRYB PRACY 3 jest przeznaczony dla urządzeń przeciwpożarowych sterowanych przerwą prądową lub impulsem prądowym, wyposażonych w elektromagnesy lub elektrozawory zasilane napięciem stałym 24 V.

Uzależnienia czasowe sterowań

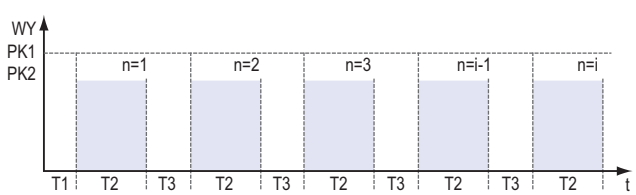
Możliwe jest niezależne zaprogramowanie uzależnień czasowych (rys. 2) dla każdego wyjścia sterującego (T1 – czas opóźnienia wysterowania, T2 – czas wysterowania, T3 – czas przerwy wysterowania), a dodatkowo dla wyjścia sterującego WY w trybie pracy 3 (MGL-60) oraz dla przekaźników wysokonapięciowych (MPW-60) i niskonapięciowych (MPD-60) także liczby impulsów sterujących N.

Programowane są również czasy kontroli zadziałania wyjść na liniach kontrolnych skojarzonych z wyjściami sterującymi WY oraz przekaźnikami PK1 i PK2 (rys. 3):

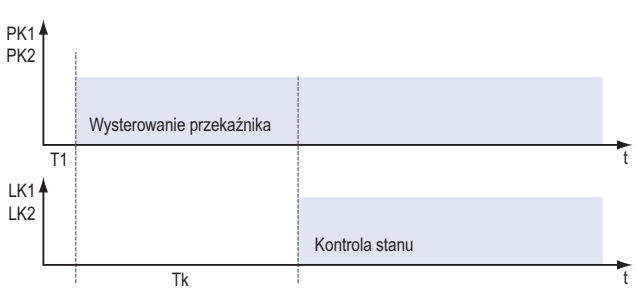
– Tk1 – czas kontroli zadziałania linii kontrolnej LK1,
– Tk2 – czas kontroli zadziałania linii kontrolnej LK2.

Przewietrzanie

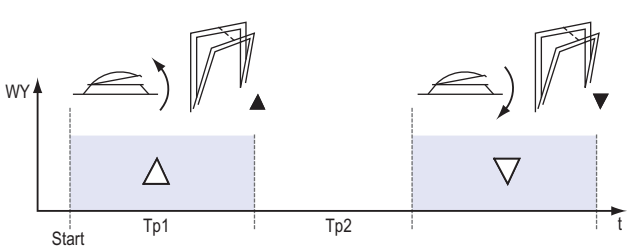
W przypadku zastosowania UCS 6000 do sterowania procesem przewietrzania danego obiektu dla każdego wyjścia sterującego niezależnie programowane są czasy przewietrzania (rys. 4):



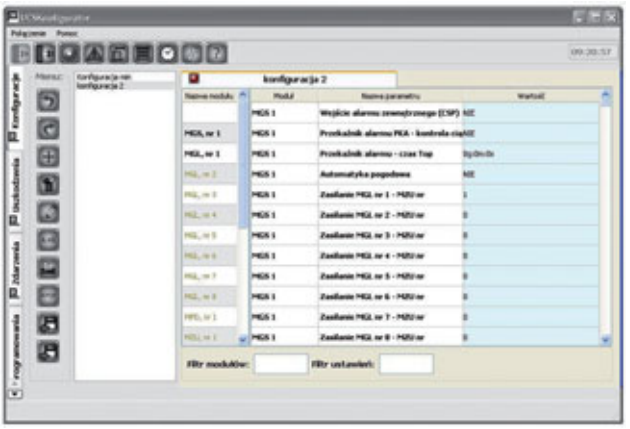
Rys. 2. Sterowanie czasowe WY, PK1 i PK2



Rys. 3. Kontrola zadziałania wyjść PK1 i PK2



Rys. 4. Przewietrzanie



Rys. 5. Aplikacja UCSKonfigurator – okno konfiguracji modułów

– Tp1 – czas otwierania okien lub klap wentylacyjnych,
– Tp2 – czas automatycznego zamknięcia okien lub klap wentylacyjnych.

Konfigurowanie i programowanie

Konfigurowanie i programowanie parametrów pracy central UCS 6000 przeprowadza się za pomocą dedykowanej aplikacji komputerowej ***UCSKonfigurator*** (rys. 5) działającej pod kontrolą systemu Windows. Centralę UCS podłącza się poprzez port USB do komputera PC. Do połączenia komputera z centralą należy użyć kabla USB zakończonego z jednej strony wtyczkami typu A, z drugiej typu B. Przy większych odległościach komputera od centrali należy użyć dodatkowo tzw. aktywnego przedłużacza kabla USB. Po podłączeniu port USB centrali UCS 6000 powinien być widziany w komputerze jako USB Serial Port (COMxxx). Przy uruchomieniu aplikacji *UCSKonfigurator* należy wybrać do połączenia widziany przez system operacyjny komputera port COMxxx.

Aplikacja umożliwia:

– konfigurowanie parametrów pracy modułów, w tym zapis konfiguracji w pliku, odczyt konfiguracji z pliku, zapis konfiguracji w pliku PDF, wydruk konfiguracji;
– odczyt uszkodzeń poszczególnych modułów, w tym zapis w pliku PDF i wydruk listy uszkodzeń;
– odczyt pamiętnika zdarzeń, w tym zapis w pliku PDF i wydruk listy zdarzeń;
– odczyt wersji oprogramowania modułów, w tym zapis w pliku PDF i wydruk wersji oprogramowania;
– ustawienie i odczyt daty i czasu systemowego centrali;
– skorzystanie z pomocy kontekstowej programu.

W kolejnej części artykułu zostaną przedstawione przykłady zastosowania systemu sterowania oddymianiem z wykorzystaniem central systemu UCS 6000.

Mariusz Sowiński
POLON-ALFA

BOSCH
Technologia bliżej nas

Bosch Security Systems to pierwszy producent w Polsce z pełną gamą certyfikowanych produktów: kontrola dostępu, systemy SAP i DSO.
Oferta naszych rozwiązań jest w pełni dostosowana do wymogów określonych polskim prawem. Firma Robert Bosch Sp. z o.o. jako pierwsza spełniła surowe wymogi normy EN 54 w odniesieniu do systemów sygnalizacji pożarowej, dźwiękowych systemów ostrzegawczych oraz systemów kontroli dostępu. Świadectwa dopuszczenia CNBOP dla naszych produktów potwierdzają najwyższą jakość oferty Bosch.

Więcej informacji na stronie internetowej: **www.boschsecurity.pl**

Czujki firmy Bosch

na miarę XXI wieku

Bezpieczeństwo życia i mienia zależy od właściwego doboru detektorów

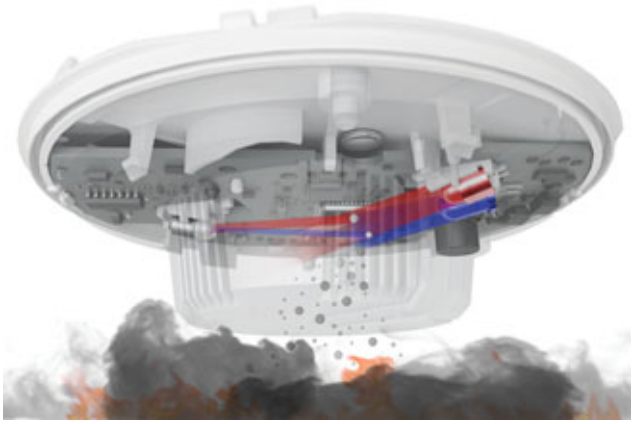
Monika Kołodziejczyk

Wszyscy boimy się pożaru. Instalacje systemów sygnalizacji pożarowej mają za zadanie zabezpieczyć nas przed skutkami tego żywiołu. Stawka jest wysoka, ponieważ w grę wchodzi życie i mienie. Skuteczna ochrona obiektu przed pożarem i ewakuacja ludzi są zależne od prędkości jego wykrycia i organizacji procesów ostrzegania, gaszenia i oddymiania. Warto zatem wybrać taki system, który umożliwi sprawne przeprowadzenie akcji ewakuacyjnej, jak również będzie niezawodny i odporny na fałszywe alarmy

Czujki pożarowe to podstawowy element systemu sygnalizacji pożarowej, który ma decydujący wpływ na czas wykrycia pożaru. Niewątpliwie najtrudniejszym zadaniem dla projektanta systemu sygnalizacji pożarowej jest właściwy dobór detektorów, który ma zapewnić jak najwyższą efektywność systemu. Należy wziąć pod uwagę różne czynniki, które mogą mieć wpływ na charakter i szybkość rozprzestrzeniania się pożaru. W projekcie systemu należy znaleźć równowagę pomiędzy czułością a odpornością na fałszywe alarmy.

Chcąc zastosować dany sensor w określonym pomieszczeniu, należy wziąć pod uwagę prawdopodobne źródła pożaru, poczynić założenia dotyczące rozwoju pożaru w początkowej fazie i przeanalizować ewentualne źródła fałszywych alarmów. Należy również pamiętać o uwzględnieniu środowiska panującego w danym pomieszczeniu, bowiem może ono mieć istotny wpływ na zdolność czujki do wykrycia pożaru, m.in. wysokość pomieszczenia i jego przeznaczenie. Głównym kryterium doboru czujek będą jednak materiały znajdujące się w zabezpieczanym obszarze. Analizując skład materiałów znajdujących się w pomieszczeniu, można określić czynniki, które mogą towarzyszyć pożarowi. Należą do nich rodzaj pożaru (płomieniowy albo bezpłomieniowy), wielkość cząsteczek dymu, gęstość dymu, jego intensywność, prędkość wzrostu temperatury, występujące gazy i ich rodzaj (np. tlenek węgla, wodór, tlenek azotu).

