CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 6(76)/2010

ZABEZPIECZENIA

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

W NUMERZE:

Panasonic
ideas for life

WYKRYWANIE TWARZY

JAKOŚĆ HD

BARDZO EFEKTYWNA KOMPRESJA H.264

ZMNIEJSZONY POBÓR MOCY DZIĘKI ZASTOSOWANIU NOWEGO MEGAPIKSELOWEGO PRZETWORNIKA MOS

i-PRO SmartHD

Z KAMERAMI I-PRO SmartHD OSZCZĘDNOŚCI SĄ GWARANTOWANE

Nowe kamery SmartHD IP Panasonic łączą w sobie zaawansowane funkcje z niższym zużyciem energii oraz obrazami jakości HD.

Inteligentne wykorzystywanie możliwości sieci oraz znakomita jakość obrazów powodują, że kamery i-Pro SmartHD są doskonałym narzędziem w walce z przestępczością, zapewniającym wysokiej jakości materiał dowodowy, pozyskiwany zarówno w dzień, jak i w nocy.

Proekologiczna polityka firmy Panasonic Eco Ideas pozwala na redukcję zużycia energii nawet o 45%.

Wykorzystanie w kamerach technologii wykrywania twarzy wraz z unikalną technologią rozszerzania zakresu dynamiki Super Dynamic firmy Panasonic, gwarantuje uzyskiwanie klarownych obrazów w trudnych warunkach oświetlenia.

WSZYSTKO MA ZNACZENIE

eco ideas

i-PRO

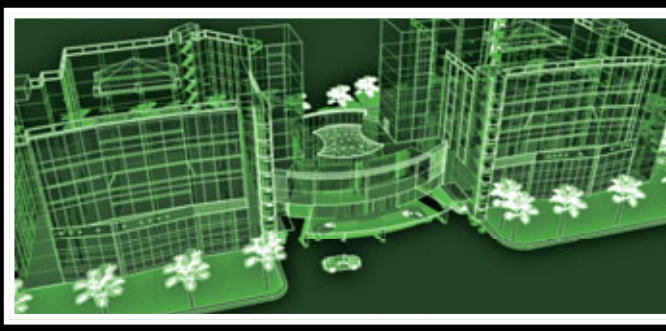
WV-SF332/335/336

WV-SP302/305/306

www.panasonic.pl

Spis treści

CZASOPISMO ZABEZPIECZENIA 6/2010



Organizacja wirtualna jako obiekt ochrony fizycznej i technicznej **26**

Sygnalizator SG-Wgw – uniwersalna sygnalizacja zdarzeń **40**

Rejestrator mobilny marki NOVUS **58**

Realne koszty systemu wykrywania pożaru (część II) **72**

Axis Communications zwiększa możliwości nadzoru wizyjnego, wprowadzając na rynek Corridor Format

Firma **Axis Communications** wprowadziła do swojej oferty **Corridor Format.** Nowe rozwiązanie pozwala zwiększyć możliwości nadzoru tam, gdzie wymagane jest pionowe ustawienie pola widzenia, między innymi na klatkach schodowych, w korytarzach, przejściach, na drogach, pasach startowych i w tunelach.

– Dostrzegamy potrzebę wprowadzania na rynek rozwiązań umożliwiających monitoring obszarów, których obserwacja jest łatwiejsza w przypadku pionowego ustawienia obrazu telewizyjnego. Chcemy, aby produkty te zapewniały najwyższą jakość obrazu, a jednocześnie ograniczały liczbę nieużytecznych pikseli. Corridor Format jest unikatowym, niedrogim i prostym w użyciu rozwiązaniem sprawdzającym się w wielu, często skomplikowanych systemach nadzoru wizyjnego – powiedział **Edwin Roobol**, dyrektor regionalny Axis Communications w Europie Środkowej.

Stosowane dotychczas poziome ustawienie obrazu telewizyjnego nie sprawdza się w przypadku obserwacji korytarzy i wąskich przejść, ponieważ znaczna część powierzchni obrazu telewizyjnego nie jest wykorzystywana. Oznacza to, że nie wykorzystujemy całej powierzchni przetwornika obrazowego, a tym samym ograniczamy faktyczną rozdzielczość obrazu telewizyjnego. Tak skonfigurowany system monitorowania niepotrzebnie zwiększa obciążenie sieci IP oraz objętość zapisywanych plików.

Corridor Format, proponowany przez firmę Axis, pozwala na tworzenie obrazów telewizyjnych ustawionych pionowo, doskonale nadających się do monitorowania wąskich obszarów. Zyskuje na tym jakość obrazu i wyeliminowany zostaje typowy problem występujący w przypadku obrazu o orientacji poziomej, polegający na nadmiernym obciążeniu sieci IP oraz złym wykorzystaniu nośnika, na którym zapisywane są obrazy. Corridor Format jest bardzo przydatny w monitorowaniu wąskich korytarzy, peronów, tuneli i przejść z wykorzystaniem nowoczesnych kamer sieciowych o rozdzielczości HD, tworzących obrazy o proporcji boków 16:9 (typowej dla telewizji HDTV), gdyż w takim przypadku powstający obraz może być wyświetlany z zachowaniem pełnych parametrów.

– Nowy sposób wyświetlania obrazu o proporcjach 9:16, charakterystyczny dla formatu Corridor Format, umożliwia uzyskanie wysokiej jakości obrazu na całej monitorowanej przestrzeni przy zastosowaniu tylko jednej kamery sieciowej, nawet jeśli znajduje się ona na znacznej wysokości – powiedział **Claude Verville**, wiceprezes Wydziału Zapobiegania Stratom, Bezpieczeństwa oraz Zarządzania Niebezpiecznymi Materiałami w Lowe's Companies.

Corridor Format można uzyskać poprzez zainstalowanie kamery w pozycji obróconej o 90 stopni lub poprzez odpowiednie ustawienie obiektywu w kamerze kopułkowej oraz programowy obrót obrazu telewizyjnego o 90 stopni. Jest to możliwe w przypadku zastosowania kamer sieciowych firmy Axis.

Corridor Format jest obsługiwany przez większość stałopozycyjnych kamer sieciowych firmy Axis, a programowe obrócenie obrazu jest możliwe dzięki wydajnym procesorom, w które wyposażone są kamery. Ponadto Corridor Format jest obsługiwany przez wiodące w branży aplikacje do zarządzania materiałem wizyjnym, opracowane przez partnerów programistycznych firmy Axis, takie jak Exacq Technologies, Genetec, Milestone Systems oraz On-Net Surveillance Systems, a także przez kolejną wersję (3.40) programu AXIS Camera Station.

Bezpośr. inf. Katarzyna Wójcik
Grayling Poland
Opracowanie: Redakcja

Nowe drukarki Fargo w ofercie chomtech.pl

Firma **chomtech.pl** wprowadziła do sprzedaży **nową linię drukarek do kart plastikowych firmy Fargo** – czołowego producenta takich urządzeń na świecie. Nowa linia drukarek jest wynikiem połączenia technologii dwóch światowych gigantów – HID Global i Fargo. Drukarki serii DTC charakteryzują się zwiększoną szybkością pracy przy zachowaniu bardzo wysokiej jakości wydruku.

Nowością jest zastosowanie taśm fluorescencyjnych i ultrafioletowych w modelu **DTC 4500**. Taśmy te poprawiają zabezpieczenie kart, jednocześnie zwiększając możliwości graficzne wydruku. Model DTC 4500 posiada również zabezpieczenie przed nieautoryzowanym wydrukiem w postaci hasła użytkownika. Może być wyposażony w kodery kart procesorowych, zbliżeniowych i magnetycznych. Dzięki temu idealnie nadaje się do wydruku kart lojalnościowych lub zaawansowanych przepustek osobistych.

Doskonałą ofertą dla małych i średnich firm usługowych jest drukarka **DTC 1000** zapewniająca połączenie doskonałej jakości wydruku i prostoty obsługi. Urządzenie jest przeznaczone do wydruku niewielkiej liczby kart kolorowych lub monochromatycznych – identyfikatorów, kart stałego klienta, rabatowych itp. DTC 1000 może być również opcjonalnie wyposażona w moduł obracający kartę, umożliwiający wykonanie nadruku obustronnego w jednym procesie wydruku. DTC 1000 można też doposażyć w kodery kart magnetycznych, stykowych i zbliżeniowych.

Ostatnią z nowo wprowadzonych do sprzedaży drukarek jest **DTC 4000**. W urządzeniu tym można zwiększyć pojemność podajnika kart do 200 szt. oraz umieścić wyjście Ethernet, dzięki któremu drukarka będzie dostępna dla autoryzowanych użytkowników w sieci. DTC 4000 może być również wzbogacona w kodery w identycznej konfiguracji jak w przypadku DTC 4500.

Nowe drukarki Fargo są obsługiwane przez specjalistyczne oprogramowanie do projektowania i wydruku Chomguard Personalizacja.

Bezpośr. inf. Tomasz Krawczyk
chomtech.pl

AXIS Q1921 i AXIS Q1921-E

nowe termowizyjne kamery sieciowe od Axis Communications

Firma **Axis Communications** powiększyła ofertę **termowizyjnych kamer IP** o dwa nowe modele – **AXIS Q1921 i AXIS Q1921-E**. Dzięki matrycom o wysokiej rozdzielczości oraz wielu dostępnym wymiennym obiektywom zapewniają one znakomitą jakość obrazu oraz obserwację rozległych terenów. Kamery rekomenduje się do stosowania w całodobowym monitorowaniu dużych obszarów, ochronie obwodowej oraz w komunikacji (tunele, drogi, lotniska).

Po udanym debiucie pierwszych termowizyjnych kamer IP AXIS Q1910/Q1910-E, które zostały wprowadzone do sprzedaży na początku tego roku, obecnie prezentujemy nowe modele – AXIS Q1921/Q1921-E. Termowizyjna kamera sieciowa AXIS Q1921-E charakteryzuje się wysoką jakością obrazu i dużym zasięgiem detekcji.

– *Rozszerzony zasięg nadzoru, szerokie pole widzenia i elastyczność będąca zasługą wymiennych obiektywów to cechy, których domagali się nasi klienci* – powiedział **Johan Paulsson**, dyrektor ds. technologii w Axis Communications. *Kamery AXIS Q1921/Q1921-E umożliwią niedrogą i elastyczną detekcję strefową i obwodową, która sprawdzi się w większości instalacji. AXIS Q1921 i AXIS Q1921-E doskonale zintegrują się z każdym sieciowym systemem nadzoru wizyjnego, zapewniając wszystkie korzyści monitoringu IP* – dodał Paulsson.

Kamery termowizyjne tworzą obraz na podstawie ciepła wydzielanego przez wszystkie obiekty. Dzięki temu mogą działać w całkowitej ciemności, dostarczając obrazów, które pozwalają operatorom wykrywać podejrzaną aktywność i niezwłocznie podejmować odpowiednie działania. Są również skuteczniejsze od konwencjonalnych kamer w trudnych warunkach, na przykład we mgle, w kurzu i dymie.

Kamera AXIS Q1921 jest przeznaczona do instalacji wewnętrznych, a AXIS Q1921-E, dzięki obudowie o klasie szczelności IP66, najlepiej sprawdzi się w monitorowaniu otwartych obszarów. Każdy z modeli jest kompatybilny z jednym z czterech obiektywów o ogniskowych 10, 19, 35 i 60 mm. Rozdzielczość 384x288 i zaawansowany procesor obrazu dodatkowo zwiększają skuteczność nadzoru strefowego i obwodowego. Kamery umożliwiają detekcję ludzi z odległości do 200 m przy 55-stopniowym polu widzenia oraz nawet do 1200 m przy 9-stopniowym polu widzenia. Ponadto oferują funkcje mające kluczowe znaczenie w systemach nadzoru IP, takie jak algorytmy kompresji H.264 i Motion JPEG, dwukierunkowe przesyłanie dźwięku, lokalne przechowywanie danych i zasilanie Power over Ethernet. Inteligentne funkcje wizyjne są podstawową zaletą każdej kamery termowizyjnej. AXIS Q1921/Q1921-E są szczególnie bogato wyposażone – alarmują o próbach ingerencji, wykrywają ruch, obsługują również platformę aplikacyjną AXIS.

Termowizyjne kamery sieciowe AXIS Q1921/Q1921-E są obsługiwane przez aplikacje do zarządzania materiałem wizyjnym, opracowane w ramach programu partnerskiego Axis Application Development, a także przez oprogramowanie AXIS Camera Station. Ponadto spełniają wymagania wynikające ze specyfikacj ONVIF, która określa zasady zgodności operacyjnej między sieciowymi produktami wizyjnymi.

Kamery AXIS Q1921/Q1921-E są dostępne od września 2010 roku w sieci dystrybucji firmy Axis.

Bezpośr. inf. Katarzyna Wójcik
Grayling Poland
Opracowanie: Redakcja

Nowe czytniki Mifare 13,56 MHz w ofercie firmy chomtech.pl

Firma **chomtech.pl** wprowadziła do sprzedaży nową linię czytników **Mifare 13,56 MHz**. Nowe czytniki charakteryzują się nowoczesnym wzornictwem i bogatą kolorystyką (ponad osiem wersji kolorystycznych). Czytniki odczytują każdy rodzaj kart i tagów Mifare (*standard, ultralight*). Dzięki temu mogą być rozwiązaniem alternatywnym wobec innych, już obecnych na naszym rynku czytników Mifare.

Czytniki są dostępne w wersji wewnętrznej i zewnętrznej. Mogą być wyposażone w klawiaturę mechaniczną lub dotykową. Każdy czytnik posiada wbudowany czujnik antysabotażowy. Opcjonalnie urządzenia mogą być również zintegrowane z kontrolerem. Wówczas mogą stanowić w pełni autonomiczny punkt kontroli dostępu. Sygnalizacja stanów alarmowych odbywa się poprzez sygnalizator akustyczny lub za pomocą kolorowych piktogramów.

Czytniki Mifare są przeznaczone do pracy z dowolnym kontrolerem (wersja Wiegand) lub z interfejsem RS485 i TCP/IP (wówczas mogą współpracować z komputerem PC i urządzeniami automatyki przemysłowej).

Rodzaje i miejsca zastosowań czytników Mifare:
– kontrola dostępu,
– rejestracja czasu pracy,
– hotele,
– parkingi,
– stołówki.

Bezpośr. inf. Tomasz Krawczyk
chomtech.pl

Nowy moduł komunikacyjny TCP/IP w kamerach modułowych AutoDome firmy Bosch

Zaawansowana, dwustrumieniowa technologia kompresji H.264

Firma **Bosch Security Systems** wprowadza na rynek **nowy moduł komunikacyjny TCP/IP do systemu kamer AutoDome**. Nowy moduł zawiera zaawansowane opcje obsługi technologii IP i udostępnia funkcje kompresji H.264 Main Profile, inteligentnej analizy obrazu oraz zarządzania alarmami. Moduł jest zgodny ze standardem *Open Network Video Interface Forum* (ONVIF).

W modułowych kamerach AutoDome firmy Bosch z mechanizmem uchylno-obrotowym (*Pan/Tilt/Zoom* – PTZ) zastosowano platformę składającą się z wymiennych komponentów. Dzięki temu możliwa jest wymiana modułów bez konieczności wymiany całego systemu kamer. Nowy moduł komunikacyjny TCP/IP można w łatwy sposób dodać do zainstalowanych kamer modułowych AutoDome z mechanizmem PTZ. Pozwala to rozbudować istniejące systemy zabezpieczeń przez dodanie najnowszych rozwiązań technologicznych z dziedziny monitoringu.

Moduł komunikacyjny TCP/IP wykorzystuje kompresję H.264 obrazu o jakości DVD. W zależności od konkretnego środowiska i ustawień mających wpływ na jakość może to oznaczać nawet o połowę mniejsze zapotrzebowanie na pamięć masową w porównaniu z kompresją MPEG4.

Opcja trójstrumieniowego przesyłania obrazu pozwala na równoczesne generowanie dwóch niezależnych strumieni H.264 o maksymalnej rozdzielczości 4CIF przy częstotliwości odświeżania wynoszącej do 25 lub 30 klatek na sekundę, a także jednego strumienia JPEG przeznaczonego do tworzenia obrazów na urządzeniu przenośnym. Zintegrowana obsługa urządzeń iSCSI umożliwia zapis skompresowanych danych wizyjnych bezpośrednio z kamer na macierzy RAID typu iSCSI.

Ponadto dzięki zastosowanemu w module dwurdzeniowemu procesorowi można równolegle uruchamiać wszystkie funkcje oprogramowania do inteligentnej analizy obrazu (*Intelligent Video Analysis* – IVA) bez wpływu na wydajność systemu. Oprogramowanie IVA umożliwia przetwarzanie sygnału wizyjnego przez kamery modułowe AutoDome i automatyczne powiadamianie operatorów o potencjalnych zagrożeniach. Jedna kamera modułowa AutoDome wyposażona w mechanizm PTZ jest w stanie przeanalizować nawet dziesięć ujęć w poszukiwaniu poruszających się obiektów, przekraczania linii i innych możliwych zagrożeń. Wystarczy do tego jedna licencja na oprogramowanie IVA. Klienci uzyskują zaawansowane funkcje analizy obrazu za niewielką cenę.

Rozbudowane mechanizmy kontroli alarmów umożliwiają elastyczne zarządzanie powiadomieniami generowanymi przez kamery modułowe AutoDome. Algorytmy oparte na regułach pozwalają uruchamiać różnorodne sekwencje działań, w tym złożone funkcje obsługi kopułki kamery. Nowy moduł komunikacyjny umożliwia również wysyłanie powiadomień o zdarzeniach pocztą elektroniczną.

Moduł jest zgodny ze standardem ONVIF, dzięki czemu możliwa jest bezproblemowa integracja kamer AutoDome z rozwiązaniami pochodzącymi od różnych dostawców. Instalatorzy oraz integratorzy systemów mają dzięki temu znaczną swobodę przy określaniu konfiguracji systemu.

Kamery modułowe Bosch AutoDome oferowane są w czterech wersjach, począwszy od podstawowej kamery z kopułką stałopozycyjną, a skończywszy na inteligentnej kamerze z serii 500i z mechanizmem PTZ. Kamery AutoDome wyposażone w nowy moduł mają możliwość hybrydowej pracy dzięki obsłudze zarówno połączeń przez Ethernet, jak i połączeń analogowych z istniejącymi urządzeniami.

Bezpośr. inf. Bosch Security Systems

Firma **ROGER** udostępniła dodatkowy numer telefonicznej linii wsparcia technicznego

Wychodząc naprzeciw oczekiwaniom swoich klientów, z dniem 01.10.2010 firma **ROGER** udostępniła dodatkowy numer telefonicznej linii wsparcia technicznego. Pod numerem telefonu **GSM +48 664 294 087**, w godzinach 8:00-20:00 w dni robocze, dostępna będzie pomoc techniczna dotycząca wszystkich produktów firmy ROGER. Dzięki temu kontakt z pracownikami działu wsparcia technicznego będzie łatwiejszy, a nasi klienci będą mogli liczyć na fachową poradę z zakresu konfiguracji i funkcjonowania urządzeń kontroli dostępu, także poza standardowymi godzinami pracy firmy.

Bezpośr. inf. Filip Paprocki
ROGER Dariusz Wensker, Grzegorz Wensker

Seria kamer IP 200

rozszerzona o kamery kopułkowe zgodne ze standardem ONVIF

Firma **Bosch Security Systems** powiększyła ofertę **kamer IP z serii 200** o kompaktowe kamery kopułkowe zgodne ze standardem ONVIF (*Open Network Video Interface Forum*). Zgodność ta oznacza pełną kompatybilność serii 200 z innymi służącymi do nadzoru wizyjnego urządzeniami obsługującymi standard ONVIF, a tym samym większą swobodę w projektowaniu systemów. Pozwala to również zmniejszyć koszty przyszłej modernizacji lub migracji.

Urządzenia serii 200, obejmującej cztery modele, są łatwe w instalacji i obsłudze. Każda kamera jest wyposażona w kartę pamięci flash Secure Digital (SD), co umożliwia zapis całodobowych nagrań telewizyjnych bez podłączania komputera PC. Skonfigurowanie kamer nie wymaga wiedzy technicznej – użytkownik po prostu wkłada kartę SD, podłącza kamerę, po czym może natychmiast oglądać i rejestrować obrazy. Pojedyncze połączenie kablowe zapewnia zasilanie przez sieć Ethernet (*Power over Ethernet*) oraz umożliwia oglądanie i rejestrowanie obrazów telewizyjnych. Nie jest potrzebny żaden dodatkowy sprzęt.

Rozwiązanie to można łatwo rozbudować, podłączając rejestrator wizyjny, na przykład Bosch Divar serii 700 lub serwer iSCSI. Ponadto efektywna kompresja obrazu H.264 zmniejsza wymaganą pojemność pamięci masowej nawet o 30% w porównaniu z konwencjonalnymi technologiami monitorowania, co znacznie obniża koszty eksploatacji systemów.

Specjalne oprogramowanie do monitorowania (bezpłatne dla 16 kamer) umożliwia zdalne oglądanie obrazu z wielu kamer na komputerze PC. Nagrania wizyjne mogą być archiwizowane w celu przyszłego wykorzystania lub zlokalizowania określonych zdarzeń za pomocą funkcji szybkiego wyszukiwania. Ponadto kamery są wyposażone we wbudowane funkcje wykrywania ruchu, ingerencji lub sygnału dźwiękowego, które mogą uruchamiać alarm lub podwyższyć jakość nagrania w celu wychwycenia dodatkowych szczegółów w obrazie. Dwukierunkowa transmisja dźwięku umożliwia operatorowi komunikowanie się za pośrednictwem kamery z gośćmi lub pracownikami.

Urządzenia można instalować w małych biurach, sklepach detalicznych i spożywczych czy salach lekcyjnych.

Bezpośr. inf. Bosch Security Systems

Kompleksowa oferta produktów HD

Wysoka rozdzielczość obrazu dzięki nowym produktom firmy Bosch przeznaczonym do nadzoru wizyjnego

Celem, jaki stawia sobie firma **Bosch** – mająca już ponad 40-letnie doświadczenie w dziedzinie produkcji urządzeń pracujących w systemach zabezpieczeń – jest dostarczanie wysokiej jakości systemów – łatwych w użyciu, inteligentnych oraz zgodnych z obowiązującymi standardami. Obecnie firma wprowadziła nowe rozwiązania umożliwiające uzyskanie obrazu o rozdzielczości HD, co stanowi odpowiedź na rosnące zapotrzebowanie na systemy HD pracujące w sieci IP i spełniające nowe wymagania dotyczące jakości obrazu. Dzięki wyższej rozdzielczości obrazu operator może rozróżnić drobne szczegóły obserwowanej sceny, co ma istotne znaczenie przy rozpoznawaniu twarzy i w innych podobnych zastosowaniach.

– W chwili obecnej nadarza się znakomita okazja do wprowadzenia kompletnego rozwiązania HD, które obejmuje przechwytywanie, wyświetlanie i archiwizację obrazów HD oraz zarządzanie nimi – powiedział **Gert van Iperen**, dyrektor Bosch Sicherheitssysteme. *– Wszystkie nasze produkty HD są specjalnie zaprojektowane z myślą o zapewnieniu wysokiej jakości obrazu. Obsługują zaawansowany standard kompresji wizji H.264, mają intuicyjne oprogramowanie, są zgodne z ONVIF oraz wyświetlają obraz w wygodnym do oglądania formacie 16:9.*

Implementacja H.264 umożliwia transmisję obrazu o wysokiej jakości przy zmniejszeniu ilości zajmowanego miejsca nawet o 50% w porównaniu z MPEG-4. Przechwytywanie wszystkich szczegółów obrazu nie odbywa się kosztem zmniejszenia częstotliwości ramki, co ma istotne znaczenie dla rozpoznawania obiektów. Bosch oferuje także skalowalne rozwiązania do zapisu wizji, które umożliwiają łatwą modernizację systemów zabezpieczeń, dostosowującą je do standardu HD. Pozwala to obniżyć początkowe nakłady oraz umożliwia stopniową rozbudowę systemu.

Wszystkie produkty HD firmy Bosch są w pełni zgodne z ONVIF i można łatwo zintegrować je z rozwiązaniami innych firm. Dzięki intuicyjnemu oprogramowaniu operatorzy systemu monitoringu mają dostęp do kamer zarówno wysokiej, jak i niskiej rozdzielczości. Użycie systemu jest więc łatwiejsze, a integrator może wybrać rozwiązanie, które jest najbardziej odpowiednie dla każdej lokalizacji.

Opracowana przez firmę Bosch funkcja IVA (*Intelligent Video Analysis*) zapewnia inteligentną analizę obrazu oraz automatyczne alarmowanie i wyszukiwanie. Funkcja ta, zoptymalizowana pod kątem standardu HD, prezentuje więcej informacji w tym samym polu widzenia, co pozwala na lepszą i dokładniejszą analizę.

Bezpośr. inf. Bosch Security Systems

Systemy sygnalizacji pożarowej Schrack Seconet w nowoczesnych obiektach sportowych

W związku z przygotowaniami do mistrzostw EURO 2012 prowadzonych jest wiele inwestycji mających na celu modernizację lub budowę obiektów sportowych, w tym stadionów i hal widowiskowo-sportowych o najwyższym, europejskim standardzie. Z końcem sierpnia oraz września br. zostały ukończone dwa tego typu obiekty – Stadion Miejski w Poznaniu oraz hala sportowo-widowiskowa Ergo Arena na granicy Gdańska i Sopotu. Oba obiekty zostały wyposażone w wysokiej klasy systemy sygnalizacji pożarowej Schrack Seconet.

Z dniem 20 września 2010 r. lista referencyjna firmy **Schrack Seconet Polska** została poszerzona o kolejny obiekt sportowy – **Stadion Miejski w Poznaniu**. Będzie on jedną z czterech aren mistrzostw EURO 2012, na której zostaną rozegrane trzy mecze grupowe.

Ten niezwykle nowoczesny, siedmiokondygnacyjny, w pełni zadaszony obiekt o powierzchni użytkowej 250 tys. m^2 oraz kubaturze 1,3 mln m^3 może pomieścić ponad 40 tys. widzów. W projekcie uwzględniono również 18 sekcji VIP. Dzięki zastosowanym rozwiązaniom technicznym na powierzchni dachu powstała gra światłocieni powodująca złudzenie miękkości i pofalowania powierzchni. Precyzyjne oświetlenie jest zapewnione przez 320 reflektorów, a 12 kamer umożliwia płynną transmisję telewizyjną.

Obiekt został doskonale wyposażony w systemy bezpieczeństwa, między innymi w system sygnalizacji pożarowej Schrack Seconet. Na stadionie znajduje się 1,7 tys. inteligentnych, multisensorowych czujek CUBUS MTD 533 wykrywających pożary zarówno tlewne, jak i otwarte już we wczesnej fazie ich rozwoju. Mogą one być zastosowane także jako czujki dymu, ciepła lub dualne – dymu/ciepła, a dzięki dynamicznemu filtrowi alarmów rozpoznają i eliminują alarmy fałszywe.

System składa się z sześciu modułowych central sygnalizacji pożarowej Integral Evolution, których architektura odpowiada idei stuprocentowej redundancji sprzętowej, a dzięki zastosowaniu rozbudowanych kart pamięci każda centrala ma zdolność zapamiętania do 65 tys. zdarzeń. W centrale te wyposażono również dwie serwerownie. Wszystkie te elementy nadzoruje intuicyjny system wizualizacji i zarządzania SecoLOG, a starannie dopracowane, wyposażone w kolorowy wyświetlacz pola obsługi gwarantują przejrzystość systemu.

Kolejnym obiektem, który z dniem 18 sierpnia br. znalazł się na liście referencyjnej Schrack Seconet, jest h**ala sportowo-widowiskowa Ergo Arena**, zlokalizowana na granicy Gdańska i Sopotu.

Ten wielofunkcyjny obiekt został zaprojektowany tak, by zapewnić odpowiednie warunki do organizacji różnego typu najwyższej rangi imprez sportowych, kulturalnych oraz rozrywkowych. Kubatura hali to ok. 380 tys. m^3, a trybuny wyposażono w ok. 11 tys. miejsc siedzących z możliwością dodania dodatkowych trzech tys. miejsc. Hala została wyposażona w 11 lóż VIP, a dla zwiększenia komfortu wszystkich widzów nad areną zawieszono cztery telebimy, które z pewnością umożliwią dokładną transmisję najciekawszych momentów spotkania.

Nad bezpieczeństwem widzów oraz całego obiektu czuwają nowoczesne systemy sygnalizacji pożarowej Schrack Seconet. Hala została wyposażona w ponad 1200 innowacyjnych optyczno-temperaturowych czujek CUBUS MTD 533 oraz osiem central Integral Evolution.

Bezpośr. inf. Schrack Seconet Polska

Nowe minikamery Samsung z analizą treści obrazu

Samsung wprowadza na rynek nową serię minikamer do dyskretnego monitoringu, np. do monitorowania bankomatów.

SCB-2020 i SCB-3020 to minikamery z opcją dzień/noc, generujące obraz o rozdzielczości 600 linii telewizyjnych i wykorzystujące procesor DSP Samsung A1. Kamery mają niewielkie rozmiary (44,5×44,5×20,1 mm), wbudowany obiektyw o ogniskowej 3,7 mm oraz uchwyt montażowy.

Obie kamery mogą maskować strefy prywatności, czyli wyłączyć z obserwacji strefy wrażliwe, np. klawiaturę bankomatu. Ponadto dysponują wieloma zaawansowanymi funkcjami, takimi jak cyfrowa redukcja szumów (*Digital Noise Reduction* – DNR) czy cyfrowa stabilizacja obrazu (*Digital Image Stabilization* – DIS), zapewniającymi wysoką jakość obrazu.

Sterowanie przez kabel koncentryczny (w standardzie CCVC) oraz wielojęzyczne menu ekranowe to tylko niektóre z funkcji przyjaznych dla użytkownika, znacznie ułatwiających stosowanie i obsługę kamer SCB-2020 i SCB-3020. Analiza treści obrazu wykorzystuje wirtualną linię umożliwiającą ochronę ogrodzeń oraz wykrywanie intruzów. Powyższe funkcje pozwalają alarmować pracowników nadzoru w przypadku wykrycia podejrzanie zachowujących się osób.

Kamera SCB-3020 dysponuje funkcją poszerzania zakresu dynamiki (*Wide Dynamic Range* – WDR), która umożliwia prawidłową pracę kamery w trudnych warunkach oświetleniowych. Z kolei progresywne skanowanie zapobiega rozmyciu obrazów szybko przemieszczających się obiektów podczas obserwowania ich na monitorze.

– Chociaż kamery SCB-2020 i SCB-3020 są rekomendowane do monitoringu bankomatów, mogą być stosowane również przez instalatorów poszukujących małogabarytowych kamer z uchwytami, służących do ochrony innych obiektów, np. pulpitów kasowych w sklepach – twierdzi **Peter Ainsworth**, główny kierownik produktu w **Samsung Techwin Europe**.

Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: Redakcja

Samsung wprowadza na rynek

serię kompaktowych, płaskich kamer kopułkowych

Trzy nowe kamery kopułkowe o niewielkich wymiarach 100×115×42 mm zaprojektowano z myślą o montażu w ciasnych pomieszczeniach, np. w windach, holach wejściowych, klatkach schodowych, środkach transportu i małych sklepach.

SNV-5010 jest zgodną ze standardem ONVIF kamerą kopułkową o rozdzielczości 1,3 Mpx. Kamera ma podwyższoną odporność na udary mechaniczne, jest wodoodporna, posiada procesor DSP WiseNet1 zaprojektowany z myślą o rozdzielczościach megapikselowych. Do kamery SNV-5010 dołączono bezpłatne oprogramowanie służące do inteligentnej analizy treści obrazu (*Intelligent Video Analytics* – IVA), umożliwiające detekcję przekroczenia wirtualnych stref definiowanych w obserwowanej scenie, wykrywanie kierunku ruchu obiektów, a także stwierdzanie faktu ich pojawiania się lub znikania (*Appear/Disappear*). Oprogramowanie IVA posiada także funkcję detekcji sabotażu z generowaniem alarmu, np. w przypadku zabrudzenia obiektywu kamery farbą w sprayu albo przemieszczenia kamery.

Kamera SNV-5010 wykorzystuje technikę progresywnego skanowania gwarantującą wysoką jakość obrazu przemieszczających się obiektów.

SCD-2010F posiada procesor DSP W-5 zapewniający przetwarzanie obrazu o rozdzielczości 600 linii telewizyjnych, powstałego przy natężeniu światła zaledwie 0,04 lx. Wyposażona w obiektyw o ogniskowej 3,0 mm i kącie widzenia 90° kamera SCD-2010F wykorzystuje opracowaną przez firmę Samsung technologię redukcji szumów (*Samsung Super Noise Reduction* – SSNRIII).

Mimo niewielkich rozmiarów kamera **SCD-2010F** ma wiele funkcji przydatnych dla instalatora, takich jak sterowanie przez kabel koncentryczny (*Coaxial Control*), kompensacja silnego oświetlenia (*High Light Compensation*), wykrywanie ruchu (*Motion Detection*), szeroki zakres dynamiki (*Samsung Super Dynamic Range* – SSDR) oraz wielojęzyczne menu ekranowe ułatwiające konfigurację. Funkcja Privacy umożliwia zdefiniowanie 12 obszarów prywatności.

Kamera SCV-2010F jest wandaloodporną wersją kamery SCD-2010F o klasie szczelności IP66.

Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: Redakcja

Jednokanałowy serwer IP marki Samsung zgodny ze standardem ONVIF

Firma **Samsung** wprowadziła nowy jednokanałowy serwer IP pozwalający na łatwe dodawanie analogowych kamer do systemu monitoringu IP.

Serwer SPE-100 umożliwia przesyłanie do sieci obrazów generowanych przez analogową kamerę z rozdzielczością 4CIF i w czasie rzeczywistym. Funkcja transmisji wielostrumieniowej w standardach kompresji H.264, MPEG-4 lub MJPEG pozwala na optymalizację wykorzystania pasma sieciowego dzięki przesyłaniu strumieni wizyjnych o różnej rozdzielczości i prędkości odświeżania do różnych lokalizacji w sieci.

– *Serwer SPE-100 zaprojektowano z myślą o klientach pragnących wykorzystać zalety transmisji sygnału wizyjnego za pomocą protokołu IP z jednoczesnym wykorzystaniem możliwości użytkowanych kamer analogowych* – twierdzi **Peter Ainsworth**, główny kierownik produktu w **Samsung Techwin Europe**. – *Warto podkreślić, że serwer SPE-100 posiada zaimplementowane protokoły sterowania telemetrycznego Pelco P/D oraz protokoły firmy Samsung. Jest to szczególnie ważne dla klientów pragnących zintegrować analogowe kamery szybkoobrotowe z systemami monitoringu IP.*

Serwer SPE-100 można zaprogramować tak, że w przypadku alarmu kamera szybkoobrotowa otrzyma polecenie ustawienia się w ustalonej pozycji (presecie), co pozwoli na zapis obrazów związanych z alarmem na karcie pamięci SD i jednocześnie wysłanie powiadomienia e-mailem.

Bezpłatne oprogramowanie NET-I Viewer firmy Samsung, dostarczane wraz z serwerem SPE-100, oferuje łatwy w obsłudze graficzny interfejs użytkownika. Uprawnieni użytkownicy mogą również uzyskiwać dostęp do obrazów transmitowanych na żywo albo zapisanych na karcie pamięci włożonej do gniazda kart pamięci SD w serwerze SPE-100 przez przeglądarkę internetową.

Serwer SPE-100 jest zgodny ze standardem ONVIF. Posiada przelotowe wejścia wizyjne, które umożliwiają dodatkowe wykorzystanie pochodzących z kamery sygnałów wizyjnych w rejestratorze lub bezpośrednio na monitorze. Serwer SPE-100 oferuje także dwukierunkowe przesyłanie sygnału dźwiękowego, co umożliwia interaktywną komunikację pomiędzy miejscem, w którym zainstalowany jest serwer, a centrum monitoringu.

Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: Redakcja

Samsung wprowadza nowe rozwiązania przeznaczone do systemów kontroli dostępu

Firma **Samsung** wprowadziła na rynek nowy asortyment opartych na technologii RFID i technologii biometrycznej urządzeń do systemów kontroli dostępu, które mogą mieć wiele zastosowań – od pojedynczych drzwi po duże systemy w biurowcach lub wielu lokalizacjach.

Asortyment ten obejmuje kontrolery zintegrowane, standardowe kontrolery jedno- i czterodrzwiowe, a także czytniki i oprogramowanie, które jest dostępne w wersjach dostosowanych do pracy z kontrolerami autonomicznymi albo w wersji sieciowej z wykorzystaniem protokołu TCP/IP lub RS485.

Kontrolery autonomiczne

Kontrolery autonomiczne mają wbudowane czytniki na karty zbliżeniowe i karty inteligentne z pamięcią, a także czytniki linii papilarnych i rozpoznawania twarzy. Posiadają wbudowaną klawiaturę kodu PIN z przyciskami funkcyjnymi do rejestracji czasu pracy. Są to doskonałe rozwiązania do kontroli pojedynczych przejść, które mogą współpracować z innymi kontrolerami w systemie bez udziału komputera i programu nadzorczego. W takiej opcji istnieje możliwość współdzielenia bazy danych biometrycznych. Możliwa jest również współpraca z programami nadzorczymi firmy Samsung, co ułatwia wymianę danych dotyczących kart.

Standardowe kontrolery jedno- i czterodrzwiowe

W przypadku standardowych kontrolerów firmy Samsung do pojedynczych drzwi istnieje możliwość wyboru formatu Mifare lub Samsung bezpośrednio w urządzeniu, natomiast rozwiązanie czterodrzwiowe można zamawiać w formacie Mifare lub Samsung. Obie wersje mają możliwość pracy sieciowej z wykorzystaniem protokołu RS485 lub, opcjonalnie, TCP/IP. W przypadku przejść kontrolowanych dwustronnie możliwe jest włączenie funkcji kontrolnej *antipassback*. Wersja jednodrzwiowa posiada dwa porty czytników, a wersja czterodrzwiowa – cztery.

Czytniki

Asortyment czytników marki Samsung obejmuje dwa formaty: Mifare lub własny – firmy Samsung. Obudowy czytników mogą być wykonane w wersji standardowej lub wzmocnionej, odpornej na wandalizm. Mogą zawierać wbudowaną klawiaturę kodu PIN i czytniki różnych typów kart lub cech biometrycznych. Wszystko to umożliwia instalatorom wybór rozwiązania najbardziej odpowiedniego do danego systemu. Na uwagę zasługuje również fakt, że czytniki kart firmy Samsung są objęte rozszerzoną na cały okres użytkowania gwarancją.

Oprogramowanie

Programy nadzorcze do kontroli dostępu firmy Samsung (*Samsung Access Management Software* – SAMS) bazują na konfiguracji serwer – klient i są dostępne w dwóch wersjach: podstawowej i profesjonalnej.

Podstawowa wersja oprogramowania serwera – **SAMS Basic Lite** – umożliwia pełne administrowanie systemem kontroli dostępu i jest w stanie dostarczać szczegółowych raportów dotyczących użycia kart w systemie, które mogą być eksportowane do pliku programu Excel lub tekstowego. Umożliwia to integrację z programami do kontroli czasu pracy i obecności (RCP) lub programami kadrowymi.

Wersja profesjonalna – **SAMS Pro Lite** – oferuje te same funkcje, a dodatkowo funkcje zaawansowane, takie jak integracja z systemem telewizji dozorowej. Taka integracja umożliwia np. wyświetlanie obrazu z kamery zainstalowanej przed czytnikiem po włożeniu karty do czytnika przez wybranego użytkownika. Program oferuje również wizualizację systemu poprzez system zdefiniowanych przez operatora elektronicznych map z naniesionymi aktywnymi ikonami przypisanymi do elementów systemu – czytników, linii dozorowych, wyjść sterujących i kamer.

Definiowanie uprawnień operatorów programów SAMS Basic Lite i SAMS Pro Lite umożliwia upoważnionym pracownikom wykonywanie takich zadań administracyjnych, jak dodawanie i usuwanie kart oraz przeglądanie zdarzeń bez dostępu do opcji konfiguracji systemu.

– Samsung nadal szybko ewoluuje, stopniowo stając się dostawcą pełnych rozwiązań w dziedzinie bezpieczeństwa. Wprowadzenie serii produktów do systemów kontroli dostępu jest widocznym znakiem naszego dążenia do oferowania produktów i technologii z różnych dyscyplin, integrujących się razem w sposób dający rzeczywiste korzyści końcowemu użytkownikowi – powiedział **David Cawley, Access Control Product Manager w Samsung Techwin Europe**, komentując wprowadzenie nowej serii rozwiązań do kontroli dostępu.