W celu ułatwienia doboru czujek pod kątem wyżej wymienionych czynników klasyfikuje się je na podstawie wyników pożarów testowych TF (ang. *Test Fire*) przeprowadzanych zgodnie z normami. W komorze pożarów testowych sprawdza się, jak wykrywają określony rodzaj pożaru. Badania są przeprowadzane w specjalnie do tego przystosowanych laboratoriach, w których symulowane są warunki jak najbliższe rzeczywistym, występującym podczas pożaru. Badania te wykazują, że punktowe czujki dymu są w stanie wykryć różne rodzaje pożarów w zależności od sensorów, w jakie są wyposażone, i zasady ich działania. Do badania wybierane są losowo po cztery czujki tego samego rodzaju lub typu. Na podstawie ich działania w trakcie różnych pożarów testowych określany jest stopień ich przydatności. Dana czujka zostaje sklasyfikowana jako bardzo przydatna (A), przydatna (B), jeszcze przydatna (C) albo nieprzydatna (N) w przypadku danego typu pożaru.



Przydatność czujek w różnych typach pożarów

Tabela 1 przedstawia charakterystykę pożarów opracowaną na podstawie norm EN-54-7 (od TF2 do TF5) i dodatkowo na podstawie ISO/TS 7240-9:2006 (TF1, TF6, TF7, TF8, TF9).

Pożar TF 1 odpowiada warunkom, jakie panują w początkowej fazie palenia się drewna czy papieru – jest płomień i szybki przyrost temperatury; dym zazwyczaj występuje, ale jest niewidoczny (tzw. pożar płomieniowy). Jest to pożar wykrywany przez czujki termiczne lub wielosensorowe, np. optyczno-termiczne. Ostatnio pozytywne wyniki w TF1 mają również wybrane czujki optyczne.

Pożar TF2 odpowiada powolnemu tleniu się drewna czy rozkładowi termicznemu przewodów elektrycznych. Jest to typ pożaru bezpłomieniowego, któremu towarzyszy niewielki wzrost temperatury i duża ilość dymu.

Pożar TF3 odpowiada tleniu się materiałów włókienniczych, dywanów, wykładzin. Towarzyszy mu dym, niewielki wzrost temperatury i znaczna ilość CO.

Pożar TF4 występuje w momencie spalania się materiałów wykończeniowych z tworzyw sztucznych. Charakterystyczny jest szybki przyrost temperatury i bardzo ciemny dym.

Pożar TF5 pojawia się w momencie spalania paliw płynnych (np. ropy naftowej). W przypadku takiego pożaru obserwujemy szybki wzrost temperatury i ciemny dym.

Pożar TF6 to na przykład spalanie się spirytusu albo niektórych rozpuszczalników nie wydzielających dymu. Jest to typowy pożar płomieniowy, któremu towarzyszy szybki wzrost temperatury i brak dymu. Badaniu przydatności podczas takiego

Test	TF1	TF2	TF3	TF4	TF5	TF6	TF7	TF8	TF9
Rodzaj pożaru (paliwo)	Płomieniowe spalanie celulozy	Szybki rozkład termiczny piroliza (drewna)	Pożar tlący (bawełna)	Płomieniowe spalanie tworzywa (poliuretan)	Spalanie cieczy wydzielającej dym (n-heptan)	Spalanie cieczy nie wydzielającej dymu (alkohol etylowy)	Powolne tlenie się drewna	Spalanie cieczy wydzielającej dym bez ciepła (dekalina)	Tlenie się bawełny złożonej
Wzrost temperatury	Silny	Do pominięcia	Do pominięcia	Silny	Silny	Do pominięcia	Do pominięcia	Do pominięcia	Do pominięcia
Prędkość wznoszenia	Duża	Mała	Bardzo mała	Duża	Duża	Duża	Mała	Mała	Mała
Dym	Jest	Jest	Jest	Jest	Jest	Nie ma	Jest	Jest	Jest
Widmo dymu	Przeważnie niewidoczne	Przeważnie widoczne	Przeważnie niewidoczne	Częściowo niewidoczne	Przeważnie niewidoczne	Nie ma	Przeważnie widoczne	Przeważnie widoczne	Przeważnie widoczne
Część widzialna dymu	Ciemna	Jasna, silnie rozpraszająca	Jasna, silnie rozpraszająca	Bardzo ciemna	Bardzo ciemna	Nie ma	Jasna, silnie rozpraszająca	Ciemna	Ciemna
Występowanie CO	Nie ma	Znaczne	Duże	Słabe	Słabe	Nie ma	Znaczne	Bardzo słabe	Duże

Tab. 1. Charakterystyka pożarów testowych

pożaru jak TF6 poddawane są czujki termiczne lub wielosensorowe.

Pożar TF7 to na przykład powolne tlenie się drewna. Jest podobny do pożaru TF2. Test TF7 przeprowadza się w USA. Czujki, których przydatność została w tym teście potwierdzona, są przeznaczone głównie do pomieszczeń mieszkalnych. Wynika to z tego, iż badania przeprowadzane są analogicznie do testów TF2 (komora jest jednak obniżona do trzech metrów).

Pożar TF8 jest taki jak w przypadku spalania dekaliny. W trakcie spalania wydziela się ciemny dym o niewielkiej prędkości wznoszenia się i następuje bardzo niewielki przyrost temperatury. W podobny sposób mogą spalać się niektóre pasty, tworzywa sztuczne, żywica. W TF8 testowane są najczęściej czujki wielosensorowe.

Pożar TF9 to na przykład tlenie się złożonej bawełny. Jest to pożar, w trakcie którego emitowane są duże ilości tlenku węgla, a wzrost temperatury jest niewielki.

Nowy trend na rynku – czujki optyczne i wielosensorowe z pozytywnymi wynikami testu TF9

Do niedawna czujki dostępne na rynku polskim nie były poddawane przez producentów testowi TF9. Norma EN-54 nie definiuje bowiem tego pożaru testowego. Postęp technologiczny i rosnące wymagania wobec systemów sygnalizacji pożaru, w tym czujek, a także globalizacja, wymusiły jednak na producentach posiadanie w ofercie jak największej liczby różnych czujek, również czujek, które uzyskały pozytywny wynik w TF9. Najlepszym dowodem na to są czujki Boscha.

W ostatnim czasie wszystkie czujki serii FAP4 20 zostały dodatkowo przebadane na wykrywanie pożarów TF9. Mimo założenia, że pożar testowy TF9 wykrywany jest przez dedykowany sensor chemiczny w czujce, badaniu takiemu zostały poddane również czujki optyczne i optyczno-termiczne. Badanie zostało przeprowadzone zgodnie z wytycznymi opisanymi w normie ISO 7240-9. Wszystkie wymienione w tabeli 2 czujki uzyskały wynik pozytywny, zatem mogą być stosowane w miejscach, gdzie wymagane są takie parametry. Na rynku systemów pożarowych do rzadkości należą pozytywne wyniki testu TF9 w przypadku czujek optycznych.

Czujka z pozytywnymi wynikami testu TF9 jest przeznaczona do wykorzystania w miejscach, w których może wystąpić pożar bezpłomieniowy z dużym stężeniem tlenku węgla, tj. w pomieszczeniach, w których znajdują się materiały włókiennicze, dywany, wykładziny. Należy jednak pamiętać, żeby czujek optycznych i optyczno-termicznych, które sprawdziły się podczas testu TF9, nie stosować w pomieszczeniach, w których pożar tlący może rozwijać się bez dopływu świeżego powietrza, a także w przypadku detekcji schłodzonego dymu.

W pożarach testowych przetestowano całą serię czujek FAP 420 firmy Bosch. Seria FAP-420 została powiększona o trzy produkty z nowym podwójnym czujnikiem optycznym firmy Bosch: FAP-DO 420 (detektor dymu z podwójnym czujnikiem optycznym), FAP-DOT 420 (detektor z podwójnym sensorem optycznym i sensorem termicznym) i FAP-DOTC 420 (detektor z podwójnym sensorem optycznym, sensorem termicznym i chemicznym). W efekcie liczba detektorów wchodzących w skład tej

Model	Czujka	Opis	Zastosowanie	Pożary testowe							
				TF1	TF2	TF3	TF4	TF5	TF6	TF8	TF9
FAH-T 420	Czujka termiczna, nadmiarowo-różnicowa	Precyzyjne wykrycie zmian temperatury. Czujka alarmuje po przekroczeniu określonego progu temperatury otoczenia oraz w przypadku szybkiego wzrost temperatury w pomieszczeniu.	Obiekty, w których może pojawić się szybko rozprzestrzeniający się ogień	✓			✓	✓	✓		
FAP-O 420	Optyczna czujka dymu	Idealne rozwiązanie dla obszarów wymagających wczesnego ostrzeżenia o sytuacji pożarowej	Obiekty, w których może wystąpić pożar bezpłomieniowy		✓	✓	✓	✓		✓	✓
FAP-DO 420	Dwusensorowa czujka optyczna	Dualny sensor optyczny wykorzystujący różne długości fali zapewnia niezawodną detekcję różnych typów pożarów.	Obiekty, w których może dojść do pożarów różnych typów	✓	✓	✓	✓	✓		✓	✓
FAP-OT 420	Multisensorowa czujka optyczno-termiczna	Kombinacja zasady pomiaru rozproszenia światła oraz pomiaru wzrostu temperatury	Obiekty, w których może pojawić się szybko rozprzestrzeniający się ogień, ale także pożary bezpłomieniowe	✓	✓	✓	✓	✓	✓	✓	✓
FAP-DOT 420	Dwusensorowa czujka optyczno-termiczna	Dualny sensor optyczny wykorzystujący różne długości fali optycznej oraz sensor termiczny zapewniają wczesne wykrycie pożaru w każdych warunkach.	Obiekty, w których mogą być różne warunki	✓	✓	✓	✓	✓	✓	✓	✓
FAP-OTC 420	Multisensorowa czujka optyczno-termiczno-chemiczna	Kombinacja zasady pomiaru rozproszenia światła, pomiaru wzrostu temperatury, jak również wykrycie produktów spalania	Obiekty, w których tlenek węgla może zagrozić życiu ludzi	✓	✓	✓	✓	✓	✓	✓	✓
FAP-DOTC 420	Multisensorowa czujka optyczno-termiczno-chemiczna	Kombinacja dualnego sensora optycznego, sensora termicznego i sensora chemicznego umożliwia najszybszą detekcję pożaru w każdych, nawet najtrudniejszych warunkach.	Obiekty, w których mogą być trudne warunki i w których tlenek węgla może zagrozić życiu ludzi	✓	✓	✓	✓	✓	✓	✓	✓

Tab. 2. Wyniki pożarów testowych TF dla czujek serii 420

serii wzrosła do siedmiu. Nowe czujki pożarowe Bosch serii 420 zapewniają jeszcze szybsze wykrywanie pożaru niż dotychczas i mniej fałszywych alarmów. Wskutek tego seria ta gwarantuje najwyższą niezawodność we wszystkich warunkach i środowiskach. Podobnie jak dotychczasowe czujki z tej serii, nowe czujki są wyposażone w technologię ISP firmy Bosch, co tworzy wyjątkowe połączenie precyzyjnej technologii Dual Ray i zaawansowanego algorytmu wykrywania pożaru. Wszystkie czujki zostały przebadane pod kątem przydatności w zależności od charakterystyki pożarowej. Wyniki tych testów są przedstawione w tabeli 2.

FAH-T 420 to czujka termiczna, która jest wyposażona w termistor pełniący rolę detektora termicznego w sieci rezystancyjnej (jest to element, który przez konwerter analogowo-cyfrowy w regularnych odstępach czasu dokonuje pomiaru napięcia zależnego od temperatury). Detektor wywołuje alarm w przypadku przekroczenia temperatury 54°C lub 69°C (czujki nadmiarowe) lub w przypadku wzrostu temperatury o określoną wartość w danym czasie (czujki różnicowe). Czujki FAHT420 są przeznaczone do wykrywania pożarów płomieniowych. Można więc zastosować je w miejscach zagrożonych ogniem, który może szybko się rozprzestrzeniać (np. w kuchniach, kotłowniach, pralniach). Czujka termiczna nie powinna być stosowana w miejscach, w których istnieje ryzyko pożaru bezpłomieniowego, któremu towarzyszy niewielki wzrost temperatury.

FAP-O 420 jest czujką optyczną, w której sensor optyczny działa na zasadzie pomiaru rozproszenia światła. Dioda LED wysyła światło do komory pomiarowej, gdzie zostaje ono pochłonięte przez strukturę labiryntową. Podczas pożaru unoszący się dym dostaje się do komory pomiarowej. Światło jest rozpraszane przez cząsteczki dymu. Rozproszone światło pada na fotodiody, które zamieniają informacje o ilości światła na proporcjonalny sygnał elektryczny. Jest to klasyczna czujka optyczna, która nadaje się do wykrywania pożarów bezpłomieniowych. Miejsca zabezpieczane przez tę czujkę nie powinny być narażone na działanie czynników wywołujących fałszywe alarmy, takich jak kurz, pył czy para wodna. Czujka nadaje się na przykład do zabezpieczania biur, przestrzeni międzystropowych i międzypodłogowych, pokoi pielęgniarek, gabinetów lekarskich.

FAP-DO 420 to czujka optyczna, więc teoretycznie powinna mieć zastosowanie w obiektach, w których może wystąpić pożar bezpłomieniowy, jednakże dzięki podwójnemu sensorowi optycznemu jest w stanie wykryć również pożary płomieniowe. Podwójny sensor optyczny wykorzystuje dwa zakresy długości fal światła – podczerwień i niebieskie (technologia Dual Ray). Umożliwia to wczesne wykrywanie pożarów dzięki precyzyjnej detekcji niewielkiej ilości dymu. Pozytywne rezultaty uzyskano w testach TF1, TF2,TF3,TF4,TF5,TF8. Wypadła dobrze także w teście TF9. Czujka sprawdzi się w miejscach, gdzie występują zarówno materiały palące się płomieniowo, jak i materiały palące się bezpłomieniowo. Może być zatem zastosowana tam, gdzie może wystąpić pożar cieczy lub płomieniowy pożar drewna. Można ją wykorzystać zamiast czujki jonizacyjnej, jest również bardziej od nich odporna na fałszywe alarmy spowodowane na przykład podmuchem powietrza, wilgocią, pyłem, kurzem, parą wodną czy dymem papierosowym. Ta odporność jest możliwa dzięki konstrukcji czujki – wykorzystuje ona dwa typy fotodiod, podczerwoną i niebieską, i ma w pamięci zapisane charakterystyki około 5000 różnych typów pożarów. Konserwacja tej czujki jest również dużo tańsza niż konserwacja czujki jonizacyjnej. Jeżeli zabezpieczane miejsce nie wymaga czujek wielosensorowych, a ze względu na znajdujące się w nim materiały potrzebna jest czujka z pozytywnym wynikiem TF1 czy TF9, wtedy czujka FAP-DO 420 będzie rozwiązaniem dobrym i tańszym niż czujka optyczno-termiczno-chemiczna. Czujkami FAP-DO 420 można zabezpieczać bary, lobby, pokoje hotelowe, biura, restauracje, łazienki, archiwa, biblioteki itd.

FAP-DOT 420 i **FAP-OT 420** to czujki wielosensorowe, które stanowią kombinację dwu sensorów – optycznego i termicznego lub termicznego z podwójną optyką. Pozwalają na wykrycie większej liczby różnych pożarów niż każdy z detektorów osobno. Te czujki uzyskały pozytywny wynik w testach TF1–TF9. Ponadto są odporne na różnego rodzaju fałszywe alarmy. Należy stosować je w pomieszczeniach, w których znajdują się materiały o różnych charakterystykach spalania oraz w miejscach narażonych na fałszywe alarmy, np. w garażach podziemnych, pokojach hotelowych, laboratoriach, na stacjach benzynowych, w rafineriach, kuchniach, restauracjach, barach.

FAP-OTC 420 i **FAP-DOTC 420** to wielosensorowe czujki Boscha wykorzystujące sensor gazowy i zapewniające zdecydowanie najszybszą reakcję na pożary, w których początkowej fazie pojawiają się różnego rodzaju gazowe produkty spalania, np. dwutlenek węgla, wodór, tlenek azotu. Metoda pomiaru polega na utlenianiu CO i określeniu wielkości prądu generowanego podczas tego procesu. Wielkość sygnału detektora jest proporcjonalna do stężenia gazu. Dzięki kilku sensorom czujki FAP-OTC 420 i FAP-DOTC 420 wykrywają różne rodzaje pożarów. Czujki z sensorem chemicznym służą przede wszystkim do zabezpieczenia miejsc, w których konieczne jest bardzo wczesne wykrycie pożaru – przede wszystkim obiektów, w których na stałe są ludzie, np. hoteli, szpitali, domów opieki społecznej, kin, teatrów, ale również serwerowni, pomieszczeń technicznych itp., ponieważ takie czujki są wykryją przegrzewanie się kabli czy elementów elektrycznych. Znajdą one również zastosowanie w pomieszczeniach narażonych na zakłócenia, w których może być pył, kurz czy para wodna, np. w drukarniach, kuchniach biurowych, tam, gdzie może być para z czajników elektrycznych, w łazienkach, pomieszczeniach przed saunami, w tartakach, fabrykach, stoczniach, na salach operacyjnych.

Podsumowanie

Nowoczesna technologia Dual Ray i ISP to gwarancja bezpieczeństwa zabezpieczanego obiektu i przebywających w nim ludzi. Czujki z serii FAP 420 zadowolą nawet najbardziej wymagających projektantów i umożliwią zabezpieczenie miejsc, w których panują trudne warunki mogące skutkować fałszywymi alarmami.

Nowoczesna technologia Dual Ray i ISP to gwarancja bezpieczeństwa zabezpieczanego obiektu i przebywających w nim ludzi. Czujki z serii FAP 420 zadowolą nawet najbardziej wymagających projektantów i umożliwią zabezpieczenie miejsc, w których panują trudne warunki mogące skutkować fałszywymi alarmami.

Monika Kołodziejczyk
Bosch Security Systems

Zaawansowany System Kontroli Dostępu Wersja PREMIUM

KaDe

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.