Bezpośr. inf. David Solomons
DRS Marketing
Tłumaczenie: Redakcja

MicroMade członkiem PISA

Informujemy, że na posiedzeniu w dniu 6 października 2010 r. zarząd Polskiej Izby Systemów Alarmowych podjął uchwałę o przyjęciu firmy MicroMade w poczet członków PISA.

Firma **MicroMade Gałka i Drożdż sp.j.** jest polskim producentem (z 20-letnią tradycją) urządzeń elektronicznych. W ramach swojej działalności produkuje między innymi urządzenia do systemów kontroli dostępu i ewidencji czasu pracy.

Bezpośr. inf. MicroMade

Firma APS wybrała głowice uchylno-obrotowe marki Videotec do systemu monitoringu wizyjnego

Firma APS jest liderem w produkcji energii elektrycznej w Arizonie i największym stanowym operatorem sieciowym dostarczającym od ponad 100 lat wysokiej jakości energię elektryczną w rozsądnej cenie. APS obsługuje ponad 1,1 miliona klientów w 11 spośród 15 hrabstw w stanie Arizona. APS chce monitorować najbardziej wrażliwą cześć infrastruktury i swoje podstacje rozsiane po całym stanie, z których część znajduje się w obszarze trudno dostępnym. APS posiada już systemy monitoringu wyposażone w głowice uchylno-obrotowe z kamerami termicznymi. Z powodu wysokiej awaryjności dotychczas stosowanych urządzeń, wysokich kosztów ich utrzymania i w celu uzyskania efektywnego systemu monitoringu APS wybrał rozwiązania firmy **Videotec**.

Głowica uchylno-obrotowa ULISSE składa się z wysokiej jakości mechanizmu napędowego, obudowy, odbiornika telemetrycznego i dwóch promienników podczerwieni LED. Obrót w płaszczyźnie poziomej jest ciągły ze zmienną prędkością dochodzącą do 40°/s. W płaszczyźnie pionowej głowica może obracać się w zakresie od +90° do -40° z maksymalną prędkością 30°/s. ULISSE steruje trasami obserwacji z dokładnością do 0,02°.

Głowice ULISSE z dwoma bliźniaczymi oświetlaczami IRBD o szerokości wiązki 20 stopni wyposażono w kamery z przetwornikami CCD 1/2" i z obiektywami motor-zoom, tworząc punkty kamerowe umożliwiające obserwację terenu na odległość do 275 m w nocy i do 400 m w świetle dziennym. Głowica uchylno-obrotowa ULISSE może być zintegrowana z wieloma instalacjami dzięki wielu wbudowanym protokołom lub połączona z systemami IP dzięki bezproblemowej integracji z większością aplikacji VMS.

W 2010 roku firma APS rozmieściła 40 opisanych powyżej systemów, aby monitorować podstacje energetyczne, przy czym w każdej z tych podstacji zainstalowano od dwóch do dziewięciu głowic. System monitoringu ULISSE PTZ składa się z oświetlaczy podczerwieni, które zapewniają dobre oświetlenie promieniowaniem podczerwonym, co w konsekwencji pozwala na uzyskanie obrazów o wyższej jakości aniżeli w przypadku innych systemów monitoringu wizyjnego.

Bezpośr. inf. Martina Panighel
Tłumaczenie: Redakcja

Videotec ujawnił tajwańskie podróbki produktów

Podczas międzynarodowej wystawy **Essen 2010 International Security Show** firma **Videotec** podjęła stanowcze kroki w celu ochrony własnych praw patentowych i uzyskała natychmiastowy zakaz dystrybucji z konfiskatą podrabianych produktów wystawianych przez kilku tajwańskich producentów naruszających prawa patentowe Videoteca. Uprawnione władze udały się na odpowiednie stoiska wystawowe i skonfiskowały produkty naruszające prawo. Jest to kolejny tego typu przypadek, a podobną akcję przeprowadzono podczas targów Essen w 2008 roku.

Od 25 lat firma Videotec jest producentem certyfikowanych, profesjonalnych produktów wykorzystywanych do budowy systemów monitoringu wizyjnego. Przez ten okres często angażowała się w akcje ochrony własnych praw patentowych przed nieuczciwą konkurencją niektórych dalekowschodnich producentów, którzy próbowali wykorzystać dobrą reputację produktów Videotec na rynku CCTV i sprzedawać tanie podróbki o niskiej jakości.

– *To bardzo ważne dla producentów, aby stawić czoła tym haniebnym fałszerstwom i ochronić własne prawa, jak również swoich klientów. Naprawdę mam nadzieję, że to drugie uderzenie w producentów podróbek silnie umocni przekonanie, że walka z fałszerstwami musi być częścią strategii firmy* – wyjaśnia **Moreno Barbieri**, dyrektor zarządzający Videotec.

Bezpośr. inf. Martina Panighel
Videotec
Tłumaczenie: Redakcja

ULISSE NETWORK CAM
nowa głowica uchylno-obrotowa do kamer IP

ULISSE NETWORK CAM jest uchylno-obrotową głowicą przeznaczoną do kamer sieciowych ze zintegrowanym odbiornikiem telemetrycznym i obudową przeznaczoną do zastosowań zewnętrznych. Rozwiązanie to jest polecane zwłaszcza w przypadku zastosowania kamer IP z telemetrycznym wyjściem RS232/RS485.

Głowica uchylno-obrotowa może być sterowana poprzez sieć, jeżeli kamera posiada wyjście telemetryczne RS232/RS485, lub poprzez dedykowaną linię szeregową RS485. ULISSE NETWORK CAM może współpracować zarówno z kamerami ze zintegrowanymi obiektywami o zmiennej ogniskowej, jak i z kamerami wyposażonymi w obiektywy typu motor-zoom.

Głowice ULISSE NETWORK CAM są dostępne w wersji ze zintegrowaną wycieraczką i promiennikami diodowymi (LED). Mogą one nieprzerwanie obracać się z prędkością dochodzącą do 100°/s i przemieszczać się w płaszczyźnie pionowej w zakresie od +90° do -40° z maksymalną prędkością dochodząca do 40°/s. Głowica ULISSE NETWORK CAM umożliwia sterowanie funkcjami tras obserwacji i skanowania. Dokładność pozycjonowania dla presetów wynosi 0,02°.

Obudowa stosowana w głowicy ULISSE NETWORK CAM jest wyposażona w grzałkę sterowaną termostatem, przez co zapewnia optymalne warunki temperaturowe dla pracy kamer i obiektywów.

System pozycjonujący może być stosowany w ochronie wybrzeża i granic, monitorowaniu portów, miast, autostrad i dróg, a także stadionów, obiektów przemysłowych, zakładów karnych i obiektów militarnych. Ponadto głowica może być stosowana w systemach ochrony perymetrycznej.

Bezpośr. inf. Martina Panighel
Videotec
Tłumaczenie: Redakcja

ULISSE PLUS – uchylno-obrotowa głowica
przeznaczona do kamer z obiektywami o długiej ogniskowej

Seria zewnętrznych głowic uchylno-obrotowych ULISSE firmy **Videotec** została powiększona o model **ULISSE PLUS**. Głowica charakteryzuje się większą obudową do kamer w porównaniu do modeli ULISSE i tym samym pozwala na instalację obiektywów o długich ogniskowych.

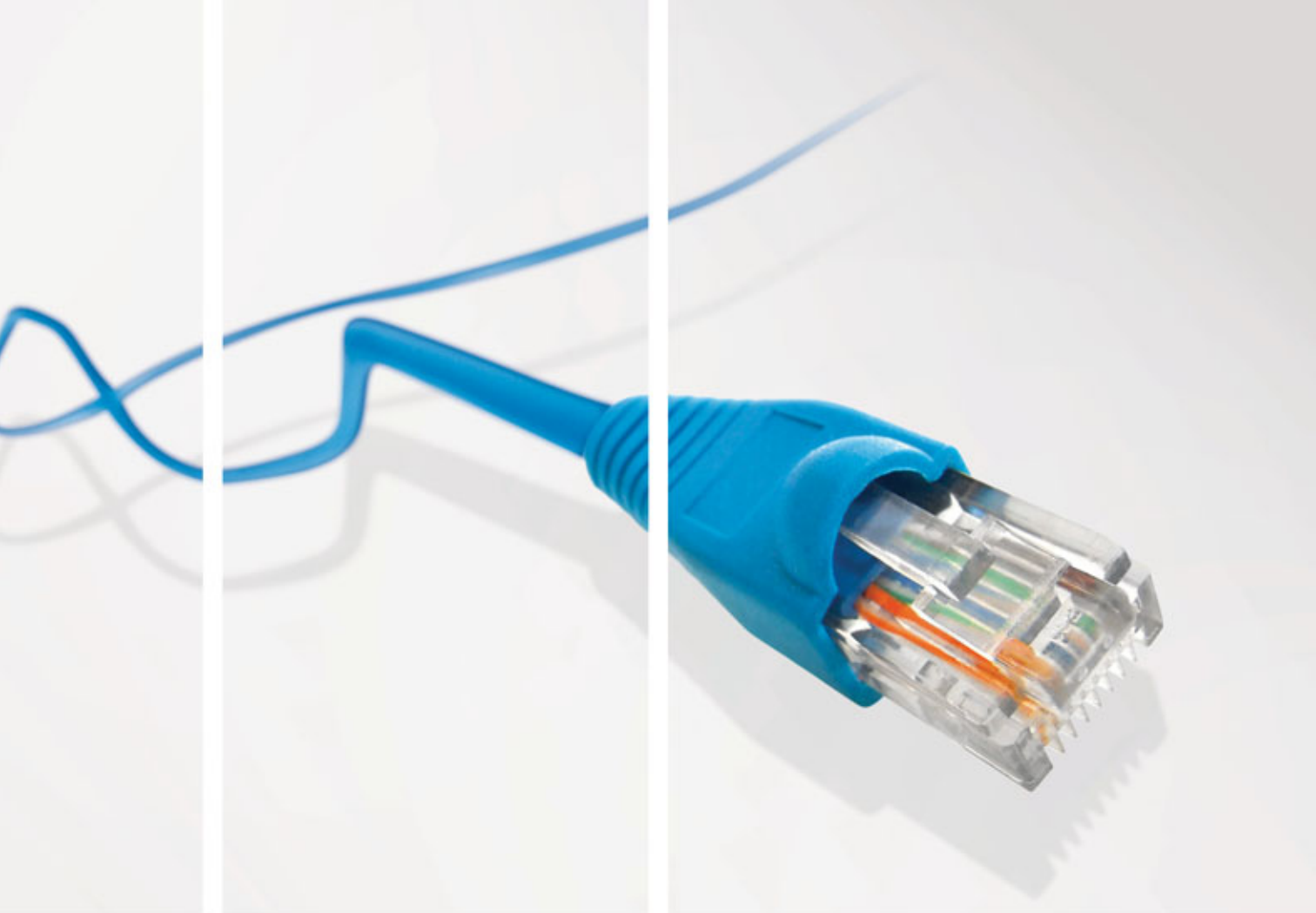
Głowice ULISSE PLUS składają się z wysokiej jakości mechanizmu uchylno-obrotowego, odbiornika telemetrycznego i obudowy do kamer wyposażonej w wycieraczkę.

ULISSE PLUS może obracać się ruchem ciągłym w płaszczyźnie poziomej, ze zmienną prędkością dochodzącą do 100°/s, i pochylać w zakresie od +90° do -40° z maksymalną prędkością 50°/s. Ma funkcje autoskanowania i patroli z dokładnością pozycjonowania 0,02° dla ujęć programowalnych. W celu optymalizacji trasy patrolu prędkości przemieszczania się pomiędzy poszczególnymi pozycjami mogą być różne.

Głowica ULISSE PLUS jest wyposażona w grzałkę sterowaną termostatem i osłonę przeciwsłoneczną, co pozwala na zachowanie optymalnych temperaturowych warunków pracy kamer i obiektywów.

System pozycjonujący może być stosowany w ochronie wybrzeża i granic, a także w monitorowaniu portów, miast, autostrad i dróg, stadionów, obiektów przemysłowych, zakładów karnych i obiektów militarnych. Ponadto głowica może być stosowana w systemach ochrony perymetrycznej.

Bezpośr. inf. Martina Panighel
Tłumaczenie: Redakcja



just connect.

ULISSE COMPACT IP

Nowe urządzenie PTZ bazujące na adresie IP; pełna integrowalność w systemie network i sterowanie wszystkimi funkcjami PTZ w oparciu o adres IP.

www.videotec.com

VIDEOTEC

Na Targach Kielce wszystko jest pod kontrolą

Na targach **SPORT-OBIEKT i ALARM** swoje produkty zaprezentowało 45 wystawców z całej Polski. Specjalistyczne konferencje **„Bezpieczny stadion”** i **„Bezpieczne miasto”** zgromadziły blisko 500 słuchaczy. Na uroczystej gali wręczono medale Targów Kielce oraz puchary PZPN za wieloletnią pracę na rzecz poprawy bezpieczeństwa na stadionach piłkarskich.

Na Wystawie Wyposażenia i Budowy Obiektów Sportowych SPORT-OBIEKT można było zapoznać się ze świetnie sprawdzającym się już na wielu stadionach sprzętem oraz z najnowocześniejszymi rozwiązaniami służącymi poprawie bezpieczeństwa w obiektach sportowych. Głównym elementem wystawy, jak co roku, była współorganizowana przez PZPN konferencja „Bezpieczny stadion”. Gośćmi spotkania byli m.in. komendant główny policji gen. insp. **Andrzej Matejuk** oraz prezes PZPN **Grzegorz Lato**.

Na konferencji mówiono przede wszystkim o stanie przygotowań do EURO 2012, bezpieczeństwie, a także roli służb porządkowych i informacyjnych oraz spottersów, czyli, ogólnie mówiąc, policjantów wyznaczonych do ochrony stadionów. Ponadto podsumowano prace Rady Bezpieczeństwa Imprez Sportowych. Poruszono również tematy związane z rozgrywkami Ekstraklasy, dotyczące m.in. identyfikacji kibiców na stadionach. Zakończeniem obrad była uroczysta gala, podczas której kilkanaście osób zostało uhonorowanych pucharami za całokształt działalności związanej z bezpieczeństwem na meczach piłki nożnej. Najlepszych z najlepszych wytypowali Ekstraklasa SA, Piłkarska Liga Polska oraz Polski Związek Piłki Nożnej. Nagrody wręczył Janusz Matusiak, wiceprezes ds. piłkarstwa profesjonalnego PZPN (lista nagrodzonych oraz fotoreportaż na *www.zabezpieczenia.com.pl* – przyp. red.).

Puchar przyznano również komendantowi głównemu policji – generalnemu inspektorowi Andrzejowi Matejukowi. Obowiązki zmusiły go jednak do wcześniejszego powrotu do stolicy, dlatego nagrodę wręczył mu prezes PZPN Grzegorz Lato podczas konferencji „Bezpieczny stadion”.

Z kolei na dwudniowej wystawie ALARM, która w tym roku odbyła się już po raz jedenasty, przedstawiono różne formy zabezpieczeń, systemy sygnalizacji i ostrzegania, systemy monitoringu wizyjnego, a także wyposażenie

specjalistycznych grup prewencyjnych. Targom od lat towarzyszy konferencja pod hasłem „Bezpieczne miasto". Spotkanie jest poświęcone monitoringowi wizyjnemu miast, ale również małych miejscowości, osiedli, szkół, autobusów, a nawet obiektów sakralnych. Ze względu na katastrofy, jakie dotknęły Polskę tego lata, tematyka spotkania objęła również problem powodzi. Mówiono zatem również o przeciwdziałaniu i likwidowaniu jej skutków.

Dowodem wysokiej rangi imprez są autorytety, które objęły nad nią honorowy patronat: minister spraw wewnętrznych i administracji **Jerzy Miller**, minister sprawiedliwości **Krzysztof Kwiatkowski**, świętokrzyski komendant wojewódzki policji w Kielcach mł. insp. **Mirosław Schossler**, Polski Komitet Olimpijski, wojewoda świętokrzyski **Bożentyna Pałka-Koruba**, marszałek województwa świętokrzyskiego **Adam Jarubas** oraz prezydent Kielc **Wojciech Lubawski**.

W sumie stoiska zwiedziło ponad 1500 specjalistów.

Bezpośr. inf. Targi Kieleckie


SPORT-OBIEKT
X Ogólnopolska Wystawa Wyposażenia i Budowy Obiektów Sportowych
10th Exhibition of Sport Facilities, Fittings and Construction
X Międzynarodowa Konferencja
BEZPIECZNY STADION
ALARM
BEZPIECZNY STADION


PZPN
TargiKielce


PZPN
TargiKielce


PZPN
TargiKielce


PZPN


SPORT-OBIEKT
BEZPIECZNY STADION
ALARM
BEZPIECZNY STADION


X Ogólnopolska Wystawa Wypos
10th Exhibition of Sport Fa
X Międzynarodow
BEZPIECZNY ST


PZPN
TargiKielce


TargiKielce


Targi


TargiKielce


TargiKielce

PISA w Kielcach

W dniach 4–5 listopada 2010 r. zwiedzający wystawę **ALARM 2010** i uczestnicy odbywającej się równolegle konferencji *Bezpieczne Miasto – Monitoring Wizyjny Miast* mieli możliwość zapoznania się z wybranymi rozwiązaniami technologicznymi i sprzętowymi firm członkowskich **Polskiej Izby Systemów Alarmowych (PISA)**.

W ramach zorganizowanego przez PISA – po raz pierwszy w takiej formule – przestrzennego stoiska pod hasłem *Przegląd technologii stosowanych w systemach monitoringu wizyjnego miast i obiektów sportowych* zaprezentowały się firmy: **C&C Partners Telecom, Microsystem, Robert Bosch, Siemens, Sprint, UTC Fire&Security Polska**. Na stoisku zaprezentowano kamery stacjonarne, zintegrowane kamery szybkoobrotowe, kamery megapikselowe, systemy rejestracji i archiwizacji, analogowe i cyfrowe systemy transmisji sygnałów wizyjnych i sterujących, systemy transmisji radiowej i systemy inteligentnej analizy obrazu.

Firma Robert Bosch dostała medal Targów Kielce za inteligentną analizę wizyjną. Wyróżnienia Targów Kielce otrzymała firma Microsystem za bezzałogową jednostkę latającą pionowego startu i lądowania 11D4-200 oraz firma Sprint za system monitoringu wizyjnego oparty na bezprzewodowej komunikacji.

Obok stoiska PISA obecne były także stoiska innych firm członkowskich, takich jak **ACSS ID Systems, Fortuna Communication, Gunnebo Polska, ISM Eurocenter.**

Firma ISM Eurocenter otrzymała Puchar Polskiego Związku Piłki Nożnej za Avigilon – kompleksowy system wideonadzoru wysokiej rozdzielczości przeznaczony do stosowania w obiektach sportowych – oraz wyróżnienie Targów Kielce za Nice Situator.

W trakcie konferencji Waldemar Więckowski, doradca Zarządu PISA, omówił technologie i urządzenia wykorzystywane w systemach monitoringu wizyjnego, a także wskazał optymalne warunki ich zastosowania na tle wymagań projektu rozporządzenia MSWiA w sprawie utrwalania przebiegu imprezy masowej. Z danych PISA wynika, że projekt rozporządzenia znajduje się obecnie na etapie notyfikacji Unii Europejskiej.

Dobrym uzupełnieniem wystąpienia przedstawiciela PISA była samodzielna konferencyjna prezentacja Andrzeja Jarzyny z firmy członkowskiej S.P.S. Trading zatytułowana *Monitoring telewizyjny w technologii High Definition – zastosowania na potrzeby administracji lokalnej.*

Opracował: Henryk Dąbrowski
PISA

БЕЗПЕКА 2010

podsumowanie

W dniach **26–29 października br. w Kijowie** odbyła się 15. jubileuszowa międzynarodowa wystawa **BEZPEKA 2010** (**BEZPIECZEŃSTWO 2010**). Wśród około 170 wystawców znalazły się firmy z Ukrainy, Austrii, Białorusi, Niemiec, Holandii, Polski, Rosji i Francji. Zaprezentowały pełne spektrum technologii, sprzętu i usług mających służyć zapewnieniu bezpieczeństwa prowadzonej działalności, ludzi i ich mienia. Pokazano urządzenia i systemy sygnalizacji włamania i napadu, telewizji dozorowej i kontroli dostępu. Zaprezentowały się również (co należy do rzadkości na targach SECUREX) firmy zajmujące się bezpośrednią ochroną fizyczną. Swoje stoiska miały również Narodowa Akademia Nauk Ukrainy, Ministerstwo Spraw Wewnętrznych, Służba Bezpieczeństwa Ukrainy (organizacja na wzór naszych byłych straży przemysłowych) i Ukraińska Federacja Profesjonalnego Bezpieczeństwa (ta organizacja jest członkiem Europejskiego Klubu Organizacji Branży Ochrony ESBOC).

Przy okazji wystawy odbyły się **tematyczne konferencje**, w tym dwie zorganizowane przez Ukraińską Federację Profesjonalnego Bezpieczeństwa. **Pierwsza**, w dniu 26 października, dotyczyła wpływu pozarządowych organizacji branży ochrony na rynek bezpieczeństwa krajów europejskich.

W konferencji wzięła udział Polska Izba Ochrony (PIO), która przygotowała prezentację dotyczącą historii branży ochrony w Polsce, uwarunkowań prawnych jej funkcjonowania, a także tendencji rozwojowych w nadchodzących latach. Prezentacja spotkała się z bardzo dużym zainteresowaniem

VI Konferencja „Razem bezpieczniej"

W dniach **6–8 października 2010 r.** w województwie zachodniopomorskim już po raz szósty odbyła się konferencja **„Razem bezpieczniej"** współorganizowana przez **Komendanta Wojewódzkiego Policji w Szczecinie** oraz **Fundację „Razem Bezpieczniej"** przy współudziale zarządu województwa zachodniopomorskiego **OSIiTZTiZB „POLALARM"**.

Mimo upływu lat konferencja jak zwykle cieszyła się dużym powodzeniem. Wzięło w niej udział 52 uczestników, wśród których można było spotkać zarówno przedsiębiorców prowadzących koncesjonowaną działalność w zakresie ochrony osób i mienia, jak i osoby odpowiedzialne za ochronę w instytucjach oraz obiektach podlegających obowiązkowej ochronie.

Jak co roku w konferencji uczestniczyli przedstawiciele Ministerstwa Spraw Wewnętrznych i Administracji, Komendy Głównej Policji, Polskiej Izby Ochrony, a także Komendy Wojewódzkiej Policji.

Rozpoczęcia i otwarcia konferencji dokonał komendant wojewódzki policji w Szczecinie nadinsp. **Wojciech Olbryś**, który wysoko ocenił jej znaczenie i zapewnił uczestników, że w następnym roku VII konferencja będzie także zorganizowana. W kolejnych wystąpieniach prezes zarządu Fundacji „Razem Bezpieczniej" podinsp. **Waldemar Palejko** oraz prezes zarządu województwa zachodniopomorskiego OSIiTZTiZB „POLALARM" **Krzysztof Borowy** powitali uczestników konferencji i dokonali krótkiej oceny dotychczasowych spotkań. Wspólnie ocenili, że jednym z pozytywnych efektów tychże konferencji jest nie tylko poprawa współdziałania firm ochrony z policją zachodniopomorską, ale także poprawa współpracy pomiędzy podmiotami gospodarczymi, które na co dzień stanowią wobec siebie konkurencję.

Tematy, jakie poruszano w czasie konferencji, dotyczyły:

– przygotowań do mistrzostw w piłce nożnej EURO 2012,
– zmian w ustawie o ochronie osób i mienia,
– analiz kontroli SUFO ochraniających obiekty, w których gromadzone są dobra kultury,
– bezpieczeństwa imprez masowych,
– problemów związanych z cofnięciem koncesji,
– oceny działalności SUFO na terenie województwa zachodniopomorskiego.

Pierwsze dwa tematy – *Przygotowania prywatnych firm branży ochrony do zadań związanych z bezpieczeństwem MPN EURO 2012, wynikających z ustawy o ochronie imprez masowych oraz Propozycje zmian w ustawie o ochronie osób i mienia zgłoszone przez branżę ochrony podczas spotkania w dniu 2 lutego 2010 r. w MSWiA* – przedstawił prezes Polskiej Izby Ochrony **Sławomir Wagner**. Podczas swojego wystąpienia połączonego z prezentacją zapoznał uczestników z wnioskami płynącymi z dotychczasowych spotkań w kraju oraz z partnerami zagranicznymi, które miały związek z udziałem polskich przedsiębiorców zajmujących się ochroną osób i mienia w imprezie EURO 2012. Przedstawił uczestnikom także stan prac nad zmianami w ustawie oraz składane przez branżę ochrony propozycje zmian w tej ustawie. W czasie dyskusji na powyższe tematy poruszono także problemy wynikające z rozporządzenia MSWiA z dnia 7 września 2010 r.

uczestników, co wynika z faktu, że branża ochrony na Ukrainie, w przeciwieństwie do Polski, nie ma żadnych obwarowań prawnych swojej działalności. Działalność ta ma też ograniczony zakres (mały segment rynku bezpieczeństwa).

Druga konferencja, w dniu 27 października, dotyczyła walki z dumpingiem cen na rynku zabezpieczeń. Jak wynikało z wystąpień, rynek ukraiński również zmaga się z problemem zaniżania cen usług. Zaproszony przez organizatora konferencji przedstawiciel PIO przedstawił problem dumpingu cen w Polsce. Zwrócił szczególną uwagę na patologie spowodowane stosowaniem się do ustawy o zamówieniach publicznych, w tym stosowaniem jedynego kryterium przy wyborze wykonawcy, jakim jest cena – i to najniższa.

W dniu 28 października miało miejsce wydarzenie, które jest rzadkością na tego typu imprezach. Po raz kolejny odbył się **finał konkursu Miss Security Ukrainy 2010**. Przedstawicielki płci pięknej, które są pracownicami ukraińskich firm ochrony (takie są założenia tego konkursu) zaprezentowały się przed wystawcami i publicznością targów. Nie są to profesjonalne modelki, ale zostały profesjonalnie przygotowane przez osobę z dużym doświadczeniem w tym zakresie. Organizatorzy powierzyli przewodniczenie jury konkursu przedstawicielowi Polskiej Izby Ochrony. Trzeba przyznać, że zorganizowanie takiego konkursu jest znakomitym pomysłem. Może należałoby rozważyć zorganizowanie podobnego konkursu podczas kolejnej edycji naszych targów SECUREX. W polskich firmach branży *security* też pracuje dużo przedstawicielek płci pięknej.

Sławomir Wagner
Redakcja

w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne. Korzystając z udziału przedstawicieli Komendy Głównej Policji w konferencji, wyjaśniano wątpliwości związane z interpretacją niektórych zapisów tegoż rozporządzenia. Szczególne uznanie wzbudziły rzeczowe wyjaśnienia nadkomisarz **Katarzyny Olejnik** – naczelnik Wydziału Nadzoru nad SUFO Biura Prewencji KGP.

Kolejny temat, omówiony przez starszego aspiranta **Bogdana Jankowskiego** z Głównego Sztabu Policji KGP, to *Przygotowanie polskiej policji do zapewnienia bezpieczeństwa i zadania jednostek organizacyjnych policji garnizonu zachodniopomorskiego oraz współpraca z podmiotami pozapolicyjnymi w ramach policyjnego zabezpieczenia EURO 2012*. Bardzo dobrze przygotowana prezentacja pozwoliła uzmysłowić uczestnikom konferencji, jak wielkim przedsięwzięciem organizacyjnym, wymagającym wiele wysiłku i czasu, jest przygotowanie zabezpieczenia tego typu imprezy.

Temat ten był ściśle związany z kolejnym tematem, omówionym przez nadkomisarza **Konrada Kornemana** z GSP KGP – *Uprawnienia członków służb porządkowych i członków służb informacyjnych organizatora imprezy masowej w aspekcie uregulowań ustawy o bezpieczeństwie imprez masowych i przepisów wykonawczych.* Prelegent pokazał, jak duża odpowiedzialność spoczywa na wszystkich uczestnikach procesu przygotowawczego i etapu realizacyjnego związanego z organizacją ochrony imprezy masowej, wskazując jednocześnie na ich obowiązki w tym procesie.

W związku z tym, że wielu przedsiębiorców zajmuje się ochroną imprez masowych, podczas dyskusji omawiano problemy, które napotykają oni w praktycznym działaniu, oraz wyciągano wnioski dotyczące ich dalszej pracy.

Analiza kontroli SUFO sprawujących ochronę w muzeach i innych obiektach, w których gromadzone są dobra kultury narodowej przeprowadzonych przez Policję w latach 2008–2010 to temat omówiony przez nadkomisarz **Katarzynę Olejnik**, jak zawsze znakomicie przygotowaną. Przedstawiła wyniki kontroli, wyraźnie eksponując niedociągnięcia, jakie występowały w ochronie tychże obiektów. Przedsiębiorcy zajmujący się ochroną tego typu obiektów powinni zatem wyeliminować popełniane błędy – poprzez stałą ochronę fizyczną lub ochronę w systemie dozoru sygnałów. Oprócz przedsiębiorców w dyskusji na ten temat aktywny udział wziął przedstawiciel Pionu Ochrony Muzeum i Bezpieczeństwa Zbiorów Muzeum Narodowego w Szczecinie.

Temat *Cofnięcie koncesji – praktyka oraz orzecznictwo sądów w tym zakresie* omówiła **Agnieszka Bronisz** – naczelnik Wydziału Kontroli MSWiA. Oprócz aspektów prawnych oraz danych statystycznych dotyczących postępowań oraz cofnięcia koncesji omówiła proces postępowania w przypadku zamiaru cofnięcia koncesji, w tym także uprawnienia podmiotu, w stosunku do którego wystąpiono z zamiarem cofnięcia koncesji.

Policję zachodniopomorską reprezentował mł. insp. **Piotr Ostrowski** – naczelnik WPA KWP w Szczecinie. Temat jego wystąpienia to *Przedstawienie sprawozdania z kontroli działalności SUFO na terenie województwa zachodniopomorskiego.* Dokonał on analizy wyników omawianej kontroli. W trakcie swojego wystąpienia zwrócił szczególną uwagę na najczęstsze rodzaje uchybień w ochronie. Prelekcja wywołała ożywioną dyskusję, podczas której nie tylko przedstawiano swoje racje, ale także szukano rozwiązań konkretnych problemów.

Podsumowania konferencji dokonali wspólnie naczelnik WPA KWP w Szczecinie, prezes zarządu Fundacji „Razem Bezpieczniej" oraz prezes zarządu województwa zachodniopomorskiego OSIiTZTiZB „POLALARM". Zapewnili, że – tak jak zapowiedział komendant wojewódzki policji w Szczecinie – dołożą wszelkich starań, żeby VII konferencja została przygotowana. Poza tym zasugerowali uczestnikom spotkania wysłanie do przedsiębiorców zajmujących się ochroną osób i mienia ankiety, w której mogliby zaproponować tematy, jakie w przyszłym roku powinny być omawiane podczas konferencji.

Krzysztof Borowy

Ogólnopolskie warsztaty SAP 2010

Już po raz osiemnasty, w dniach 23–25 września br., **firma POLON-ALFA Zakład Urządzeń Dozymetrycznych** zorganizowała jedne z największych w Polsce warsztatów pod nazwą *Sygnalizacja i automatyka pożarowa SAP 2010*. Impreza, jak co roku, miała na celu poszerzanie wiedzy z zakresu ochrony przeciwpożarowej oraz zapoznanie uczestników z nowymi rozwiązaniami, trendami i regulacjami prawnymi – ze szczególnym uwzględnieniem praktycznego wykorzystania przekazywanych informacji.

Tegoroczne spotkanie dotyczyło instalacji sygnalizacji i automatyki pożarowej. Wybór takiej tematyki miał związek z wątpliwościami wielu instalatorów systemów sygnalizacji pożarowej dotyczącymi między innymi instalowania sygnalizatorów w pętlach dozorowych, a także zasad projektowania i wykonywania instalacji zawierających rozproszone elementy systemu oraz ich ochrony przed przepięciami i zakłóceniami.

W tym roku impreza zmieniła nazwę. Inne były też termin i miejsce, w którym się odbyła. Urocze zakątki kujawsko-pomorskiego Zacisza zamieniono na nie mniej ciekawe okolice łódzkich Smardzewic.

Program warsztatów objął wystąpienia wielu osób – znanych i cenionych w środowisku związanym z ochroną pożarową.

Referat **Edwarda Skiepko** *Zasilanie urządzeń przeciwpożarowych i sterowanie urządzeniami automatyki pożarowej zasilanymi napięciem 230 / 380 V_{AC}* dotyczył problemów z zakresu automatyki pożarowej niskich napięć i automatycznych urządzeń do wentylacji pożarowej, coraz częściej stosowanych.

W referacie pt. *Rozproszone zasilanie w pożarowych instalacjach sygnalizacji i ostrzegania* **Janusz Sawicki** z Instytutu Techniki Budowlanej poruszył problem zapewnienia ciągłości dostaw energii, koniecznej do poprawnej pracy urządzeń systemów sygnalizacji pożarowej.

Referat **Jerzego Ciszewskiego** z Instytutu Techniki Budowlanej pt. *Instalacje systemów rozproszonych i sieciowych* dotyczył zagadnień związanych z tworzeniem instalacji w rozległych i rozproszonych obiektach. Wystąpienie to zakończyło się bardzo ciekawą i długą dyskusją obecnych na sali słuchaczy.

Pierwszy dzień warsztatów zakończył się uroczystą kolacją, po której uczestnicy mogli poczuć się jak w Las Vegas. Przed wszystkimi chętnymi stało otworem Casino. Nagrody dla najlepszych graczy były cenne, dlatego każda z gier cieszyła się niezwykłą popularnością. Aby tradycji stało się zadość, impreza zakończyła się tańcami.

Piątek powitał uczestników warsztatów pięknym słońcem na prawie bezchmurnym niebie. Jako pierwszy wystąpił **Mirosław Zielenkiewicz** z firmy **RST** z Białegostoku. Jego referat nosił tytuł *Zabezpieczenie pożarowych instalacji alarmowych przed przepięciami i zakłóceniami elektromagnetycznymi*. Omówione w nim problemy dotyczą zwłaszcza regionów Polski narażonych na częste występowanie wyładowań atmosferycznych. Uczestnicy z wyraźnym zaangażowaniem dzielili się uwagami na temat stosowanych w zabezpieczaniu urządzeń.

Następny referat pt. *Bezpieczne instalacje przeciwpożarowe* wygłosiła **Alina Rychlik-Paradowska** z firmy **Dynamik** z Krakowa. Uczestnicy przyjęli jej wystąpienie z dużym zainteresowaniem. Informacje dotyczące stosowania różnego typu przewodów były dla nich niezwykle cenne.

Następnie wystąpił **Piotr Okniński** z firmy **BAKS** z Karczewa, który wygłosił referat pt. *Prowadzenie kabli pożarowych w instalacjach sygnalizacji i automatyki z wykorzystaniem elementów systemu BAKS*. Nawiązał on do wystąpienia Aliny Rychlik-Paradowskiej.

Sygnalizatory w pętlach dozorowych central – wykorzystanie i zasady instalowania oraz *Lokalizacja sygnalizatorów w pożarowych instalacjach alarmowych* to tytuły dwóch kolejnych referatów – **Mariusza Sobeckiego** z legnickiego oddziału **SITP** i **Mariusza Sowińskiego** reprezentującego organizatora.

Jako ostatni wystąpił **Władysław Markowski** z firmy **POLON-ALFA** z referatem *Instalacje wykrywania pożaru w przestrzeniach zagrożonych wybuchem*, w którym poruszył problem instalacji iskrobezpiecznych w obiektach przemysłowych.

Później przyszedł czas na rozrywkę – zawody strzeleckie (broń długa, krótka, łuk), zorbing, most tybetański, quady, chodzenie po rozżarzonych węglach, pokaz tańca z ogniem. Wszystkie te atrakcje cieszyły się niezwykłą popularnością – tym bardziej, że do zaciętej rywalizacji motywowała perspektywa zdobycia atrakcyjnych nagród. Wieczór i noc spędzono przy ognisku, rozmawiając na tematy związane nie tylko z branżą. Najwytrwalsi udali się na spoczynek, gdy zaczęło świtać.

Taki był przebieg osiemnastych, już ogólnopolskich warsztatów SAP 2010. Organizatorzy dziękują wszystkim uczestnikom za wspólnie spędzony czas i mają nadzieję, że wprowadzone zmiany zostały przez nich życzliwie przyjęte, a warsztaty, prócz źródła wiedzy fachowej, stały się imprezą integrującą środowisko.

Bezpośr. inf. Elżbieta Czajka
POLON-ALFA

Seminarium eksperckie Polskiej Izby Systemów Alarmowych

podsumowanie

21 października 2010 r. w Windsor Palace Hotel w Jachrance k/Warszawy **Polska Izba Systemów Alarmowych (PISA)** zorganizowała i przeprowadziła, przy współpracy z **Instytutem Mechaniki Precyzyjnej**, pierwsze seminarium eksperckie poświęcone **realizacji zabezpieczeń elektronicznych i mechanicznych na podstawie wymagań** *Rozporządzenia ministra spraw wewnętrznych i administracji w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne.*

W seminarium, które zgromadziło pięćdziesięciu słuchaczy, wzięli udział eksperci i specjaliści PISA oraz liczni przedstawiciele wojska, policji, banków i wiodącego towarzystwa ubezpieczeniowego.

Seminarium było edukacyjnym zwieńczeniem merytorycznego zaangażowania Polskiej Izby Systemów Alarmowych w prace nad projektem rozporządzenia.

Nowe rozporządzenie Ministra Spraw Wewnętrznych i Administracji zostało podpisane 7 września 2010 r. i opublikowane w Dz.U. z 2010 r. Nr 166, poz. 1128.

Nowością w stosunku do poprzedniego rozporządzenia jest załącznik nr 1 *Wymagania dla elektronicznych systemów zabezpieczeń* oparty na projekcie Polskiej Izby Systemów Alarmowych, który, z niewielkimi zmianami wynegocjowanymi w trakcie konsultacji, został zatwierdzony w dokumencie końcowym. W pracach nad projektem rozporządzenia PISA efektywnie współpracowała z Instytutem Mechaniki Precyzyjnej tworzącym propozycje załączników dotyczących zabezpieczeń mechanicznych.

W trakcie prac nad rozporządzeniem PISA zorganizowała dwie konferencje – *Ochrona wartości pieniężnych i bezpieczeństwo banków w świetle nowych wymagań normatywnych dla systemów alarmowych. Przełom czy kompromis?* (25 listopada 2009 r., bank PEKAO SA) oraz *Wymagania i wytyczne stosowania nowych polskich norm w praktyce projektowania i budowy systemów alarmowych* (28 kwietnia 2010 r., SECUREX) – poświęcone projektowanym wymaganiom rozporządzenia w powiązaniu z zasadami budowy systemów alarmowych określonymi w nowym dokumencie normatywnym.

Jak podkreślono na wstępie seminarium, wejście w życie rozporządzenia spowodowało bardzo duże zainteresowanie praktycznymi aspektami jego wymagań. Tym bardziej, że wymagania te mają ścisłe powiązanie z nie tak dawno uchwaloną nową polską normą (PN-EN 50131-1) dotyczącą systemów alarmowych.

Przez ponad osiem godzin eksperci PISA, którzy odegrali wiodącą rolę w pracach nad normą europejską i rozporządzeniem, wspólnie omawiali, analizowali i komentowali m.in.: uwarunkowania normatywne nowego rozporządzenia, zmiany w treści rozporządzenia, zapisy załącznika nr 1 i 2 do rozporządzenia, wymagania normatywne na tle wymagań rozporządzenia ze szczególnym uwzględnieniem 2. stopnia zabezpieczenia, problemy w dostosowaniu realizacji zabezpieczeń technicznych do wymagań rozporządzenia, a eksperci Instytutu Mechaniki Precyzyjnej – konsultanci treści załącznika nr 2 rozporządzenia – objaśniali wymagania wobec pomieszczeń, urządzeń i pojemników do przechowywania wartości w powiązaniu z ich wielkością, wymagania wobec bankowozów z zakresu zabudowy mechanicznych urządzeń zabezpieczających, a także obowiązujące w tych dziedzinach zasady badań i certyfikacji.

Autorami seminarium byli: **Maksymilian Majerski** – ekspert PISA, wykładowca Ośrodka Szkoleniowego PISA, przedstawiciel PISA w Komitecie Technicznym 52 przy PKN, tłumacz i współautor polskich wersji norm grupy PN-EN 50131; **Andrzej Tomczak** – ekspert PISA, wykładowca Ośrodka Szkoleniowego PISA, przedstawiciel PISA w Komitecie Technicznym 52 przy PKN, autor projektu tekstu załącznika nr 1 *Wymagania dla elektronicznych systemów zabezpieczeń* rozporządzenia MSWiA z 7 września 2010 r.; **Jerzy Chytła** – kierownik akredytowanego laboratorium badawczego Instytutu Mechaniki Precyzyjnej (IMP), ekspert w dziedzinie projektowania i badań wyrobów do przechowywania i transportowania wartości, konsultant opracowania załącznika nr 2 *Limity wartości pieniężnych przechowywanych lub transportowanych w pomieszczeniach i urządzeniach* rozporządzenia MSWiA z 7 września 2010 r.; **Miron Durzewski** – kierownik techniczny akredytowanego laboratorium badawczego Instytutu Mechaniki Precyzyjnej, ekspert w dziedzinie projektowania i badań mechanicznych urządzeń zabezpieczających, konsultant opracowania załącznika nr 2 *Limity wartości pieniężnych przechowywanych lub transportowanych w pomieszczeniach i urządzeniach* rozporządzenia MSWiA z 7 września 2010 r.

Opracował: Henryk Dąbrowski
dyrektor PISA

INT-KSG

manipulator **sensoryczny**

Manipulator sensoryczny INT-KSG wprowadza nową jakość w obsłudze systemu bazującego na centralach INTEGRA...

...funkcje MAKRO, personalizowane menu i konfigurowalny wygaszacz ekranu. Wejdź na **www.satel.pl** i sprawdź co jeszcze może Ci zaoferować nowy manipulator sensoryczny INT-KSG.

Nowość

20 1990 2010 | Satel

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

Organizacja wirtualna

jako obiekt ochrony fizycznej i technicznej

Marek Blim

Artykuł ma charakter problemowy i ma na celu przybliżenie tematyki realizacji zadań ochronnych w warunkach tworzenia i funkcjonowania współczesnych biznesowych organizacji wirtualnych z uwzględnieniem roli ochrony fizycznej i technicznej w uczestniczącej firmie

Wprowadzenie

O środowisku wirtualnym zaczęto mówić w końcówce lat 80. minionego wieku, kiedy to pojawiły się pierwsze gry realizowane w świecie nierzeczywistym (specjalne hełmy lub gogle zapewniały wizualizację nieistniejącego świata, rękawice i dywanik z sensorami nacisku/ruchu przenosiły nas w głąb nieistniejącej przestrzeni), co czasami wykorzystywano w realizacji innych zadań (wirtualny przewodnik z 1986 r. po katedrze w Reims – po nieistniejących jej fragmentach, zburzonych w czasie I i II Wojny Światowej, a odtworzonych komputerowo, włącznie z fakturą gotyckich murów i widokami, na podstawie zgromadzonej dokumentacji fotograficznej; na jej podstawie fakturę poddano rekonstrukcji, którą ukończono w 1996 r.). Warto wspomnieć o współczesnych polskich dokonaniach – po trzech latach prac przeniesiono na ekran lot Liberatorem B-24 nad powstańczą Warszawą w 1944 roku (zaprezentowany w telewizji w lipcu 2010 roku), co jest wirtualnym odzwierciedleniem już nieistniejącej rzeczywistości (na podstawie historycznych materiałów fotograficznych).

O organizacji wirtualnej zaczęto mówić po roku 2000., kiedy to wraz z rozwojem techniki i technologii informacyjnych I&CT (*Information and Communication Technology*) oraz tendencją do globalizacji gospodarki rozpoczęto modyfikację dotychczasowych stosunków gospodarczych – przestała istnieć i liczyć się na rynku „stara, dobra firma" z jej tradycjami i stosunkami społeczno-socjalnymi, ulokowana w jednym miejscu.

O wirtualizacji pisano od początku ostatniej dekady minionego wieku. Zaczęło się od terminu „uczące się organizacje" (P. Senge – 1990 r.), później pojawiły się określenia „organizacje po reengineeringu" (M. Hammer, J. Champy – 1994 r.) i „organizacja wirtualna" (termin wprowadzony przez W. Dawidowa i M. Malone'a w 1992 r., a spopularyzowany przez J. Byrne'a w 1993 r.[1]). Było też wiele mniej czy bardziej udanych określeń uzupełniających (np. „zwariowane organizacje" – T. Peters, 1994 r.). W końcu w różnych pracach badawczych utrwalił się jednoznaczny termin „organizacja wirtualna" (J. Kisielnicki – lata 1997 i 1998; P. Siber, J. Grise – 1998 r.).

Sam termin „wirtualny" wywodzi się od łacińskich słów *virtualis*, czyli „skuteczny", i *virtus*, czyli „moc", i może oznaczać stan teoretycznie możliwy do zaistnienia.

1) Byrne J., „The Virtual Corporation", w: „Business Week" z 8 lutego 1993 r., s. 98–103.

1. Czym jest organizacja wirtualna?

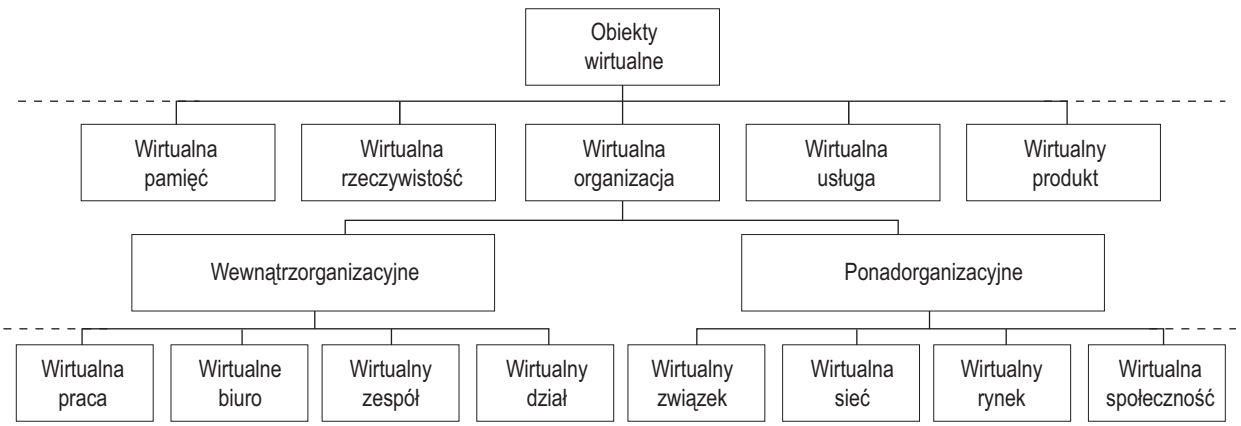
W czasie przerwy I Konferencji Zarządzania Bezpieczeństwem Obiektów, realizowanej w ramach Securex 2010, przedstawiciel jednej z organizacji zajmujących się ochroną różnych instytucji biznesowych zadał konfidencjonalne pytanie: „Kiedy to wszystko jest w jednym miejscu, w jednej firmie, i ja to ochraniam, to sprawa jest dla mnie prosta i zrozumiała, ale co to za wirtualne bezhołowie, gdzie nie sposób znaleźć odpowiedzialnego za realizację choćby podstawowej faktury za wykonaną ochronę fizyczną elementów ich struktur?" Nie ukrywam, że nie umiałem wówczas udzielić krótkiej i jednoznacznej odpowiedzi, stąd też inspiracja dla niniejszego wyjaśnienia.

Czym więc jest obecnie **organizacja wirtualna**? Liczba definicji i określeń jest olbrzymia. Poszczególne zapisy mówią, że jest to:

- **czasowa sieć** niezależnych przedsiębiorstw (dostawców, klientów, nawet wcześniejszych konkurentów) połączonych technologią informacyjną w celu dzielenia umiejętności i kosztów dostępu do nowych rynków;
- **sztuczny twór**, który ze względu na maksymalną użyteczność dla klienta i opierając się na indywidualnych kompetencjach bazowych, realizuje integrację niezależnych przedsiębiorstw w procesach (łańcuchowych) kreowania produktów, nie wymagając dodatkowego nakładu na koordynację oraz nie uszczuplając znaczenia klienta przez swoją wirtualność.

Czasami zapisy, odwołując się do szerzej rozumianych formuł, stwierdzają, że:

- **wirtualna organizacja gospodarcza** to zbiór jednostek organizacyjnych, przestrzennie rozproszonych (nawet w skali globalnej), realizujących wspólne przedsięwzięcie gospodarcze, wybieranych dynamicznie – według kryterium procesowego – do realizacji i na czas realizacji określonych zadań.
- **wirtualne przedsiębiorstwo** to forma współpracy (kooperacji) prawnie niezależnych przedsiębiorstw, instytucji i/lub osób fizycznych, które dostarczają na rynek dobra i usługi na bazie wspólnego stosunku gospodarczego, występując przy tym wobec innych podmiotów gospodarczych jako jednolite przedsiębiorstwo.



Rys. 1. Schemat pojmowania wirtualizacji obiektów i jej powiązań (Brzozowski M., „Ewolucja pojmowania wirtualności", KSiTZ AE Poznań, materiały „Management Forum 2020", SGH, Warszawa 2006.)

Globalizacja działań biznesowych to obecnie szukanie na rynku pracy jak najniższych kosztów a zarazem dobrej marki końcowego produktu/usługi, najlepiej bez kosztów pośrednich (mają być jak najniższe lub wręcz zerowe).

Przykładem wirtualnych przedsiębiorstw o charakterze globalnym mogą być dwaj znani producenci obuwia sportowego – amerykańska firma Nike i niemiecka Puma. W istocie rzeczy firmy te nie utrzymują własnych fabryk, lecz tylko zlecają produkcję kooperantom (głównie z Azji), zajmując się (w siedzibach narodowych) przede wszystkim projektowaniem i marketingiem oraz wsparciem działań kooperacyjnych[2]. Nie można tutaj mówić wyłącznie o kooperacji ponadnarodowej, bowiem są one wiodącymi przedsiębiorstwami w organizacji wirtualnej, na rzecz której dbają o jakość i utrzymanie marki na rozpoznanym i pod wieloma względami zdominowanym od strony produktu rynku globalnym.

Problem oceny organizacji wirtualnej wynika z jej na ogół krótkotrwałego, poniekąd zadaniowego działania i spłaszczonej struktury kierowania, a także wysokiej wymagalności etycznych zachowań jej członków co do sposobu i zakresu realizacji podjętego wspólnego przedsięwzięcia.

2) http://www.dot-com.net.pl/~bg.wolf/organizacja_wirtualna

2. Co podlega ochronie w tradycyjnie rozumianej organizacji?

Firma to budynek, mienie i ludzie, wszystko w jednym miejscu. Organizacyjnie i funkcjonalnie, od prezesa po szeregowego pracownika – tradycyjny, czytelny układ, obecnie mało prawdopodobny do zrealizowania, zwłaszcza w wielonarodowych korporacjach.

Charakterystyka bezpieczeństwa tak rozumianego przedsiębiorstwa dotyczy ściśle określonej lokalizacji, odpowiednio wcześniej określonej struktury firmy, objętej codzienną ochroną oraz weryfikowaną (według wcześniej określonych potrzeb i wymagań) identyfikacją zdarzeń. Wszystko to jest opisane i zdefiniowane w dokumentach dotyczących zapewnienia bezpieczeństwa – zgodnie z wymaganiami przepisów i zaleceniami norm.

Przykładem formalnym może być poniższa tabela.

1	Dokumenty koncepcji zabezpieczenia i ochrony siedziby firmy oraz systemu organizacyjno-technicznego zabezpieczenia i ochrony fizycznej tego obiektu
2	Wskazanie pionu organizacyjnego i osób lub opisanie struktury firmy – z uwypukleniem pionu odpowiedzialnego za zabezpieczenie i ochronę danej siedziby
3	Zakres obowiązków osób odpowiedzialnych za bezpieczeństwo fizyczne i techniczne firmy oraz nadzorujących przygotowanie koncepcji i systemu organizacyjno-technicznego zabezpieczenia i ochrony fizycznej obiektu
4	Dokumentacja projektowa systemów zabezpieczenia i ochrony siedziby firmy
5	Plany/harmonogramy/inne dokumenty dotyczące strategii budowy systemów zabezpieczenia i ochrony siedziby firmy
6	Umowy dotyczące serwisu i konserwacji systemów zabezpieczenia i ochrony siedziby firmy
7	Wewnętrznie zatwierdzone standardy/wytyczne/zalecenia dotyczące zabezpieczenia i ochrony obiektu, jakim jest siedziba firmy
8	Inne wymagania dotyczące zabezpieczenia i ochrony siedziby firmy
9	Wykaz firm zajmujących się ochroną techniczną i fizyczną oraz potwierdzenia ich uprawnień do wykonywania usług, tj. koncesje MSWiA na wykonywanie usług w zakresie ochrony fizycznej i zabezpieczenia technicznego (w określonym cyklu czasowym – według wymagań prawnych)
10	Dokumenty powołujące służby ochrony i osoby odpowiedzialne
11	Dokumentacja systemu organizacyjno-technicznego zabezpieczenia i fizycznej ochrony siedziby firmy oraz dokumentacja techniczna systemów zabezpieczenia technicznego
12	Plan ochrony obiektu (w szczególnych przypadkach uzgodniony z KW PP)
13	Polityka fizycznego i technicznego zabezpieczenia obiektu
14	Plany/instrukcje postępowania w sytuacjach kryzysowych i zagrożeń
15	Istniejąca (ewentualnie) prawna interpretacja zaklasyfikowania zabezpieczenia i ochrony siedziby do określonej grupy – według ustawy o ochronie osób i mienia oraz ustawy o ochronie informacji niejawnych, z uwzględnieniem innych wymagań ustawowych
16	Analizy zagrożeń dla siedziby (stałej i zapasowej), ujmujące w szczególności zagrożenia kryminalne i terrorystyczne
17	Plany ciągłości ochrony obiektu
18	Dokumentacja służby ochrony obiektu
19	Koncesje MSWiA dla podmiotów wykonujących prace na rzecz budowy systemów zabezpieczenia i ochrony siedziby firmy oraz świadczących usługi na rzecz zabezpieczenia i ochrony tej siedziby
20	Instrukcje ruchu osobowo-materiałowego i pojazdów stosowane w firmie
21	Zasady przechowywania i wydawania kluczy
22	Zasady przechowywania dokumentacji podlegającej ochronie w zakresie tajemnicy biznesowej

Tab. 1. Wykaz potrzebnych dokumentów dotyczących bezpieczeństwa budynku firmy (Materiały szkoleniowe VI kursu rzeczoznawców STZOiMoZB POLALARM, Warszawa, listopad 2007 – czerwiec 2008)

Wymienione w tabeli dokumenty odpowiadają sformułowanemu w prawie polskim oraz w stosowanych normach wymogowi zapewnienia pełnego bezpieczeństwa obiektu, który musi być chroniony.

Czy (i w jakim zakresie) podobne wymagania obowiązują w organizacji wirtualnej? W jaki sposób są spełniane w dziedzinie fizycznej i informacyjnej?

Trudno jest jednoznacznie odpowiedzieć na te pytania. Faktem jest szczelna ochrona siedzib i systemów informacyjnych jednej z wspomnianych wcześniej firm produkujących obuwie i odzież sportową (Nike)[3], będącej podręcznikowym przykładem wirtualnej organizacji funkcjonującej w warunkach globalizacji produkcji i handlu.

Spróbujmy zatem wstępnie ocenić zagrożenia dla organizacji wirtualnej i określić skutki ich materializacji w postaci ryzyka kosztów (szczególnie tych zlekceważonych lub pominiętych).

3. Zagrożenia dla organizacji wirtualnej

Przyglądając się obecnie znanym i skutecznie funkcjonującym organizacjom wirtualnym (OW), zauważamy dwie grupy działań mających na celu przeciwdziałanie dominującym zagrożeniom:

– zapewnienie bezpieczeństwa fizycznego, technicznego i informacyjnego firmie/przedsiębiorstwu będącemu członkiem OW;
– zapewnienie technicznej i fizycznej ochrony przekazów informacji oraz półproduktów w ramach OW.

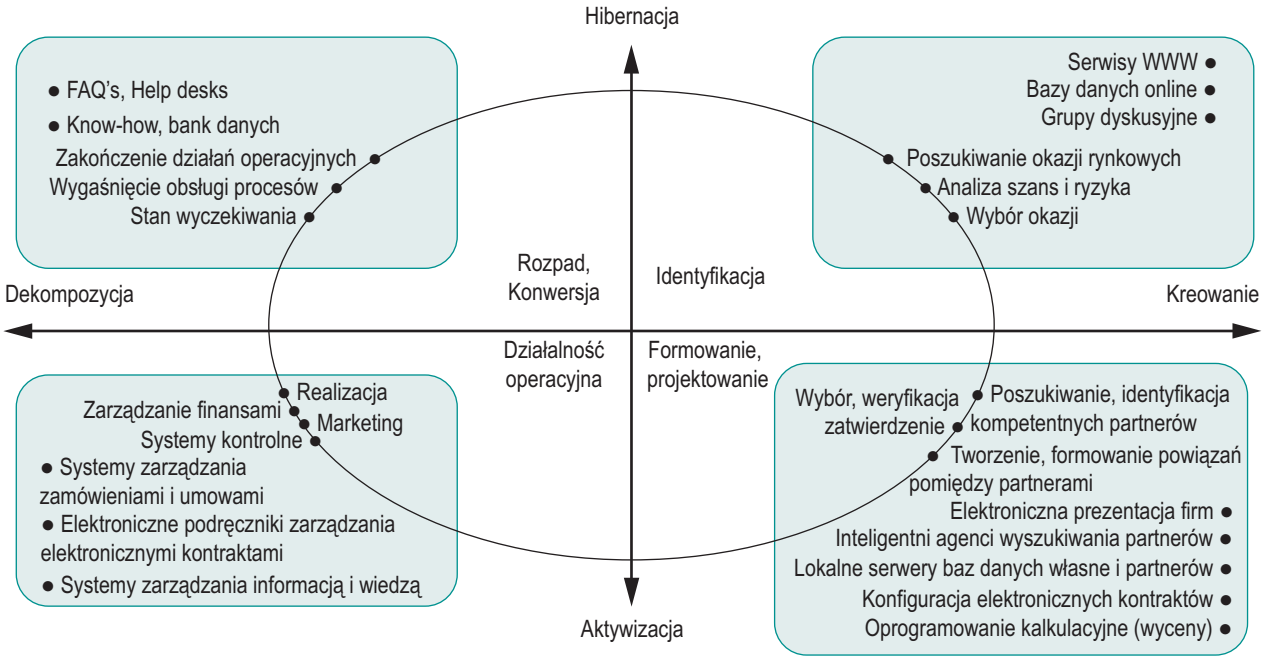
W ramach tej pierwszej grupy lokowane są również osobiste spotkania robocze szefów poszczególnych firm, odbywające się zwykle w odpowiednio zabezpieczonych pomieszczeniach jednej z nich, bowiem głównym zagrożeniem dla wspólnoty interesów firm-członków OW jest przedwczesne ujawnienie zamierzeń biznesowych i planowanego kierunku działań rynkowych OW jako całości. Specyficznym działaniem jest w tym przypadku tworzenie swoistego repozytorium OW dla danej grupy produktów/segmentu rynku w firmie wiodącej przy zachowaniu rygorów ochronnych dla takiego zasobu.

W ramach drugiej grupy obowiązują głównie rygory bezpieczeństwa informacyjnego (bezpieczne łącza – VPN, kryptografia biznesowa – SecurityID, szyfrowanie i kodowanie fonii oraz wizji w łączach telekonferencyjnych – np. system TANNBERG), ale równolegle stosowane są dodatkowe przedsięwzięcia ochronne o charakterze techniczno-technologicznym w odniesieniu do receptur, surowców i składu półproduktów (np. nie zgłasza się patentów i wzorów użytkowych/przemysłowych, spełnia się wyłącznie wymogi dotyczące utrzymania własności intelektualnej w tajemnicy – Art. 39 TRIPS).

Role tak chronionych technologii teleinformatycznych na każdym z poziomów funkcjonowania organizacji wirtualnej przedstawia rysunek 2.

Szczególnie serio traktowane są zagrożenia związane z zachowaniem personelu (wymogi kontraktów menedżerskich, zjawisko *head-hunting* czyli polowanie na pracowników, nielojalność) oraz nielojalnym/nieetycznym postępowaniem innych firm w związku z każdym z przedstawionych kierunków/etapów rozwoju i funkcjonowania organizacji wirtualnej.

3) Werner K., Weiss H., „Czarna lista firm. Intrygi światowych koncernów", Hidari, Stargard Szczeciński 2009.



Rys. 2. Technologia ICT w rozwoju organizacji wirtualnej (Jurg A., „Rola technologii teleinformatycznej w rozwoju organizacji wirtualnej", artykuł opublikowany 7 lipca 2009 r. na blogu „Agile".)

4. Ryzyka funkcjonowania w organizacji wirtualnej

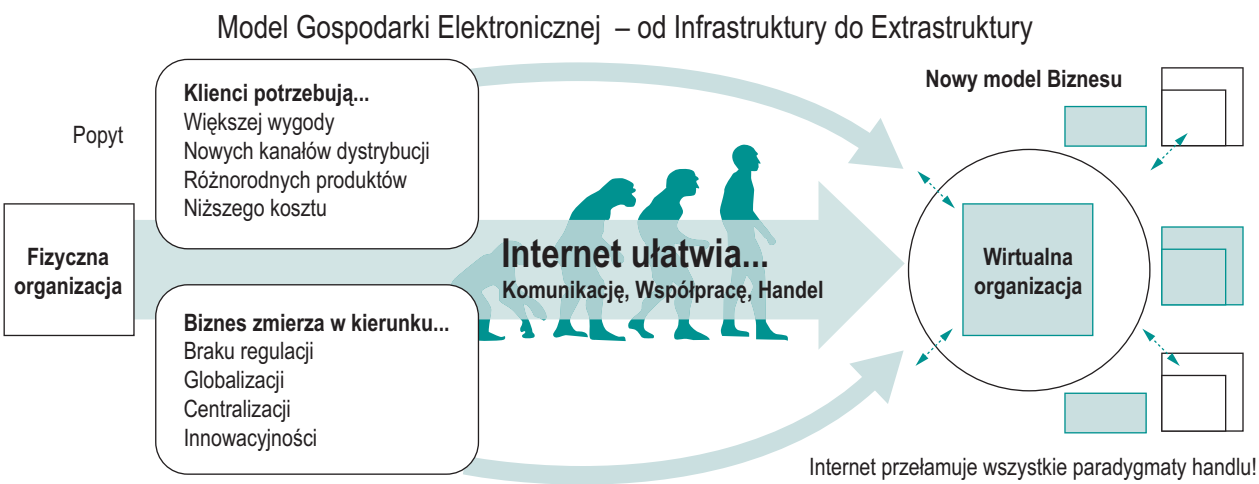
Pamiętając o pytaniu postawionym w punkcie 2, musimy powiedzieć wprost – ochrona fizyczna i techniczna każdego nadzorowanego obiektu materialnego jest związana z incydentami i zagrożeniami, które jako zdarzenia zachodzą w samym obiekcie i jego bezpośrednim otoczeniu. Jeśli zatem mamy organizację wirtualną, której elementy fizyczne znajdują się w Europie, Ameryce Łacińskiej i Azji (projektowanie, surowce, produkcja), to analiza zagrożeń i ocena ryzyka (mimo dokonania jej według ujednoliconych zasad) będzie oparta na różnych rozwiązaniach prawnych w odmiennych warunkach kulturowych, a jedynymi „twardymi", wspólnymi realiami będą ustalenia finansowe co do kosztów i ewentualnych strat.

Analiza tych wielu postaci ryzyka wskazuje na jeden czynnik główny – ryzyko nieetycznego działania jednej z firm/jednego z elementów składowych organizacji wirtualnej. Ryzyka związane z fizyczną i techniczną ochroną obiektu są z zasady przenoszone na lokalne agencje ochrony (do miejsca funkcjonowania danej części OW), a głównym dobrem chronionym jest gospodarka elektroniczna (rysunek 3).

Ryzyka funkcjonalne OW są w praktyce związane z rozległością fizyczną i czasową realizowanych procesów biznesowych (projektowanie, produkcja, marketing, sprzedaż), w których bardzo często obecni uczestnicy (firmy współpracujące przy ofercie OW lub na danym rynku) zajmują się jedynie fragmentarycznymi działaniami na rzecz produktu wspólnego, przy zachowaniu trwałości i ciągłości własnych lokalnych działań firmowych[4].

To, czy i na ile spełnione będą wymagania ochronne, założone przez firmę-lidera OW dla danej lokalizacji firmy współpracującej, jest wynikiem biznesowych uzgodnień dotyczących deklarowanej/powierzonej części procesu produkcji/sprzedaży oferowanego przez OW towaru. Działania chroniące OW przed ujawnionymi w danej firmie ryzykami funkcjonalnymi

4) Kwiatkowska L., Kierkowski Z., „Wirtualna organizacja pracy", mat. Instytutu Edukacji Interaktywnej, estakada.pl.



Rys. 3. Zmiany modelowe w gospodarce XXI wieku (Materiały z wykładów prof. J. Kisielnickiego, www.organizacja-wirtualna.ezin.pl.)

muszą być wzajemnie uzgadniane z uwzględnieniem wszystkich zależności kształtujących w OW architekturę bezpiecznego biznesu (do jej analizy i oceny bardzo przydatna jest metodologia SABSA).

Odrębnym problemem jest wirtualizacja poszczególnych miejsc pracy w ramach OW (przy zachowaniu dostępności trwających procesów), ale kwestia ta dotyczy z zasady wysoko specjalizowanych pracowników korzystających z przygotowanych, chronionych fizycznie i technicznie, stanowisk (*workstations*), w warunkach odbiegających od ogólnie znanego zjawiska telepracy. Współzależności są pokazane na poniższym schemacie wzajemnego rozwoju i oddziaływań, nawigowania i „zanurzania się" w wirtualny świat pracy[5].

Biorąc pod uwagę zagrożenia funkcjonalne wyżej wymienionych specjalizowanych miejsc pracy OW, należy uwzględniać ich wysoką immersyjność w odniesieniu do pracownika wnikającego w wielogodzinnych okresach w wirtualny świat swojej pracy, w którym dosłownie otoczony jest przez wielosensoryczne, responsywne środowisko[6].

W literaturze dostępne są informacje o przypadkach, w których immersja przybiera charakter skrajny – użytkownik jest tak zanurzony w świecie wirtualnym, że – według A. Pisarskiego opisującego cyberprzestrzeń – przestaje odróżniać świat fikcyjny od rzeczywistego (syndrom Don Kichota).

Jest to zatem zagrożenie funkcjonalne, ale występuje w wyjątkowo specyficznych warunkach i dotyczy tylko części osób w OW (projektanci Visio, specjaliści od wirtualnego marketingu itp.). Trzeba o nim pamiętać ze względu na rozwój reklamy 3D połączonej z możliwością wnikania klienta do wirtualnego świata celem lepszego poznania możliwości i zasad stosowania oferowanego produktu.

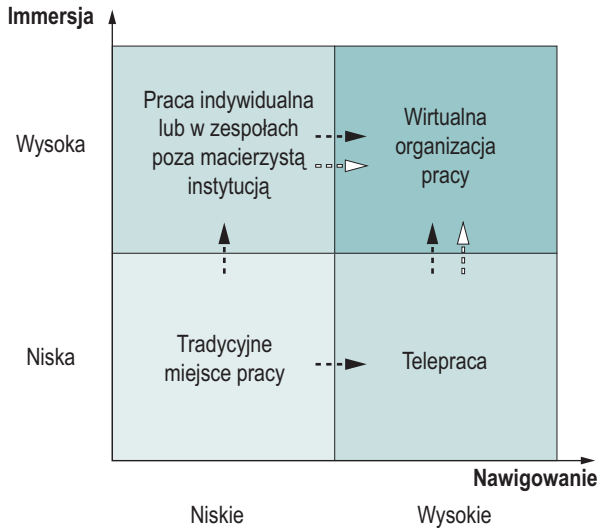
5. Organizacja wirtualna jako zbiór obiektów ochrony

Agencja ochrony, która jest odpowiedzialna za ochronę fizyczną i techniczną firmy będącej częścią organizacji wirtualnej, musi być przygotowana także na większą niż zazwyczaj odpowiedzialność, np. za elementy fizycznego transportu zewnętrznego (o ile występują w danej OW), a także na dodatkowe wymagania ochronne infrastruktury ICT (stosownie do przyjętych uzgodnień i zaleceń lidera OW).

To, co decyduje o sprawności i szybkości działania OW (reakcja na zmiany rynkowe, indywidualne potrzeby klienta, otwierające się nisze zbytu), jest związane głównie z komunikacją między partnerami-uczestnikami procesu biznesowego. Zbiorem obiektów w OW, które wymagają z tego powodu szczególnej ochrony, są elementy wspólnej infrastruktury teletechnicznej i teleinformatycznej. Ochrona fizycznego dostępu do nich

5) Tamże.

6) Użycie tutaj pojęcia immersyjności jest przywołaniem zjawiska z zakresu fizyki – poznawanie szczegółów zjawiska wymaga otoczki pozwalającej lepiej rozpoznawać i rozróżniać napływające sygnały – i odnosi się do konieczności przyswojenia niespotykanych w rzeczywistym środowisku sygnałów z wirtualnego otoczenia. Pojawia się więc kwestia przyswojenia przez człowieka, za pomocą jego naturalnych zmysłów, sytuacji wyobrażalnych, obrazowanych wieloma różnymi, skojarzonymi w umyśle odbiorcy sygnałami (wielosensoryczność), na podstawie których ocenia on reakcje tego wirtualnego otoczenia oraz skutki własnego w nim działania (responsywność).



Rys. 4. Schemat zależności we współczesnej organizacji pracy

nie odbiega od działań dotychczasowych, ochrona dostępności do zbiorów danych i informacji (hasła, kodowanie, kryptografia biznesowa) jest natomiast elementem realizowanej polityki bezpieczeństwa informacji i IT. Przyjęte zasady tej ochrony muszą zapewniać pewien wspólnie uzgodniony w OW poziom bezpieczeństwa informacyjnego poszczególnych jej uczestników (niezależnie od fizycznych, technicznych i prawnych uregulowań).

6. Paradoks: wirtualne pieniądze a rzeczywiste straty

Jako ciekawostkę biznesową traktowano uruchomioną w 2002 roku w USA w ramach porozumienia międzyuczelnianego (wiodącą instytucją był kalifornijski UCLA) wirtualną giełdę projektów uczelnianych[7], która z założenia miała poprawić zaangażowanie młodego personelu naukowego i przyśpieszyć (szczególnie wśród kadry uczelnianej) procesy wdrażania nowoczesnych rozwiązań zarządczych z zakresu ekonomii czasu pracy.

Przedstawiane w wirtualnym świecie rozwiązania były wstępnie wyceniane przez autorów, oceniane przez potencjalnych użytkowników w ramach działań wirtualnej giełdy oraz rekomendowane do stosowania w świecie realnym. Trwający zaledwie rok eksperyment został zamknięty, gdy w rzeczywistej sprzedaży ukazały się rozwiązania bezprawnie skopiowane (przez osoby trzecie), a dochodzenie strat przez autorów pomysłów napotkało na brak podstaw prawnych ze względu na brak uregulowań dotyczących własności ofert przedstawianych w wirtualnym świecie.

Zjawiska o podobnym charakterze (przenoszenie wirtualnych zobowiązań do realnego świata) występują obecnie w wielu wirtualnych grach, o czym warto pamiętać, gdy deklaruje się swój udział w takiej internetowej rozrywce – koszty są bowiem realne.

Podsumowanie

Jesteśmy obywatelami świata XXI wieku – z wszelkimi wynikającymi z tego konsekwencjami. Globalna wioska, połączona (ale i zarazem spętana) niezliczonymi więzami informacyjnymi, jest już dziś istniejącym środowiskiem, w którym z lepszym lub gorszym skutkiem działamy. Istnieje zatem jakaś struktura organizacyjna, w której procesy informacyjne oraz towarzyszące im zbiory, a także stanowiska przetwarzania informacji, muszą być chronione. Przyczyny takiego stanu rzeczy wynikają z rozwoju biznesu – także globalizacji handlu i rozwoju organizacji wirtualnych. W świetle tych zmian stanowisko kierującego/menedżera/zarządcy firmy można więc porównać do kokpitu samolotu, a zachowania – do zachowań pilota[8] (przywołuję ten przykład mimo przykrych skojarzeń). Mądrość i wiedza umożliwiają wnikliwą obserwację tych wskaźników, które w danej sytuacji są najistotniejsze. Pilot nie może przecież z taką samą uwagą obserwować wskaźniki wysokości i poziomu paliwa podczas startu i w trakcie lądowania. Istotność konkretnych parametrów podlegających obserwacji ulega zmianie. Menedżer powinien wiedzieć, co ma być obserwowane i jakie wartości są poprawne, a jakie wskazują na konieczność podjęcia działań korygujących.

Proces informacyjny i jego trwałe bezpieczeństwo staje się więc „być albo nie być" istnienia firmy/organizacji, co tym bardziej każe przyjrzeć się wszelkim związanym z nim ryzykom i zagrożeniom.

Działania służb bezpieczeństwa i ochrony (w tym także nadzór i eksploatacja systemów ICT) możemy porównać do roli i funkcji obsługi technicznej samolotu – musi wykonać wszystko to, co jest niezbędne, aby zapewnić bezpieczeństwo podczas startu i lądowania oraz poprawne, czyli bezpieczne zachowanie maszyny w trakcie całego lotu. Niniejszy artykuł ma za zadanie pokazać, jak wielkie znaczenie ma dualna ochrona obiektu, czyli zwrócić uwagę na to, jak ważne jest bezpieczeństwo samego obiektu (tzn. organizacji realnej lub wirtualnej, niezależnie od jej struktury) oraz każdej informacji o nim i jego elementach składowych.

Opracował: dr inż. Marek Blim

Bibliografia

1) Bednarczyk M., *Organizacja i zarządzanie przedsiębiorstwem wirtualnym*, w: *Przedsiębiorstwo przyszłości* (pod red. W. M. Grudzewskiego i I. K. Hejduk), Difin, Warszawa 2000.
2) Bieniasz D., *Realizacja zlecenia w organizacji wirtualnej*, mat. konferencyjne, Instytut Inżynierii Produkcji, Politechnika Opolska, Opole 2004.
3) Drucker P. F., *Zarządzanie w XXI wieku*, Muza SA, Warszawa 2000.
4) Jurga A., *Rola technologii teleinformatycznej w organizacji wirtualnej*, mat. konferencyjne, Instytut Inżynierii Zarządzania, Politechnika Poznańska, Poznań 2009.
5) Penc J., *Strategiczny system zarządzania. Holistyczne myślenie o przyszłości. Formułowanie misji i strategii*, Agencja Wydawnicza Placet, Warszawa 2001.
6) Woźniak K., *System informacji menedżerskiej jako instrument zarządzania strategicznego w firmie*, Akademia Ekonomiczna w Krakowie, Kraków 2005.
7) Zimniewicz K., *Współczesne koncepcje i metody zarządzania*, PWE, Warszawa 2000.

7) Branatt Ch., „Office, Space, Cyberspace & Virtual Organizations", w: „Journal of General Management", Vol. 20, No. 4.

8) za: R.S Kaplan i D. Norton „Strategiczna karta wyników", wyd. PWN, Warszawa 2001, s.21

Samsung security solutions

Integrated into modern life

CCTV

Technologie IP i sieciowe

Systemy domofonowe

Kontrola dostępu

Systemy alarmowe

Systemy bezpieczeństwa Samsung chronią ludzi i mienie na całym świecie.

Integracja przełomowych technologii, kompleksowość rozwiązań i najwyższa jakość pozwoliły firmie Samsung sprostać wymaganiom współczesnego życia.

Firma Samsung oferuje elastyczne i w pełni skalowalne rozwiązania, które można dostosować, gdy zmienią się wymagania, co zapewnia uzyskanie maksymalnych korzyści z inwestycji.

Wszystkie produkty marki Samsung objęte są pełnym trzyletnim okresem gwarancyjnym oraz bezpłatnym doradztwem projektowym i wsparciem technicznym.

Skontaktuj się z nami, aby dowiedzieć się, jak możemy pomóc przy realizacji kolejnego projektu.

2010
PSI PREMIER AWARDS
WINNER

T +420 222 866 002, +420 602 532 103
E STEsecurity@samsung.com
W samsungsecurity.com

Biuro Regionalne:
Samsung Techwin Europe Ltd
Římská 20, 120 00, Praha 2, Czechy

SAMSUNG

Zarządzanie kryzysowe i ochrona obiektów infrastruktury krytycznej

w zadaniach straży gminnych i miejskich

Paweł Kamiński

Bezpieczeństwo[1] stanowi znaczącą i nadrzędną wartość w funkcjonowaniu państwa. Wyrazem tego jest zapis art. 5 Konstytucji Rzeczypospolitej Polskiej z 2 kwietnia 1997 roku: „Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju”[2]

1) Przegląd definicji – zob. np. J. Stańczyk, „Współczesne pojmowanie bezpieczeństwa”, ISP PAN, Warszawa 1996; J. Czaputowicz, „System czy nieład? Bezpieczeństwo europejskie u progu XXI wieku”, WNPWN, CSM, Warszawa 1998; „Słownik terminów z zakresu bezpieczeństwa narodowego”, AON, Warszawa 2002.

2) Dz.U. z 1997 r. Nr 78, poz. 483 z późniejszymi zmianami

Fot. 1. Działania straży w ochronie obiektów infrastruktury krytycznej

Bezpieczeństwo zależy w dużym stopniu od organów administracji publicznej, które wykonują wiele zadań w związku z kryzysem i sytuacją kryzysową[3]. Ze wszystkimi opisanymi w niniejszym tekście sytuacjami związany jest stan zagrożenia, który może budzić obawy co do poziomu akceptowanego bezpieczeństwa.

Proponowane rozwiązania powinny być obligatoryjnie wykorzystywane do podwyższenia poziomu bezpieczeństwa. Bez względu na to, jaki charakter będą miały wspomniane sytuacje, zawsze udział w nich będzie miał człowiek. „Człowiek może być sprawcą zamierzonych i niezamierzonych sytuacji kryzysowych. Natomiast zawsze powinien być podmiotem zarządzającym tymi sytuacjami, ostatnim ogniwem usuwającym lub neutralizującym przyczyny i skutki sytuacji kryzysowych i kryzysów[4]".

Zgodnie z zapisami ustawy osobą odpowiedzialną za zarządzanie kryzysowe na terenie gminy lub miasta jest wójt, burmistrz lub prezydent miasta, który kieruje monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie gminy[5]. W tym celu tworzy on między innymi plan zarządzania kryzysowego.

Plan Zarządzania Kryzysowego (PZK) zostaje najczęściej przygotowany i ogłoszony w uzgodnieniu z komendantem państwowej straży pożarnej, komendantem policji, dyrektorem pogotowia ratunkowego, starostą, państwowym powiatowym inspektorem sanitarnym, powiatowym lekarzem weterynarii, powiatowym inspektorem nadzoru budowlanego, komendantem straży gminnej/miejskiej, a zatwierdza go odpowiedni terytorialny wojewoda.

Na PZK składają się między innymi plan główny i procedury reagowania kryzysowego. Plan główny zawiera charakterystyki zagrożeń, określa ryzyko ich wystąpienia oraz siły i środki niezbędne do ich neutralizacji, a także opisuje możliwości wykorzystania i skuteczność administracji publicznej w sytuacjach kryzysowych. Z kolei procedury reagowania kryzysowego dotyczą postępowania w przypadku wystąpienia: zdarzeń radiacyjnych; zagrożenia epidemicznego i epidemii; zagrożeń chorobami zakaźnymi zwierząt; powodzi oraz działań związanych z zagrożeniami meteorologicznymi; poważnych awarii przemysłowych; zagrożenia bezpieczeństwa paliwowego państwa i zakłóceń na rynku paliw; stanu klęski żywiołowej; dużych pożarów; innych sytuacji kryzysowych; stanu wyjątkowego i stanu wojennego. W analizie funkcjonowania administracji publicznej, jej skuteczności i możliwości wykorzystania jej w sytuacjach kryzysowym opisana jest rola straży gminnych/miejskich[6].

3) Sytuację kryzysową należy postrzegać jako każde duże nieszczęście, jakie może przydarzyć się grupie obywateli lub państwu.

4) A. Czupryński, „Siły zbrojne w kształtowaniu bezpieczeństwa publicznego", materiały z konferencji „Bezpieczeństwo publiczne w rejonie zurbanizowanym", która odbyła się 19 listopada 2009 roku w PWSZ w Kaliszu.

5) Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz. U. z dnia 21 maja 2007 r. art. 19 pkt. 1 i 2.

6) „Plan Reagowania Kryzysowego dla Miasta Kalisza", Urząd Miejski w Kaliszu, Wydział Zarządzania Kryzysowego i Spraw Obronnych, WZKO-53270-2/09, s. 28.