Oświetlenie
w systemach nadzoru wizyjnego (część 1)

Agata Majkucińska

Wybierając kamerę do dozoru wizyjnego w ciągu dnia lub w nocy, musimy wziąć pod uwagę kilka czynników wpływających na jakość obrazu. Niniejszy artykuł ma na celu uświadomienie czytelnikom, jak oświetlenie wpływa na obraz i jakie czynniki należy brać pod uwagę przy oświetlaniu obserwowanych obszarów

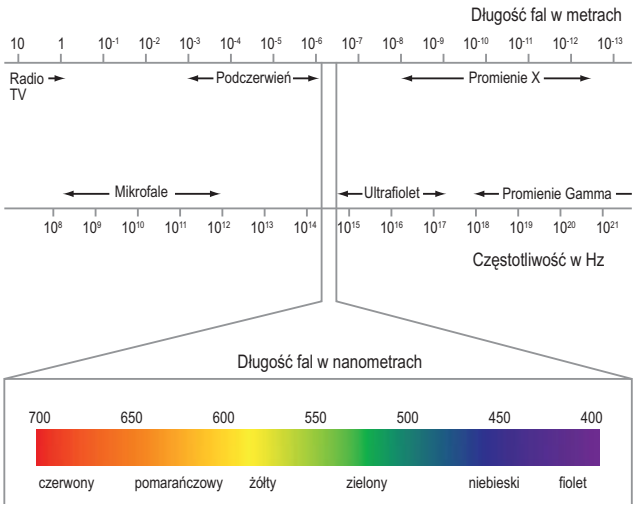
Czym jest światło?

Działanie systemów dozoru wizyjnego zależy głównie od światła. To właśnie światło odbite od obserwowanych przedmiotów sprawia, że obrazy są widoczne zarówno dla ludzkich oczu, jak też dla kamer. Dlatego skuteczność działania dowolnego systemu dozoru wizyjnego zależy nie tylko od kamer i obiektywów, ale również ilości, jakości i rozkładu oświetlenia. Światło jest energią w postaci promieniowania elektromagnetycznego. Długość fali światła określa jego kolor i charakter. Jedynie bardzo wąski zakres długości fal elektromagnetycznych jest widoczny dla ludzkiego oka – od około 400 nm (fiolet) do 700 nm (czerwony). Kamery telewizyjne reagują jednak na światło spoza zakresu widzialnego dla ludzkiego oka, co pozwala wykorzystywać je nie tylko w świetle białym, ale również w świetle mieszczącym się w zakresie bliskiej podczerwieni (od 715 nm do 950 nm) do dozoru nocnego.

Zachowanie światła zmienia się w zależności od materiału lub powierzchni, na którą pada – ulega ono odbiciu, rozproszeniu lub wchłonięciu. Światło odbija się od większości powierzchni. Im jaśniejsza jest powierzchnia, tym więcej światła odbija. Czarne powierzchnie pochłaniają, zaś białe odbijają padające na nie światło widzialne. Światło mieszczące się w zakresie podczerwieni nie zawsze zachowuje się w taki sam sposób jak światło widzialne. Zależy to od rodzaju materiału, na który pada (zob. wykres współczynnika odbicia na następnej stronie).

Czym jest kolor?

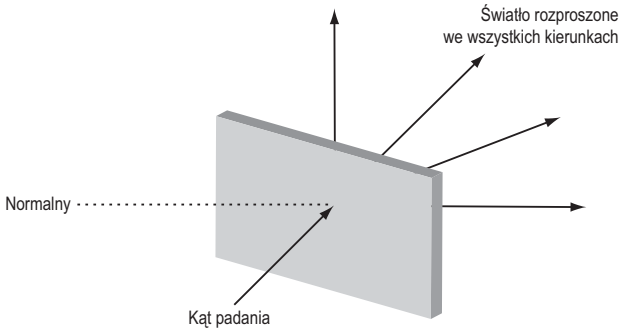
Procesy, dzięki którym człowiek widzi kolory, są bardzo złożone, a podana tu definicja koloru jest z konieczności uproszczona. Monochromatyczne światło widzialne jest interpretowane przez mózg jako barwne w zależności od jego długości fali, przy czym 400 nm odpowiada barwie fioletowej, a 700 nm odpowiada czerwieni. Wszystkie inne widzialne barwy światła monochromatycznego (indygo, niebieski, błękitny, zielony, żółty i pomarańczowy) mieszczą się pomiędzy tymi długościami fal, co można dostrzec, oglądając tęczę. Obserwacja światła zawierającego wszystkie te długości fal daje wrażenie światła białego. Zielony liść wygląda na zielony, ponieważ odbija światło o długości fali odpowiadającej barwie zielonej, obecne w świetle białym. Jeżeli ten sam liść zostanie oświetlony monochromatycznym światłem czerwonym, będzie robił wrażenie czarnego, ponieważ w świetle czerwonym nie występują długości fal odpowiadające zieleni. To samo ma miejsce, gdy kupujemy kolorowe elementy ubioru i podchodzimy do drzwi lub okna, by sprawdzić, jak wyglądają w świetle dziennym. Odcień koloru zmienia się na skutek tego, że rozkład spektralny fal składających się na oświetlenie wewnętrzne jest nieco inny niż w przypadku oświetlenia zewnętrznego. Z dokładnie takimi samymi zależnościami mamy do czynienia w nadzorze wizyjnym. Barwa światła emitowanego przez reflektor wpływa na barwę obrazu widzianego przez kamerę, jak to ma miejsce na przykład w przypadku żółtawego światła lamp sodowych stanowiących oświetlenie uliczne. By zapewnić poprawną reprodukcję barw w obrazie, źródła światła białego muszą zapewnić poprawne oświetlenie, dopasowane spektralnie do widma światła widzialnego. Kolorowe obiekty odbijają światło wybiórczo, to znaczy odbijają tylko wybrane fragmenty widma i wchłaniają resztę. Na przykład czerwony kwiat zawiera cząstki pigmentu, które pochłaniają wszystkie składniki światła białego inne niż czerwone, a światło czerwone jest jedynym odbijanym składnikiem. Fale świetlne, których długość mieści się poniżej granicy widma widzialnego, są określane jako ultrafioletowe (UV). Mogą one powodować poparzenia skóry i dlatego nie są stosowane w wizyjnych systemach dozorowych. Fale świetlne, których długość mieści się powyżej granicy widma widzialnego, są określane jako podczerwone.



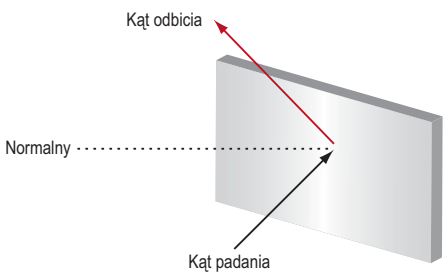
Rys. 1. Długości fal widma widzialnego

Czym jest podczerwień?

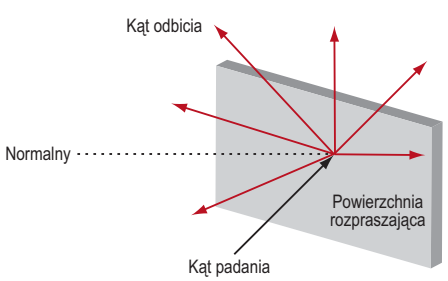
Podczerwień (IR) jest światłem o długościach fal mieszczących się powyżej granicy światła widzialnego. W systemach nadzoru wizyjnego wykorzystywane jest światło podczerwone, którego widmo mieści się w zakresie pomiędzy 700 nm a 1100 nm. Ten zakres jest również znany jako bliska podczerwień (NIR). Jako że kamera może „widzieć" światło podczerwone, które jest niewidoczne dla oka ludzkiego, istnieje wiele form prezentacji tak powstałych obrazów na ekranie komputera. Zwykle pokazywany jest obraz czarno-biały, podobny do postrzeganego przez ludzkie oko w widmie



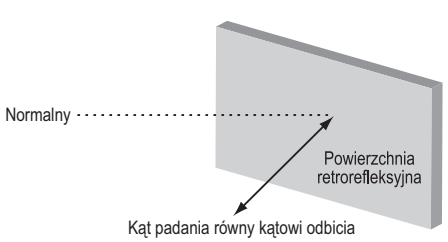
Rys. 2. Dyfuzja światła



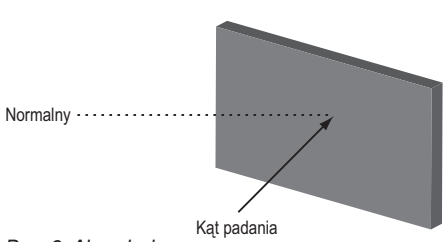
Rys. 3. Odbicie lustrzane



Rys. 4. Odbicie rozproszone



Rys. 5. Odblask



Rys. 6. Absorbcja

widzialnym, lecz pozbawiony barw. Dla uwypuklenia fragmentów obrazu powstałych z użyciem światła podczerwonego stosowane są sztucznie wprowadzone barwy. Czasami znajduje to zastosowanie w zobrazowaniach tworzonych dla potrzeb naukowych. Oświetlenie z użyciem światła podczerwonego jest bardzo przydatne w zastosowaniach wymagających dyskretnego nadzoru lub całkowitego braku oświetlenia światłem widzialnym.

Obrazy kolorowe czy monochromatyczne?