Straże gminne/miejskie działają na podstawie ustawy o strażach gminnych z 29 sierpnia 1997 roku i są tworzone przez radę gminy lub miasta, po zasięgnięciu opinii właściwego terytorialnie komendanta wojewódzkiego policji oraz po zawiadomieniu wojewody. Do zadań straży w zaistniałych sytuacjach kryzysowych należy między innymi: współdziałanie z właściwymi podmiotami w zakresie ratowania życia i zdrowia obywateli, pomoc w usuwaniu awarii technicznych i skutków klęsk żywiołowych oraz innych miejscowych zagrożeń, zabezpieczenie miejsca katastrofy lub innego podobnego zdarzenia albo miejsc zagrożonych takim zdarzeniem przed dostępem osób postronnych lub zniszczeniem śladów i dowodów do momentu przybycia właściwych służb, ochrona obiektów komunalnych i urządzeń użyteczności publicznej oraz informowanie społeczności lokalnej o stanie i rodzajach zagrożeń[7].

Należy wspomnieć także o codziennych planowych patrolach na terenie miasta, w czasie których zespoły kontrolne dokonują systematycznych kontroli ulic, placów, parków, budynków mieszkalnych, otoczenia zakładów pracy i obiektów użyteczności publicznej, sprawdzając, czy przestrzegane jest prawo lokalne i czy utrzymany jest porządek i czystość. Straże gminne/miejskie sygnalizują służbom komunalnym stwierdzone w toku lustracji gminy czy miasta zaniedbania lub przypadki wymagające niezwłocznej interwencji, a w szczególności awarie sieci energetycznej, gazowej, wodno-kanalizacyjnej i ciepłowniczej. Strażnicy informują właściwe służby o złym stanie nawierzchni jezdni i ciągów pieszych, nieprawidłowym oznakowaniu i oświetleniu ulic oraz o stanie zabezpieczenia i oznakowania prac prowadzonych na pasach drogowych. Ważnym zadaniem jest również utrzymywanie systematycznej współpracy z policją w zakresie ochrony obywateli i utrzymania porządku publicznego, a także w przypadku katastrof i klęsk żywiołowych. Funkcjonariusze przeciwdziałają niszczeniu zieleni miejskiej, obiektów przyrodniczych, parków oraz zanieczyszczaniu wód, przyczyniając się w ten sposób do ograniczenia degradacji środowiska naturalnego[8].

W celu wykonywania wspomnianych zadań w strażach często tworzy się dodatkowe, specjalistyczne sekcje (takie jak sekcja

7) Dz.U. z 1997 r. Nr 123, poz. 779 z późniejszymi zmianami.

8) B. Kunik-Szymczak, „Straż gminna (miejska) oraz jej rola w eliminowaniu potencjalnych zagrożeń", [w:] „Nowe zarządzanie kryzysowe w praktyce" pod red. Janusza Bagińskiego, Wydawnictwo Forum, Poznań 2008, 9/2, s. 4.

Fot. 2. Przykładowa dyslokacja pełnionej przez strażników służby

Fot. 3. Patrol z sekcji monitorowania środowiska ujawnia nielegalne odprowadzanie ścieków

monitorowania środowiska, sekcja interdyscyplinarnego reagowania), wprowadza się całodobową służbę dyżurną itd.

Straże monitorują stan środowiska i kontrolują poszczególne dzielnice miasta w celu sprawdzenia, czy utrzymany jest porządek i czystość. Ujawniają przypadki wadliwego drzewostanu terenów zielonych (w szczególności roślinności, która swym stanem zagraża bezpieczeństwu osób lub mienia) oraz bezprawne odprowadzanie nieczystości ciekłych do koryt rzecznych i nielegalne wysypiska śmieci. Działalność straży obejmuje także zapobieganie bezdomności i niewłaściwemu traktowaniu zwierząt. Strażnicy przeciwdziałają zagrożeniom dla życia i zdrowia ludzi w związku z utrzymywaniem zwierząt domowych i gospodarskich. Sprawdzają, czy właściciele posesji posiadają przyłącza kanalizacyjne lub domowe oczyszczalnie ścieków i szamba bezodpływowe. Straż prowadzi też działalność profilaktyczną i prewencyjną na rzecz poprawy czystości i porządku w mieście, realizując w kaliskich placówkach oświatowych programy edukacyjne dotyczące dbania środowisko naturalne oraz ochrony zwierząt, a także prowadząc za pośrednictwem mediów kampanie propagujące segregację śmieci, sprzątanie po psach, dbałość o tereny zielone itp. Oprócz tego zajmuje się koordynacją działań podczas neutralizowania skutków naruszenia środowiska naturalnego, a także podczas likwidowania skutków klęsk naturalnych[9].

W sytuacjach kryzysowych straże gminne/miejskie przyjmują zgłoszenia dotyczące zagrożenia życia lub zdrowia mieszkańców miasta i podejmują współpracę z innymi jednostkami oraz służbami, która ma na celu wyeliminowanie tych zagrożeń. Zgłaszają instytucjom oraz odpowiednim osobom potrzebę podjęcia działań zmierzających do usunięcia zagrożeń, a także biorą udział w ratowaniu zdrowia i życia obywateli. Do zadań straży należy pomoc w usuwaniu awarii technicznych, skutków klęsk żywiołowych oraz innych zagrożeń, a także pomoc w zaprowadzaniu porządku w strefach dotkniętych klęskami (np. poprzez zabezpieczanie miejsca katastrofy oraz miejsc zagrożonych przed dostępem osób postronnych i zniszczeniem śladów). Działania interdyscyplinarne to również kontrola (wraz z odpowiednimi podmiotami) przestrzegania oraz stosowania przepisów prawa budowlanego[10].

Wskazany przez komendanta przedstawiciel straży gminnej/miejskiej bierze udział w pracach zespołu zarządzania kryzysowego, który jest organem pomocniczym wójta, burmistrza lub prezydenta miasta, mającym zapewnić wykonywanie zadań związanych z zarządzaniem kryzysowym[11]. Uczestniczy on w ocenianiu występujących i potencjalnych zagrożeń mogących mieć wpływ na bezpieczeństwo publiczne, a także w prognozowaniu tych zagrożeń i przygotowywaniu propozycji działań ujętych w Planie Reagowania Kryzysowego[12].

9) Zarządzenie Nr 12 Komendanta Straży Miejskiej Kalisza z dn. 20 marca 2008 roku w sprawie powołania Sekcji Monitoringu Środowiska.

10) Zarządzenie Nr 3 Komendanta Straży Miejskiej Kalisza z dn. 18 lutego 2008 roku w sprawie utworzenia Samodzielnego Stanowiska ds. Interdyscyplinarnego Reagowania.

11) Zarządzenie Nr 416 Prezydenta Miasta Kalisza z dnia 10 września 2007 r. w sprawie powołania Zespołu Zarządzania Kryzysowego dla Miasta Kalisza oraz ustalenia Regulaminu Organizacji i Pracy Zespołu Zarządzania Kryzysowego dla Miasta Kalisza, s. 1.

12) Zarządzenie Nr 309 Prezydenta Miasta Kalisza z dnia 15 lipca 2008 r. w sprawie szczegółowych zasad i trybu informowania Miejskiego Centrum Zarządzania Kryzysowego o zagrożeniach i zdarzeniach zaistniałych na terenie miasta Kalisza, s. 1.

Fot. 4. Stanowisko dyżurnego straży gminnej/miejskiej

Straże mają również obowiązek przyjmowania zgłoszeń od mieszkańców oraz podmiotów i instytucji zewnętrznych, a także interweniowania, a dyżurni straży współpracują i wymieniają informacje z podmiotami zewnętrznymi, m.in. w związku z ujawnieniem awarii lub zdarzeniami wymagającymi działań będących w kompetencji innych służb. Współdziałają między innymi z Centrum Zarządzania Kryzysowego[13]. Każdorazowo, w sytuacji kryzysowej, dyżurny ma obowiązek postępować zgodnie z zasadami zawartymi w regulaminach postępowania. Dotyczą one między innymi postępowania w przypadkach zgłoszeń o: podłożeniu ładunku wybuchowego, pożarze, powodzi, obfitych opadach śniegu, anormalnym zachowaniu się ptaków, tonącej osobie, awariach, katastrofach i wypadkach losowych w zasobach mieszkaniowych, konieczności usunięcia śniegu i lodu z budynków i innych obiektów czy zwierzętach zagrażających porządkowi, zdrowiu lub bezpieczeństwu.

W wielu ośrodkach w Polsce straże miejskie dysponują monitoringiem wizyjnym[14]. Dzięki wykorzystaniu systemu monitoringu wizyjnego w miejscach objętych nadzorem następuje radykalne ograniczenie liczby przestępstw. Jest on pomocny w analizowaniu zagrożeń, w zabezpieczaniu imprez sportowych i kulturalnych, służy też do szybkiej oceny sytuacji w mieście[15].

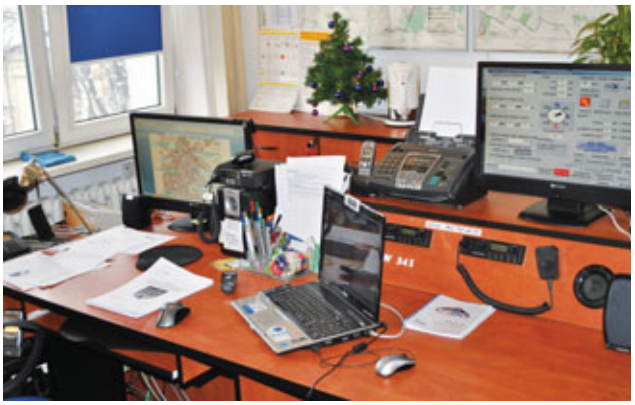
Komendant straży gminnej/miejskiej zobowiązany jest do niezwłocznego przekazywania wójtowi, burmistrzowi lub prezydentowi miasta informacji o zdarzeniach zaistniałych na terenie gminy lub miasta, a w szczególności o:

– zdarzeniach związanych z prowadzeniem akcji ratowniczo-gaśniczych na terenie budynków mieszkalnych, obiektów użyteczności publicznej (szkół, przedszkoli, kin, teatrów, hal sportowych, stadionów, zakładów opieki zdrowotnej, obiektów handlowych etc.), lasów, obszarów leśnych i parkowych, gazociągów i stacji paliw;
– powodziach;
– katastrofach komunikacyjnych;
– skażeniach chemicznych i katastrofach ekologicznych lub zagrożeniach mogących doprowadzić do takiego skażenia i (lub) katastrofy;
– skutkach anomalii pogodowych;
– awariach łączności;
– ujawnieniu niewybuchów lub niewypałów;
– katastrofach budowlanych;
– zbiorowych naruszeniach ładu i porządku publicznego;
– niepokojach i protestach społecznych;
– zakłóceniach w ruchu drogowym (doraźnych i planowanych);
– aktach terroru;

13) *Zarządzenie Nr 21 Komendanta Straży Miejskiej Kalisza z dn. 14 lipca 2008 roku w sprawie usprawnienia pracy dyżurnych SMK.*

14) *Jest to system przekazywania informacji polegający na planowym (ciągłym, prowadzonym w ściśle określony sposób za pomocą regulaminów i zasad postępowania) obserwowaniu i rejestrowaniu za pomocą środków technicznych zdarzeń, które zachodzą w określonym miejscu.*

15) *Materiały z konferencji naukowej „Bezpieczeństwo publiczne w rejonie zurbanizowanym", zorganizowanej w dniu 19 października 2009 r. przez PWSZ im. Prezydenta S. Wojciechowskiego w Kaliszu.*



Fot. 5. Przykładowe stanowisko w centrum zarządzania kryzysowego

– skutkach innych sytuacji kryzysowych i zdarzeń nadzwyczajnych[16].

Jeśli straż funkcjonuje w systemie 24-godzinnym, to informacje te najczęściej przekazywane są przez dyżurnego straży lub inną osobę upoważnioną przez komendanta w trybie doraźnym – całodobowo (również w dni wolne od pracy), telefonicznie, niezwłocznie po zaistnieniu zdarzenia lub zagrożenia. Przekazywane są informacje, które są dostępne w danej chwili. Powinny one dotyczyć czasu, miejsca, charakteru, zasięgu, znanych przyczyn lub innych znanych okoliczności zdarzenia (zagrożenia), sił i środków ratowniczych oraz zakresu podejmowanych działań.

16) *Zarządzenie Nr 309 Prezydenta Miasta Kalisza z dnia 15 lipca 2008 r. w sprawie szczegółowych zasad i trybu informowania Miejskiego Centrum Zarządzania Kryzysowego o zagrożeniach i zdarzeniach zaistniałych na terenie miasta Kalisza, s. 1.*

Fot. 6. Ujęcie wody – obiekt infrastruktury krytycznej

Powinny także obejmować prognozę skutków zagrożenia lub zdarzenia kryzysowego, a także wnioski oraz ewentualne prośby o wsparcie działań przez wójta, burmistrza lub prezydenta miasta poprzez działające Centra Zarządzania Kryzysowego[17].

Ustawa o zarządzaniu kryzysowym jednoznacznie wskazuje, że na terenie gminy lub miasta organem odpowiedzialnym za organizację i realizację zadań z zakresu ochrony infrastruktury krytycznej jest wójt, burmistrz lub prezydent miasta[18].

Ta sama ustawa precyzuje definicję infrastruktury krytycznej:

„Infrastruktura krytyczna to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych”[19].

W art. 3 wspomnianej ustawy zawarta jest również definicja ochrony infrastruktury krytycznej[20].

„Infrastruktura krytyczna” i „obiekty infrastruktury krytycznej” to określenia nowe. We wcześniejszych aktach prawnych związanych z samorządem terytorialnym używano określeń „obiekty komunalne” i „urządzenia użyteczności publicznej”[21]. O obiektach komunalnych i urządzeniach użyteczności publicznej wspomina również ustawa o gospodarce komunalnej z dnia 20 grudnia 1996 r.[22]. Według art. 1 ust. 2 cyt. ustawy gospodarka komunalna obejmuje zadania związane z użytecznością publiczną, których celem jest bieżące i nieprzerwane zaspokajanie potrzeb ludności, m.in. dostarczanie ciepła i energii elektrycznej, usługi kanalizacji, zapewnianie łączności, oczyszczanie ścieków, utylizacja odpadów, wywożenie śmieci[23]. Użyteczność publiczna to nic innego jak zaspokajanie zbiorowych potrzeb wspólnoty samorządowej i jest prawnym kryterium wyznaczającym dopuszczalny zasięg działalności samorządu terytorialnego[24].

W obecnym stanie prawnym ustawodawca nadal nie definiuje wspomnianych pojęć w przepisach prawnych, jednak w dalszym ciągu posługuje się nimi[25]. Zostały one użyte także w ustawie o strażach gminnych z 1997 roku, zgodnie z którą ochrona tych obiektów należy do zadań straży gminnych[26] i polega na przeciwdziałaniu zniszczeniu, uszkodzeniu lub dewastacji obiektów oraz mienia, które się w nich znajduje, a także na uniemożliwieniu lub ograniczeniu dostępu do nich osobom nieupoważnionym[27].

W warunkach związanych z sytuacjami kryzysowymi, wymagającymi konkretnych i adekwatnych działań mających charakter lokalny, wiodącą rolę pełni administracja lokalna[28]. Prawidłowe działanie zakładów, obiektów czy urządzeń odgrywa zasadniczą rolę w funkcjonowaniu gmin lub miast. Wszelkiego rodzaju zakłócenia mogą stanowić poważne zagrożenie dla zdrowia lub życia mieszkańców, a także mają wpływ na ich bezpieczną egzystencję w danym środowisku[29]. W zaistniałych sytuacjach wójt, burmistrz czy prezydent miasta może wykorzystać podległą sobie straż do wsparcia działań innych podsystemów wykonawczych w zakresie bezpieczeństwa i może polegać to między innymi na przejęciu niektórych ich zadań, wynikających głównie z ustawowych kompetencji[30]. Takie przedsięwzięcia będą zmierzały do podwyższenia poziomu zabezpieczenia chronionych obiektów, a jednocześnie będą wpływały na coraz większe zaangażowanie straży gminnych/miejskich w działania związane z zarządzaniem kryzysowym w Polsce.

mgr Paweł Kamiński
Państwowa Wyższa Szkoła Zawodowa
im. Prezydenta Stanisława Wojciechowskiego w Kaliszu
Akademia Obrony Narodowej w Warszawie

17) Tamże, s. 2.

18) „Ustawa o zarządzaniu kryzysowym” z dnia 26 kwietnia 2007 r., Dz.U. z dnia 21 maja 2007 r., art. 19, p. 1 i 2.

19) Tamże, art. 3, p. 2.

20) „Wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.”.

21) Ustawa o samorządzie terytorialnym z dnia 8 marca 1990 r., Dz.U. z 1990 r. Nr 16, poz. 95.

22) Dz.U. z 1997 r. Nr 9, poz. 43 z późniejszymi zmianami.

23) W. Kotowski, „Straże gminne. Komentarz praktyczny”, Dom Wydawniczy ABC, Warszawa 2004, s. 158.

24) A. Pakula, „Interes publiczny i użyteczność publiczna jako kryteria zadań samorządu terytorialnego”, [w:] „Administracja i prawo administracyjne u progu trzeciego tysiąclecia”, Łódź 2000, s. 356.

25) J. Lemańska, K. Klonowski, „Zamówienia publiczne w sektorze użyteczności publicznej”, www.lex.com.pl [stan z 23.12.2009], s. 253–257.

26) Art. 11, ust. 1, p. 5 (Dz.U. z 1997 r. Nr 123, poz. 779 z późniejszymi zmianami).

27) I. Kobus, I. Dziugieł, „Straż miejska i gminna (akty prawne i komentarz do uprawnień”, Wydawnictwo Dorix, Szczytno 2007, s. 753.

28) W. Kitler, „Potrzeby i wyzwania w zakresie bezpieczeństwa społeczności lokalnej”, [w:] „Realizacja zadań bezpieczeństwa przez samorząd terytorialny”, wyd. Stowarzyszenie Ruch Wspólnot Obronnych, Warszawa 2006, s. 37.

29) A. Tyburska, M. Nepelski, „Ochrona infrastruktury krytycznej”, wyd. WSP, Szczytno 2009, s. 19.

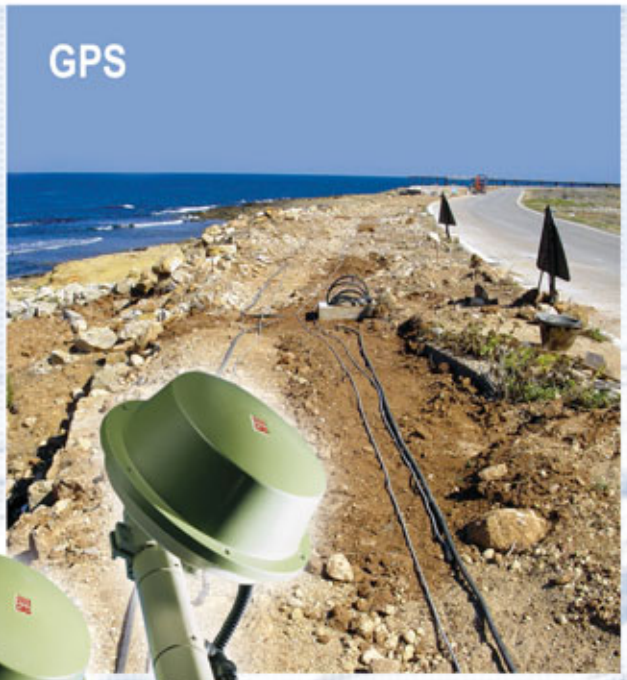
30) K. Gąsiorek, „Zapewnienia bezpieczeństwa i porządku publicznego”, [w:] „Samorząd terytorialny w obronie narodowej RP”, AON, Warszawa 2005, s. 221.

ZSJZ
AQAP 2110:2009
ISO 9001:2008

więcej na: **www.atline.pl**

firma **ATLine®**
kompleksowe zabezpieczanie obiektów

KAMERA
TERMOWIZYJNA
PT - Series



AN 307

ERMO 482XPRO

PROJEKTOWANIE KOMPLEKSOWYCH DOKUMENTACJI

- technicznych, architektoniczno - budowlanych wraz z niezbędnymi branżami specjalistycznymi obiektów biurowych i przemysłowych
- innowacyjnych systemów ochrony
- teletechnicznych, elektrycznych i automatyki przemysłowej

WYKONAWSTWO

zaawansowanych technologicznie systemów ochrony i bezpieczeństwa

SPRZEDAŻ

nowoczesnych systemów ochrony

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

Sygnalizator SG-Wgw

uniwersalna sygnalizacja zdarzeń

Szymon Ratajski

Firma W2 Włodzimierz Wyrzykowski, poszerzając swój asortyment produktów, wprowadziła do sprzedaży kolejny wyrób z rodziny sygnalizatorów z komunikatem słownym – sygnalizator SG-Wgw. Jest on przeznaczony do przekazywania informacji o zdarzeniach komunikatem słownym (dowolny dźwięk w formacie WAV oraz akustycznym sygnałem ostrzegawczym. Sygnalizator SG-Wgw jest przystosowany do pracy w pomieszczeniach zamkniętych. Umożliwia użytkownikowi odtwarzanie do sześciu sekwencji alarmowych (w zależności od konfiguracji). Każdy parametr sekwencji może być dowolnie modyfikowany przez użytkownika. Każda sekwencja jest programowana niezależnie. Parametry sygnalizatora są definiowane za pomocą darmowego programu SG, dostępnego na firmowej stronie internetowej

Co wyróżnia sygnalizator SG-Wgw spośród innych sygnalizatorów?

Sygnalizator SG-Wgw może odtwarzać dowolny dźwięk zapisany w formacie WAV, o czasie trwania do 65 s. Jako źródło dźwięku zastosowano głośnik dynamiczny, dzięki czemu osiągnięto wysoką jakość odtwarzanego dźwięku. Inne zalety sygnalizatora SG-Wgw to:

– trzy tryby pracy: akustyczny (do sześciu sekwencji), z możliwością wyciszania (do trzech sekwencji), z możliwością wyzwalania komunikatu (do trzech sekwencji);
– proste adresowanie komunikatów poprzez podanie napięcia zasilania na odpowiednie zaciski sygnalizatora;
– możliwość współpracy z sygnalizatorami powtarzającymi w celu tworzenia sieci sygnalizatorów do nagłaśniania większych pomieszczeń;
– prosta konfiguracja za pomocą oprogramowania SG oraz karty SD;
– 35 wzorców syren;
– szeroki zakres napięcia zasilającego (10–32 V_{DC}).

Sygnalizator SG-Wgw projektowano z myślą o stworzeniu wyrobu nie będącego typowym sygnalizatorem, lecz urządzeniem akustycznym o jak najszerszym spektrum zastosowań. Oprócz głównego przeznaczenia sygnalizatora – sygnalizacji niebezpiecznych zdarzeń – może on być wykorzystany w wielu nietypowych aplikacjach.

Oprogramowanie SG

Oprogramowanie SG zostało stworzone po to, aby w jak największym stopniu ułatwić programowanie sygnalizatora. Umożliwia programowanie parametrów urządzenia w zależności od potrzeb użytkownika oraz tworzenie plików projektu, możliwych do wykorzystania w kolejnych aplikacjach. Programowanie sygnalizatora jest podzielone na sześć etapów, w których użytkownik ustawia interesujące go parametry pracy. Efektem pracy jest stworzenie pliku *.bw2, który jest plikiem konfiguracyjnym sygnalizatora, wgrywanym do urządzenia za pomocą karty SD.

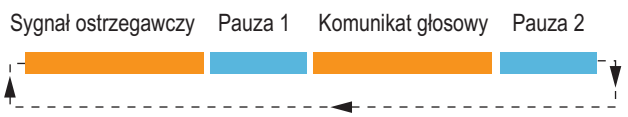
Fot. 1. Sygnalizator SG-Wgw

Do podstawowych funkcji oprogramowania należą:

– wybór trybu pracy sygnalizatora,
– ustalanie liczby komunikatów,
– wybór parametrów sygnału akustycznego (rodzaj oraz czas trwania),
– wybór dźwięku nagrania (plik *.wav lub nagranie z mikrofonu podłączonego do komputera),
– filtracja nagrania, regulacja głośności (również z wykorzystaniem wbudowanego kompresora dynamiki),
– ustalenie parametrów sekwencji (czasy pauz).

Aby utworzyć komunikat słowny, użytkownik może wygenerować plik *.wav, korzystając z syntezatora mowy (np. dostępnego na stronie internetowej www.ivona.com). Dzięki syntezatorowi mowy użytkownik zamienia komunikat tekstowy na dźwiękowy w formacie WAV.

Po odpowiednim zaprogramowaniu przez użytkownika sygnalizator może pracować w wielu aplikacjach, do których możemy zaliczyć między innymi: sygnalizację zdarzeń komunikatem słownym, sygnalizację zdarzeń nietypowym sygnałem alarmowym, odtwarzanie komunikatów w reakcji na sygnał wyzwolenia (np. z czujnika ruchu), nagłaśnianie pomieszczeń biurowych itp.



Rys. 1. Sekwencja alarmowa odtwarzana przez sygnalizator SG-Wgw

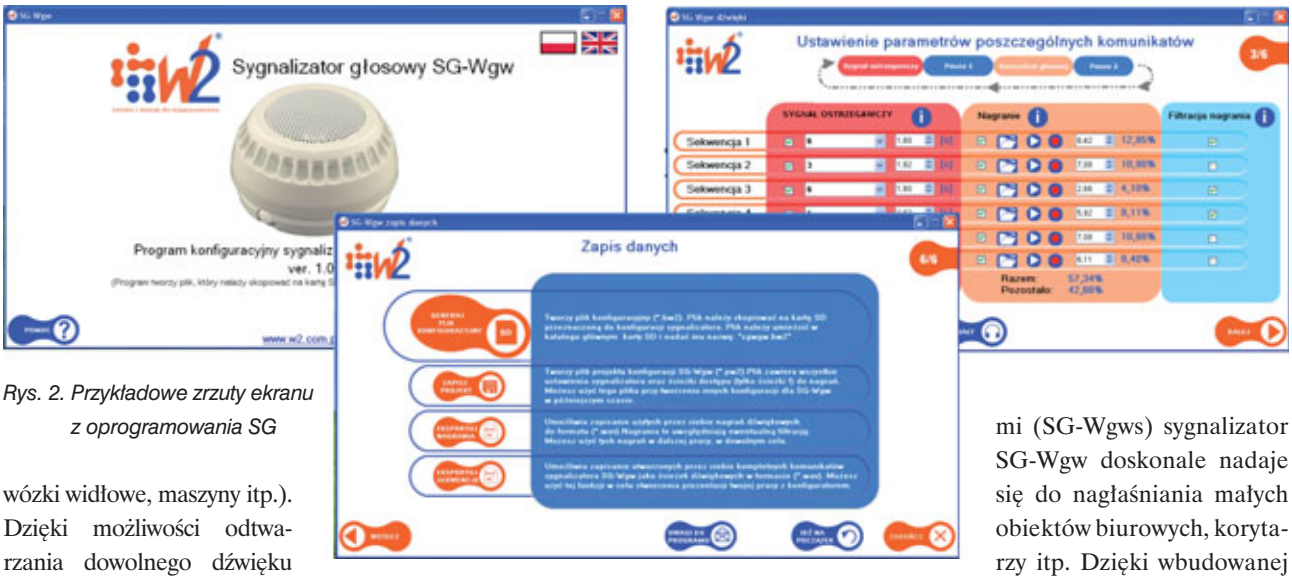
Sygnalizowanie niebezpiecznych zdarzeń komunikatem słownym

Doskonałym miejscem do stosowania sygnalizatorów serii SG są obiekty, w których występuje wiele sygnałów akustycznych, które potencjalnie mogą utrudnić rozpoznanie sygnału alarmowego. Do dźwięków tych można zaliczyć np. odgłosy pracujących maszyn, wózków widłowych itp. W momencie wystąpienia alarmu, wywołanego awarią lub innym zdarzeniem, ludzie znajdujący się w strefie, na którą oddziałuje wiele dźwięków, mają duży problem z rozpoznaniem sygnału zagrożenia. W celu uniknięcia tego typu niebezpiecznych sytuacji należy dążyć do tego, aby sygnały informujące o niebezpieczeństwie były odpowiednio rozpoznawalne na tle innych dźwięków oraz spotykały się z odpowiednią reakcją ludzi. Dzięki sygnalizowaniu niebezpiecznych zdarzeń komunikatem słownym sygnalizatory serii SG znacznie zwiększają skuteczność alarmowania o zagrożeniu.

Komunikat ostrzegawczy musi być poprawnie sformułowany, aby właściwie ostrzegać o zagrożeniu. W połączeniu z ostrzegawczym sygnałem akustycznym powinien być jednoznacznie interpretowany przez osoby znajdujące się w strefie działania sygnalizatora.

Sygnalizacja niebezpiecznych zdarzeń nietypowym sygnałem akustycznym

W praktyce często zachodzi potrzeba stosowania alarmów o nietypowym sygnale akustycznym. Ma to związek z wymaganiami różnego rodzaju instalacji lub po prostu służy odróżnieniu dźwięku alarmu od licznych sygnałów akustycznych, które występują w określonym środowisku (np. dźwięków wydawanych przez



Rys. 2. Przykładowe zrzuty ekranu z oprogramowania SG

wózki widłowe, maszyny itp.). Dzięki możliwości odtwarzania dowolnego dźwięku sygnalizator SG-Wgw doskonale nadaje się do tego typu zastosowań. Umożliwia odtwarzanie dźwięków o łącznym czasie trwania do 65 s.

Odtwarzanie komunikatów

Jednym z ciekawszych zastosowań jest praca sygnalizatora w roli urządzenia witającego gości w sklepie. W aplikacji tej wykorzystane jest wejście TRIG, służące do wyzwalania komunikatu. Po odpowiednim połączeniu wejścia TRIG z czujnikiem ruchu sygnalizator, w momencie otrzymania sygnału wyzwolenia, zaczyna odtwarzać komunikat, przy czym możliwe jest określenie długości przerwy pomiędzy odtwarzaniem komunikatu (w celu uniknięcia błędnego działania w momencie występowania licznych sygnałów wyzwolenia). Opcja ta może być wykorzystana również w celu przypominania o określonych zdarzeniach (np. w celu przypomnienia pracownikowi o potrzebie wykonania określonych czynności przed opuszczeniem stanowiska pracy).

Sygnalizator SG-Wgw może również pracować w roli urządzenia dostarczającego informacji o określonych przedmiotach (np. w sklepie – po naciśnięciu przycisku użytkownik otrzymuje informację o określonym produkcie).

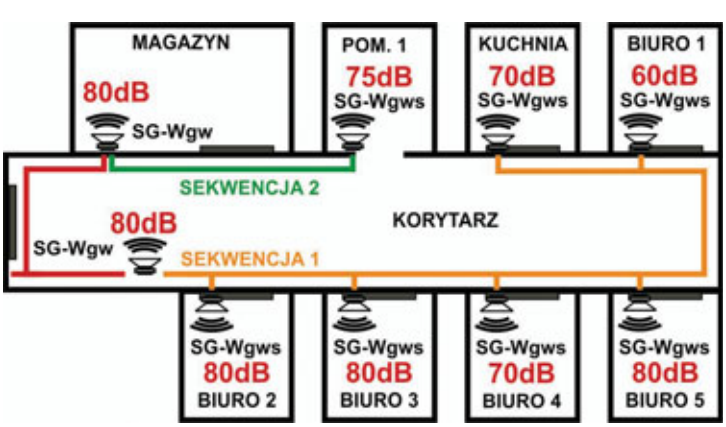
Tworzenie sieci sygnalizatorów w celu nagłaśniania większych obszarów

Dzięki możliwości prostego adresowania sekwencji (poprzez podanie napięcia zasilania na określone wyprowadzenie) oraz możliwości współpracy z sygnalizatorami powtarzającymi (SG-Wgws) sygnalizator SG-Wgw doskonale nadaje się do nagłaśniania małych obiektów biurowych, korytarzy itp. Dzięki wbudowanej regulacji głośności możliwe jest dobranie natężenia dźwięku do poziomu tła akustycznego pomieszczenia.

Kolejną istotną funkcją oprogramowania sygnalizatora jest odtwarzanie sygnału akustycznego z liniowym zwiększaniem jego głośności od poziomu minimalnego do poziomu maksymalnego w zadanym przez użytkownika czasie (tzw. funkcja rampy). Ta funkcja jest szczególnie przydatna, gdy trzeba odtworzyć alarm w pomieszczeniu, w którym występuje niski poziom tła akustycznego lub znajdują się osoby, które są wrażliwe na nagłe zmiany natężenia dźwięku (małe dzieci, osoby starsze). Nietrudno jest wyobrazić sobie sytuację, w której podczas pracy, np. w bibliotece, gdzie poziom tła akustycznego jest bardzo niski, nagle włącza się sygnalizator i zaczyna odtwarzać dźwięk o natężeniu 90 dB. Dzięki funkcji rampy możliwe jest wygenerowanie sygnału z powolnym zwiększaniem natężenia dźwięku (np. zwiększanie głośności w ciągu 10 s).

Rozwój produktu oraz oprogramowania

Wprowadzenie oprogramowania SG dało firmie W2 nowe możliwości zrealizowania „sprzężenia zwrotnego" od klientów. W oprogramowaniu SG zawarta jest funkcja, za pomocą której użytkownik może przedstawić swoje uwagi dotyczące zarówno sygnalizatora SG-Wgw, jak i samego oprogramowania. Jeżeli użytkownik stwierdzi, że w oprogramowaniu brakuje funkcji, która jego zdaniem powinna się w nim znaleźć, może napisać wiadomość i przedstawić w niej swoje uwagi. Każda uwaga jest analizowana. Jeśli proponowane zmiany są możliwe do wprowadzenia, oprogramowanie jest modyfikowane, dzięki czemu sygnalizator SG-Wgw (w przyszłości także inne sygnalizatory z komunikatem słownym) jest w ciągłym rozwoju, a to z kolei sprawia, że firma na bieżąco zaspokaja potrzeby klientów. Przykładem takiego działania jest wprowadzenie funkcji odtwarzania losowego komunikatu w odpowiedzi na impuls wyzwolenia (funkcję tę zaproponował jeden z klientów, który zamówił sygnalizator do własnego sklepu). Funkcja ta będzie dostępna w oprogramowaniu SG v.1.1.



Rys. 3. Nagłaśnianie pomieszczeń biurowych

Szymon Ratajski
W2 Włodzimierz Wyrzykowski

seria radius

RACS 4

System Kontroli Dostępu

- Do 250 podsystemów w jednym systemie.
- Do 32 kontrolerów dostępu w jednym podsystemie.
- Do 1000 kontrolerów w całym systemie.
- Bezpłatne oprogramowanie do zarządzania systemem KD.

RCP Master *PR602LCD*

Rozwiązania Kontroli Dostępu i Rejestracji Czasu Pracy

roger®

www.roger.pl

Rozszerzono funkcjonalność systemu **RACS 4** o możliwość wyświetlania zdarzeń na ekranie monitorów telewizji przemysłowej oraz o możliwość tworzenia wielopoziomowych graficznych map systemu.

Nowe drukarki do kart plastikowych

Daniel Bobola

Firma **Control System FMN**, jako autoryzowany dystrybutor produktów największych światowych producentów drukarek – Fargo, HID Global i Datacard, ma przyjemność przedstawić dwie nowe linie drukarek do kart plastikowych

SR200

DTC 4500

DTC 4000

DTC 1000

HID Global wprowadził w tym roku do sprzedaży całkiem nowy zestaw drukarek z serii Fargo DTC. Drukarki te to wynik połączenia doświadczeń uznanej na całym świecie dzięki tworzeniu doskonałych drukarek firmy Fargo oraz słynącej z zaawansowanych systemów zabezpieczeń firmy HID Global. Drukarki charakteryzują się dużą wszechstronnością i niezawodnością oraz zapewniają najwyższy stopień bezpieczeństwa. Zastosowanie innowacyjnej technologii wydruku pozwoliło uzyskać niebywale nasycone, żywe kolory oraz ostry obraz, uwidaczniający nawet małe detale, przy jednoczesnym wzroście prędkości nadruku.

Duży nacisk położono również na łatwość obsługi. Zastosowano rozwiązanie z taśmami w zespolonych zasobnikach oraz nowy, intuicyjny interfejs użytkownika, a także zainstalowano prosty zestaw narzędzi diagnostycznych. Umieszczenie rolek czyszczących w pojemnikach z taśmą pozwala wydłużyć okres pomiędzy przeglądami serwisowymi i zapewnia większą niezawodność działania, co z kolei znacznie obniża koszty eksploatacji. Dodatkowym atutem jest konstrukcja modułowa, dzięki której w każdej chwili można rozbudować drukarkę, jednocześnie dostosowując ją do swoich wymagań oraz potrzeb.

Wszystkie drukarki z nowej serii DTC mają zainstalowaną aplikację Swift ID pozwalającą tworzyć własne identyfikatory w kilka sekund, bez konieczności instalowania dodatkowego oprogramowania. Drukarki mają elegancką, nowoczesną, kompaktową budowę. Dzięki małym gabarytom zmieszczą się na każdym stanowisku pracy.

Dla małych i średnich przedsiębiorstw do nadruku monochromatycznego oraz kolorowego doskonale nadaje się drukarka **Fargo DTC 1000**. Do jej podstawowych zalet drukarki należą:

– wysoka jakość nadruku,
– łatwość obsługi,
– niewielkie wymiary,
– szybkość wydruku,
– podajnik na 100 szt. kart,
– możliwość nadruku wielokrotnego na jednej karcie,
– możliwość nadruku na kartach samoprzylepnych.

Drukarkę DTC 1000 można opcjonalnie wyposażyć w kodery kart magnetycznych, zbliżeniowych i stykowych oraz moduł odwracający, umożliwiający nadruk dwustronny w jednym procesie.

Fargo DTC 4000 to wszechstronna drukarka, którą zaprojektowano z myślą o średniej wielkości przedsiębiorstwach, szkołach, urzędach i instytucjach państwowych. To idealne rozwiązanie dla organizacji poszukujących drukarki łatwej i elastycznej w zastosowaniu, oferującej doskonałą jakość wydruku i mającej możliwość kodowania kart procesorowych.

W każdej chwili można zwiększyć możliwości drukarki:

– wyposażyć ją w moduł drukowania dwustronnego,
– umieścić podajnik i odbiornik kart po tej samej stronie drukarki,
– zwiększyć pojemność podajnika kart do 200 szt.,
– wyposażyć ją w złącze Ethernet umożliwiające udostępnienie drukarki wielu użytkownikom w sieci,
– zainstalować koder kart stykowych i bezstykowych.

Wszechstronność drukarki Fargo DTC 4500 jest nieoceniona (od produkcji kart lojalnościowych i identyfikatorów po najbardziej zaawansowane zastosowania kart procesorowych). Dzięki zastosowaniu taśm o dużej pojemności oraz podwójnego podajnika drukarka zapewnia największą ilość nadruków bez konieczności ingerencji operatora. Ekstremalnie zwiększono moc silnika wydruków, co umożliwia wydajną, szybką i niezawodna pracę.

Fargo DTC 4500 to również synonim bezpieczeństwa. Drukarka posiada zabezpieczenie przed nieautoryzowanym użyciem w postaci hasła. Ponadto ma możliwość nadruku z taśm fluorescencyjnych oraz ultrafioletowych, a dodatkowa opcja zastosowania laminatora pozwala lepiej zabezpieczyć powierzchnię karty przed zużyciem.

Z kolei firma **Datacard** – jeden z wiodących producentów systemów personalizacji kart plastikowych oraz drukarek do produkcji kart i identyfikatorów – ma do zaoferowania najnowsze drukarki retransferowe serii SR, które umożliwiają nadruk na kartach plastikowych od krawędzi do krawędzi, z niebywałą jakością. Zastosowanie nowej technologii nadruku, która jest oparta na poziomej orientacji karty, pozwoliło zminimalizować niepożądane przenikanie się barw. Dzięki temu uzyskujemy dużo lepszą gradację barw, tonalne przejścia i doskonały kontrast obrazów. Zastosowana technologia umożliwia uzyskanie wydruku o niesamowitej ostrości i nasyceniu barw oraz odtworzenie większego zakresu kolorów w porównaniu z rozwiązaniami konkurencji.

Intuicyjna obsługa drukarek SR oraz kilka użytecznych elementów, takich jak panel LCD wyświetlający informacje o statusie drukarki czy taśmy znajdujące się w kasetach, znacznie upraszczające proces wymiany kaset na nowe – sprawiają, że modele SR200 i SR300 są bardzo proste w użyciu.

Ponadto drukarki mogą być używane wszędzie tam, gdzie oprócz wymagań jakościowych istotny jest wysoki stopień bezpieczeństwa. Dzięki zastosowaniu unikatowej technologii szyfrowania przesyłanych danych IPSEC oraz możliwości automatycznego usuwania danych z czarnego panelu taśmy (za pomocą której zwykle odbywa się drukowanie danych personalnych i wszelkiego rodzaju innych informacji) drukarki serii SR wyznaczają nowe światowe standardy w dziedzinie bezpieczeństwa nadruku kart. Za pomocą elektronicznego zamknięcia oprócz danych chronione są również materiały eksploatacyjne oraz karty.