Jeśli chce się wybrać oświetlenie do systemu nocnego nadzoru wizyjnego, należy zastanowić się, czy potrzebny jest obraz kolorowy czy monochromatyczny. Często preferowany jest obraz kolorowy, jednak w takich przypadkach trzeba zwrócić uwagę na zapewnienie poprawnej reprodukcji barw, co można osiągnąć przy użyciu oświetlaczy emitujących światło o odpowiednim składzie widmowym. Rozważmy żółte światło dostarczane przez niskociśnieniowe uliczne lampy sodowe – niczym nie przypomina ono światła białego i w takim przypadku żadna, nawet najlepsza kamera nie jest w stanie zapewnić poprawnej reprodukcji barw. Światło podczerwone powinno być z zasady stosowane we wszystkich przypadkach, w których białe światło byłoby zbyt inwazyjne lub gdy wymagany jest dyskretny nadzór. Podczerwień może być również stosowana jako element dodatkowego oświetlenia rozległych obszarów, na dystansach niedostępnych dla światła białego o podobnej intensywności.

Jaskrawość światła

Jaskrawość światła jest subiektywnym odczuciem wynikającym z intensywności oświetlenia danego obszaru. Intensywne światło może powodować odblaski skutkujące nadmiernym wzrostem kontrastu pomiędzy jasnymi i ciemnymi obszarami w obrębie pola widzenia. Stanowi to większy problem w warunkach nocnych, gdy kontrast pomiędzy jasnymi i ciemnymi obszarami utrudnia ludzkiemu oku (i kamerom wykorzystującym światło podczerwone) dostosowanie się do zmian w jaskrawości.

Światło i powierzchnie

To, w jaki sposób reagujemy na światło, jest zależne od jego składu widmowego i od właściwości powierzchni, na którą to światło pada. Promieniowanie monochromatyczne jest interpretowane przez mózg ludzki jako światło o określonej barwie w zależności od długości fali tego promieniowania. Wrażenie światła białego daje mieszanina wielu rodzajów promieniowania, która ma ciągłe pokrycie widmowe w zakresie od 400 nm (fiolet) do 700 nm (czerwień). W przypadku światła odbitego od jakiejś powierzchni wrażenie barwy oraz intensywności światła jest zależne od rodzaju tej powierzchni, co jest krótko opisane poniżej.

Dyfuzja

Materiał o działaniu dyfuzyjnym rozprasza przechodzące przezeń światło, zmieniając kierunek i intensywność promieniowania w zależności od rodzaju tego materiału.

Odbicie

Kiedy światło pada na jakąś powierzchnię, może ulec odbiciu. Rodzaj powierzchni wpływa na sposób, w jaki światło się odbija. Bardzo szorstkie powierzchnie rozpraszają światło ze względu na drobne nieregularności w ich budowie, a gładkie, takie jak lustro, zapewniają ukierunkowane odbicie.

Odbicie zwierciadlane

Jeżeli powierzchnia odbija światło jak lustro, mówi się, że mamy do czynienia z odbiciem lustrzanym. W przypadku powierzchni lustrzanych kąt padania jest równy kątowi odbicia.

Odbicie rozproszone

Powierzchnie rozpraszające odbijają światło we wszystkich kierunkach ze względu na drobne nieregularności w ich budowie. Na przykład drobnoziarnista faktura odbije światło w różnych kierunkach. Powierzchnie rozpraszające odbijają światło we wszystkich kierunkach w równych proporcjach.

Odblask (retrorefleksja)

Odblask powstaje, gdy powierzchnia odbijająca odbija światło dokładnie w kierunku, z jakiego ono pochodzi. Znaki drogowe i tablice rejestracyjne pojazdów mają powierzchnie retrorefleksyjne.

Poziomy odbicia

Odbicie jest miarą mocy odbitej w stosunku do mocy padającej. Obiekty odbijają światło z różną intensywnością, a część energii, która nie uległa odbiciu, zostaje wchłonięta i zamieniona w ciepło. Obiekty o niskim współczynniku odbicia pochłaniają dużo energii, dlatego np. ściany z cegieł nagrzewają się na skutek oświetlenia światłem słonecznym. Należy pamiętać, że kamera obserwująca daną scenę nie reaguje na światło padające, wykrywane przez światłomierz, tylko na światło odbite przez obiekty znajdujące się na obserwowanym obszarze.

Absorbcja

Każda powierzchnia wchłania część padającego na nią światła. Kolorowe powierzchnie absorbują część światła i odbijają resztę, dlatego mają określoną barwę. Czarna powierzchnia wchłania większą część padającego na nią światła. Energia świetlna jest zwykle zamieniana w ciepło, więc ciemne materiały łatwo się nagrzewają.

Źródła światła

Żarówki (w tym halogenowe)

Żarówki były pierwszymi elektrycznymi źródłami światła skonstruowanymi przez człowieka. Mają one niską wydajność, marnują 90% pobieranej energii, zamieniając ją na ciepło, co powoduje, że silnie się nagrzewają. Żarówki halogenowe mają większą sprawność, ale nadal marnują 85% pobieranej energii, zamieniając ją na ciepło. Żarówki są mało przydatne jako elementy oświetleniowe w wizyjnych systemach dozorowych.

Lampy fluorescencyjne

Wykorzystanie tych lamp w systemach nadzoru wizyjnego jest ograniczone ze względu na efekt pulsowania obrazu wytwarzanego przez kamerę. Lampy te mają przeważnie niski pobór mocy i są przeznaczone głównie do zastosowań wewnątrz pomieszczeń. Mają one duże rozmiary, dlatego trudno jest zbudować oświetlacz pozwalający na skupienie strumienia światła.

Lampy HID (*High Intensity Discharge*)

Są to wydajne źródła światła, które zapewniają poprawną reprodukcję barw i mają dużą żywotność dochodzącą do 12000 godzin. Lampy HID mogą być stosowane w systemach dozorowych, ale ich mankamentem jest długi czas uruchamiania (2–3 minuty). Ponadto nie mogą być natychmiast włączone, nawet w przypadku ich krótkotrwałego wyłączenia.

Lampy wykorzystujące diody LED

Diody elektroluminescencyjne stanowią najszybciej rozwijający się rodzaj oświetlaczy stosowanych w systemach dozoru wizyjnego. Ich sprawność wynosi przeciętnie 80–90% i jest największa w przypadku diod emitujących światło podczerwone.

Oświetlenie LED jest często stosowane w systemach dozoru wizyjnego z powodu swoich zalet, do których należy bardzo niskie zużycie energii, niska temperatura pracy i stabilność widmowa w całym cyklu eksploatacji. W odróżnieniu od tradycyjnych żarówek diody LED są bardzo trwałe, odporne na wibracje, a ich konstrukcja sprawia, że trudno je uszkodzić. Są one również w stanie emitować światło o wymaganej długości fal bez konieczności stosowania filtrów i zaczynają świecić natychmiast po doprowadzeniu zasilania. Ze względu na dużą sprawność diod LED koszty utrzymania systemu dozorowego, w którym są zastosowane, są najniższe w porównaniu z systemami wykorzystującymi inne źródła światła (ich nominalna moc jest relatywnie niska i nie przekracza 100 W dla pojedynczych paneli). Ponadto wyróżnia je długi czas działania dochodzący do 100000 godzin (10 lat). Dla porównania żywotność świetlówek to zazwyczaj maksymalnie 10000 godzin, a żywotność żarówek jest jeszcze mniejsza i nie przekracza 1000 godzin.

Oświetlenie w nadzorze wizyjnym. Dobór długości fal

Światło białe

Światło białe to mieszanka zapewniająca równomierne pokrycie widma w zakresie od 400 nm do 700 nm.

Praktyczne zastosowania światła białego:

- oświetlenie obszaru obserwowanego przez system dozoru wizyjnego,
- oświetlenie o charakterze ogólnym w pomieszczeniach, w których pracują ludzie,
- zmniejszanie przestępczości dzięki oświetleniu obszaru, na którym mogą zdarzyć się włamania,
- może być stosowane z kamerami monochromatycznymi, kolorowymi, pracującymi w trybie dzień/noc.

Podczerwień

Oświetlacze wykorzystujące widmo w zakresie od 715 nm do 730 nm wytwarzają wyraźnie widoczną czerwoną poświatę, podobną do czerwonych świateł ulicznych, co stwarza problemy z ich ukryciem.

Oświetlacze wykorzystujące widmo w zakresie od 815 nm do 850 nm wytwarzają słabo widoczną czerwoną poświatę umożliwiającą ich częściowe ukrycie.

Oświetlacze wykorzystujące widmo w zakresie od 940 do 950 nm są niewidoczne dla ludzkiego oka, dlatego łatwo je ukryć.

Praktyczne zastosowania podczerwieni:

– zapewnienie dyskretnego lub ukrytego oświetlenia w wizyjnych systemach dozorowych,
– zapewnienie intensywnego oświetlenia o dużym zasięgu,
– możliwość współpracy z kamerami monochromatycznymi lub z kamerami działającymi w trybie dzień/noc.

Światło a bezpieczeństwo

Światło białe jest widoczne dla oka ludzkiego. Organizm ludzki zapewnia nam naturalną ochronę przed nadmierną ekspozycją. Tęczówki i powieki zamykają się, by zredukować ilość widzialnego światła absorbowanego przez oko ludzkie. Jeżeli to nie wystarcza, po prostu odwracamy się od źródła światła. Nie możemy zobaczyć światła podczerwonego, dlatego nasze oczy nie mogą automatycznie dostosować się do nadmiernej ekspozycji. Podczerwień wytwarza jednak ciepło, które może być wykorzystane jako miernik bezpieczeństwa. Jeżeli czujemy ciepło bijące od oświetlacza IR, starajmy się nie patrzeć na to źródło światła. Nawet najpotężniejsze oświetlacze IR, wytwarzające wiązki o szerokości dziesięciu stopni, nie stwarzają zagrożenia dla oka ludzkiego, o ile odległość od oświetlacza przekracza dwa metry.