Do nadruku jednostronnego na kartach przeznaczony jest model **SR200**. Opcjonalnie drukarka może być wyposażona w laminator. Standardowo jest wyposażona w elektroniczne zamknięcie kontrolujące dostęp do materiałów eksploatacyjnych do drukowania oraz kart.

Model **SR300** ma ponadto możliwość nadruku dwustronnego oraz kodowania kart z procesorem stykowym, zbliżeniowym lub z paskiem magnetycznym.

Jeżeli potrzebujesz urządzeń do drukowania kart plastikowych lub identyfikatorów, u nas znajdziesz rozwiązanie odpowiadające potrzebom twojej firmy.

Serdecznie zapraszamy na naszą stronę internetową *www.cs.pl*, na której można znaleźć dodatkowe informacje.

Daniel Bobola
Control System FMN

ODKRYJ SZYBKOŚĆ INSTALACJI

DSC

WT5500
Bezprzewodowa klawiatura LCD

WT4989
Bezprzewodowy pilot
z wyświetlaczem LCD

WS4904W
Bezprzewodowe czujki PIR

WS4945
Bezprzewodowa
czujka kontaktronowa

Wyłączny dystrybutor produktów DSC w Polsce:

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

ALEXOR PC9155

BEZPRZEWODOWY SYSTEM ALARMOWY
O KOMUNIKACJI DWUKIERUNKOWEJ

- Obsługa maksymalnie 32 urządzeń bezprzewodowych i 16 breloków
- Kompatybilność z urządzeniami o komunikacji jednokierunkowej
- Obsługa do 4 sygnalizatorów i klawiatur bezprzewodowych
- Funkcja automatycznego przypisywania urządzeń bezprzewodowych
- Szablony programowania skracające czas instalacji
- 16 kodów użytkownika, 1 kod główny, 1 kod konserwatora
- Funkcja sprawdzania kodu identyfikacyjnego systemu
- Alternatywna komunikacja przez sieć GSM/GPRS lub TCP/IP
- Wbudowany sygnalizator akustyczny o mocy 85dB
- 2 zaciski I/O, które mogą być zaprogramowane jako wyjścia PGM lub przewodowe linie dozorowe
- 200mA obciążalności prądowej wyjścia AUX
- Rejestr 500 zdarzeń
- Podwójne zabezpieczenie antysabotażowe przed otwarciem obudowy lub oderwaniem od ściany
- 24 godzinne podtrzymanie baterii

Pozostałe urządzenia bezprzewodowe kompatybilne z centralą PC9155:

WS4939, PT4
Bezprzewodowy pilot i brelok zbliżeniowy

TL265GS, GS2065
Komunikatory alarmowe wysyłające kody raportujące przez sieć GSM/GPRS i TCP/IP

WT4901
Bezprzewodowy sygnalizator wewnętrzny

WT4911
Bezprzewodowy sygnalizator zewnętrzny

WS4916
Bezprzewodowa czujka dymu

WS4985
Bezprzewodowa czujka zalania wodą

WLS912L
Bezprzewodowa czujka zbicia szyby

WS4975
Bezprzewodowa czujka kontaktronowa

Detekcja termiczna

Nowy trend w nadzorze wizyjnym

Agata Majkucińska

Axis Communications upowszechnia technologię obrazowania termicznego dzięki nowym kamerom termowizyjnym AXIS Q1921 i Q1921-E

Większość kamer dotychczas używanych w nadzorze wizyjnym charakteryzuje się podstawowym ograniczeniem – do prawidłowego spełniania swoich funkcji potrzebuje światła. Owszem, wykorzystanie trybu dziennego i nocnego pozwala niektórym modelom działać w warunkach bardzo słabego oświetlenia, rzędu ułamka luksa. Światło naturalne można też zastąpić elektrycznym, widocznym dla ludzkiego oka, albo podczerwonym, jednak w niektórych sytuacjach rozwiązania te okazują się drogie i nieefektywne, a na skutek intensywnego oświetlenia powstają cienie, w których może ukryć się intruz. Dobrym rozwiązaniem jest technologia obrazowania termicznego. Do tej pory, ze względu na wysokie koszty i ograniczoną ofertę, była ona wykorzystywana przede wszystkim przez wojsko. Wychodząc naprzeciw oczekiwaniom klientów, na początku 2010 roku Axis Communications wprowadził dwie kamery termowizyjne: AXIS Q1910 do zastosowań wewnętrznych i AXIS Q1910-E do zastosowań zewnętrznych. We wrześniu asortyment produktów termowizyjnych powiększył się o kolejne modele, które na pewno będą doskonałym uzupełnieniem każdego profesjonalnego systemu monitoringu IP.

Nowa era monitoringu

Światło widzialne, które jest dostrzegane przez ludzkie oko i może być wykrywane przez standardowe kamery, wymaga źródła, takiego jak słońce lub reflektor. Nawet kamery dzienno-nocne, które wykorzystują pasmo bliskiej podczerwieni, wymagają odrobiny światła naturalnego albo emitowanego przez lampę pracującą w podczerwieni. Kamera termowizyjna nie wymaga żadnego źródła światła, ponieważ działa przez wykrywanie długofalowego promieniowania podczerwonego emitowanego przez obserwowane obiekty. Promieniowanie podczerwone jest emitowane przez wszystkie obiekty, nawet bardzo zimne, takie jak lód. Natężenie promieniowania różni się w zależności od temperatury i emisyjności obiektów. Dzięki temu kamera może wykrywać zmiany temperatury i wizualizować obiekty w ciemności i innych trudnych warunkach bez konieczności występowania zewnętrznego źródła światła. Natężenie promieniowania emitowanego przez obiekt rośnie wraz z temperaturą, a zatem kamera termowizyjna umożliwia użytkownikowi obserwowanie różnic temperatury. Ciepłe obiekty wyróżniają się na zimniejszym tle i odwrotnie. Obrazy termiczne widziane na monitorze zawierają intensywne kolory, pomimo tego, że kamera działa poza spektrum światła widzialnego. Barwy te są tworzone cyfrowo, są to tzw. pseudokolory. Każdy kolor lub odcień reprezentuje inną temperaturę. Zazwyczaj biel i czerwień oznaczają wyższe temperatury, a zieleń, błękit i fiolet – niższe. Wynika to głównie ze względów praktycznych, ponieważ ludzkie oko lepiej rozróżnia kolory niż odcienie szarości.

Duże korzyści dla systemów nadzoru dzięki AXIS Q1921 i Q1921-E

Termowizyjne kamery sieciowe stanowią idealną pierwszą linię obrony, dzięki której służby ochrony mogą wykrywać i identyfikować obiekty oraz zdarzenia, a następnie błyskawicznie podejmować niezbędne działania. Ma to duży wpływ na ogólną skuteczność całego systemu nadzoru. Kamery termowizyjne szybko i bezbłędnie wykrywają każdy incydent zachodzący w ich polu widzenia, nawet w całkowitej ciemności oraz bardzo trudnych warunkach atmosferycznych, takich jak deszcz, mgła czy gęsty dym. Tych kamer nie można oślepić silnym światłem ani unieszkodliwić wskaźnikiem laserowym. Eliminują one także problemy z cieniami, dzięki czemu znakomicie sprawdzają się w profesjonalnej analizie materiału wizyjnego. Ich funkcjonalność oraz odporność przekłada się również na znacznie większą dokładność i skuteczność niż w przypadku konwencjonalnych kamer w większości inteligentnych systemów nadzoru.

Fot. 1. Kamera Axis Q1921-E

W ofercie Axis Communications znajdują się różne termowizyjne kamery IP, przystosowane zarówno do instalacji wewnętrznych, jak i zewnętrznych. Najnowsze modele – przeznaczony do zastosowań wewnętrznych AXIS Q1921 oraz AXIS Q1921-E, który dzięki obudowie o klasie szczelności IP66 najlepiej sprawdzi się na zewnątrz – sprostają aktualnym wyzwaniom rzuconym systemom nadzoru wizyjnego. Wyjątkową zaletą tych kamer jest możliwość dobrania do każdej z nich jednego z czterech obiektywów – o ogniskowej 10, 19, 35 lub 60 mm. Kamery te umożliwiają wykrywanie ludzi z odległości do 200 m przy 55-stopniowym polu widzenia i nawet 1200 m przy 9-stopniowym polu widzenia. Ponadto oferują kluczowe funkcje nadzoru IP, takie jak obsługa formatów H.264 i Motion JPEG, dwukierunkowe przesyłanie dźwięku, lokalne przechowywanie danych i zasilanie Power over Ethernet. Inteligentne funkcje wizyjne są kluczową zaletą każdej kamery termowizyjnej. AXIS Q1921/-E są szczególnie bogato wyposażone – alarmują o próbach ingerencji, wykrywają ruch, obsługują również platformę aplikacyjną AXIS. Dzięki rozdzielczości 384×288 i zaawansowanemu procesorowi obrazu kamery AXIS Q1921 i AXIS Q1921-E dodatkowo zwiększają skuteczność nadzoru, zarówno obszarowego, jak i obwodowego. W przypadku nadzoru obszarowego detekcja termiczna na otwartej przestrzeni powoduje wczesną reakcję w sytuacjach niestandardowych, umożliwiając skuteczną prewencję i minimalizując tym samym zagrożenie wandalizmem, włamaniami i fałszywymi alarmami. Systemy wykorzystujące kamery AXIS Q1921-E zwykle znajdują zastosowanie na parkingach, w placówkach edukacyjnych i innych obiektach

Fot. 2. Kamera Axis Q1921

budowlanych, które wymagają wysokiego stopnia zabezpieczenia. Drugim wspomnianym przykładem skutecznego wykorzystania kamer termowizyjnych jest utworzenie systemu ochrony obwodowej. Wirtualne ogrodzenie zapewnia dyskretną detekcję, stanowiąc jednocześnie skuteczne i ekonomiczne rozwiązanie alternatywne wobec detekcji radiowej, wplatanych w ogrodzenia kabli detekcyjnych czy kamer CCTV połączonych z reflektorami. Systemy z kamerami AXIS Q1921 zdadzą egzamin w portach i przystaniach, elektrowniach, zakładach użyteczności publicznej i w więzieniach. Doskonale uzupełniają również zabezpieczenia fizyczne, nie wymagają oświetlenia w widmie podczerwieni oraz nie są widoczne dla intruzów.

Praktyczne korzyści

Kamery termowizyjne, w miarę wzrostu ich dostępności, są coraz częściej stosowane w nowoczesnych systemach nadzoru IP. Pojawia się cały szereg możliwych i uzasadnionych ekonomicznie zastosowań, innych niż dotychczasowe. Kamery termowizyjne stanowią doskonałe uzupełnienie systemów monitorowania w wielu sytuacjach, w których konwencjonalne kamery są nieodpowiednie lub nie wystarczają. Oczywiście są niedoścignione w warunkach całkowitej ciemności. Przydają się również w nadzorze obszarów, które trudno jest skutecznie oświetlić, np. brzegu morza. Krótko mówiąc, kamery termowizyjne doskonale uzupełniają sieciowy system monitorowania, gwarantując wykrywanie obiektów, ludzi i zdarzeń przez 24 godziny na dobę.

Agata Majkucińska
Key Account Manager
Axis Communications

Pomóż przedsiębiorstwom **skoncentrować się na wynikach.**

Dobry system nadzoru wizyjnego daje więcej niż tylko nagrywanie zdarzeń. Zwiększa on zdolność do zapobiegania niepożądanym zdarzeniom i ich kontroli-pozwalając skoncentrować się na bieżących sprawach biznesowych.

Połącz nową linię kompaktowych, ekonomicznych sieciowych kamer Axis z serii M z oprogramowaniem AXIS Camera Station lub rozwiązaniem do zarządzania materiałem wizyjnym któregoś z naszych partnerów, by stworzyć prawdziwie efektywny system nadzoru HDTV.

Łatwy do zainstalowania i obsługi, system sieciowego nadzoru Axis dostarcza jakość obrazu, która może stanowić dowód w sprawie, jak też elastyczność i skalowalność potrzebną by uwzględniać zmieniające się potrzeby. Możemy więc spokojnie postawić na wybór bezproblemowego nadzoru wizyjnego, który pozwala koncentrować się, na tym co rzeczywiście jest dla nas ważne.

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

Kamery sieciowe AXIS M11, AXIS M32 i AXIS M10, w połączeniu z oprogramowaniem AXIS Camera Station dostarczają kompletne rozwiązanie sieciowego nadzoru wizyjnego do 50 kamer ze wsparciem HDTV,H.264 i Power over Ethernet.

AXIS COMMUNICATIONS

Godny następca

Rejestrator Aper serii PDR-X

Mariusz Witulski

Dwa lata temu na rynku CCTV pojawiły się rejestratory Aper serii PDR-S. Urządzenia te bardzo szybko zyskały popularność i uznanie wśród instalatorów oraz użytkowników. Zawdzięczały to w dużej mierze ogromnej funkcjonalności, niezawodności, stabilności działania oraz intuicyjnej i łatwej obsłudze. PDR-S znajdowały zastosowanie w większości typowych systemów telewizji dozorowej o małych i średnich rozmiarach. W dziedzinie CCTV wciąż trwa dynamiczny i nieustanny postęp technologiczny. Udoskonalane są metody kompresji, stosowane są coraz szybsze procesory, dzięki czemu poprawie ulega efektywność pracy urządzeń i wygoda użytkowania. Naturalny rozwój dotyczy również urządzeń rejestrujących, a jego wyrazem są nowe rejestratory cyfrowe Aper PDR-X.

W dziedzinie CCTV wciąż trwa dynamiczny i nieustanny postęp technologiczny. Udoskonalane są metody kompresji, stosowane są coraz szybsze procesory, dzięki czemu poprawie ulega efektywność pracy urządzeń i wygoda użytkowania. Naturalny rozwój dotyczy również urządzeń rejestrujących, a jego wyrazem są nowe rejestratory cyfrowe Aper PDR-X.

Seria PDR-X jest następcą udanej serii PDR-S i jest przeznaczona do zastosowania w klasycznych instalacjach nadzoru wizyjnego. Zapewnia dostateczną wydajność zapisu i jednocześnie oferuje wiele możliwości wyższych modeli PDR. Rejestratory PDR-X mają także zdolność pracy systemowej i mogą być elementem bardziej rozwiniętej architektury CCTV.

Urządzenia te występują w wersji 8- i 16-kanałowej. Należą do klasy rejestratorów autonomicznych, działających na bazie systemu Embedded Linux. Platforma ta gwarantuje stabilność i bezpieczeństwo. Rejestrator PDR-X jest w stanie wykonywać cztery operacje równolegle – zapis, podgląd na żywo/odtwarzanie, archiwizację i transmisję sieciową – zatem jest to tzw. kwadrupleks.

Zwykła obsługa odbywa się za pomocą monitora głównego podłączonego poprzez analogowe wyjście wizyjne (BNC), wyjście VGA lub HDMI. Zarządzanie rejestratorem i jego konfiguracja jest przeprowadzana z użyciem prostego i przyjaznego menu ekranowego w języku polskim, a proces podstawowego przygotowania urządzenia jest wydatnie skracany dzięki opcji szybkiej konfiguracji (*Quick Setup*).

Ponadto, niezależnie od wymienionych operacji monitora nadrzędnego, na ekranie pomocniczym (tzw. spocie) dostępny jest podgląd na żywo obrazu z pojedynczych kamer – na żądanie, w trybie alarmowym lub w sekwencji.

Kontrola nad urządzeniem PDR-X może być sprawowana na różnorakie sposoby, zarówno lokalnie, jak i zdalnie. Lokalnie odbywa się ona przy użyciu dotykowej klawiatury panelu przedniego, myszy USB lub adresowalnego pilota IR (administrowanie maks. 99 urządzeniami), który jest dostarczany w komplecie z rejestratorem.

Urządzenia PDR-X są zdolne do pracy w rozproszonych strukturach telewizji dozorowej. Do zarządzania wykorzystywany jest zewnętrzny pulpit (PDR-KBD lub GSC-4000J), komunikujący się poprzez interfejs RS485 (do 99 jednostek). Możliwe jest też manewrowanie kamerami obrotowymi.

Jeśli z rejestratora korzysta wiele osób, konieczne jest określenie poziomów uprawnień. Urządzenie PDR-X przewiduje indywidualne definiowanie kont operatorów w zakresie takich uprawnień, jak odtwarzanie, archiwizacja, kierowanie kamerami obrotowymi, zdalna transmisja, załączanie/wyłączanie zapisu, konfiguracja urządzenia.

Obecnie znaczna część instalowanych rejestratorów jest podłączana do sieci IP, co umożliwia użytkownikom zdalny dostęp do ich zasobów. Znaczący wpływ na użyteczność rejestratorów ma więc oprogramowanie sieciowe. Urządzenie PDR-X umożliwia kilka sposobów nadzoru i wykonywanie różnorodnych zadań. Można dozorować, wykorzystując przeglądarkę internetową lub bezpłatne oprogramowanie – CMS Lite, xCMS-DVRPlayer lub EMS. Podstawową obsługę gwarantuje przeglądarka oraz aplikacje CMS Lite lub xCMS-DVRPlayer *(Central Management Suite)*. Służą one do zarządzania pracą rejestratora, wprowadzania zmian w konfiguracji, wyświetlania i nagrywania obrazu w czasie rzeczywistym, manewrowania głowicami obrotowymi, kontrolowania stanu, wglądu w zapisany materiał (odtwarzania lub archiwizacji z użyciem komputera). Natomiast do monitorowania zaawansowanego systemu złożonego z wielu jednostek (do 1000) przeznaczone jest oprogramowanie EMS (*Enhanced Management Suite*). Poza funkcjami CMS-a EMS posiada mnóstwo innych narzędzi przystosowanych do działania w dużej instalacji. Jednym z nich jest mechanizm tworzenia tzw. obiektów wirtualnych, grupujących kamery z różnych rejestratorów fizycznych. Umożliwia on zebranie obrazów z nawet 64 kamer w jednym oknie i ich prezentację na ekranie komputera. Jeżeli to nie wystarcza, można otworzyć kolejne, niezależne okna (maksimum osiem) w celu obserwacji wizji z innych kamer lub rejestratorów. Dysponując stanowiskiem wielomonitorowym, użytkownik jest w stanie stworzyć rozbudowane centrum dozoru.

Fot. 1. Ekran główny

Fot. 2. Menu ekranowe

Zawiadywanie systemem monitorowania usprawnia funkcja e-map, która jest przeznaczona do administrowania rozległą instalacją CCTV. Bazuje ona na graficznej reprezentacji nadzorowanego systemu – obiektu lub grupy obiektów. Elementy e-mapy odpowiadają rejestratorom, kamerom, wyjściom

alarmowym lub submapom i służą do wyświetlenia obrazu na żądanie, raportowania statusu czy sterowania urządzeniami wykonawczymi (sygnalizatorami, oświetleniem itp.).

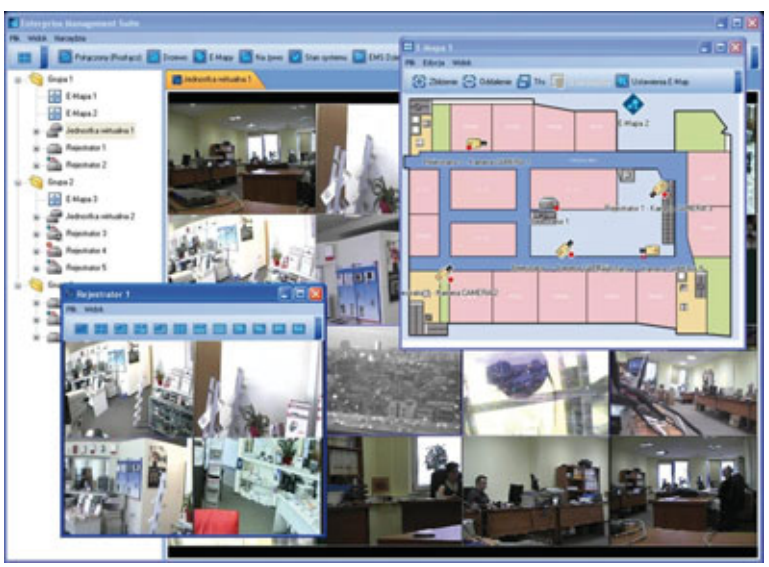
Oprócz obserwacji obrazu centrum dozoru wymaga nieprzerwanego kontrolowania stanu składników systemu. Oprogramowanie EMS bezustannie nadzoruje stan rejestratorów oraz odbiera komunikaty o alarmach, wykrytym ruchu, zanikach sygnału wizyjnego czy krytycznych awariach. Informacje te mogą być prezentowane w formie graficznej (w oknie stanu lub na e-mapie), dźwiękowej, tekstowej (w postaci odświeżanego na bieżąco dziennika zdarzeń lub okienek z notyfikacjami) oraz obrazowej (jako wyskakujące okna z podglądem na żywo).

Podobnie jak w przypadku przydzielania uprawnień użytkowników na poziomie poszczególnych jednostek, uprawnienia operatorów mogą być ustalane w samej stacji monitorowania, w ramach oprogramowania.

Oprogramowanie EMS jest zgodne ze starszymi seriami rejestratorów PDR. Dzięki temu modernizacja istniejących systemów przez dodawanie nowych jednostek nie stanowi problemu. W jednej instalacji mogą kooperować zróżnicowane modele urządzeń PDR.

Poza standardową zdalną obsługą możliwe jest połączenie z rejestratorem z platform mobilnych, takich jak PDA lub telefon komórkowy. Ten rodzaj dostępu pozwala uzyskać obrazy wyświetlane w trybie na żywo oraz sterować kamerami obrotowymi.

Fot. 3. Opcjonalny pulpit sterujący



Fot. 4. Oprogramowanie Aper EMS – tryb „multiwindow”

Fot. 5. Oprogramowanie Aper EMS – tryb „multicamera”

Rejestrator PDR-X stosuje najpopularniejszą obecnie metodę kompresji – H.264, która w dziedzinie CCTV jest najbardziej uniwersalną metodą komprymacji materiału wizyjnego. Pozwala ona uzyskać strumień/rozmiar klatki, który jest dużo mniejszy niż w przypadku JPEG-a czy MPEG-a. Owocuje to niewielką zajętością dysków, na których rejestrowane są nagrania, i małym obciążeniem sieci IP przy transmisji obrazu, a także obniża związane z tym koszty.

Urządzenia serii PDR-X umożliwiają zapis materiału wizyjnego w długich przedziałach czasowych. Jest to zasługą przede wszystkim kompatybilności z nośnikami SATA o znacznych pojemnościach (2 TB). Rejestracja jest dokonywana na wewnętrznym dysku. Po zdemontowaniu nagrywarki CD/DVD możliwe jest podłączenie drugiego dysku (sumarycznie do 4 TB). Konstrukcja rejestratora nie wyklucza stosowania nośników o jeszcze większych rozmiarach. W najbliższej przyszłości pojawią się na rynku dyski o pojemnościach 2,5 TB i 3,2 TB, które będą mogły być wykorzystane.

Dopasowanie do warunków w monitorowanym obiekcie ułatwiają rozmaite tryby rejestracji: ciągłej lub w harmonogramie, po detekcji ruchu i alarmowej (z pre- i postalarmem). Jeżeli system CCTV nie wymaga nieprzerwanego zapisu obrazu, pozwala to znacznie zaoszczędzić pamięć dyskową.

Archiwizacja, podobnie jak rejestracja, może być dokonywana lokalnie lub zdalnie, w oparciu o sieć IP, za pomocą oprogramowania klienckiego. W trakcie lokalnego kopiowania nagrań (na płytę CD/DVD lub nośnik USB flash) wraz z właściwym materiałem wizyjnym na nośnik automatycznie przegrywana jest aplikacja odtwarzająca. Użytkownik nie musi instalować na komputerze dodatkowego oprogramowania w celu odtworzenia zawartości archiwum.

Głównym zadaniem rejestratora jest nagrywanie obrazu (i dźwięku). Jednak PDR-X jest w stanie również przechowywać informacje o ważnych zdarzeniach (wykonywanych operacjach, odnotowanych sytuacjach alarmowych itp.). Dane te są zapisywane w dzienniku zdarzeń. W połączeniu z materiałem wizyjnym stanowią cenne źródło informacji na temat nadzorowanego obiektu. Komunikaty dotyczące kluczowych zdarzeń, takich jak pobudzenie wejścia alarmowego, detekcja ruchu, zanik sygnału wizyjnego czy awaria dysku, mogą być sygnalizowane za pomocą ikon pojawiających się na ekranie, przez emisję sygnałów dźwiękowych, wzbudzenie wyjść alarmowych (w przypadku urządzeń wykonawczych) i wysyłanie informacji pocztą elektroniczną na wskazany adres e-mail. Ponadto poczta elektroniczna w połączeniu z usługami sieci komórkowych umożliwia powiadomienia poprzez SMS. Te same informacje o zdarzeniach mogą być odbierane na bieżąco za pośrednictwem oprogramowania sieciowego. Wizualizacja zdarzeń alarmowych pozwala łatwo kontrolować stan całego systemu i poszczególnych rejestratorów wchodzących w jego skład. Działanie większej instalacji CCTV usprawnia synchronizacja czasu.

Fot. 6. Aplikacja Aper PDAViewer

Równie wygodny jest wgląd w nagrania powiązane z zaistniałymi zdarzeniami poprzez interfejs w postaci kalendarza graficznego z zaznaczonymi liniami czasowymi. Fakt rejestracji alarmowej lub detekcji ruchu jest sygnalizowany zmianą koloru. Dzięki temu można znacznie szybciej znaleźć interesujący fragment obrazujący zdarzenie w materiale wideo.

Olbrzymią zaletą rejestratorów PDR-X jest kompatybilność z urządzeniami Aper innych generacji oraz oprogramowaniem sieciowym przeznaczonym do ich obsługi. Zgodność ta wynika z tego, iż obecnie wszystkie rejestratory PDR mają zbliżone możliwości konfiguracyjne. Zatem ustawienia, opcje i narzędzia PDR-X dorównują tym, które są stosowane w wyższych modelach rejestratorów Aper, a różnica dotyczy szybkości rejestracji czy liczby dysków twardych. Dzięki temu rejestratory PDR-X znajdują zastosowanie nie tylko w małych i prostych instalacjach telewizji dozorowej. Mogą być z powodzeniem wykorzystywane w tych częściach bardziej zaawansowanych systemów CCTV, w których instalowanie urządzeń o wysokich prędkościach zapisu nie znajduje uzasadnienia, a od zastosowanego rejestratora oczekujemy rozsądnej wydajności przy zachowaniu dobrej jakości i funkcjonalności.

Mariusz Witulski
S.P.S. Trading

Fot. 7. PDR-X3016 – panel przedni

Fot. 8. PDR-X3016 – panel tylny

PixelPro
nowa technologia marki GANZ

CBC Group

CBC Group wprowadza na rynek nową serię kamer hybrydowych IP H.264, zgodnych ze standardem ONVIF i wyposażonych w szereg innowacyjnych rozwiązań. Rodzina PixelPro obejmuje kamery Full HD w wersji kompaktowej oraz kopułkowej – w obudowach wandaloodpornych. Rozdzielczości kamer wynoszą odpowiednio, w zależności od modelu – VGA, 1.3 MP (720p) oraz 2 MP (1080p)

Rys. 1. Kamery z serii PixelPro

Wyposażenie kamer zostało ujednolicone i przystosowane do pracy z rozdzielczością Full HD, tak więc wersja kompaktowa jest kompatybilna z obiektywami typu Full HD, ze szczególnym wskazaniem na wybrane modele obiektywów COMPUTAR. Cała seria PixelPro to kamery dualne z automatycznym filtrem IR-Cut, zapewniające bardzo dobrą jakość obrazu w zmiennych warunkach oświetleniowych. Przetwornik CMOS 1/2.5" ze skanowaniem progresywnym o rozdzielczości 2592×1944 pikseli jest kluczowym elementem, decydującym o wysokiej jakości i wyrazistości obrazu na miarę tej nowoczesnej technologii.

Dual-codec, czyli podwójny kodek obrazu, pozwala korzystać z dwóch niezależnych strumieni wizyjnych jednocześnie (H.264 oraz MJPEG). Wydajność kodeka gwarantuje uzyskanie 25 kl./s dla maksymalnej rozdzielczości 2 MPix (1080p). Dzięki hybrydowej budowie kamer PixelPro na dodatkowym wyjściu analogowym (BNC) dostępny jest kompozytowy sygnał wizyjny o rozdzielczości 600 TVL. Każdy model posiada dwukierunkowy kanał akustyczny z możliwością transmisji dźwięku poprzez IP.

Przysłona typu P-IRIS

Tradycyjna przysłona automatyczna wprowadza rozmycie w obrazie megapikselowym, szczególnie przy bardzo dobrym oświetleniu – odpowiada za to zjawisko dyfrakcji. Innowacyjnym rozwiązaniem w kamerach PixelPro jest nowy rodzaj przysłony automatycznej, tzw. P-IRIS. Rozwiązanie to zostało opracowane przez CBC Group. Służy ono do uzyskiwania optymalnej jakości obrazu przez kamery wysokorozdzielcze i obecnie jest wprowadzane do wybranych obiektywów COMPUTAR. Sterowanie przysłoną odbywa się za pomocą silnika krokowego poprzez podawanie odpowiedniej ilości impulsów sterujących. Dzięki takiemu rozwiązaniu operator ma pełną kontrolę nad stopniem

otwarcia przysłony, a co za tym idzie – nad jakością obrazu. Metoda P-IRIS umożliwia znacznie bardziej precyzyjne kontrolowanie jakości obrazu w porównaniu z tradycyjnym sterowaniem metodą DC (*Direct Drive*). Praktyczne korzyści wynikające ze stosowania przysłony P-IRIS są ogromne. Dzięki niej można precyzyjnie „dostroić" optykę i uzyskać maksymalną wartość funkcji przenoszenia kontrastu MTF. Wysoka wartość funkcji MTF przekłada się na wyrazistość (ostrość) obrazu. Kolejnym atutem przysłony P-IRIS jest pełna kontrola nad głębią ostrości, czyli możliwość optymalnego dostosowania obrazu do oczekiwań użytkownika. Oczywistym efektem stosowania przysłony P-IRIS jest również pełna kontrola apertury obiektywu.

A zatem nie tylko liczba megapikseli ma wpływ na wyrazistość obrazu. Prześciganie się w jej zwiększaniu nie ma sensu, jeśli pomija się inne, jakże istotne parametry kamer, takie jak czułość, liczba klatek na sekundę, wielkość strumienia danych wyjściowych itp.

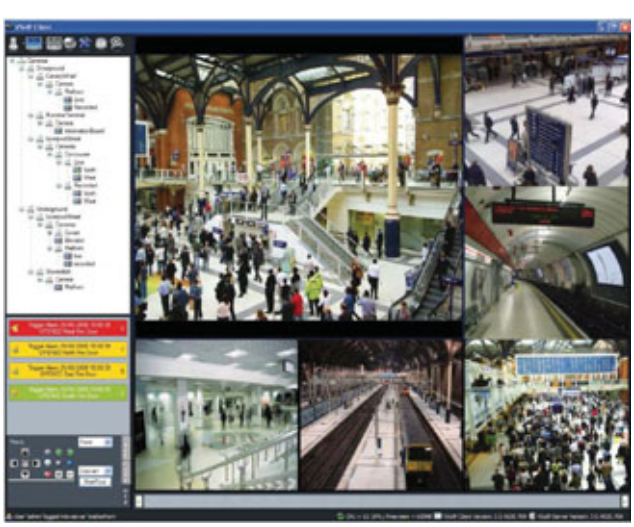
MFZ – zdalne sterowanie obiektywem

Kolejną innowacją, którą zastosowano w kopułkowej wersji kamer PixelPro, jest obiektyw o zmiennej ogniskowej z silnikowym napędem mechanizmów regulacyjnych (*Motorized Focus & Zoom*). Jego zastosowanie zwiększa funkcjonalność kamery, a przede wszystkim ułatwia regulację obiektywu podczas montażu. Nie jest ona łatwa, szczególnie w przypadku kopułkowych kamer megapikselowych z nakładanym kloszem sferycznym. Dzięki zastosowaniu precyzyjnych silników krokowych regulacja obiektywu może być przeprowadzona zdalnie, z bardzo dużą dokładnością. Jest to innowacyjne, a jednocześnie bardzo praktyczne i skuteczne rozwiązanie.

Zastosowanie w obiektywach kamer PixelPro dwóch innowacji, czyli przysłony P-IRIS oraz funkcji MFZ polepsza parametry jakościowe obrazu oraz zwiększa funkcjonalność kamer.

Lokalna rejestracja na karcie SD

Kamery PixelPro są wyposażone w gniazdo kart typu Micro SD o dowolnej pojemności. Nośnik lokalny w kamerze może być wykorzystany do rejestracji wybranych zdarzeń, a także do rejestracji ciągłej, co zapewnia redundancję nagrywania w systemie jako dodatkowe zabezpieczenie przed utratą nagrań.



Rys. 2. Aplikacja VSoIP

Pełna obsługa alarmów

Wejście i wyjście alarmowe w kamerach PixelPro umożliwia zintegrowanie tych urządzeń z innymi systemami. Dzięki detekcji ruchu oraz możliwości rejestracji obrazów w trybie pre- i postalarmowym kamera PixelPro, wyposażona dodatkowo w kartę Micro SD, może funkcjonować w systemie jako autonomiczne urządzenie. Funkcja emailowego powiadamiania o zdarzeniach oraz obsługa protokołu FTP zwiększają możliwości tych kamer, czyniąc je bardziej niezależnymi urządzeniami, które mogą na przykład odciążać centralne oprogramowanie zarządzające.

Kamery PixelPro są kompatybilne między innymi z oprogramowaniem VSoIP (CBC) oraz NetStation (ALNET). Dzięki pełnej zgodności ze standardem ONVIF wszystkie modele PixelPro mogą również być stosowane w systemach z innymi aplikacjami, które są zgodne z tym standardem, zwiększając swobodę w projektowaniu systemów CCTV IP.

Obsługa poprzez oprogramowanie sieciowe VSoIP

VSoIP daje nowe możliwości projektantom cyfrowych systemów CCTV IP. Koncepcja tego rozwiązania wywodzi się z najbardziej wymagających aplikacji służących do nowoczesnego monitorowania wizyjnego i opartych na cyfrowej technologii IP.

Rozproszona struktura systemu składającego się z wielu elementów pozwala na dużą swobodę skalowania i konfiguracji. Dzięki redundantnej rejestracji wizyjnej zapewnione jest bezpieczeństwo danych, nawet w sytuacjach awaryjnych. VSoIP integruje takie elementy systemów CCTV, jak kamery IP, kamery megapikselowe z kompresją H.264, rejestratory cyfrowe oraz serwery wizyjne. Połączenie wszystkich tych elementów wraz z centralnym modułem zarządzającym VSoIP Server daje kompletny system monitorowania o bardzo rozbudowanej funkcjonalności.

Aplikacja VSoIP Server jest rdzeniem całego systemu VSoIP, który przechowuje wszystkie informacje o użytkownikach, urządzeniach, mapach, konfiguracjach systemowych oraz prawach dostępu. Służy do tego unikatowy system bazodanowy, który jest zintegrowany z aplikacją VSoIP Server.

Dostęp do zasobów i konfiguracji serwera uzyskujemy z poziomu aplikacji klienckiej VSoIP Client, która posiada intuicyjny oraz łatwy w obsłudze interfejs użytkownika. VSoIP Server zarządza rejestrami całego systemu oraz przepływem wszystkich strumieni danych. W przypadku aktywacji nagrywania przez jakiekolwiek urządzenie w systemie (np. kamerę IP), VSoIP Server uruchamia tę usługę lokalnie na jednostce NVR, zapewniając autonomiczne nagrywanie strumienia nawet w sytuacji własnej awarii.

CBC Group

Rejestrator mobilny marki NOVUS

Patryk Gańko

W *Zabezpieczeniach* nr 2/2010, w artykule „Rejestratory econo marki NOVUS”, scharakteryzowałem rejestratory serii E oraz zapowiedziałem wydanie oprogramowania do zarządzania rejestratorami pod nazwą E-Viewer. W międzyczasie seria E została uzupełniona o rejestrator do zastosowań mobilnych, o wielu bardzo ciekawych i unikatowych cechach. Z tych powodów w niniejszym artykule chciałbym opisać rejestrator NDR-EA3104M oraz oprogramowanie E-Viewer służące do jego obsługi

NDR-3104M

Montowany w dedykowanym uchwycie rejestrator NDR-EA3104M ma specjalną konstrukcję, która zabezpiecza go przed uszkodzeniem na skutek wibracji oraz wstrząsów. Dzięki temu możliwy jest montaż urządzenia w różnego rodzaju pojazdach, takich jak samochody osobowe, samochody ciężarowe, autobusy itp. Ponadto rejestrator jest wyposażony w dysk twardy 2,5" 250 GB (laptopowy), fabrycznie montowany w kieszeni, charakteryzujący się większą wytrzymałością na udary mechaniczne aniżeli typowe dyski desktopowe.

W celu umożliwienia pracy rejestratora w różnych typach instalacji (różne standardy dla samochodów osobowych i ciężarowych) rejestrator może być zasilany napięciem stałym, mieszczącym się w szerokim przedziale od 12 do 36 V, a maksymalny pobór mocy wynosi 64 W. Dodatkowo, w celu uproszczenia instalacji systemu monitorowania w pojeździe, rejestrator został wyposażony w wyjścia dostarczające napięcia 12 V_{DC} o sumarycznej wydajności prądowej 1,6 A, służące do zasilania kamer oraz jednego monitora. Tym samym instalacja zasilająca kamer oraz monitora jest realizowana równolegle z instalacją transmisji wizji i nie wymaga stosowania dodatkowych elementów, takich jak przetwornice czy rozdzielacze.

W przypadku wielu zastosowań ważną kwestią jest utrzymanie procesu rejestracji przez zdefiniowany czas po wyłączeniu pojazdu. Umożliwia to np. monitorowanie pasażerów wchodzących do autobusu stojącego na przystanku lub monitorowanie pojazdu na parkingu. Po wyłączeniu stacyjki pojazdu proces rejestracji może być realizowany jeszcze przez co najmniej godzinę dzięki zasilaniu według schematu przedstawionego na rys. 1 i dokonaniu odpowiednich ustawień w menu. Oczywiście czas ten musi uwzględniać wydajność akumulatora.

Rejestrator może bezawaryjnie pracować w zakresie temperatur od –20°C do 40°C. W przypadku włączenia urządzenia, co w większości przypadków należy utożsamiać z uruchomieniem stacyjki pojazdu, w temperaturze poniżej +5°C rejestracja nie będzie mogła być realizowana bezpośrednio na twardym dysku, gdyż mogłoby to doprowadzić do jego mechanicznego uszkodzenia. W takiej sytuacji uruchamiana jest grzałka oraz wentylator w celu zapewnienia prawidłowej cyrkulacji ogrzanego powietrza. W zależności od temperatury otoczenia proces nagrzewania dysku może trwać od kilku do kilkunastu minut. Do momentu jego nagrzania obrazy mogą być rejestrowane na karcie SD znajdującej się w kieszeni dysku twardego. Obsługiwane są karty o pojemności do 16 GB.

Rejestrator ma również odbiornik GPS wraz z zewnętrzną anteną. Dzięki temu można nie tylko rejestrować obrazy z kamer, ale także zapisywać aktualne koordynaty położenia monitorowanego obiektu. Podczas odtwarzania zapisanego materiału wizyjnego przez sieć lub skopiowanego materiału w formacie własnym rejestratora (pliki z rozszerzeniem .strg) za pomocą oprogramowania E-Viewer w dodatkowym panelu wyświetlana jest mapa z serwisu GoogleMapy z naniesionym aktualnym położeniem obiektu. Pozwala to na odtworzenie jego trasy przemieszczania się.

Rejestrator posiada czujnik G, który rejestruje aktualne przeciążenia w celu zredukowania ilości zapisywanego materiału. Zasada działania czujnika jest podobna do działania funkcji detekcji ruchu, która w przypadku przemieszczających

Fot. 1. Rejestrator mobilny NDR-EA3104M

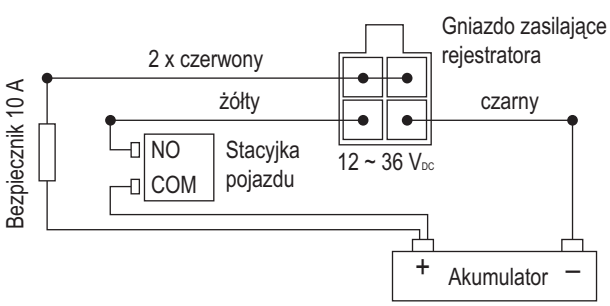
się obiektów jest całkowicie bezużyteczna. Czujnik przeciążeń ma regulowaną czułość i, w przypadku gwałtownego hamowania lub kolizji drogowej, może uruchomić rejestrację obrazów z wybranych kamer przez określony czas i ze zwiększoną prędkością zapisu, a także aktywować funkcje nagrywania przedalarmowego.

Rejestrator może rejestrować dane tekstowe i odtwarzać je wraz z materiałem wideo z innych systemów zainstalowanych w pojeździe (np. kasy fiskalnej). Dane te, przechwytywane poprzez porty RS232 i RS485, muszą być generowane w standardzie ASCII. Szybkie wyszukiwanie zapisanych danych jest realizowane poprzez słowa kluczowe.

Podczas eksploatacji urządzenia ważne jest zapewnienie szerokiego spektrum możliwości kopiowania i archiwizowania zapisanych strumieni wizyjnych. Bezpośrednio z rejestratora dane mogą być kopiowane na pamięci typu flash lub dysk twardy poprzez port USB. Ponadto, po otwarciu klapki, możliwe jest wyjęcie kieszeni z dyskiem twardym w celu podłączenia jej do komputera PC i odtwarzania lub kopiowania nagrań zawartych na dysku. Proces kopiowania jest realizowany poprzez gniazdo mini USB umieszczone na kieszeni. Dane mogą też być kopiowane poprzez sieć – za pomocą przeglądarki IE lub programu E-Viewer.

Na panelu czołowym rejestratora nie ma przycisków. Rejestrator może być obsługiwany za pomocą myszy USB, pilota IR lub klawiatur NV-KBD30 i NV-KBD70. Wszelkich ustawień rejestratora można dokonywać zdalnie – przez sieć (poprzez IE, E-Viewer lub aplikację do telefonów iPhone).

Rejestrator mobilny, wykorzystujący system operacyjny Linux, pracuje w trybie kwadrupleks i umożliwia zapis, podgląd na żywo, odtwarzanie i kopiowanie nagrań oraz połączenie sieciowe równocześnie. Może zapisywać do czterech kanałów wizji i dźwięku z prędkością do 100 klatek na sekundę (przy rozdzielczości CIF) oraz do 25 klatek na sekundę (przy rozdzielczości D1). Zapis wizji i dźwięku jest realizowany zgodnie z algorytmem kompresji H.264, co umożliwia nawet trzydziestoprocentową



Rys. 1. Schemat podłączenia zasilania rejestratora.

Fot. 2. Aplikacja E-Viewer w trybie odtwarzania wraz z panelem mapy

redukcję przestrzeni dyskowej lub pasma transmisji w porównaniu z algorytmem MPEG4. Wielkość archiwum jest redukowana także dzięki możliwości odrębnego definiowania prędkości i jakości nagrywania w przypadku każdej z kamer, zaawansowanym funkcjom harmonogramu nagrywania i detekcji ruchu, a także funkcjom przed-alarmu i po-alarmu.

Pod innymi względami rejestrator NDR-EA3104M jest identyczny z pozostałymi rejestratorami serii E, które zostały opisane w Zabezpieczeniach nr 2/2010. Ze względu na ramy niniejszego artykułu skupiłem swoją uwagę na unikatowych cechach rejestratora NDR-EA3104M, odróżniających go od pozostałych modeli serii, i pominąłem m.in. tak ważne funkcje, jak autodiagnostyka, powiadamianie o zdarzeniach krytycznych, poziomy dostępu i autoryzacja hasłem, pozostawiając je dociekliwości czytelników.

E-Viewer

Uzupełnieniem systemu wykorzystującego rejestratory serii E jest oprogramowanie do zdalnego zarządzania E-Viewer. Ma ono podobne funkcje, jak oprogramowanie RASplus, służące do obsługi rejestratorów serii H. Aplikacja E-Viewer umożliwia równoczesne łączenie się z wieloma rejestratorami i wyświetlanie do 128 obrazów z kamer w dwóch niezależnych oknach w podziale 8×8. Układy kamer mogą być dowolnie definiowane, zapamiętywane i następnie łatwo wywoływane przez operatorów. Połączenia z rejestratorami mogą być realizowane zarówno „na żywo", jak i w trybie odtwarzania. Z poziomu oprogramowania możliwa jest również zdalna konfiguracja rejestratorów, niemalże identyczna z lokalną.

Aplikacja zawiera moduł E-Viewer Callback, który realizuje funkcję połączenia zwrotnego (przesyłanie informacji o zdarzeniach systemowych na zdefiniowane adresy sieciowe) i pozwalający na reakcję tylko na zdefiniowane wcześniej zdarzenia, optymalizując tym samym pracę operatora. Ponadto oprogramowanie zawiera moduł zdalnego monitorowania zdarzeń systemowych (utrata sygnału wideo, aktywacja wejść/wyjść alarmowych, detekcja ruchu).

Na potrzeby niniejszego artykułu zostało zrealizowane nagranie testowe z rejestratora zainstalowanego w pojeździe. Można na nim zobaczyć, jak działa rejestrator mobilny, funkcja wizualizacji położenia obiektu na mapie oraz aplikacja E-Viewer. Pod poniższym adresem znajduje się plik w formacie STRG, skopiowany z mobilnej lokalizacji: *http://www.novuscctv.pl/pl/webfm_send/2587*. Pod adresem *http://www.novuscctv.pl/pl/node/6613* można ściągnąć aplikację E-Viewer do odtworzenia powyższego pliku oraz ewentualnie instrukcję obsługi aplikacji. Ponadto pod adresem *http://www.novuscctv.pl/pl/demo* znajduje się udostępniona wersja demo rejestratora serii E, współpracująca z oprogramowaniem E-Viewer.

Patryk Gańko
AAT Holding

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Rejestrator cyfrowy do zastosowań mobilnych

HDD 2.5" SATA i karta SD

Rejestrator posiada jeden dysk SATA 2.5" umieszczony w wyjmowanej kieszeni. Mocowania dysku twardego oraz samego rejestratora zostały wykonane z wykorzystaniem nowoczesnej, absorbującej wibracje i uderzenia technologii. Dodatkowo kieszeń dysku została wyposażona w gniazdo mini USB umożliwiające bezpośrednie podłączenie dysku twardego do komputera PC, w celu odtwarzania lub kopiowania nagrań zawartych na nośniku. W niskich temperaturach otoczenia, wykraczających poza zakres pracy dysku twardego, rejestracja odbywa się na kartę SD.

Odbiornik GPS

Wbudowany odbiornik GPS, z dołączoną anteną zewnętrzną, pozwala na zapisywanie aktualnych koordynat położenia, a tym samym śledzenie i rejestrację prędkości obiektu. System korzysta z dedykowanej do rejestratora aplikacji E-Viewer oraz serwisu Google Maps, precyzyjnie obrazujących przebytą trasę i prędkość pojazdu.

Czujnik przeciążeń (G-sensor)

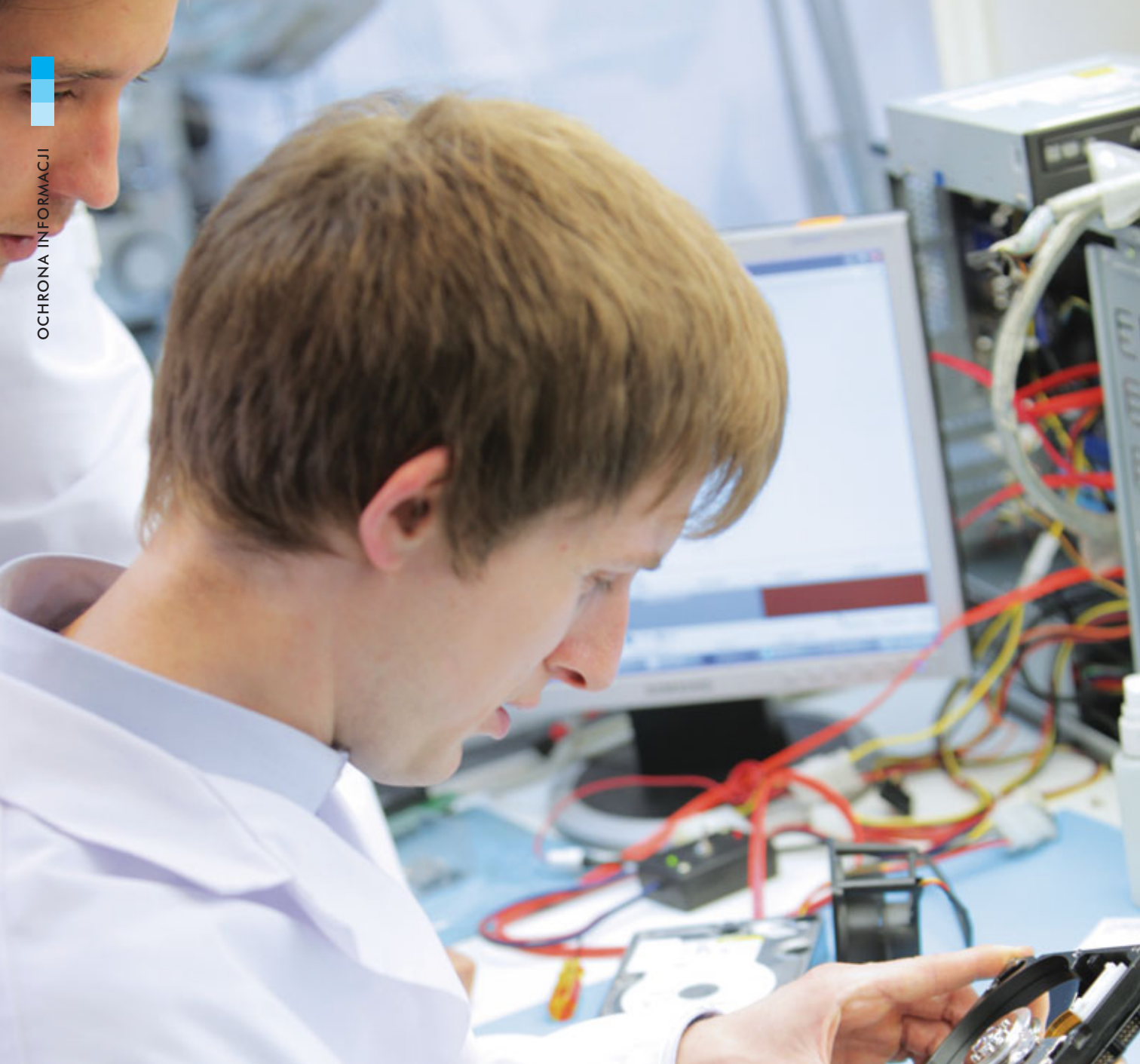
Wbudowany czujnik przeciążeń umożliwia wywołanie alarmu rejestratora w przypadku zderzenia, stłuczki czy gwałtownego hamowania. Dzięki jego zastosowaniu, powyższe zdarzenia drogowe mogą zostać zarejestrowane według parametrów zdefiniowanych dla nagrywania alarmowego.

E seria

E-Viewer Compatible

- Quadrupleks: równoczesny zapis, podgląd „na żywo"/odtwarzanie nagrań, kopiowanie nagrań i połączenie sieciowe
- Prędkość nagrywania do 100 obr/s
- Algorytm kompresji H.264
- Rozdzielczość nagrywania: 720x576, 720x288, 360x288
- Funkcje przed-alarmu i po-alarmu
- Funkcja przechwytywania danych tekstowych z urządzeń fiskalnych
- Możliwość rejestrowania do 4 kanałów audio
- Praca w sieci komputerowej, w tym możliwość połączenia z wieloma rejestratorami jednocześnie oraz wysyłanie wiadomości e-mail o sytuacjach alarmowych
- Auto-diagnostyka systemu z automatycznym powiadamianiem
- Menu w języku polskim
- Mocowanie zapewniające ochronę przed wibracjami i wstrząsami
- Zasilanie: 12 ~ 36 VDC

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



Czy twoje archiwa cyfrowe to tykająca bomba zegarowa?

Paweł Odor

Archiwa taśmowe, mimo iż przewiduje się wycofanie ich z użycia i ich rynkową śmierć, wciąż mają się dobrze i pozostają jedną z dominujących kopalni danych, między innymi kluczowych dokumentów biznesowych. Przeprowadzone niedawno przez Enterprise Strategy Group (ESG) badanie pokazuje, że 82 procent organizacji wciąż stosuje popularne taśmy w swych procedurach backupowych. Co ciekawe, niektóre z firm tworzą kopie swoich starych dokumentów wyłącznie na taśmach

Fot. 1. Specjaliści Kroll Ontrack przed odzyskiwaniem danych z dysku twardego

Mimo iż coraz więcej firm używa dysków w procesach backupowych przeprowadzanych online, rozmiary danych przechowywanych na offsite'owych taśmach wzrastają, głównie z powodu zwiększającej się ilości gromadzonych informacji cyfrowych. Jak wskazują naukowcy, ilość ta może dochodzić nawet do jednego zetabajta. Dlatego też właściwa polityka zarządzania danymi i upewnienie się, że tylko istotne informacje są magazynowane w odpowiednim czasie i na najbardziej adekwatnych nośnikach, takich jak dyski czy taśmy, jest dla firm istotne bardziej niż dotychczas.

Wiele firm nadal nie uwzględnia właściwej polityki zarządzania danymi w swych strategiach, co powoduje, że wiele danych jest niepotrzebnie przechowywanych na zasobach taśmowych. Wzmaga to niebezpieczeństwo utraty danych i niekorzystnie odbija się na ich budżecie, gdy pojawiają się problemy z dostępem do kluczowych informacji. Niestety wciąż zbyt wiele organizacji ma nadzieję, że przypadki utraty danych z ich zasobów cyfrowych nie będą miały miejsca, a zasoby offline'owe będą dostępne o każdej porze dnia i nocy.

Obecnie specjaliści rozróżniają kilka najważniejszych zagrożeń związanych z dostępem do danych, takich jak między innymi: błąd człowieka, awaria nośników danych (niszczejące z wiekiem taśmy), awaria oprogramowania czy przestarzałe formaty zapisu, które nie są kompatybilne z systemami stosowanymi obecnie. Istotne staje się wsparcie specjalistów, którzy ułatwiają firmom prawidłowe przechowywanie danych lub ich odzyskanie. Dzieje się to szczególnie wtedy, gdy w grę wchodzą dziesiątki tysięcy plików.

Co istotne, organizacje nie powinny polegać na fałszywym poczuciu bezpieczeństwa, jakie dają m.in. archiwa taśmowe, lecz korzystać z doświadczenia firm, które od lat pomagają środowiskom biznesowym w prawidłowym prowadzeniu bibliotek archiwalnych danych. Największe laboratoria odzyskiwania danych i informatyki śledczej proponują obecnie efektywne i relatywnie tanie usługi zarządzania informacjami, a także odzyskiwania i migracji informacji z taśm. Używają one najnowszych dostępnych technologii. Na jaką pomoc mogą więc liczyć obecnie firmy? Pomoc ta może obejmować:

– przeprowadzanie operacji na nawet najbardziej egzotycznych urządzeniach,
– przeprowadzenie operacji na niemal wszystkich rodzajach oprogramowania i nośników,
– odzyskiwanie danych z fizycznie zniszczonych nośników,
– przeprowadzanie zdalnych operacji na danych udostępnionych online (bez konieczności fizycznego kontaktu z nośnikiem danych).

Zarządzanie cyklem życia danych i jego wpływ na archiwa cyfrowe

By dokładnie nakreślić problem archiwów, należy przede wszystkim poznać cykl życia informacji danej organizacji. Jest to konieczne, by zrozumieć, dlaczego tak istotne są kwestie prowadzenia właściwej polityki ochrony danych firmowych. Amerykańskie Stowarzyszenie Przemysłu Sieci Składowania Danych (*www.SNIA.org*) definiuje Zarządzanie Cyklem Życia Informacji jako:

– zasady, procesy, praktyki, usługi i narzędzia używane do zestrojenia biznesowej wartości informacji z najbardziej właściwą i efektywną kosztowo infrastrukturą od czasu powstania informacji do jej końcowego umiejscowienia,
– uporządkowanie informacji zgodnie z zapotrzebowaniem biznesowym poprzez zarządzanie zasadami i poziomami usług powiązanymi z aplikacjami, metadanymi i danymi.

Ciekawe jest to, iż określenie „nośnik danych" nie jest zawarte w definicji SNIA. Mimo iż definicja jest odpowiednia dla innych dyscyplin technicznych, takich jak zabezpieczanie informacji, bezpieczeństwo, architektura przedsiębiorstwa itd., jest stworzona także po to, by pouczyć organizacje o strategiach zarządzania informacją, taktykach i wykorzystywanych metodach.

Istnieje wiele podstawowych pytań, które są nierozerwalnie związane z koncepcją korporacyjnego zarządzania danymi. Jakie dane organizacja aktualnie przechowuje? Czy są one zlokalizowane na miejscu, czy u sprzedawcy powierzchni do przechowywania danych, a jeśli tak, to na której taśmie? Które dane są faktycznie niezbędne do utrzymania ciągłości biznesu lub do celów prawnych, a które są zduplikowane lub niepotrzebne? Pewne informacje, takie jak opatentowane rysunki, prototypy, wzory, nigdy nie tracą aktualności i mogą być przechowywane. Jeśli te i innego rodzaju dane muszą być zachowywane przez coraz dłuższe okresy, to jak zapewnić ich dostępność, gdy bieżąca technologia stanie się przestarzała i nie będzie można dłużej ponosić kosztów operacyjnych, by zachować zdezaktualizowane systemy tylko i wyłącznie w celu ich przywrócenia?

Jeśli przedsiębiorstwo nie zarządza odpowiednio cyklem życia informacji, przechowuje zbędne dane w przestarzałych systemach. W praktyce informacje o typach zarządzania są rzadko śledzone, co niepotrzebnie generuje koszty i potęguje ryzyko.

Zgodnie z ostatnim badaniem Enterprise Strategy Group (ESG) 82 procent przedsiębiorstw wciąż używa taśm do całościowego lub częściowego tworzenia kopii zapasowych w firmie. Raport stwierdza: „zmiana nastąpi, gdy więcej firm będzie używać dysków w procesach tworzenia kopii zapasowych lokalnie, jednak oczekuje się, że pojemność taśm będzie rosnąć". Mimo to coraz więcej firm chce właściwej ochrony, częściowo z powodu zwiększenia ilości kluczowych danych firmowych.

Zaprzestanie używania taśm jako ochrony nowo powstałych informacji jest odległe, mimo iż przewiduje się ich wycofanie. Ciągle pozostają one dominującym środkiem składowania informacji historycznych – szczególnie istotnych biznesowych wpisów, z których niektóre mogą być zobowiązujące, jeżeli kategoryzowane są jako regulujące lub dotyczące kwestii prawnych.

Problem dostępności danych

Organizacje rutynowo tworzą kopie zapasowe i przechowują informacje, gdyż wydaje im się, że wykonywane procesy archiwizacji danych są wystarczające, a dane są dzięki nim bezpieczne. Należy jednak pamiętać też o tym, że wiele czynników może utrudniać odzyskanie danych, a niektóre z nich nie są identyfikowalne, dopóki organizacja nie znajdzie się w czysto reaktywnym kryzysie, podczas którego rozpoczyna walkę w poszukiwaniu alternatywy. Firma ma obowiązek rozsądnie

chronić istotne dane z uwagi na wymogi prawne, niezależnie od kwestii technicznych. Co więcej, jest jasne, że zarządzanie danymi w sposób, który czyni to trudnym, jeśli nie niemożliwym, nie zwalnia firmy z obowiązku ich odzyskania. Niektóre organizacje mają nadzieję, że ich archiwa nie będą przeszkodą i będzie istniała możliwość ich wykorzystania, gdy tylko zajdzie taka potrzeba.

Przejdźmy do najbardziej powszechnych zagrożeń dostępu, które wymieniają specjaliści.

1) **Błędy oprogramowania archiwizującego dane** – dotyczą oprogramowania archiwującego dane, które jest skonfigurowane poprawnie. Proces przebiega sprawnie, jednak bieżące kopie zapasowe nie są weryfikowane.
2) **Błędy nośników do przechowywania danych** – to najczęściej błędy urządzeń do odczytywania taśm bądź błędy spowodowane uszkodzeniem taśmy. Zapisana na taśmie informacja nie może zostać odczytana z powodu błędów logicznych w zapisie. Istnieje znacząca różnica pomiędzy danymi z ostatniej kopii zapasowej a danymi z ostatniego miejsca, przy którego odczycie pojawia się błąd.
3) **Błędy człowieka** – to powszechne błędy, takie jak przypadkowe ponowne zainicjowanie taśmy lub nieaktywowanie dodatkowych opcji przed rozpoczęciem tworzenia kopii zapasowej.
4) **Objętość danych i ich dostępność** – dotyczy czystego wolumenu danych i zdolności do znalezienia określonej zawartości w korporacji. Jak dowiedzieć się, czy dane zostały utracone lub brakuje ich? Na przykład – kiedy firmy dokonują fuzji, dane operacyjne, księgowe i klienckie obu firm muszą zachować ciągłość, aby były dostępne. Zróżnicowane scenariusze tworzenia kopii zapasowych musza zostać zharmonizowane.
5) **Starzenie się systemów i nośników** – dotyczy potrzeby utrzymania ważnych danych, konwertowania starych, statycznych systemów do innego formatu lub nowszej technologii. Audytorzy mogą wnioskować o podporządkowanie starych wpisów danych (np. w przypadku jednego banku nastąpiło podporządkowanie 17 000 zestawów wpisów z lat 80. XX wieku; taśmy były dostępne, jednak oprogramowanie i napędy nie są już w powszechnym użyciu).
6) **Katastrofy naturalne** – szkody powstałe na skutek pożaru, działania wody, błota, bardzo niskich lub wysokich temperatur lub innych czynników naturalnych są często powodem skażenia taśm, ich uszkodzenia i tym samym braku możliwości odczytania ich w podstawowym zakresie.

Fot. 2. Specjalista Kroll Ontrack podczas odzyskiwania danych w laboratorium Kroll Ontrack

Cztery porady dotyczące zarządzania ustrukturyzowanym drzewem bazy informacji, gdy istnieje ryzyko związane z dostępnością danych

W szerszym kontekście procesu zarządzania długością życia informacji organizacje poszukują ekspertów w dziedzinie zarzą-

dzania danymi, aby pomogli im zarządzać przechowywanymi informacjami w sposób bardziej wydajny, pozwalający zredukować obciążenie załogi działu IT i infrastruktury. Jako część rozwiązania należy rozważyć poniższe porady.

Porada pierwsza: Zdefiniuj plan

Powodzenie planu projektu dotyczącego przekształcania przechowywanych danych zależy od zidentyfikowania i zrozumienia projektowanych możliwości i wyzwań. Dlatego też mogą one być planowane odpowiednio. Na przykład:

1) Jak wygląda struktura danych? Czy wszystkie dane przechowywane w systemach przechowywania danych i media zostały zidentyfikowane?
2) Czy firma posiada doświadczenie w dostarczaniu rozwiązań w otoczeniu zupełnie różnych systemów?
3) Jaki jest cel danego projektu i dostępny budżet?
4) Czy występują prawne lub kontrolne wymagania terminów?

Rejestrowanie rodzajów nośników i ich stanu jest tak ważne, jak określenie, który rodzaj nośnika jest najbardziej odpowiedni w danym przypadku. Nawet w przypadku pozornie nieodwracalnego uszkodzenia nośnika (spowodowanego np. działaniem wody lub ognia) można poddać nośnik procesowi odzyskiwania danych. Jest duża szansa na to, że uda się odzyskać dane. Zazwyczaj istnieje także możliwość zaaranżowania długookresowej polityki tworzenia kopii zapasowych. W przypadku uszkodzenia nośnika należy działać szybko, zanim nośniki rzeczywiście staną się całkowicie bezużyteczne, np. z powodu korozji. Jest to bardzo ważne. Jeśli przenoszone do nowych formatów lub na nowe nośniki dane nie mogą opuścić murów firmy, konwersja musi być przeprowadzona na miejscu lub też przestarzałe serwery muszą zostać przebudowane w taki sposób, aby poprzednie prawa dostępu mogły być w pełni odtworzone. Definiowanie projektu, jego zakresu oraz identyfikacja zasobów technicznych i ludzkich jest czynnością, której nie można pominąć lub wykonać jedynie częściowo.

Porada druga: Analiza danych

Firma powinna zidentyfikować zawartość nośników, aby w późniejszym czasie móc podejmować decyzje dotyczące zbierania, niszczenia i dopasowywania danych odczytywalnych w celu osiągnięcia zgodności z wymogami prawa. W zależności od potrzeb biznesowych, skanowanie, katalogowanie lub indeksowanie nośników może pomóc organizacji w skupieniu uwagi na istotnych nośnikach. Jednakże przeznaczone dla firm oprogramowanie do backupu jest stworzone do zarządzania dużymi ilościami danych, a nie w celu identyfikacji zapisanej zawartości. Jest ono kompleksowe i wymaga relacyjnej bazy danych, potrzebnej do zarządzania m.in. parametrami tworzenia kopii zapasowej, sesjami, zaplanowanymi zadaniami, błędami. Mimo iż oprogramowanie do tworzenia kopii zapasowej systematycznie śledzi to, co jest zapamiętywane,

Fot. 3. Eksperci odzyskiwania danych w laboratorium Kroll Ontrack

szczegółowe informacje o aktualnej zawartości kopii zapasowej mogą być trudne do uzyskania. Typowym przykładem jest przejęcie biznesu. W kilka lat po zakupie, podczas procesu sądowego i procesu wydobywania danych, wszystkie długoterminowe dane firmowe muszą zostać zbadane i wydobyte przez biegłego sądowego. Bez oryginalnego oprogramowania do tworzenia kopii zapasowej lub wyposażenia w określone urządzenie nagrywające identyfikacja zawartości może okazać się największą przeszkodą i jednym z najbardziej kosztownych elementów projektu.

Katalogowanie i indeksowanie mają różne znaczenia wśród dostawców nośników do tworzenia kopii zapasowych w długim terminie. Katalog długoterminowych kopii zapasowych zazwyczaj odnosi się do sesji tworzenia kopii zapasowych na zestawie nośników. Niektórzy dostawcy usług związanych z tworzeniem kopii zapasowych zapisują identyfikujące metadane na taśmie. Wzrasta jednak liczba dostawców oprogramowania do tworzenia kopii zapasowych, którzy umieszczają ID nośników, ID kopii zapasowej lub ID sesji na nośnikach, które są odniesieniem do oprogramowania relacyjnych baz danych. Ponadto kopie zapasowe sesji, które są linearne w swym zasięgu i w których dane są zapisane jednocześnie na nośniku, stają się rzadkie. By utrzymać w kopii zapasowej poziom operacji IOP (wejścia/wyjścia operacji na sekundę) i wydajności systemu, wiele platform tworzących kopie zapasowe stosuje tzw. zapis rozproszony i fragmentację danych. W tym przypadku wiele strumieni danych i procesów jest wykonywanych równolegle. Aby na nośniku można było zapisać wiele kopii zapasowych, oprogramowanie będzie przechowywać jedną sesję w określonym rozmiarze przestrzeni w MB lub GB, a następnie przełączy się na inny strumień tworzenia kopii zapasowej. Jedynym wyróżnikiem tego, co jest aktualnie zapisywane na nośniku, jest ID nośnika, ID kopii zapasowej lub ID sesji – relacyjna baza danych przechowuje resztę przypisanych metadanych. Dokonując odczytu zawartości taśmy, na której znajduje się kopia zapasowa, administrator może jednak stanąć w obliczu niejasnych informacji, które otrzyma, korzystając z linii poleceń komend. Różne znaczenia i terminologie mogą utrudnić oszacowanie zestawów nośników informacji lub kopii zapasowych. Dane wyjściowe z linii poleceń mogą zostać zinterpretowane jako „indeksowanie nośnika kopii zapasowej". Wtedy też wszystkie z zamontowanych nośników są wyświetlone, a ich status jest widoczny, jednak administratorowi bazy lub menedżerowi projektu konsolidacji nośników nie wyświetla się zawartość nośników. Firmy zajmujące się zarządzaniem danymi, które dostarczają usługi dostępu do danych, mogą zidentyfikować taśmy z sesjami i następnie dostarczyć raportowanie na wyższym poziomie, wskazując dokładną zawartość, która jest zapisana na długoterminowej kopii zapasowej. Indeksowanie może być dokonane poprzez bezpośredni odczyt taśmy. Nie jest konieczne posiadanie oprogramowania, które pierwotnie zostało użyte do stworzenia kopii zapasowej. Dzięki pracy poza warstwą oprogramowania tworzącego kopie zapasowe i zaufaniu do metadanych bazy danych zarządzanie danymi może dostarczyć firmie kompletnego spisu pozyskanych lub skompilowanych plików. Taki poziom szczegółowej analizy sprawi, że projekt konsolidacji danych zmieści się w zaplanowanym budżecie.

Porada trzecia: Zarządzanie i udoskonalanie danych

Organizacje regularnie tworzą kopie zapasowe – przyrostowe (codziennie/co tydzień) i pełne (na koniec miesiąca). Pomimo tego, że jest to powszechna praktyka branżowa, w rezultacie tworzy się wiele kopii tych samych danych. Bazując na poprzednich analizach i wiedzy przedsiębiorstwa o procedurach tworzenia kopii zapasowych, można nadal zbierać odpowiednie pakiety danych i – zakładając, że nie ma ograniczeń prawnych – wykasować duplikaty danych. Jeśli dane te muszą zostać utrzymane, kopie zapasowe mogą być skonsolidowane poprzez przeniesienie ich na taśmy o większej pojemności. Niepotrzebne pliki systemowe mogą także zostać usunięte.

Porada czwarta: Poddaj rewizji potrzeby konwersji danych oraz metody, które są wykorzystywane w celu ich przeprowadzenia

Definiując zasięg projektu, firma może mieć potrzebę konwersji danych i/lub ich przekształcenia. Istotne jest przy tym zrozumienie stopnia kompleksowości zaangażowania w celu utrzymania projektu w terminie i w ryzach budżetu.

Prosta konwersja

Niektóre z konwersji są proste i nie wymagają skomplikowanych działań. Należy do nich m.in. kopiowanie plików z jednej platformy komputerowej (tym samym są one odczytywalne na innej platformie). Inne konwersje mogą wymagać większej wiedzy technicznej. Chodzi tutaj na przykład o rozważenie różnic w wykazach cyfrowej zawartości pomiędzy wysokowydajnymi stacjami roboczymi, komputerami średniego szczebla i komputerami biurowymi. Komputery IBM i AS/400 używają kodu EBCDIC reprezentującego alfabet, podczas gdy w większości przypadków normą jest kod ASCII. Utrzymanie dostępności informacji w bazach danych wymaga ich konwersji z kodu EBCDIC na ASCII lub eksportu tychże informacji z bazy danych do zwykłych plików z rozszerzeniem .csv.

Kompleksowa konwersja i przekształcenie danych

Bardziej kompleksowa konwersja może polegać na przekształceniu pól w bazie danych. Na przykład przemysł kart płatniczych zgodnie wymaga ukrycia danych posiadacza karty w procesie przechowywania numerów kart kredytowych. W tym wypadku ekspert w dziedzinie zarządzania danych może rozszerzyć i wyciągnąć zawartość, znaleźć numery posiadacza karty i zastosować znaki maskujące (takie jak „X") na stosownych danych.

Paweł Odor

Autor jest głównym specjalistą polskiego oddziału Kroll Ontrack, największej na świecie firmy zajmującej się odzyskiwaniem i kasowaniem danych oraz informatyką śledczą.

Focus on the details.

GANZ PixelPro

computar
MFZ VARIFOCAL
Zdalne sterowanie obiektywu
(zoom & focus)

Prezentujemy nową serię kamer GANZ PixelPro H.264 zoptymalizowanych zgodnie ze standardem HD, o bogatej funkcjonalności i wysokiej jakości, oraz wyjątkowo korzystnej cenie.

- Dostępne rozdzielczości: VGA, 1.3MP oraz 2MP (HD)
- Day/Night z automatycznym filtrem IR-CUT
- Dual-Stream, czyli podwójny strumień video
- Wejście/Wyjście audio z dwukierunkową transmisją
- Zdalne sterowanie Zoom/Focus w modelach kopułkowych
- Przysłona typu P-IRIS z pełną kontrolą głębi ostrości
- Zasilanie 12VDC / 24VAC / PoE
- Obsługa kart Micro SD do rejestracji lokalnej
- Wejście/Wyjście alarmowe, powiadamianie mailowe
- Bufor pamięci do rejestracji pre/post-alarmu
- Zgodne ze standardem ONVIF

DEALERZY:

ATOM SERVICE SP. J.
Gdynia,
Tel. 509 949 649
Tel. 509 949 849

DTS-SYSTEM
Lublin, Tel. 81 748 93 33
Rzeszów, Tel. 17 852 04 27
Kraków, Tel. 12 614 51 27
Łódź, Tel. 42 212 25 01

EUROALARM
Bydgoszcz, Tel. 52 325 40 10
Toruń, Tel. 56 659 83 77
Koszalin, Tel. 94 345 83 30
Gorzów Wlkp, Tel. 95 729 83 37
Wrocław, Tel. 71 349 27 72

NEKMA
Łódź, Tel. 42 2565510
Częstochowa, Tel. 34 361 07 74
Sosnowiec, Tel. 32 263 44 55
Opole, Tel. 77 453 76 15

SAWEL
Rzeszów,
Tel. 17 857 80 60
Tel. 17 857 79 87

ONVIF – zgodne ze standardem ONVIF

VSoIP – kompatybilne z platformą VSOIP

ALNET – zgodne z oprogramowaniem ALNET

CBC Poland Sp. z o.o.

CBC (Poland) Sp. z o.o. ul. Krasińskiego 41A, 01-755 Warszawa, tel. 22 633 90 90, fax. 22 633 90 60, www: www.cbcpoland.pl

Demagnetyzacja danych

Tomasz Filipów

Coraz szybszy rozwój technologiczny spowodował konieczność bardzo częstej wymiany sprzętu IT. Sprzęt ten w postaci nośników danych, np. dysków twardych, kaset do napędów taśmowych (streamerów), pamięci flash, może zawierać kluczowe dla firmy informacje, które w przypadku dostania się w nieodpowiednie ręce mogą stanowić potencjalne zagrożenie dla przedsiębiorstwa bądź instytucji. To sprawia, że ochrona danych przed niepowołanym dostępem jest ważna jak nigdy wcześniej. Niestety w Polsce wiedza dotycząca ochrony danych cyfrowych jest obecnie bardzo znikoma. Firmy nie do końca zdają sobie sprawę z konsekwencji, jakie mogą ponieść z powodu niewłaściwego obchodzenia się z cyfrowymi dokumentami. Skuteczne niszczenie danych jest jednym z podstawowych warunków bezpieczeństwa każdej organizacji i jej klientów. Nieudane zniszczenie danych może negatywnie wpłynąć na wizerunek firmy, a nawet przysporzyć wielu problemów prawnych

W instytucjach i przedsiębiorstwach, w których zarządza się niejawnymi informacjami (takimi jak np. dane osobowe, numery kart kredytowych, numery kont, informacje o produktach, raporty sprzedaży itp.), może dojść do niekontrolowanego wycieku tych informacji. Instytucje, takie jak banki, firmy ubezpieczeniowe czy telekomunikacyjne, obarczone są obowiązkiem usuwania danych z urządzeń i nośników elektronicznych, które są przeznaczone do likwidacji, przekazania albo naprawy (reguluje to np. ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r.). Niestety, część z nich nie robi tego w sposób skuteczny, a to grozi nie tylko kosztami spowodowanymi utratą danych, ale również odpowiedzialnością karną. Dlaczego niektóre instytucje i firmy borykają się z problemami wycieku informacji poufnych? Przyczyna najczęściej tkwi w braku wiedzy dotyczącej zasad skutecznego kasowania poufnych danych.

Jak bezpowrotnie usunąć dane?

Skasowanie plików przez użytkownika nie oznacza, że dane zostały usunięte z nośnika (mimo, że już nie są one widoczne). Dobry informatyk jest w stanie odzyskać dane usunięte poleceniem „*delete*", nawet jeśli zostały one skasowane z pominięciem kosza. System operacyjny nie usuwa bowiem fizycznie plików z systemu plików, a jedynie informację o ich lokalizacji. Również formatowanie dysku twardego z poziomu BIOS-u (*low level formatting*) nie jest bezpiecznym rozwiązaniem – dane wciąż można odzyskać. Brak tej wiedzy powoduje, iż znaczna część instytucji sprzedaje bądź wyrzuca stare komputery wraz z dyskami twardymi, na których pozostają niezwykle ważne i poufne dane dotyczące funkcjonowania firmy czy też dane kontrahentów.

W zasadzie istnieją dwie metody skutecznego usuwania danych: **metoda programowa (tzw. miękka) oraz sprzętowa (twarda)**.

Pierwsza, niezwykle skuteczna metoda bezpiecznego usuwania danych z dysków twardych (2,5", 3,5", ATA, SATA, SCSI itp.) polega na kasowaniu informacji za pomocą specjalistycznego, certyfikowanego między innymi przez ABW czy CESG (brytyjski odpowiednik polskiego ABW) oprogramowania, które poprzez wielokrotne nadpisanie danych według jednego ze specjalnych algorytmów (np. algorytmu Petera Gutmanna) powoduje niemożność ich późniejszego odczytania, nawet w specjalnych laboratoriach odzyskiwania danych. Zaletą tego typu rozwiązania jest możliwość późniejszego wykorzystania nośników, z których usunięto dane, gdyż nie zostały one uszkodzone w sposób fizyczny. Wadą logicznego kasowania danych jest fakt, iż dane można usunąć jedynie z dysków sprawnych mechanicznie, a cały proces jest stosunkowo wolny oraz kosztowny.

Drugą metodą jest przeprowadzenie procesu demagnetyzacji z użyciem specjalistycznego sprzętu – **demagnetyzerów**. Znajduje ona zastosowanie w przypadku kasowania danych zarówno ze sprawnych, jak i z uszkodzonych taśm magnetycznych lub dysków. Jeśli nośnik został uszkodzony w macierzy dyskowej, laptopie czy standardowym komputerze, a producent dostarczył na wymianę nowy dysk, czy też wymieniamy nośnik na szybszy, o większej pojemności etc., możliwe jest przeprowadzenie demagnetyzacji w celu bezpowrotnego skasowania danych. Demagnetyzacja może być zastosowana także wtedy, gdy pragniemy pozbyć się niewykorzystywanych już nośników (np. chcemy wykorzystać nowszą technologię – np. wymienić kasety typu DDS czy LTO/Ultrium 1 na LTO/Ultrium 4) lub bezpowrotnie usunąć wiele dysków twardych z macierzy bądź standardowych komputerów. Zaletą tej technologii jest pewność, iż dane zostaną skutecznie wykasowane, a także szybkość i bezpieczeństwo całego procesu. Wadą jest niewątpliwie wysoka cena sprzętu odpowiedniej jakości, dlatego wielu klientów decyduje się na skorzystanie z usług wyspecjalizowanej firmy.

Na czym polega demagnetyzacja?

Demagnetyzacja polega na bezpowrotnym skasowaniu zapisanych informacji za pomocą urządzeń zwanych **demagnetyzerami** lub **degausserami**. Nośniki są poddawane działaniu silnego impulsu magnetycznego, który niszczy wszystkie zapisy dokonane w warstwie magnetycznej. Po przeprowadzeniu demagnetyzacji dane zostają bezpowrotnie utracone. Po procesie demagnetyzacji nośniki, takie jak dyski twarde 2,5"/3,5", kasety LTO, 3592, T10K, nie nadają się do ponownego wykorzystania ze względu na ścieżki servo, które zostają całkowicie wymazane. Niektóre nośniki taśmowe, zwłaszcza te starsze technologicznie, np. DLT, DDS, kasety audio i wideo (analogowe), odzyskują swe pierwotne właściwości magnetyczne, gdyż demagnetyzacja zmniejsza do zera tzw. pozostałość magnetyczną, a do tego nośniki te nie posiadają ścieżek servo. Dzięki tym właściwościom taśmy nadają się do dalszego użytkowania nawet po przeprowadzeniu procesu demagnetyzacji.