Podsumowanie

Problematyka doboru właściwych urządzeń do nadzoru wizyjnego jest wciąż gorącym tematem, szczególnie dla firm, które jako nowe wchodzą na ten obszar rynku lub zaczynają instalować systemy IP zamiast systemów analogowych, a także, a może przede wszystkim dla użytkowników końcowych, którzy, zdecydowawszy się na implementację takiego systemu, powinni otrzymać to, czego oczekują.

Mam nadzieję, że publikacja przewodnika Axis zawierającego wiele informacji o oświetleniu przyczyni się do lepszego zrozumienia zagadnień z nim związanych i umożliwi właściwy dobór urządzeń, poparty testami i uwzględniający całokształt warunków panujących w miejscu docelowej instalacji, a nie tylko kilka parametrów podanych w karcie katalogowej urządzenia.

Ciąg dalszy w numerze 6 *Zabezpieczeń*.

Opracowała:
Agata Majkucińska
Axis Communications

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

Pronto

MAGICARD

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

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

Specyfikacja techniczna

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

Taśmy

- YMCKO 5 paneli nadruk 300 kart (MA300YMCKO)
- YMCKO 5 paneli nadruk 100 kart (MA100YMCKO)
- Monochromatyczna czarna nadruk 1000 kart (MA1000K-BLACK)
- Monochromatyczna czarna plus overlay nadruk 600 kart (MA600KO)
- Monochromatyczna biała nadruk 1000 kart (MA1000K-WHITE)
- Monochromatyczna czerwona nadruk 1000 kart (MA1000K-RED)
- Monochromatyczna niebieska nadruk 1000 kart (MA1000K-BLUE)
- Monochromatyczna zielona nadruk 1000 kart (MA1000K-GREEN)
- Monochromatyczna złota nadruk 1000 kart (MA1000K-GOLD)
- Monochromatyczna srebrna nadruk 1000 kart (MA1000K-SILVER)

Karty

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

Zestaw czyszczący

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

Dystrybucja:

ACSS ID Systems Sp. z o.o.
ul. Karola Miarki 20C
01-496 Warszawa

tel. 22 832 47 44, faks 22 832 46 44
e-mail: biuro@acss.com.pl
http://www.acss.com.pl

Nowy, ekskluzywny panel wideodomofonowy iKALL

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

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

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

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

iKALL - najważniejsze parametry i funkcje:

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

Dystrybucja:

Alarmnet Sp. j.
ul. Karola Miarki 20c
01-496 Warszawa

tel. 22 663 40 85, faks 22 833 87 95
e-mail: biuro@alarmnet.com.pl
http://www.alarmnet.com.pl

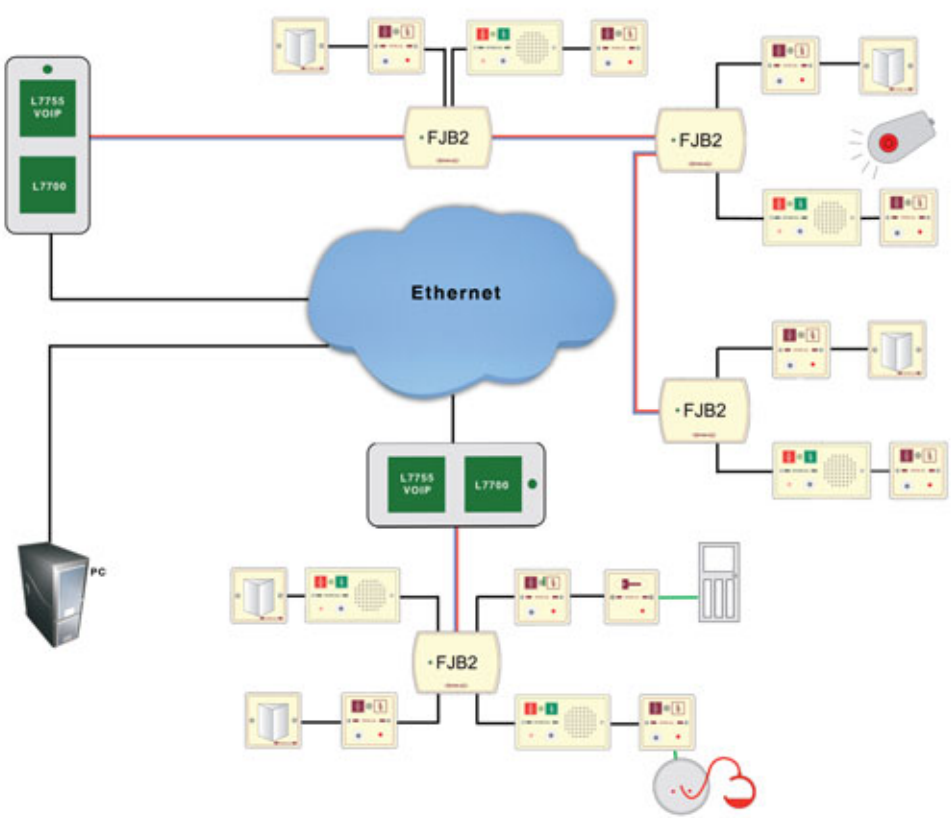
Intercall – szpitalny system przywoławczy

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®

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

Kamera IVC5055VR

CNB TECHNOLOGY Inc.

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

Zaletami kamery są:

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

Właściwości:

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

Dystrybucja: &GDE POLSKA

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

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

Kamera LJL-21S

CNB TECHNOLOGY Inc.

Kamera LJL-21S to zewnętrzna kamera wandaloodporna o wysokiej czułości i wysokiej rozdzielczości 600 TVL, wyróżniająca się estetyczną obudową.

To podstawowa zewnętrzna kamera wandaloodporna. Cechą wyróżniającą jest zastosowanie procesora Monalisa oraz technologii Intelligent IR. Intelligent IR to nowy rodzaj oświetlenia w podczerwieni opracowany przez firmę CNB. Eliminuje on efekt przejaskrawienia i rozmycia obrazu gdy obserwowany obiekt zbliża się do kamery. W standardowym rozwiązaniu jasność świecenia jest stała, dlatego bliskie obiekty są oświetlone tak samo intensywnym światłem jak dalekie, co w praktyce może spowodować prześwietlenie fragmentów obrazu. Intelligent IR steruje jasnością oświetlenia w zależności od odległości obserwowanego obiektu od kamery.

LJL-21S to idealna dodatkowa kamera do wideodomofonów Commax i Abaxo. Niewielka, estetyczna, znakomicie wkomponuje się w miejsce montażu.

Monitory analogowe Commax i Abaxo mają co najmniej jedno wejście, które można wykorzystać do podłączenia kamery telewizji dozorowej.

Zaletami kamery są:

- wbudowany obiektyw o stałej ogniskowej 3,8 mm
- możliwość pracy w dzień i w nocy
- oświetlenie w podczerwieni o zasięgu 15 m
- Intelligent IR – adaptacyjne oświetlenie w podczerwieni

Właściwości:

- kolorowa kamera dzień/noc
- przetwornik 1/3" Sony Super HAD
- wysoka rozdzielczość 600 TVL (kolor), 650 TVL (B/W)
- automatycznie przełącza się w tryb B/W
- czułość 0,1 lx (kolor), 0,00 lx (B/W)
- obiektyw o ogniskowej 3,8 mm
- AGC, BLC, AWB – automatyczne
- obudowa przystosowana do montażu na ścianie albo pod sufitem

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:

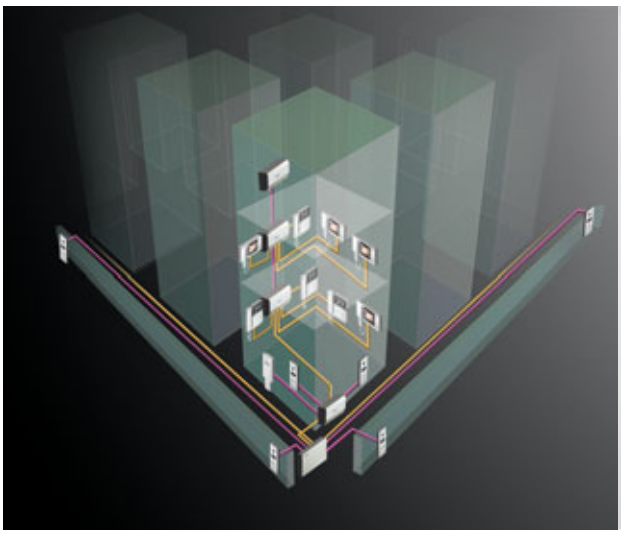
- monitor kolorowy
- wyświetlacz 10,2" Color TFT-LCD 16:9
- standard sygnału wizyjnego PAL/NTSC
- obsługuje dwa wejścia (dwa panele wejściowe)
- obsługa kamer CCTV (wyświetlanie PIP – picture-in-picture)
- wbudowany moduł pamięci 128 obrazów
- możliwość podłączenia dodatkowego monitora
- współpraca z 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

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

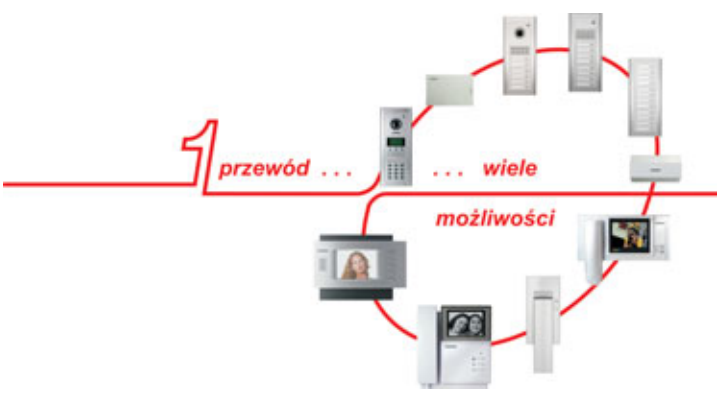
System wieloabonentowy serii 2400

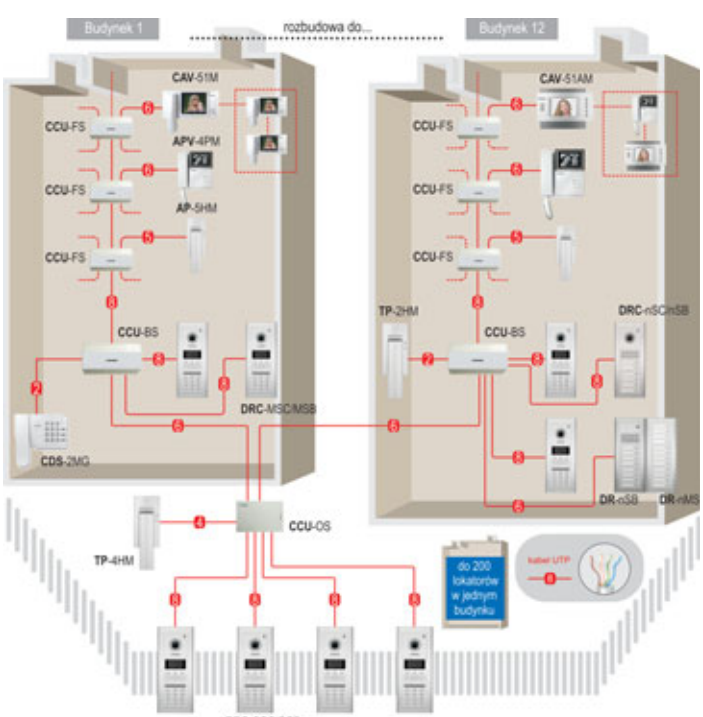


System wieloabonentowy serii 2400 przeznaczony jest do instalacji zarówno w prostych, jak i w bardzo rozbudowanych aplikacjach - maksymalna ilość obsługiwanych przez system abonentów wynosi 2400. U każdego lokatora może być zainstalowane do 3 urządzeń (jedno urządzenie typu Master i dwa urządzenia typu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

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

bibi-Przedszkole
Zestaw do ewidencji czasu pobytu dzieci w przedszkolu

W skład zestawu wchodzą:

- 2 czytniki kart zbliżeniowych bibi-R33
- 2 kolorowe szyldy do czytników
- 1 kontroler bibi-K12
- 1 interfejs do komputera bibi-F21
- obudowa metalowa Pulsar AWO150
- moduł zasilacza ZS12D EBS
- akumulator 7 Ah 12 V
- płyta CD z licencjonowanym oprogramowaniem biPrzedszkole
- 2 klucze do szyfrowania danych w systemie bibiHAK
- instrukcja instalacji systemu

Opcjonalne rozszerzenia zestawu:

- rygiel elektromagnetyczny blokujący drzwi wejściowe
- LEDowy wyświetlacz pokazujący czas kontrolera bibi-W10
- czytnik na biurko ułatwiający wprowadzanie kart do systemu
- podgląd raportu z rejestracjami pobytu dziecka dla rodziców przez przeglądarkę internetową

Ogólna charakterystyka zestawu:

System bibinet może być zaadoptowany do rejestracji czasu pobytu dzieci w przedszkolu. Do tego celu został opracowany zestaw bibi-Przedszkole.

Dzieci są wyposażone w identyfikatory - karty zbliżeniowe typu Mifare, które mogą zawierać zdjęcie, imię i nazwisko dziecka itp. lub breloczki zbliżeniowe. Przy wejściu do przedszkola dziecko lub opiekun przykłada kartę dziecka do czytnika wejściowego. Zostaje zarejestrowana godzina rozpoczęcia pobytu dziecka w przedszkolu. Podczas zajęć karta dziecka powinna być przechowywana w szafce. Po zakończeniu zajęć opiekun (rodzic) odbierający dziecko przy wyjściu z przedszkola przykłada kartę (breloczek) dziecka do czytnika wyjściowego. Z zarejestrowanych w ten sposób danych jest obliczany czas pobytu dziecka w przedszkolu. Do tego celu służy program biPrzedszkole. Dostarcza on wiele pomocnych raportów, m.in. miesięczne raporty indywidualne i grupowe, lista obecności grupy dzieci w wybranym dniu itp. Program umożliwia wprowadzanie taryf za czas pobytu, posiłki, zajęcia dodatkowe itp., co znacznie ułatwia obliczanie należności za pobyt dziecka w przedszkolu.

Zestaw podstawowy może być rozszerzany o dodatkowe opcje zwiększające funkcjonalność systemu.

Można wykorzystać funkcję kontroli dostępu systemu – drzwi wejściowe do przedszkola otwierane za pomocą rygla elektromagnetycznego. Wówczas opiekunowie muszą być także wyposażeni w karty (breloczki) zbliżeniowe. Wejścia i wyjścia opiekunów (rodziców) są także rejestrowane przez system.

Rozwiązanie z kontrolą dostępu utrudnia dostęp do przedszkola osobom nieuprawnionym.

Dodatkowy duży, wyraźny wyświetlacz może pokazywać aktualny czas systemu ewidencyjnego. Może służyć jako zegar czasu rzeczywistego w przedszkolu.

Dodatkowy czytnik na biurko ułatwia wydawanie kart w systemie, szczególnie w dużych przedszkolach i tych wykorzystujących opcję kontroli dostępu. Wydanie karty w przypadku zgubienia, wydanie karty nowemu opiekunowi (np. dziadkowi, babci) jest wówczas znacznie ułatwione.

Opcjonalna funkcja podglądu przez przeglądarkę internetową umożliwia rodzicom wgląd w rejestr pobytu ich dzieci w przedszkolu z domowego komputera. Tym samym ułatwia rozliczanie się za pobyt dziecka w przedszkolu.

System może pracować w trybie on-line. Wówczas wszystkie dane są na bieżąco przekazywane do komputera i wyświetlane na jego ekranie. Może też pracować w trybie off-line. Wtedy rejestracje wejść i wyjść dzieci z przedszkola zapamiętywane są w pamięci kontrolera bibi-K12 (bufor o pojemności 32000 zdarzeń).

Produkcja:

MicroMade

Micromade Gałka i Drożdż sp.j.
ul. Wieniawskiego 16
64-920 Piła

tel./faks 67 213 24 14
e-mail: mm@micromade.pl
http://www.bibinet.pl/przedszkola

RUD-3
Czytnik/Programator zbliżeniowy USB

RUD-3 jest miniaturowym czytnikiem i programatorem transponderów zbliżeniowych standardu 13,56MHz ISO/IEC 14443A oraz Mifare. Czytnik jest zasilany z portu szeregowego USB, który jest także wykorzystywany do komunikacji z urządzeniem. RUD-3 znajduje zastosowanie jako uniwersalny czytnik numerów kart w/w standardów (z poziomu programu Roger MiniReader 1.2 lub wyższy) jak również pozwala na wygodne wprowadzanie identyfikatorów użytkowników w systemie kontroli dostępu RACS (wymagany jest PR Master 4.4.6 lub wyższy). Funkcję programowania transponderów Mifare udostępniono w programie narzędziowym RARC 1.4. Dla programistów chcących zintegrować obsługę RUD-3 w innych aplikacjach przygotowano darmowy pakiet deweloperski SDK.

Zastosowanie:

RUD-3 może być wykorzystywany jako:

- czytnik do wprowadzania kart w systemie kontroli dostępu RACS,
- czytnik do odczytu kodów kart za pomocą programu Roger MiniReader,
- czytnik/programator do obsługi kart z poziomu programu RARC,
- czytnik/programator do obsługi kart w aplikacji klienta wykorzystujących bibliotekę DLL (wchodzi w skład pakietu SDK).

Obsługa kart:

RUD-3 został zaprojektowany do współpracy z kartami zbliżeniowymi standardu ISO/IEC 14443A oraz Mifare. Czytnik może być skonfigurowany do odczytu następujących numerów:

- CSN (unikalny numer seryjny karty),
- SSN (numer zapisany w dowolnym sektorze karty),
- MSN (numer adresowany przez sektor MAD).

Producent: roger®

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

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

NEO, NEO-PS – centrala alarmowa z komunikacją GSM




Centrala alarmowa NEO/NEO-PS wraz z urządzeniami współpracującymi to rozwiązanie integrujące elektroniczny system sygnalizacji włamania i automatykę domową. Wbudowany komunikator GSM pozwala na zdalną kontrolę i sterowanie systemem np. włączanie w dozór i aktywację wyjść. Dzięki modułowej konstrukcji, system może być rozbudowywany i dostosowywany do potrzeb użytkownika. Centrala jest bogato wyposażona w porównaniu do innych systemów tej klasy. Posiada wejścia binarne i analogowe, wyjścia binarne, dwukierunkowy system audio, komunikator GSM/GPRS. Umożliwia pomiar i rejestrację temperatury, realizację funkcji logicznych I/O i O/O.