Wybór demagnetyzera

Nie każdy oferowany na rynku demagnetyzer efektywnie i bezpiecznie zniszczy dane zawarte na nośnikach. Aby skutecznie wykasować zapisane informacje, siła pola demagnetyzującego musi być około dwukrotnie większa niż koercyjność magnetyczna kasowanego nośnika. W najbardziej zawansowanych modelach siła pola magnetycznego wynosi w przybliżeniu nawet 20000 Gs. Zazwyczaj są to urządzenia w pełni automatyczne. Dzięki tak dużemu polu skasowanie danych zajmuje tylko kilka sekund. Modele ręczne charakteryzują się mniejszą siłą pola (od około 4000 Gs wzwyż), co istotnie wpływa na czas, jaki trzeba poświęcić na „wyczyszczenie" jednego nośnika. W tym przypadku usunięcie danych, np. z dysku twardego, zajmuje około dwóch minut, a do tego konieczny jest czynny udział osoby, która będzie przesuwała i obracała dysk po płycie demagnetyzera. Zarówno CPD (Centra Przetwarzania Danych), jak i inne instytucje potrzebują demagnetyzacji różnego rodzaju nośników, ale nie każde urządzenie jest uniwersalne. Na przykład do taśm VHS można używać demagnetyzerów ręcznych, których pole magnetyczne jest mniejsze, ale w zupełności wystarcza do pozbycia się danych. Jeśli istnieje potrzeba zdemagnetyzowania kilku tysięcy taśm w ciągu jednego dnia, najbardziej odpowiednie będzie urządzenie automatyczne, które pracuje w trybie ciągłym. Do niszczenia danych na nośnikach cyfrowych, a szczególnie na najnowszych dyskach twardych, potrzebne są silniejsze urządzenia, o wartościach generowanego pola powyżej 10000 Gs.

Wraz z różnicami w wydajności i skuteczności różne są też ceny urządzenia. Ostatnio na rynku pojawiły się również hybrydy urządzeń niszcząco-kasujących. Jedno urządzenie w pierwszej fazie procesu demagnetyzuje nośnik, a następnie zgniata go przy użyciu stalowego kolca. Potraktowanie nośnika w ten sposób daje podwójną pewność prawidłowo przeprowadzonego procesu.

Wybór odpowiedniego demagnetyzera powinien uwzględniać przede wszystkim częstotliwość oraz intensywność jego użytkowania oraz typy nośników, z których usuwane będą dane. Obecnie na polskim rynku dostępnych jest kilkanaście modeli w bardzo szerokim zakresie cenowym. Klient może więc kupić taki model, który będzie dla niego najbardziej odpowiedni. Z doświadczenia wiemy, że dużym powodzeniem cieszą się urządzenia do ręcznego kasowania danych, których największym atutem jest atrakcyjna cena, niestety kosztem wydajności czy pewności poprawności skasowania danych (w przypadku demagnetyzerów ręcznych cały proces musi być przeprowadzony zgodnie z zaleceniami producenta – w przeciwnym razie dane mogą pozostać nienaruszone).

Ponieważ zakup odpowiedniego sprzętu do demagnetyzacji jest stosunkowo dużą inwestycją, rozwiązaniem alternatywnym jest skorzystanie z profesjonalnej usługi kasowania danych z nośników, którą można zlecić firmie zewnętrznej. Należy zwrócić uwagę na kilka szczegółów, zanim podejmie się decyzję o powierzeniu takiej firmie najważniejszej rzeczy w każdej organizacji – danych. Należy sprawdzić, czy dana firma posiada stosowne kompetencje, certyfikaty (np. ISO), zatwierdzone procedury wewnętrzne, referencje klientów, specjalizacje w zakresie kasowania danych, odpowiednio przeszkolonych pracowników oraz odpowiedni sprzęt wykorzystywany do demagnetyzacji/kasowania. Jeśli firma przyjmująca zlecenie wykonania usługi kasowania danych zatrudnia pełnomocnika ds. ochrony informacji niejawnych, posiadającego dostęp do poufnych informacji niejawnych, jest to dodatkowym atutem. Dobrze jest również sprawdzić, czy dany usługodawca posiada ważne ubezpieczenie OC oraz czy może pochwalić się swoją rzetelnością oraz historią funkcjonowania na rynku.

Niektóre firmy oferują bardzo niskie ceny za usługę demagnetyzacji lub samej utylizacji nośników danych, które nie pokrywają nawet kosztów transportu tych nośników. Należy trzymać się z dala od takich firm – nośniki, na których w dalszym ciągu zapisane są informacje (narażone są zwłaszcza dyski twarde) mogą pojawić się w najmniej oczekiwanym momencie na rynku, nawet poza granicami Polski. Firmy takie nie zarabiają na samej usłudze, ale na dalszym odsprzedaniu nośników. Użytkownikowi nie może wystarczyć samo potwierdzenie odbioru nośników przez firmę świadczącą usługi, jeśli nie wie na pewno, co później stanie się z nimi. Każdy z etapów usługi powinien być odpowiednio udokumentowany, a klient musi mieć wgląd w cały proces i kontrolę nad nim w każdym jego momencie.

Z punktu widzenia dużych przedsiębiorstw jest to bardzo praktyczne. Skorzystanie z usług profesjonalnej firmy daje pełną gwarancję szybkiego oraz bezpiecznego przeprowadzenia całego procesu, a gdy u zamawiającego takie usługi przeprowadzany będzie audyt, poszczególne działy będą mogły przedstawić dokumentację wystawioną przez wykonawcę usługi, potwierdzającą skasowanie wszystkich danych oraz przekazanie starych, już bezużytecznych nośników do dalszej utylizacji.

Problem bezpieczeństwa cyfrowych danych jest analogiczny do problemu ochrony danych w formie fizycznej, czyli dokumentów papierowych. Pamiętamy afery sprzed kilku lat, gdy okazało się, że na śmietniku można znaleźć poufne informacje klientów banków, kartoteki medyczne szpitali etc. Wydarzenia te skłoniły do większej dbałości o bezpieczeństwo dokumentów w formie papierowej. Miejmy nadzieję, że podobne wydarzenia spowodują zwrócenie należytej uwagi również na problem bezpieczeństwa danych w formie cyfrowej, a firmy i instytucje będą dbać o to bezpieczeństwo w odpowiedni sposób.

Tomasz Filipów
DISKUS Polska

światło i dźwięk dla bezpieczeństwa

SO-Wd12

SG-Pgw

SO-Pd11

SA-K7

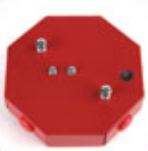
SGO-Pgz

WSD-1

PI-W6

PIP-2A

PIP-1A



W2 lider w produkcji sygnalizatorów do systemów sygnalizacji pożaru.

Dane adresowe:
W2 Włodzimierz Wyrzykowski
ul. Czajcza 6
86-005 Białe Błota
tel./fax (052) 584 01 92
tel. (052) 345 45 00
biuro@w2.com.pl

Specjalizujemy się w rozwiązaniach z zakresu elektroniki profesjonalnej. Zakres działalności firmy obejmuje projektowanie, produkcję oraz sprzedaż najwyższej jakości sygnalizatorów do systemów sygnalizacji pożaru i sygnalizacji włamania jak również osprzętu instalacyjnego.
Posiadamy certyfikaty zgodności EC oraz świadectwa dopuszczenia wydane przez CNBOP dla sygnalizatorów do systemów sygnalizacji pożaru. Jako jedyny producent w Polsce posiadamy orzeczenie i rekomendację techniczną CNBOP potwierdzającą odporność puszek instalacyjnych typu PIP na działanie wysokiej temperatury E90.

Więcej informacji na stronie **www.w2.com.pl**

Realne koszty systemu wykrywania pożaru (część II)

Grzegorz Ćwiek

W części I artykułu (*Zabezpieczenia Nr 4/2010*) opisaliśmy dwa przypadki, w których realny koszt systemu wykrywania pożaru w obiekcie miał szansę istotnie zmienić się w stosunku do tego, który został zaakceptowany przez inwestora na etapie zakupu. Należy jednak z całą stanowczością zaznaczyć, że owe dwa przypadki (dodatkowy koszt dostosowania systemu do zmieniających się przepisów prawnych oraz koszt readaptacji systemu we wstępnej fazie jego użytkowania) nie wyczerpują listy sytuacji, w których koszt systemu może wzrosnąć

Jak stwierdziliśmy poprzednio, dodatkowe i nieprzewidziane wcześniej nakłady są tym mniejsze, im lepiej rozwinięty i stabilny jest cały rynek bezpieczeństwa pożarowego, co objawiać się może przede wszystkim: lepszymi, stabilnymi przepisami i uwarunkowaniami prawnymi, większą niezależnością i jakością decyzji podejmowanych przez rzeczoznawców do spraw ochrony przeciwpożarowej, ale także większą wiedzą inwestorów oraz wysoką jakością usług świadczonych przez dostawców rozwiązań – z instalatorami tych systemów na czele.

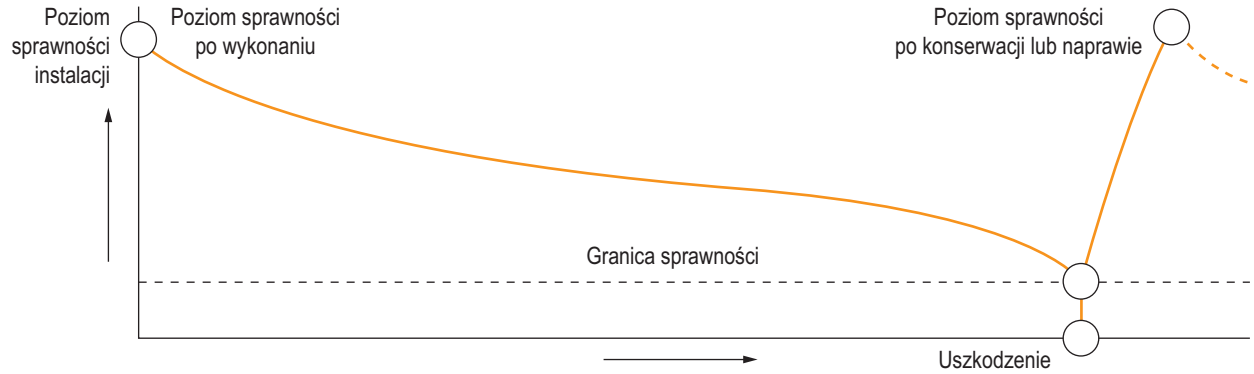
Obecnie w Polsce mamy do czynienia z rynkiem, który wprawdzie jest wysoko rozwinięty, ale dość niestabilny i pozostaje w fazie dostosowawczej (np. dostosowywania się do przepisów unijnych). Z drugiej strony, dostosowując przepisy i polskie normy na podstawie doświadczeń innych krajów, wykroczyliśmy poza przyjęte tam ramy, nadmiernie zaostrzając niektóre z nich. Na przykład wprowadziliśmy przepisy nakazujące stosowanie dźwiękowych systemów ostrzegawczych. Zdecydowanie można przyjąć, że obecność DSO w obiektach poprawia bezpieczeństwo przebywających tam osób, ale także – w sposób nieprzewidziany przez wielu właścicieli obiektów – istotnie zwiększa koszt systemu bezpieczeństwa pożarowego. Inwestorzy zagraniczni, planujący swoje inwestycje z kilkuletnim wyprzedzeniem, nie mogli przewidzieć takiej sytuacji, a zaburzenie cyklu inwestycyjnego z tego powodu kosztowało ich w rezultacie znacznie więcej. W ocenie kosztów bierze się bowiem pod uwagę nie tylko sam koszt urządzeń i ich montażu, ale także koszt dokonania zmian projektowych, czasem zmian w architekturze lub sposobie wyposażenia wnętrz (ze względu na właściwości akustyczne pomieszczeń), koszt wynikający z opóźnienia oddania obiektu do użytkowania w związku z dostosowywaniem go do nowych przepisów, wreszcie – zmieniające się koszty eksploatacji budynku, i to w długim okresie.

Z drugim przypadkiem (opisanym w pierwszej części artykułu), a więc z kosztem readaptacji systemu w początkowej fazie jego użytkowania, wiąże się kolejny czynnik mający istotny wpływ na realny koszt systemu bezpieczeństwa przeciwpożarowego. Czynnikiem tym jest dodatkowy koszt rozbudowy systemu podczas prowadzenia prac aranżacyjnych w budynku.

O ile zwykle jest on uwzględniony w kalkulacji inwestora i zazwyczaj ponoszony jest przez najemców powierzchni aranżowanych, możemy natknąć się na cały szereg wydatków nieprzewidzianych. Procedury przetargowe zwykle uwzględniają założenia dotyczące funkcjonowania systemu „teraz" i rzadko zdarza się, by wymuszały na oferentach skrupulatne i rzetelne skalkulowanie zapasów sprzętowych oraz instalacyjnych na potrzeby przyszłych aranżacji. Dzieje się tak z dwóch powodów. Po pierwsze – projekty i założenia przetargowe niestety rzadko charakteryzują się dobrą jakością. Robione w pośpiechu, przy braku skłonności projektantów do wzięcia na siebie odpowiedzialności za podejmowane decyzje i słabej koordynacji międzybranżowej po prostu nie są w stanie uwzględnić części założeń. Po drugie – często inwestorom brakuje wiedzy dotyczącej ostatecznego kształtu i zakresu możliwych aranżacji. Jeśli dodamy do tego chęć zrobienia wszystkiego najmniejszym kosztem, przyszła potrzeba zmiany aranżacji napotka na techniczne ograniczenia systemu lub infrastruktury budynku. W pierwotnej fazie instalacji, często nie przewiduje się dostatecznej nadmiarowości systemu, umożliwiającej np. odpowiednie zabezpieczenie powierzchni nowo wydzielonych z większych obszarów lub pomieszczeń o zmienionym przeznaczeniu. Najczęściej brakuje odpowiednich zapasów okablowania, miejsca na nowe okablowanie w korytach lub szachtach, często także odpowiedniej przestrzeni logicznej w systemach. Jeżeli etap projektowania oraz późniejszy etap wykonania podstawowej instalacji systemu bezpieczeństwa nie zakładały, jak wspomnieliśmy wyżej, jego nadmiarowości, koszty wzrosną lawinowo. Czasem konieczne jest np. zainstalowanie nowego systemu, którego zadaniem jest nadzorowanie tylko nowo wydzielonej powierzchni. Jest to niekorzystne nie tylko z punktu widzenia sztuki inżynierskiej, ale przede wszystkim finansowo.

Należy przy tym pamiętać, że w przypadku modyfikacji w obiekcie mamy do czynienia z czymś w rodzaju zespołu naczyń połączonych. Istotna zmiana aranżacji lub przeznaczenia pomieszczeń skutkuje koniecznością poprawienia funkcjonalności systemu SAP i powoduje konieczność zwiększenia użyteczności systemu DSO, a to z kolei stwarza potrzebę rozszerzenia funkcjonalności systemu kontroli dostępu, telewizji dozorowej, a nawet systemu BMS.

Kolejną ważną kwestią jest koszt samego utrzymania systemu wykrywania pożaru i wszystkich związanych z nim systemów zewnętrznych. Celem dokonywania na bieżąco konserwacji systemu jest utrzymanie ciągłości jego działania, a więc – tym samym – utrzymanie ciągłości funkcjonowania budynku i przedsięwzięć organizowanych w jego obrębie i nie tylko. Ta ważna cecha systemu bezpieczeństwa, jaką jest ciągłość jego działania, jest bardzo często pomijana w analizach kosztu zakupu systemu. Bardzo często kupuje się tani system, nie uwzględniając rzeczywistych wydatków związanych z jego utrzymaniem w przyszłości. To bardzo stary trik oferentów i bardzo duży problem dla nabywcy w przyszłości. Przed podjęciem decyzji o zakupie danego typu systemu należy koniecznie pozyskać informację o kosztach jego eksploatacji i serwisu, dostępności wykwalifikowanych i autoryzowanych ekip serwisowych oraz części zamiennych, a także o możliwym czasie reakcji na usterki. Sama obecność systemu wykrywania w obiekcie nie gwarantuje jego bezpieczeństwa. System ten musi działać prawidłowo, a w razie awarii – być łatwy do naprawy. Należy wybierać producentów sprzętu uznanych i sprawdzonych marek, o dobrych referencjach. Jak już wcześniej wspomnieliśmy, bardzo ważna jest dostępność specjalistów-serwisantów, posiadających odpowiednie narzędzia, często „aktualizowaną" wiedzę oraz udokumentowane doświadczenie. Praktyka polska pokazuje działania odmienne do tego, co powszechnie stosowane jest w krajach Europy Zachodniej. Przeciętny koszt konserwacji i serwisu urządzeń w Polsce jest kilkanaście razy niższy w porównaniu do kosztów w Niemczech, Austrii, Francji czy Skandynawii. Nawet nasi południowi sąsiedzi – Czesi i Węgrzy – wyceniają wartość prawidłowej konserwacji urządzeń znacznie wyżej niż my.



Rys. 1. Degradacja techniczna systemu SAP w czasie oraz wpływ napraw i konserwacji na jego stan

Dlaczego? Chyba lepiej niż my zdają sobie sprawę z faktu, że pozostawione bez opieki i kontroli urządzenia elektrotechniczne – nawet te najlepsze – z biegiem czasu stają się coraz mniej skuteczne i użyteczne. Degradacja techniczna urządzeń jest nieunikniona, a jedynie prawidłowa konserwacja jest w stanie zapewnić sprawność instalacji na długo. Producenci tworzą urządzenia, których okres działania to 10–15 lat, przy czym w przypadku sprzętu profesjonalnego okres ten może wydłużyć się nawet dwukrotnie. Realny koszt systemu zabezpieczeń będzie zatem w długim okresie tym niższy, im rzadziej będziemy doprowadzać do obniżenia jego sprawności. Wbrew pozorom wydatki na konserwację – choć mogą wydawać się duże – w długim okresie są zawsze mniejsze niż koszty wykonania napraw i koszty związane z przestojem linii produkcyjnych lub wstrzymaniem pozwolenia na użytkowanie obiektu przez służby techniczne lub Państwową Straż Pożarną. Nie bez znaczenia jest opinia ubezpieczyciela, który – w przypadku stwierdzenia niesprawności systemu zabezpieczeń – ma prawo wstrzymać wypłatę odszkodowania lub nawet nałożyć kary i dodatkowe opłaty za niewłaściwy stan tego systemu.

Najlepsi producenci systemów bezpieczeństwa pożarowego już teraz udostępniają użytkownikom szereg narzędzi pozwalających obniżyć koszt użytkowania tych systemów. Stosuje się zaawansowane systemy o budowie modułowej. Wymiana ich podzespołów jest niezwykle łatwa i szybka. Stosuje się rozwiązania programistyczne, takie jak aplikacje zdalnego dostępu i raportowania, w celu ułatwienia diagnostyki, przyspieszenia procesów naprawy i sprawdzenia poprawności działania urządzeń. Wykorzystuje się zaawansowane narzędzia diagnostyczno-serwisowe, które umożliwiają błyskawiczną ocenę stanu instalacji. W najlepszych rozwiązaniach stosuje się układy redundantne, niezwykle odporne na wszelkie zakłócenia i zmiany środowiskowe oraz uszkodzenia. Dzięki temu systemy te pozostają sprawne nawet w przypadku wykrycia poważnych usterek w układach podstawowych, gdyż mogą pracować, wykorzystując zapasowy zestaw elementów hardware'u i software'u.

Ostatnim czynnikiem wpływającym na realny koszt systemu wykrywania pożaru (ostatnim, na jaki autor chciałby zwrócić uwagę w niniejszym artykule) jest koszt jego demontażu i utylizacji po wielu latach użytkowania. W fazie podejmowania decyzji dotyczących zakupu sprzętu koszt ten jest zwykle pomijany przez inwestorów, których zamiarem jest późniejsza odsprzedaż gotowego budynku. Jest on jednak niezwykle istotny, szczególnie dla tych, którzy zamierzają opiekować się obiektem przez wiele lat. Należy wziąć pod uwagę koszt demontażu i utylizacji zużytych elementów elektronicznych oraz elementów niebezpiecznych, takich jak czujki izotopowe. Od końca lat dziewięćdziesiątych odchodzi się od systemów bazujących na elementach radioaktywnych, ale nadal niektórzy producenci – w ramach oczyszczania magazynów – proponują użytkownikom urządzenia tego typu w atrakcyjnej cenie. Co się z tym wiąże? O ile koszt demontażu i utylizacji zwykłych elementów elektronicznych nie musi być nadmiernie wysoki i nie zależy od marki czy producenta urządzeń utylizowanych (przyjmijmy, że jest taki sam dla wszystkich systemów), w przypadku systemów wykorzystujących czujki izotopowe może stanowić równowartość nowego systemu najnowszej generacji. O problemie tym wiedzą już niemal wszyscy, którzy nieopatrznie dokonali takich zakupów w ostatnich latach, a także ci, którzy kiedyś nie mieli wyjścia, bo innych systemów na rynku polskim po prostu nie było. Zarówno sam demontaż takich elementów, jak i ich składowanie oraz ostateczna utylizacja musi odbywać się według ściśle określonych reguł i norm oraz wyłącznie z udziałem wyspecjalizowanych przedsiębiorstw i instytucji (Państwowej Agencji Atomistyki).

Obecnie inwestor podejmujący decyzję o zakupie systemu, w którego skład wchodzą wyżej opisane elementy, musi założyć, że za kilkanaście lat będzie zmuszony jeszcze raz zapłacić niemal identyczną (jeśli nie większą) kwotę za pozbycie się swojego problemu.

Opisanie w niniejszym cyklu czterech czynników mogących istotnie wpłynąć na realny koszt instalacji systemu bezpieczeństwa jedynie wprowadza w problematykę, która wymaga znacznie głębszej analizy. Uogólniając powyższe rozważania, można stwierdzić, że koszty systemów bezpieczeństwa rosną w sposób nieprzewidziany i odwrotnie proporcjonalnie do rzetelności podmiotów uczestniczących w każdym etapie ich wdrożenia. Im niższa jest jakość stanowionego prawa, decyzji podejmowanych przez każdego z osobna i przez wszystkich uczestników rynku łącznie, wykonanej pracy czy produktów, tym wyższe są realne koszty instalacji – niezależnie od kosztu początkowego.

Grzegorz Ćwiek

POLVISION

Dostawca systemów nadzoru wizyjnego

ul. Witkowska 16, 51-003 Wrocław, tel. 71 327 45 94, tel. kom. 503 081 146

KAMERY MEGAPIKSELOWE H.264

połączenie wysokiej jakości obrazu HD z niskim wykorzystaniem pasma

rozdzielczości 1.3 MPIX @ 30fps, 2 MPIX @ 30fps, 3 MPIX @ 20fps

czułość w trybie nocnym od 0.04 do 0.1 Lux @ F1.2

mechaniczny filtr podczerwieni

zapis nagrań na kartach SDHC

wyjście analogowe BNC

zasilanie Power Over Ethernet

ceny detaliczne od 1100 zł do 2500 zł

bezpłatne oprogramowanie 32-kanałowe GV-NVR !!!

www.polvision.pl

OBSŁUGA 600 KAMER IP ONVIF PSIA

oprogramowanie w języku polskim

system operacyjny w pamięci typu Flash

32 kanały analogowe i sieciowe od 0.3 do 8 MPix

8 dysków 2TB w kieszeniach hot-swap

obsługa macierzy dyskowych

programowalny backup nagrań w sieci

inteligentna analiza obrazu,
m.in. śledzenie i zliczanie obiektów,
wykrywanie twarzy, identyfikacja tablic

integracja z systemami fiskalnymi, kontrolą dostępu itp.

sterowanie pilotem, 8 klawiaturami i joystickami

obsługa do 8 monitorów wysokiej rozdzielczości
VGA, DVI lub HDMI, spotowych i alarmowych

obsługa wolnych i przeciążonych łącz

otwarta architektura AVI, MDB, SDK

REJESTRATORY HYBRYDOWE I SIECIOWE STACJE MONITOROWANIA

centralne przechowywanie kont i uprawnień w sieci rejestratorów

Innowacyjne czujki z technologią Dual Ray

Krzysztof Kostecki

Techniczne Systemy Sygnalizacji Pożarowej chronią życie, zdrowie i mienie, dlatego muszą spełniać najbardziej surowe wymagania dotyczące niezawodności i jakości. Od producentów wymaga się produktów, które będą skracały czas detekcji pożaru, a przy tym nie będą generowały fałszywych alarmów. Pierwszym elementem odpowiedzialnym za spełnienie tych wymagań są czujki pożarowe

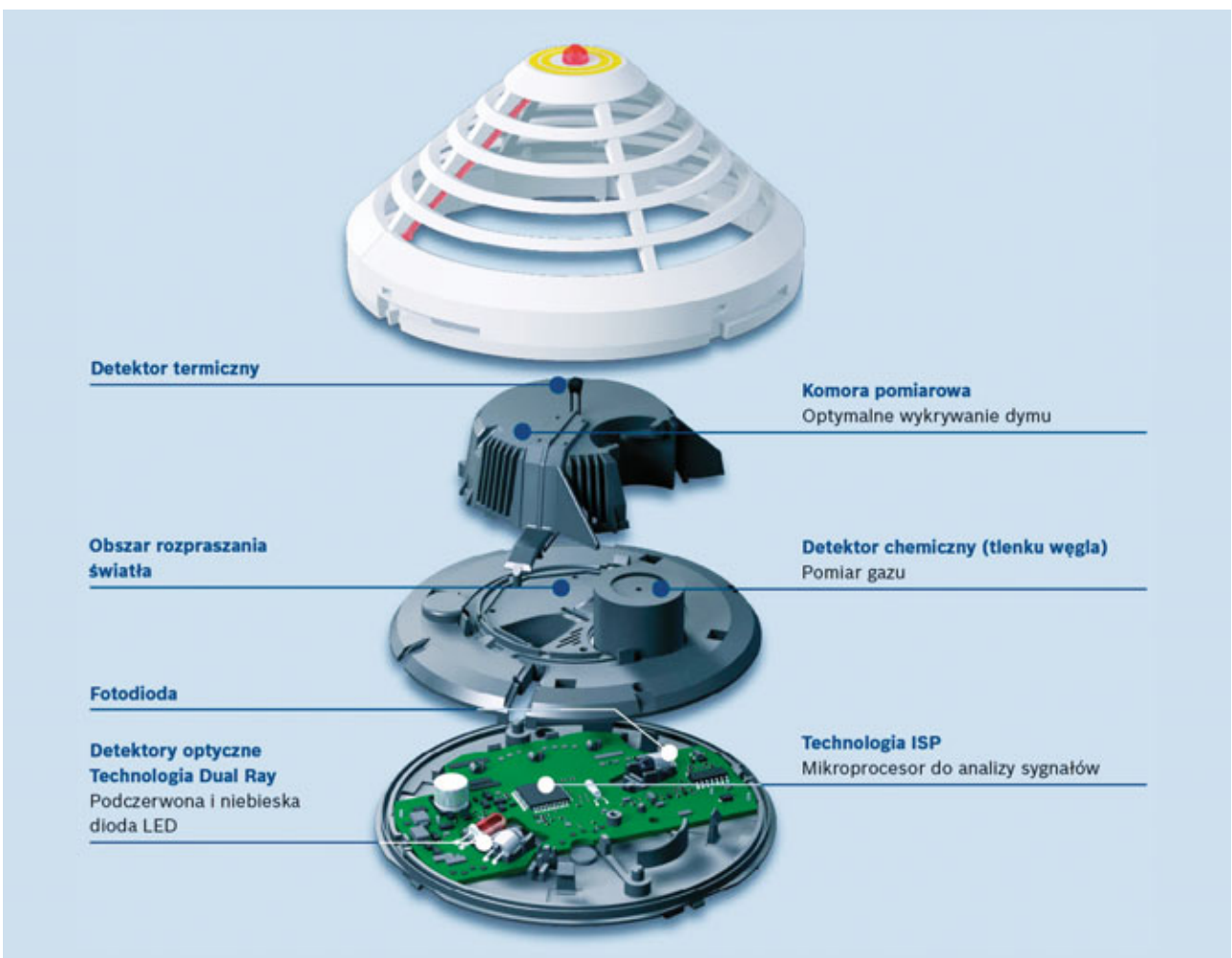
Czujka optyczna jest najbardziej popularnym elementem detekcyjnym, jednak posiada pewne ograniczenia. Wykrywa wyłącznie pożary bezpłomieniowe. Producenci prześcigają się w zwiększaniu funkcjonalności czujek. Oprócz standardowych czujek optycznych oferują różne czujki optyczno-termiczne. Dzięki nim można wykrywać pożary zarówno płomieniowe (TF1), jak i bezpłomieniowe. Niestety takie rozwiązanie wiąże się z wyższymi kosztami. Dlatego firma Bosch, wychodząc naprzeciw oczekiwaniom rynku, wprowadza do oferty czujki z technologią Dual Ray, dzięki której czujka wykrywa pożary bezpłomieniowe jak i płomieniowe w zakresie TF1–TF6, a ponadto TF8.

Cała seria nowych czujek pożarowych 420 firmy Bosch zapewnia jeszcze szybszą detekcję pożaru niż dotychczas, jednocześnie gwarantując redukcję występowania fałszywych alarmów, na przykład wywoływanych przez dym papierosowy, zapylenie, parę wodną.

Oferta Bosch obejmuje różne modele automatycznych czujek pożarowych, które można dostosować do indywidualnych potrzeb i które zapewniają inteligentne wykrywanie i najwyższy stopień ochrony. Rodzina automatycznych czujek serii 420, wykorzystująca technologię inteligentnego przetwarzania sygnału (ISP), została w tym roku powiększona o trzy nowe modele, które stosują technologię Dual Ray. Dzięki temu mamy do wyboru aż siedem modeli detektorów.

Technologia Dual Ray

Technologia Dual Ray działa w oparciu o rozpraszanie światła emitowanego przez dwie diody LED – jedną z zakresu podczerwieni, a drugą z zakresu światła niebieskiego. Gwarantuje to precyzyjne rozpoznanie wielkości cząsteczek oraz gęstość dymu. Dzięki temu oprócz pożarów tlących czujka optyczna może wykrywać również pożary płomieniowe, które emitują gazy spalinowe o bardzo małych cząsteczkach.



Fort. 1. Nowe modele czujek, FAP-D0420, FAP-DOT420 i FAP-DOTC420, oferują technologię Dual Ray wykorzystującą dwa tory optyczne – podczerwień i tor niebieski

Idea wykorzystania dodatkowej diody została oparta na podstawowych zjawiskach fizycznych, a dokładnie na teorii rozproszenia Mie. W 1908 r. niemiecki fizyk Gustaw Mie wyjaśnił, że stopień rozproszenia światła zależy od stosunku wielkości rozpraszających cząsteczek aerozolu do długości fali padającego światła.

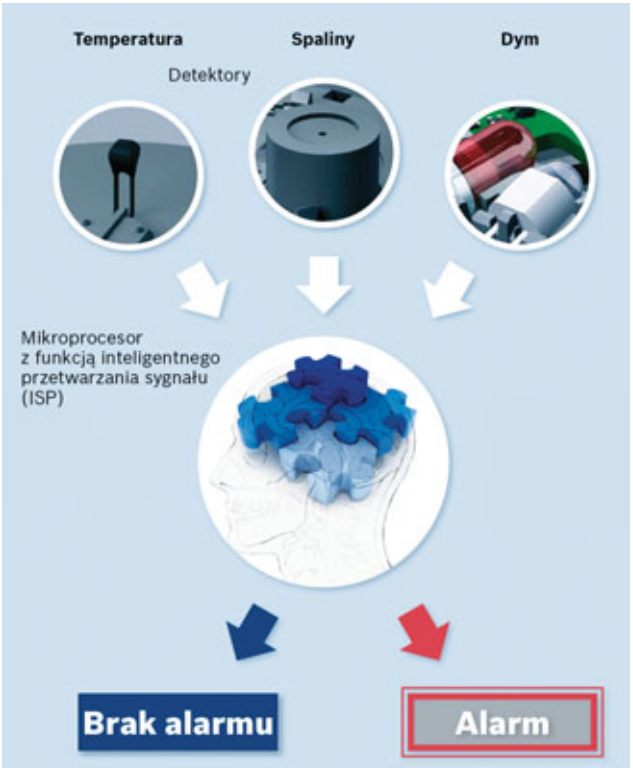
Na rynku można spotkać wiele rozwiązań, które, mając na celu jak najlepszą detekcję pożarów, wykorzystują dwie diody wyłącznie z zakresu podczerwieni lub tylko diodę niebieską. Mierzą one różne kąty załamania, ale muszą być dodatkowo wsparte detektorem termicznym, ponieważ dopiero taka kombinacja umożliwia skuteczne wykrycie pożarów płomieniowych i bezpłomieniowych.

Czujki wyposażone w technologię Dual Ray wykrywają najmniejsze cząsteczki dymu i eliminują fałszywe alarmy.

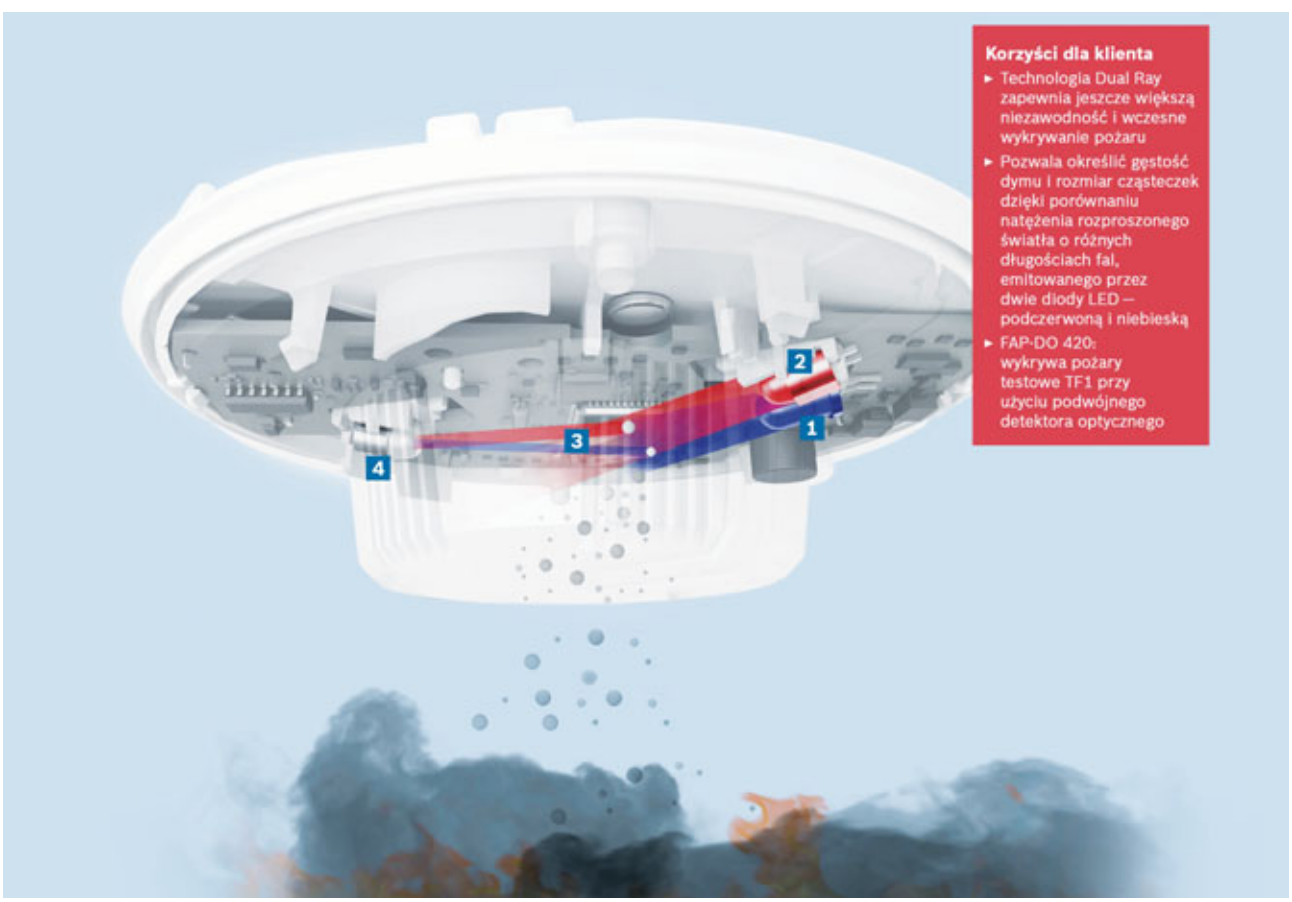
Zasada działania pozostała taka sama, czyli w razie pożaru unoszący się dym przedostaje się do komory pomiarowej, w której badane jest rozproszenie światła. Dwie długości fal emitowanych przez dwie diody LED pozwalają wykryć dym w szerokim zakresie wielkości jego cząsteczek.

Wszystkie trzy nowe modele umożliwiają wykrywanie pożarów testowych TF1. Technologia Dual Ray gwarantuje wiele korzyści inwestorom, instalatorom i konserwatorom:

– umożliwia wczesne i wiarygodne wykrycie pożaru, nawet dymu o najmniejszych cząstkach, powstających w wyniku pożarów płomieniowych,
– redukuje fałszywe alarmy dzięki wiarygodnemu odróżnieniu pożaru od innych zakłóceń,
– czujka optyczna Dual Ray (FAP-DO 420) jest po prostu tańsza od czujek multisensorowych.



Fot. 3. Rozpoznanie kombinacji dymów, gazów spalinowych i temperatury umożliwia identyfikację pożaru. ***Sposób działania funkcji ISP:*** *Sygnały z czujników są analizowane i łączone, a następnie przetwarzane przy użyciu technologii ISP i unikalnego algorytmu. Sam algorytm opiera się na regułach stworzonych w oparciu o doświadczenia z 5000 schematów powstawania pożaru.*



Fot. 2. Sposób działania czujki Dual Ray, gdzie: 1 – LED niebieska 2 – LED podczerwieni 3 – światło rozproszone 4 – fotodioda

Inteligentna Analiza Sygnału ISP

Wszystkie automatyczne czujki serii 420 zostały wyposażone w ISP (ang. *Intelligent Signal Processing*), czyli funkcję inteligentnej analizy zebranych informacji, na podstawie której czujka podejmuje decyzję o wywołaniu alarmu. Technologia ISP przetwarza wstępnie wszystkie sygnały z detektorów za pomocą odrębnego, wewnętrznego układu elektronicznego. Analizuje je i łączy we wbudowanym mikroprocesorze. Algorytm ISP wykorzystuje schematy wzorcowe, wpisane do pamięci czujki, uzyskane w wyniku doświadczeń i badań 5000 przykładowych charakterystyk powstawania pożarów. W praktyce czujka porównuje schematy wzorcowe z aktualnym pomiarem.

Alarm zostanie wywołany jedynie w sytuacji, gdy kombinacje przetworzonych sygnałów prawdziwego pożaru będą odpowiadać wartościom wzorcowym.

Takie rozwiązanie umożliwia:

– najwyższy poziom inteligentnego wykrywania pożarów,
– najlepsze w swojej klasie rozróżnienie pomiędzy realnymi pożarami a zakłóceniami, takimi jak dym papierosowy, kurz czy para wodna,
– odporność na fałszywe alarmy.

Nowe czujki, wyposażone w technologię Dual Ray oraz przetwarzanie ISP, wyznaczają nowe trendy rozwoju systemów wykrywania i sygnalizacji pożaru.

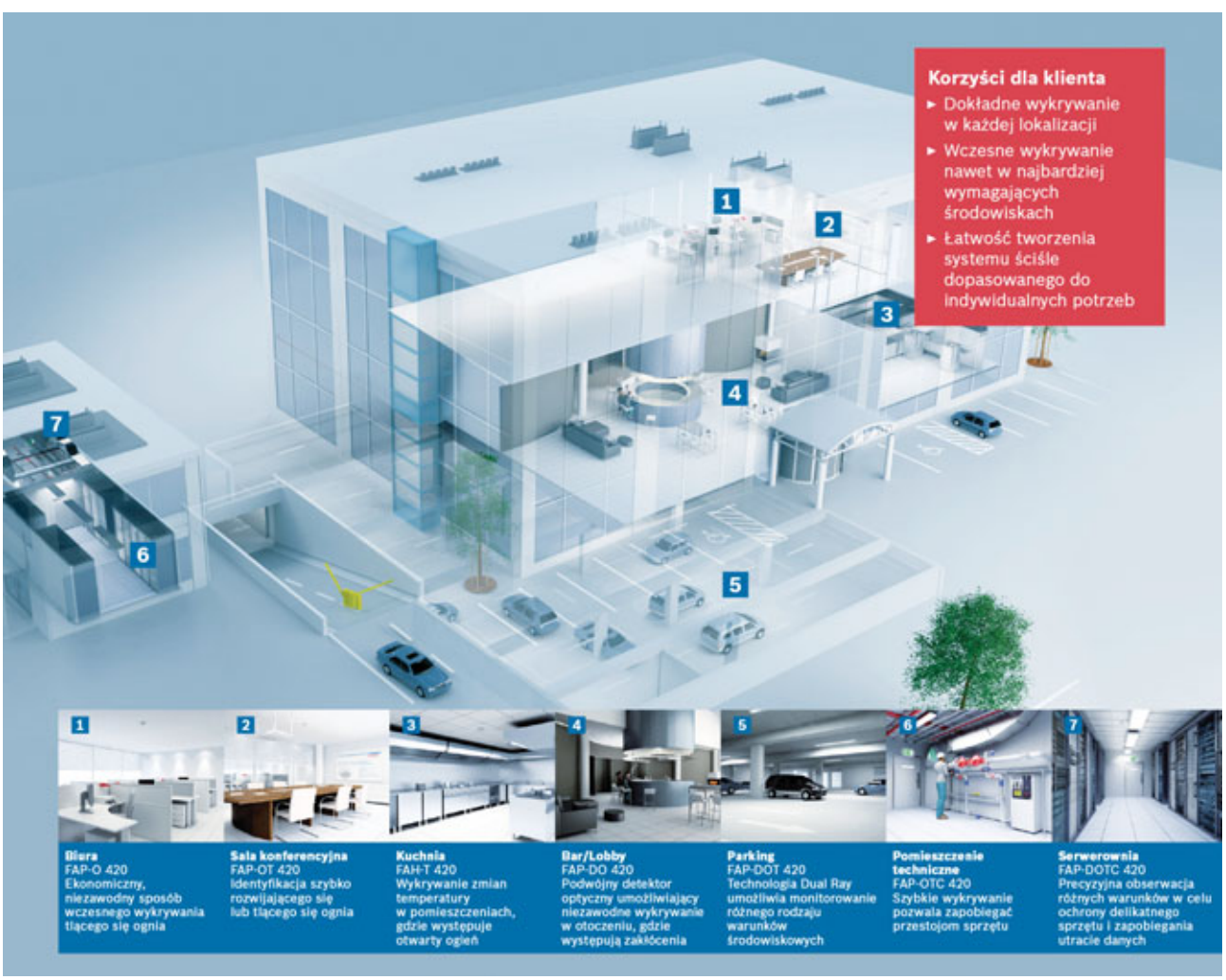
Zastosowanie

Duży wybór modeli pozwala na idealne dopasowanie czujki do wymagań i oczekiwań klienta. Spośród siedmiu modeli projektanci mogą wybrać ten, który jest najwłaściwszy ze względu na oczekiwany rodzaj zagrożenia. Duży wybór może jednak sprawić, że wiele osób będzie wahać się, nie wiedząc, jaką czujkę zastosować. Dlatego poniżej podajemy przykłady zastosowania czujek w zależności od miejsca instalacji (fot. 4).