Na uwagę szczególnie zasługują następujące elementy i funkcje systemu:

- panele dotykowe TPR-1/TPR-1F to nowoczesne, eleganckie i intuicyjne klawiatury do sterowania systemem wyposażone w unikalne funkcje,
- moduł FGR-4 do przesyłania wiadomości MMS/e-mail ze zdjęciami z kamer przemysłowych, umożliwia weryfikację wizualną stanu obiektu,
- syntezer mowy VSR-2, pozwala na przesłanie 16 komunikatów głosowych zawierających informacje o zdarzeniu lub VSR-1 pozwalający na przesłanie 1 komunikatu głosowego,
- moduł audio AMR-1 (mikrofon), pozwalający na podsłuch obiektu i weryfikacje audio,
- bramka VAR-1 i moduł FGR-4 do integracji z wideodomofonem, integracja pozwala na rozmowę telefoniczną pomiędzy bramofonem a telefonem komórkowym oraz na wysyłanie zdjęć gościa stojącego przy bramie poprzez MMS-y,
- czujniki temperatury TSR-1, służące do kontroli temperatury i funkcji termostatu,
- zasilacz systemowy z wbudowanym sterownikiem radiowym PSR-RF, pozwala na sterowanie czuwaniem systemu poprzez piloty radiowe.

Właściwości:

- konstrukcja i funkcje zgodne z PN-EN 50131-3, stopień 2
- wbudowany modem GSM/DCS/EGSM bez blokady Simlock
- modułowa i skalowalna konstrukcja
- jedna strefa główna oraz strefa wewnętrzna NOC
- wygodna obsługa systemu: panele dotykowe, SMS, sterowanie linią wejściową, piloty radiowe (PSR-RF)
- panele dotykowe w dwóch wersjach: natynkowa TRP-1 i podtynkowa TPR-1F
- 8 numerów telefonu do powiadomienia i sterowania SMS/CLIP,
- 8-20 wejść, rozbudowa poprzez panele dotykowe, moduły wejść
- niezależnie konfigurowana reakcja i typ wejścia 2EOL/NC, 2EOL/NO, EOL, NC, NO
- współpraca z modułem wejść EXP-I8
- wejście analogowe AI 0-10 V ze skalowaniem do wartości fizycznej (np. temp=°C, RH=%, p=kPa)
- 8-12 wyjść sterowanych przez SMS, CLIP, stanem systemu, z panelu dotykowego
- O1 i O2 sterowane wyjścia 12 V_{DC}/1 A z zabezpieczeniem zwarciowym, przeciążeniowym, temperaturowym i kontrolą obciążenia
- O3 - O8 sterowane wyjścia typu OC, obciążalność 100 mA, AUX, KB wyjścia zasilania 12 V_{DC}/1 A z zabezpieczeniem zwarciowym, przeciążeniowym, temperaturowym
- powiadomienie głosowe, SMS, CLIP, MMS, e-mail po zmianie stanu wejść
- Powiadomienie głosowe, SMS, CLIP po zmianie stanu wyjść
- dowolne SMS-y i komunikaty głosowe (VSR-2) przy zdarzeniach w systemie dotyczących wejścia, wyjścia, temperatury
- transmisja MMS/e-mail ze zdjęciami z kamer CCTV i wideodomofonów
- integracja audio z wideodomofonami
- integracja audio z domofonami i interkomami
- dwukierunkowy system audio, podsłuch obiektu
- pomiar i rejestracja temperatury z dwóch czujników TSR-1, dwa niezależne termostaty na 4 wyjściach
- funkcje logiczne wejścia/wyjścia -> wyjścia IO/O: AND, OR, NOR, XOR
- zegar RTC z podtrzymaniem bateryjnym
- funkcja testu łączności: SMS, SMS STAN, CLIP, MMS
- optyczna sygnalizacja pracy i zasięgu GSM
- pamięć zdarzeń; 1000 zdarzeń z nadpisywaniem
- funkcje ograniczania kosztów i ilości transmisji
- obsługa kodów USSD (kontrola kart pre-paid)
- zasilanie NEO: 12 V_{DC} z kontrolą napięcia (<11 V_{DC}), możliwość zasilania z alternatywnego źródła zasilania w obiektach bez sieci 230 V_{AC}, np. z baterii słonecznych, turbin wiatrowych, w tym przypadku wejście analogowe AI pozwala na kontrolę napięcia akumulatorów
- zasilanie NEO-PS: wbudowany zasilacz buforowy zasilany napięciem 17÷20 V_{AC} lub 20÷30 V_{DC} (II klasa izolacji), kontrola napięcia zmiennego i stałego, kontrola i dynamiczny test akumulatora

Producent:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ul. Kutrzeby 16G, 61-714 **Poznań**
tel. 32 790 76 37
faks 32 790 76 70
e-mail: poznan@e-alpol.com.pl

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

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

ul. Modzelewskiego 35/U9, 02-679 **Warszawa-Mokotów**
tel. 32 790 76 34
faks 32 790 76 69
e-mail: warszawa@e-alpol.com.pl

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

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

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: handlowy@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

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

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

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

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

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

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

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

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.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

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

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

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

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. 32 241 59 71
faks 32 258 05 98
e-mail: biuro@suma.com.pl
www.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
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	–	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	TAK
GDE Polska	–	TAK	TAK	–	TAK
HSA	–	–	TAK	–	TAK
Insap	–	TAK	TAK	TAK	TAK
ISM EuroCenter	–	–	TAK	–	TAK

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Janex International	–	TAK	TAK	TAK	TAK
KABE	TAK	TAK	TAK	TAK	TAK
KATON	–	–	TAK	–	TAK
Kolektor MR	–	TAK	TAK	TAK	TAK
Legrand Polska	TAK	TAK	TAK	–	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	–	TAK	–	–
Nuuxe – Radioton	–	TAK	TAK	TAK	TAK
OBIS	–	TAK	–	TAK	–
OMC INDUSTRIAL	–	–	TAK	–	–
Petrosin	–	TAK	–	TAK	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	–	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	–	–	–
Ramar	–	TAK	TAK	TAK	TAK
RETT-POL	–	–	TAK	TAK	–
RISCO	TAK	–	–	–	–
ROPAM Elektronik	TAK	–	TAK	–	–
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	–	–
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	–	–	–	–	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
GDE Polska	–	TAK	TAK	–	–	TAK	TAK	TAK	–
HSA	TAK	TAK	TAK	TAK	–	–	–	–	–
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
ISM EuroCenter	–	TAK	–	–	–	TAK	TAK	–	–

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
Janex International	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
KATON	–	TAK	TAK	–	–	TAK	–	–	–
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	–	–	–	–	TAK	–
Nuuxe – Radioton	–	TAK	–	TAK	–	–	–	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	–	–	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	TAK	–	–	–	TAK	TAK
Petrosin	TAK	TAK	TAK	–	–	–	–	–	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	–	–	–	–	–	–	–	TAK	–
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	TAK	–	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	–	TAK	TAK	–	–	–
RETT-POL	TAK	TAK	TAK	TAK	–	–	TAK	–	–
RISCO	TAK	–	TAK	–	–	TAK	–	–	–
ROPAM Elektronik	TAK	TAK	TAK	TAK	–	–	TAK	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
SATIE	–	–	TAK	–	–	TAK	TAK	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.M.A.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Schneider Electric Buildings Polska	–	TAK	TAK	–	–	TAK	TAK	–	–
Sprint	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SPS Electronics	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	TAK	–	–	–
SUMA	–	TAK	–	–	–	–	–	–	–
Tap – Systemy Alarmowe	TAK	–	TAK	–	–	–	–	–	–
Tayama	–	TAK	TAK	–	–	–	TAK	–	–
Technokabel	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
UNICARD	TAK	TAK	TAK	–	–	TAK	–	TAK	–
W2	TAK	–	–	TAK	–	–	–	–	–
Vision Polska	–	–	–	TAK	–	–	–	–	–

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
Marek Życzkowski

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

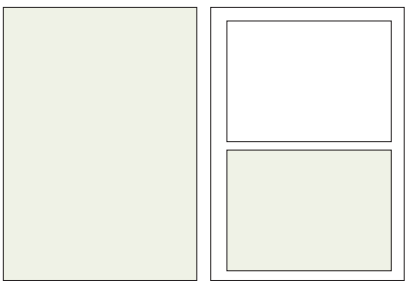
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

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)

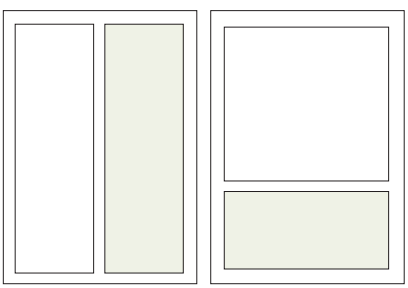
1/2 strony (170 x 125 mm)

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

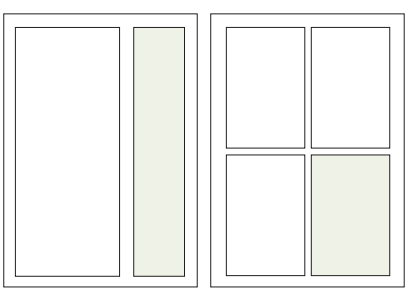


1/2 strony (83 x 260 mm)

1/3 strony (170 x 80 mm)

Spis teleadresowy:

jednorazowy wpis 70 zł



1/3 strony (54 x 260 mm)

1/4 strony (83 x 125 mm)

Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Podane ceny nie uwzględniają podatku VAT (23%)

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

Spis reklam

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

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.