W ofercie firmy Bosch można znaleźć dwa modele zwykłych czujek optycznych – czujkę klasyczną FAP-O420 oraz czujkę z technologią Dual Ray (FAP-DO420).

Klasyczną czujkę optyczną należy stosować w miejscach, w których spodziewamy się tlących pożarów bezpłomieniowych. W miejscach, gdzie może pojawić się pożar bezpłomieniowy i płomieniowy, warto zainstalować czujkę z technologią Dual Ray.

Czujki optyczno-termiczne stosujemy w miejscach, w których może wystąpić otwarty i szybko rozwijający się ogień, ale również tam, gdzie można spodziewać się pożarów bezpłomieniowych. Model FAP-DO420, wzbogacony o Dual Ray, lepiej poradzi sobie w zmiennych warunkach otoczenia, nie generując fałszywych alarmów praktycznie w żadnym środowisku.



Fot. 4. Przykłady zastosowań czujek serii 420

Tab. 1. Pełna oferta automatycznych czujek Bosch wraz z testowymi pożarami

		Kolor okręgu	Inteligenta analiza sygnału (ISP)	TF1: pożar płomieniowy celulozy (drewno bukowe)	TF2: pyroliza (rozkład termiczny) drewna	TF3: tlenie bawełny	TF4: pożar płomieniowy pianki poliuretanowej	TF5: pożar płomieniowy n-heptanu	TF6: pożar płomieniowy spirytusu	TF8: pożar dekaliny z czarnym dymem o niskiej temperaturze
FAH-T 420	**Czujka termiczna**	1 × czerwony	TAK	(+)			+	+	+	
FAP-O 420	**Optyczna czujka dymu**	bez okręgu	TAK		+	+	+	+		+
FAP-DO420	**Podwójna optyczna czujka dymu**	2 × szary	TAK	+	+	+	+	+		+
FAP-OT 420	**Multisensorowa czujka Optyczna/Termiczna**	1 × czarny	TAK	+	+	+	+	+	+	+
FAP-DOT420	**Multisensorowa czujka podwójna Optyczna/Termiczna**	2 × czarny	TAK	+	+	+	+	+	+	+
FAP-OTC 420	**Multisensorowa czujka Optyczna/Termiczna/Chemiczna**	1 × żółty	TAK	+	+	+	+	+	+	+
FAP-DOTC420	**Multisensorowa czujka podwójna Optyczna/Termiczna/Chemiczna**	2 × żółty	TAK	+	+	+	+	+	+	+

Czujki wyposażone w dodatkowe sensory, takie jak termiczny i chemiczny, mają wpływ na precyzyjniejsze i szybsze rozpoznanie różnych typów pożarów. Czujki FAP-OTC420 oraz FAP-DOTC-420 stosujemy w miejscach, w których natychmiastowa i precyzyjna detekcja, bez fałszywych alarmów, jest szczególnie pożądana.

Rodzina czujek serii 420

Nowe modele mają wszystkie dotychczasowe cechy czujek serii 420. Czujki są kompatybilne z dostępnymi na rynku centralami FPA 5000 oraz FPA 1200, instaluje się je na pętlach dozorowych LSN; wyposażono je również w obustronne izolatory zwarć.

W nowych modelach czujek można zastosować wszystkie gniazda instalacyjne oraz akcesoria, np. dodatkową pokrywę zabezpieczającą lub element grzewczy w podstawach (ochrona przed skraplaniem się pary wodnej w czujkach).

Nowość – FAP-DO420

FAP-DO420 to nowa czujka dymu, która umożliwia precyzyjne wykrywanie pożarów bezpłomieniowych i płomieniowych dzięki podwójnemu detektorowi dymu.

Nowość – FAP-DOT420

FAP-DOT420 to wielosensorowa czujka optyczno-termiczna. Zapewnia wykrywanie pożaru z zastosowaniem technologii Dual Ray oraz dodatkowego sensora termicznego.

Nowość – FAP-DOTC420

FAP-DOTC420 to wielosensorowa czujka optyczno-termiczno-chemiczna. Zapewnia wykrywanie pożaru z zastosowaniem technologii Dual Ray oraz dodatkowych detektorów – termicznego i chemicznego.

Od sierpnia 2010 roku Bosch oferuje aż siedem różnych modeli.

Wszystkie czujki posiadają umieszczoną centralnie diodę LED, dzięki której z każdego miejsca widać, która czujka aktywowała alarm. Zachowano wzornictwo charakterystyczne dla całej serii czujek. Oznaczenie kolorowymi okręgami na obudowie w prosty sposób identyfikuje zainstalowany model. Nowe czujki z technologią Dual Ray są oznaczone dwoma okręgami. Na przykład FAP-DO420, czyli optyczna czujka z technologią Dual Ray, została oznaczona podwójnym szarym okręgiem.

Instalatorzy i konserwatorzy doceniają również bardzo wygodną konserwację. Po wykręceniu czujki z podstawy wystarczy odgiąć gumowy element i wyczyścić czujkę sprężonym powietrzem. Taka konserwacja jest łatwa, szybka i nie wymaga ponownej kalibracji czujki.

Podsumowanie

Rodzina automatycznych czujek pożarowych serii 420 obejmuje urządzenia do wykrywania każdego rodzaju pożaru, które mogą mieć wiele różnych zastosowań. Klienci znajdą idealne rozwiązanie, dopasowane do warunków panujących w dowolnym środowisku. Innowacyjna technologia oraz dostępność aż siedmiu różnych wariantów detektorów sprawia, że czujki serii 420 już dziś spełniają przyszłe wymogi bezpieczeństwa, wyznaczając nowy standard w branży systemów sygnalizacji pożarów. Nowe czujki pożarowe marki Bosch z innowacyjną technologią Dual Ray i przetwarzaniem ISP są niezwykle atrakcyjnymi urządzeniami skierowanymi na rynek systemów pożarowych.

Krzysztof Kostecki
Bosch Security Systems

POLSKA IZBA OCHRONY

BIULETYN INFORMACYJNY

BIULETYN JEST:

uznawaną pozycją w branży

wysyłany systematycznie do przedsiębiorców działających w obszarze ochrony z całego kraju

adresowany do organów administracji państwowej we wszystkich województwach

propagowany podczas branżowych targów i wystaw na terenie kraju i za granicą (szczególnie Czechy, Słowacja, Węgry, Ukraina, Niemcy) gdzie cieszy się stałym zainteresowaniem

wydawany cyklicznie od 1998 roku

kolportowany bezpłatnie w nakładzie 1000 egzemplarzy

atrakcyjny w cenach reklam

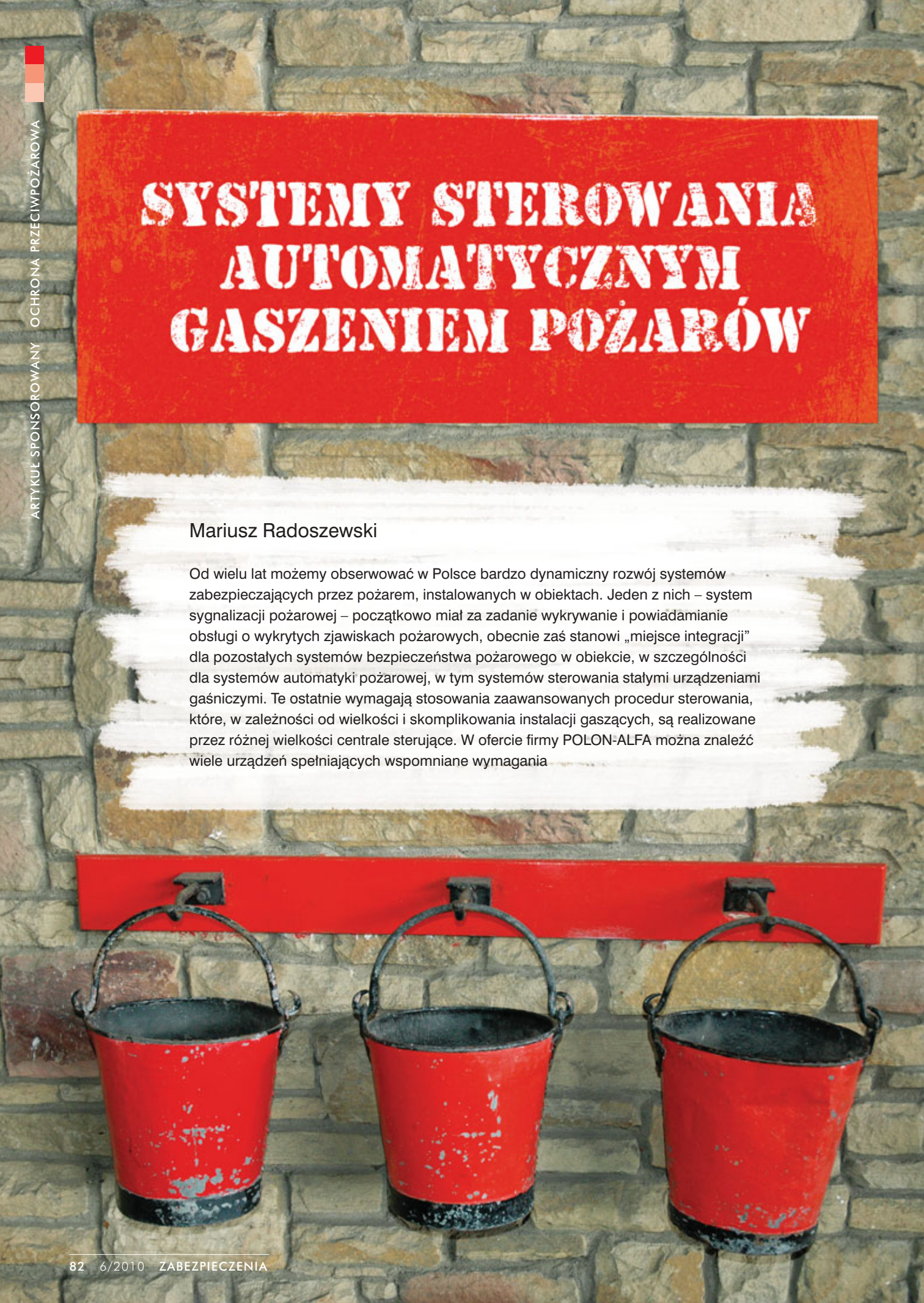
Zapraszamy do współpracy
www.piooim.pl

Polska Izba Ochrony • ul. Kasprzaka 7 • 01-211 Warszawa
tel. (022) 836 61 46 • fax: (022) 535 63 10 • e-mail: office@piooim.pl

SYSTEMY STEROWANIA AUTOMATYCZNYM GASZENIEM POŻARÓW

Mariusz Radoszewski

Od wielu lat możemy obserwować w Polsce bardzo dynamiczny rozwój systemów zabezpieczających przez pożarem, instalowanych w obiektach. Jeden z nich – system sygnalizacji pożarowej – początkowo miał za zadanie wykrywanie i powiadamianie obsługi o wykrytych zjawiskach pożarowych, obecnie zaś stanowi „miejsce integracji" dla pozostałych systemów bezpieczeństwa pożarowego w obiekcie, w szczególności dla systemów automatyki pożarowej, w tym systemów sterowania stałymi urządzeniami gaśniczymi. Te ostatnie wymagają stosowania zaawansowanych procedur sterowania, które, w zależności od wielkości i skomplikowania instalacji gaszących, są realizowane przez różnej wielkości centrale sterujące. W ofercie firmy POLON-ALFA można znaleźć wiele urządzeń spełniających wspomniane wymagania



Centrala IGNIS 1520M

Najbardziej rozpowszechnionymi instalacjami automatycznego gaszenia są małe instalacje jednostrefowe, zabezpieczające pomieszczenia serwerowni, małych archiwów itp., które mogą być sterowane przez dedykowane centrale automatycznego gaszenia. W Polsce jedną z najczęściej stosowanych central jest bez wątpienia IGNIS 1520M (następczyni pierwszej wyprodukowanej przez POLON-ALFA centrali IGNIS 1520).

IGNIS 1520M jest jednostrefową centralą przeznaczoną do:
- sygnalizowania o pożarze wykrytym przez przyłączone czujki,
- uruchamiania stałych urządzeń gaśniczych (zawierających środek gaszący w postaci gazowej, ciekłej lub w postaci aerozoli) po otrzymaniu sygnału z czujek pożarowych lub ręcznych przycisków uruchamiających „START GASZENIA",
- wysterowania przeciwpożarowych urządzeń alarmowych, zabezpieczających, uszczelniających itp.,
- przekazywania informacji o zagrożeniu pożarowym lub realizacji etapów procedury automatycznego gaszenia do systemów monitorowania lub nadrzędnego adresowalnego systemu sygnalizacji pożarowej w obiekcie.

Do centrali można przyłączyć konwencjonalne dwustanowe czujki pożarowe szeregu 40, przyciski sterujące ręcznego uruchomienia (PU-61), wstrzymania (PW-61) i blokady (PB-61) oraz sygnalizatory informacyjne SE-1 i SW-1, produkowane przez POLON-ALFA.

IGNIS 1520M jest urządzeniem, które łączy w sobie funkcje centrali sygnalizacji pożarowej i uniwersalnego sterownika automatycznego gaszenia. Wyposażono je w dwie konwencjonalne linie dozorowe, osiem wejść nadzorowanych linii kontrolnych i sterujących, sześć nadzorowanych wyjść sterujących obwodami sygnalizatorów i urządzeniami inicjującymi uwolnienie środka gaśniczego oraz zestaw jedenastu przekaźników z bezpotencjałowymi zestykami przełącznymi oraz zwiernymi, przeznaczonych do realizacji funkcji wykonawczych i monitorowania stanów centrali.

Sygnał do rozpoczęcia procesu sterowania gaszeniem pochodzi z czujek pożarowych. Zainicjowanie tego procesu jest możliwe wyłącznie po zadziałaniu dwóch czujek, zainstalowanych na dwóch oddzielnych liniach dozorowych (koincydencja). Koincydencja dwuliniowa jest w tym przypadku jednym z najbardziej skutecznych sposobów eliminacji fałszywych alarmów.

W przypadku uszkodzenia układu mikroprocesorowego blokowane jest działanie przekaźników sterujących wyzwoleniem środka gaśniczego i realizacja procesu gaszenia nie może zostać uruchomiona.

W trybie wyłącznie ręcznego sterowania, gdy źródłem sygnału alarmowego są ostrzegacze (czujki) na liniach dozorowych, sygnalizowanie alarmu może być dwustopniowe. Wówczas centrala wywołuje najpierw alarm pierwszego stopnia (alarm wstępny), a po upływie czasu opóźnienia – alarm drugiego stopnia (alarm główny), ale nie powoduje uruchomienia procedury automatycznego gaszenia. Dodatkowym sposobem uodpornienia instalacji na ewentualne fałszywe zadziałania czujek jest zaprogramowanie wariantu ze wstępnym kasowaniem.

W trybie sterowania automatycznego zadziałanie czujek nie spowoduje uruchomienia procedury automatycznego gaszenia, jeśli nie zaistnieje wcześniej koincydencja dwuliniowa, czyli pobudzenie przynajmniej jednej czujki na każdej z dwóch linii dozorowych.

Jeżeli to personel wykryje pożar, centrala umożliwi ręczne wywołanie alarmu i uruchomienie procedury automatycznego gaszenia za pomocą przycisków „START GASZENIA".

Procedura gaszenia rozpoczyna się włączeniem sygnalizacji ewakuacyjnej i rozpoczęciem odliczania zaprogramowanego czasu opóźnienia wyładowania środka gaśniczego. Poprzez naciśnięcie przycisku „STOP GASZENIA" możliwe jest wstrzymanie odliczania w celu zwiększenia opóźnienia. Po upływie zaprogramowanego czasu następuje podanie impulsu elektrycznego powodującego wyzwolenie środka gaśniczego i włączenie odpowiedniej sygnalizacji, ostrzegającej przed wejściem do pomieszczenia. Jeśli wciśnięty był przycisk „STOP GASZENIA", odliczanie czasu opóźnienia może zostać wstrzymane i wznowione po jego zwolnieniu albo trwać do końca – w zależności od skonfigurowania trybu pracy tego przycisku podczas uruchamiania centrali. W takiej sytuacji natychmiast po zwolnieniu tego przycisku nastąpi wyzwolenie środka gaśniczego.

W odpowiednim momencie realizacji procedury gaszenia centrala może uruchomić urządzenia uszczelniające (np. klapy pożarowe) w celu utrzymania odpowiedniego stężenia środka gaśniczego w założonym czasie. Sygnalizacja ostrzegawcza trwa do momentu skasowania alarmu w centrali.

Na płycie czołowej centrali zamontowany jest przycisk „BLOKADA GASZENIA", który umożliwia zablokowanie wyładowania środka gaśniczego w każdym stanie pracy centrali.

Większość zdarzeń, które centrala jest w stanie wykryć i zasygnalizować, jest rejestrowana w wewnętrznej pamięci zdarzeń i może być przesłana do współpracującego komputera za pomocą odpowiedniego oprogramowania.

Fot. 1. Centrala IGNIS 1520M oraz elementy systemu sterowania gaszeniem wykorzystującego centralę IGNIS 1520M (sygnalizatory informacyjne SE-1, SW-1 oraz sterujące przyciski PU-61 i PW-61)

Centrala POLON 4500

Instalacje wykorzystujące centralę POLON 4500 mogą być stosowane do zabezpieczenia przeciwpożarowego średnich i dużych obiektów, w których, oprócz zwykłej instalacji wykrywczo-sygnalizacyjnej, ma znajdować się wielostrefowe, stałe urządzenie gaśnicze. Ze względu na możliwość przekazywania dużej ilości informacji cyfrowych do współpracujących systemów integracji i nadzoru, a także do systemów monitoringu pożarowego, centrala POLON 4500 doskonale nadaje się do stosowania w odpowiedzialnych instalacjach bezpieczeństwa „inteligentnych" budynków (m.in. w bankach, biurach, obiektach użyteczności publicznej itp.). Stosowane w takich obiektach systemy bezpieczeństwa – w szczególności system sterowania automatycznym gaszeniem – muszą spełniać najwyższe wymagania dotyczące niezawodności i nowoczesności zastosowanych rozwiązań technicznych.

Centrala POLON 4500 oraz współpracujące z nią elementy liniowe zostały zaprojektowane z uwzględnieniem wytycznych zawartych w najnowszych edycjach dwóch serii norm europejskich – serii norm EN 12094 dotyczącej części gaśniczej (*Stałe urządzenia gaśnicze. Podzespoły do urządzeń gaśniczych gazowych*) oraz serii norm EN-54 dotyczącej części wykrywczo-sygnalizacyjnej (*Systemy sygnalizacji pożarowej*).

W części odpowiedzialnej za wykrywanie pożaru centrala współpracuje z wielostanowymi, procesorowymi czujkami szeregu 4046, jak również ze wszystkimi elementami liniowymi pracującymi w znanym na rynku interaktywnym systemie POLON 4000 (ręcznymi ostrzegaczami pożarowymi, adapterami, elementami kontrolnymi, sterującymi i kontrolno-sterującymi, sygnalizatorami itd.). W części odpowiedzialnej za proces sterowania gaszeniem bazuje na wbudowanych modułach sterujących gaszeniem MSG-45 i może dodatkowo współpracować z typowymi elementami standardowego wyposażenia systemów sterownia gaszeniem, tj. przyciskami inicjującymi, wstrzymującymi lub blokującymi procedurę gaszenia oraz sygnalizatorami informacyjnymi.

Centrala POLON 4500 jest kolejnym elementem interaktywnego systemu POLON 4000 bazującego na koncepcji inteligentnej współpracy pomiędzy wszystkimi elementami, które go tworzą. Unikalny protokół transmisji sygnałów w pętlach dozorowych oraz odpowiednie oprogramowanie centrali i elementów liniowych umożliwiają współpracę zarówno elementów liniowych z centralą, jak i wybranych elementów liniowych pomiędzy sobą. System umożliwia bardzo wczesne uzyskanie informacji o zjawiskach pożarowych w chronionych obiektach oraz zapewnia dokładną analizę obserwowanego zdarzenia, dzięki czemu można odróżnić stan zagrożenia pożarowego od krótkotrwałego zjawiska zakłócającego i podjąć odpowiedzialną decyzję o wywołaniu alarmu i uruchomieniu procedury automatycznego gaszenia.

Ważniejsze cechy charakterystyczne centrali POLON 4500

Centrala sygnalizacji pożarowej POLON 4500 ma wyposażenie dla czterech pętli adresowalnych z możliwością adresowania po 127 elementów liniowych (czujek pożarowych, ROP i innych) w każdej pętli. Standardowo wyposażona jest w dwa moduły sterowania gaszeniem MSG-45, do których podłączane są przyciski „START GASZENIA", „STOP GASZENIA" i „BLOKADA GASZENIA" oraz sygnalizatory SE-1 i SW-1 (znane już z zastosowań w systemie IGNIS 1520M). Istnieje możliwość rozbudowy centrali o kolejne dwa moduły MSG-45. W ten sposób uzyskuje się możliwość sterowania stałymi urządzeniami gaśniczymi w 2–4 strefach.

Procedura gaszenia może rozpocząć się w trybie w pełni automatycznym (po zadziałaniu co najmniej dwóch czujek pracujących w koincydencji dwuczujkowej lub grupowej, zainstalowanych w tej samej strefie gaszenia) lub w trybie ręcznym (po uruchomieniu przycisku „START GASZENIA", zainstalowanego w pobliżu gaszonej strefy, albo przycisku „START" na płycie czołowej centrali).

W centrali można programowo utworzyć 512 stref dozorowych, którym można przypisać dowolny komunikat użytkownika składający się z dwóch 32-znakowych linii tekstu. Ciekłokrystaliczny wyświetlacz (20 linii po 40 znaków w trybie graficznym) pozwala na szybkie i precyzyjne podanie obsłudze wszelkich danych umożliwiających lokalizację zagrożenia pożarowego oraz informacji o aktualnym etapie procedury gaszenia.

Istnieje możliwość konfigurowania liniowych elementów centrali w kilku trybach, między innymi w trybie automatycznej konfiguracji, w którym centrala automatycznie odczytuje elementy zainstalowane w pętli dozorowej i na odgałęzieniach i nadaje im numery adresowe. Podobne czynności można wykonać również ręcznie, za pomocą dołączonej klawiatury komputerowej. Oprogramowanie ułatwiające konfigurowanie instalacji jest dostępne w komplecie z centralą.

Dla każdej strefy dozorowej można zaprogramować jeden z 17 wariantów alarmowania. Różne warianty alarmowania, programowane w konkretnych strefach, pozwalają na poprawne wykorzystanie systemu wykrywania pożaru w określonych, indywidualnych warunkach panujących w strefie, a także umożliwiają wprowadzenie indywidualnych kryteriów w celu sprawnego zorganizowania systemu ochrony obiektu. Dodatkowo można podzielić zainstalowane w ramach pojedynczej strefy elementy na dwie grupy i uzyskać dzięki temu koincydencję w ramach jednej strefy.

Fot. 2. Centrala POLON 4500 oraz elementy systemu sterowania gaszeniem wykorzystującego centralę POLON 4500

Centrala POLON 4500 pamięta 2000 ostatnich zdarzeń oraz 10000 alarmów, które wystąpiły podczas dozorowania obiektu. Rejestr zdarzeń i alarmów może być wydrukowany na taśmie papierowej lub pokazany na wyświetlaczu centrali.

Istnieje możliwość pracy central POLON 4500 w sieci (do 31 central POLON 4500 i POLON 4900 razem), a podłączenie do centrali terminali sygnalizacji równoległej TSR-4000 umożliwia informowanie o stanie systemu sygnalizacji pożarowej w miejscu oddalonym od miejsca zainstalowania samej centrali.

Podstawowe procedury w centrali POLON 4500

Wykrywanie pożaru

Funkcja wykrywania pożaru jest realizowana przez zainstalowane na pętlach dozorowych czujki pożarowe (do dyspozycji są cztery pętle; w jednej pętli jest 127 elementów adresowalnych). Zamontowane w gaszonych strefach czujki są programowane do pracy w koincydencji. Koincydencja może zachodzić pomiędzy dwiema czujkami w tej samej strefie lub pomiędzy grupami czujek. Praca czujek jest organizowana w taki sposób w celu uniknięcia nieuzasadnionego wyładowania środka gaśniczego w gaszonej strefie w przypadku fałszywego zadziałania jednej z czujek. Zadziałanie jednej czujki nie powoduje uruchomienia procedury gaszenia. Wywołany jest jedynie alarm pierwszego stopnia w centrali, wymagający potwierdzenia przez obsługę. Dopiero zadziałanie drugiej czujki w tej samej strefie powoduje przełączenie centrali w stan realizowania procedury automatycznego gaszenia.

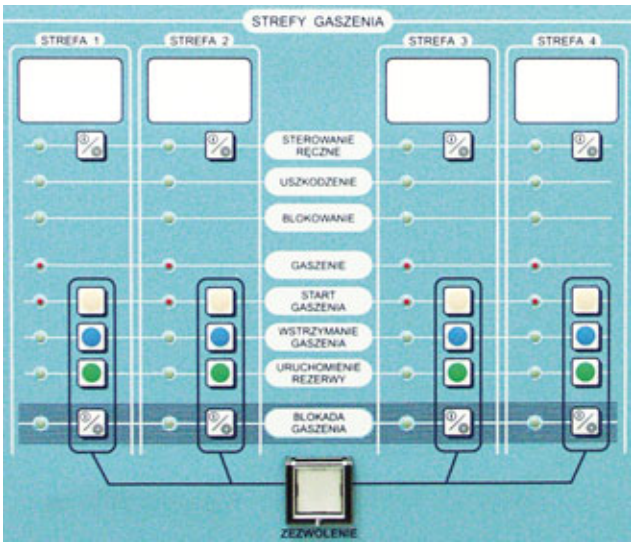
Procedura gaszenia

Sterowanie procesem automatycznego gaszenia odbywa się za pośrednictwem wyspecjalizowanych modułów sterowania gaszeniem MSG-45 (od jednego do czterech modułów w centrali). Każdy moduł jest wyposażony w 16 przekaźników sterujących i 11 wejść kontrolnych, przeznaczonych do podłączenia zewnętrznych linii sterujących i kontrolnych, m.in. do podłączania przycisków sterujących „START GASZENIA" (PU-61), „STOP GASZENIA" (PW-61), przełącznika „BLOKADA GASZENIA" (PB-61) oraz styków kontrolnych instalacji automatycznego gaszenia.

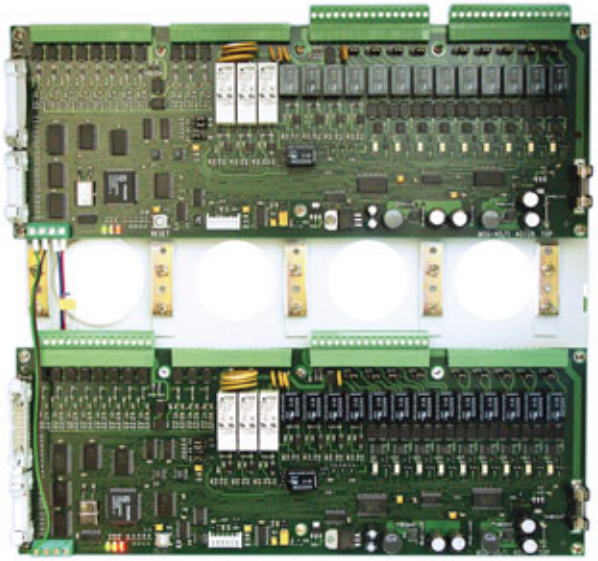
Proces automatycznego gaszenia może odbywać się w trybie automatycznym (z ewentualną ingerencją ręczną) lub w trybie wyłącznie ręcznym.

Stan uruchomienia procedury gaszenia sygnalizowany jest optycznie i akustycznie zarówno w samej centrali (przez sygnalizator dźwiękowy centrali i diody sygnalizacyjne), jak i w strefie gaszonej oraz jej otoczeniu (przez sygnalizatory informacyjne SE-1 oraz SW-1).

Fot. 3. Część „pożarowa" centrali POLON 4500



Fot. 4. Część „gaszeniowa" centrali POLON 4500



Fot. 5. Moduł MSG-45

Przed aktywacją właściwego wyjścia uruchamiającego element wyzwalający instalacji gaśniczej odliczany jest czas na ewakuację z gaszonej strefy (wysterowane zostaną wyjścia do sygnalizatorów informujących o rozpoczętej procedurze gaszenia i konieczności opuszczenia chronionej strefy). W tym czasie można wstrzymać lub zablokować procedury gaszenia poprzez wciśnięcie przycisków „STOP GASZENIA" lub „BLOKADA GASZENIA", zainstalowanych w gaszonej strefie, lub przycisków „STOP" lub „BLOKADA" na płycie czołowej centrali. Procedurę gaszenia można rozpocząć ponownie, wciskając przycisk „START GASZENIA" lub „START" (w centrali). Jest to możliwe tylko wówczas, gdy użyta została funkcja wstrzymania procedury gaszenia (przyciskiem „STOP GASZENIA" lub „STOP"). Uruchomienie funkcji zablokowania gaszenia (przyciskiem „BLOKADA GASZENIA" lub „BLOKADA" w centrali) powoduje przerwanie procedury gaszenia. Po wyłączeniu funkcji „BLOKADA" centrala powraca do stanu dozorowania.

Po zakończeniu odliczania zaprogramowanego czasu na ewakuację następuje uruchomienie wyjść sterujących, podających sygnały do elementów wyzwalających. W zależności od rodzaju instalacji gaśniczej, którą steruje centrala POLON 4500, istnieje możliwość ustawienia czasów wysterowania wyjść do elementów wyzwalających (elektrozaworów etc.). Stan wyzwolenia środka gaśniczego jest sygnalizowany w centrali. Brak wypływu środka gaśniczego (na podstawie informacji z czujników przepływu) powoduje włączenie odpowiedniej sygnalizacji takiego stanu.

Centrala ma ponadto możliwość sygnalizowania następujących stanów urządzeń instalacji gaszących:

– stanu wyładowania środka gaśniczego,
– stanu uszkodzenia modułu MSG-45,
– stanu blokowania linii kontrolnej, przekaźnika,
– stanu testowania sygnalizatorów optycznych i linii kontrolnych modułu MSG-45.

Normy związane

Elektryczne urządzenia sterujące automatycznym gaszeniem są objęte dwiema grupami norm.

Normy dotyczące wyposażenia realizującego procedurę gaszenia:

– PN-EN 12094-1:2006 *Stałe urządzenia gaśnicze. Podzespoły urządzeń gaśniczych gazowych. Część 1: wymagania i metody badań elektrycznych central automatycznego sterowania*;
– PN-EN 12094-3:2006 *Stałe urządzenia gaśnicze. Podzespoły urządzeń gaśniczych gazowych. Część 3: wymagania i metody badań ręcznych urządzeń inicjujących i wstrzymujących.*

Normy dotyczące wyposażenia realizującego wykrywanie, sygnalizację i zasilanie:

– PN-EN 54-2:2002 *Systemy sygnalizacji pożarowej. Część 2: centrale sygnalizacji pożarowej ze zmianą A1:2007;*
– PN-EN 54-4:2001 *Centrale sygnalizacji pożarowej. Część 4: zasilacze ze zmianą A1:2004 i A2:2007.*

W zakresie projektowania i instalowania instalacji gaszących można posługiwać się następującymi normami:

– PN-M-51250-01:1993 *Stałe urządzenia gaśnicze. Urządzenia na dwutlenek węgla. Zasady projektowania i instalowania;*
– PN-EN 15004-1:2008 *Stałe urządzenia gaśnicze. Urządzenia gazowe. Część 1: ogólne wymagania dotyczące projektowania i instalowania* oraz dalszymi częściami tej normy (od 2 do 10), dotyczącymi projektowania instalacji na konkretny środek gaśniczy.

Ponadto w przypadkach nieuregulowanych przez polskie normy projektanci często korzystają z amerykańskich norm NFPA:

– NFPA 12: *Standard on Carbon Dioxide Extinguishing Systems, 2008 Edition;*
– NFPA 13: *Standard for the Installation of Sprinkler Systems, 2010 Edition;*
– NFPA 15: *Standard for Water Spray Fixed Systems for Fire Protection, 2007 Edition;*
– NFPA 2001: *Standard on Clean Agent Fire Extinguishing Systems, 2010 Edition.*

Produkowane przez POLON-ALFA centrale sterujące automatycznym gaszeniem spełniają wymagania wyżej wymienionych norm, mają wymagane certyfikaty i są dopuszczone do stosowania w ochronie przeciwpożarowej w Polsce.

mgr inż. Mariusz Radoszewski
POLON-ALFA

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

POLON 4100

NOWY WYMIAR BEZPIECZEŃSTWA

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

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

Kamera BE4815PVR

CNB TECHNOLOGY Inc.

Kamera BE4815PVR to zewnętrzna kamera kompaktowa o wysokiej czułości i wysokiej rozdzielczości 550 TVL, wyróżniająca się bardzo solidną obudową i przyjaznym systemem mocowania oraz zasilaniem dualnym 12 V_{DC} / 24 V_{AC}.

Kamera dedykowana jest do zastosowań zewnętrznych wymagających precyzyjnej regulacji pola widzenia kamery oraz ustawień parametrów, takich jak DNR czy AGC.

Zalety kamery:

- wbudowany jasny obiektyw o zmiennej ogniskowej 3,8÷9,5 mm F1,2 z automatyczną przysłoną DC
- dodatkowe wyjście wideo dla instalatora
- cyfrowy zoom ×2
- mechanicznie odsuwany filtr podczerwieni zapewniający wierną reprodukcję kolorów
- funkcja DSS (Digital Slow Shutter) regulowana w zakresie do 32 ramek zwiększa czułość w nocy
- możliwość pracy w dzień i w nocy
- wbudowany promiennik podczerwieni o zasięgu do 50 m
- grzałka i wentylator

Właściwości:

- kolorowa kamera dzień/noc
- przetwornik 1/3" Sony Super HAD
- wysoka rozdzielczość 550 TVL
- wyposażona w mechanicznie odsuwany filtr IR - TDN(ICR)
- czułość 0,3 lx (kolor), 0,008 lx (DSS 32 ramki), 0,00 lx (IR LED włączone)
- obiektyw 3,8÷9,5 mm DC
- OSD
- AGC, BLC, AWB, D/N, Flickerless
- cyfrowy zoom
- zasilanie dualne 12 V_{DC} / 24 V_{AC}
- obudowa przystosowana do montażu do ściany

Dane techniczne	
Model	BE4815PVR
Standard sygnału wideo	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/3" SONY Super HAD CCD
Rozdzielczość efektywna	752(H)×582(V) 440K
Liczba linii	550 TVL
Wyjście wideo	1,0V p-p, 75 Ohm
Odstęp sygnał/szum	>50dB (wył. AGC)
Obiektyw	f=3,8~9,5 mm, F1,2 DC
Cyfrowy zoom	2×
Tryb dzień/noc	Mechaniczny filtr IR z czujnikiem
Czułość	0,3 lx (kolor) / 0,1 lx(b/w) / 0,008 lx (DSS 32ramki) / 0,00 lx (IR LED włączone)
Podczerwień	IR LED 56EA (850nm, 15°, 30°), czujnik 1EA
Zasięg doświetlenia	maks. 50 m
Funkcja DSS	do 32 ramek obrazu
Balans bieli	automatyczny
Automatyczna regulacja wzmocnienia (AGC)	wł./wył.
Kompensacja światła tylnego	BLC, wł./wył.
Redukcja migotania	wł./wył.
Elektroniczna migawka	1/50~1/120 000 s
Stopień ochrony IP	IP 65
Zasilanie	12 V_{DC} / 24 V_{AC}
Pobór prądu	maks 0,5 A (24 V_{AC}) / 1,5 A (12 V_{DC})
Wymiary (szer.×wys.×gł.)	110,8×218,6×325,7 mm
Temperatura pracy / wilgotność	-30°C ~ 50°C / 30% ~ 80% RH
Masa	1600 g

Kamera DBM-21VD

CNB TECHNOLOGY Inc.

MONALISA

DBM-21VD to kamera kopułowa o wysokiej czułości i bardzo wysokiej rozdzielczości (600 TVL w trybie kolorowym, 650 TVL w trybie B/W), wyróżniająca się bardzo dobrym i wiernym odwzorowaniem kolorów. Kolory są żywe i naturalne, a obraz ostry i wyraźny.

Kamera dedykowana jest do zastosowań wewnętrznych, wymagających precyzyjnej regulacji pola widzenia kamery oraz ustawień, takich jak DNR czy SBLC. W kamerze zastosowano procesor cyfrowej obróbki sygnału Monalisa.

Zalety kamery:

- wbudowany obiektyw o zmiennej ogniskowej 4÷9 mm z automatyczną przysłoną DC
- dodatkowe wyjście wideo dla instalatora
- regulacja położenia modułu kamery w 3 osiach: pion, poziom oraz obrót wokół własnej osi
- SBLC – ulepszona odmiana BLC, czyli kompensacji tylnego oświetlenia

Kamerą o podobnych właściwościach, bez OSD jest DFL-21S (z obiektywem o stałej ogniskowej 3,8 mm).

Właściwości:

- kolorowa kamera dzień/noc
- przetwornik 1/3" Sony Super HAD II
- bardzo wysoka rozdzielczość 600 TVL (kolor) / 650TVL (B/W)
- przełącza się w tryb B/W
- czułość 0,05 lx (kolor)
- obiektyw 4÷9 mm DC
- OSD
- regulacje jasności oraz koloru
- AGC, SBLC, AWB, DNR, Flickerless, D/N – regulacja przez OSD
- detekcja ruchu, strefy prywatności, funkcja mirror, wyostrzanie obrazu
- zasilanie 12 V_{DC}
- obudowa kopułkowa o średnicy 92 mm

Dane techniczne	
Model	DBM-21VD
Standard sygnału wideo	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/3" SONY Super HAD CCD II
Rozdzielczość efektywna	752(H)×582(V) 440K
Liczba linii	600 TVL
Wyjście wideo	1,0V p-p, 75 Ohm
Odstęp sygnał/szum	>50 dB
Obiektyw	f=4~9 mm
Tryb dzień/noc	auto
Czułość	0,05 lx
Menu OSD	angielski, chiński
Cyfrowa redukcja szumu	3 poziomy/wył.
Balans bieli	automatyczny
Automatyczna regulacja wzmocnienia (AGC)	tak
Kompensacja światła tylnego	SBLC, 3 poziomy/wył.
Redukcja migotania	wł./wył.
Strefy prywatne	4 programowalne strefy
Detekcja ruchu	4 programowalne strefy
Odbicie lustrzane obrazu	w poziomie
Elektroniczna migawka	1/50~1/120 000 s
Ręczna migawka	1/50, 1/250, 1/700, 1/1K, 1/1.6K, 1/2.5K, 1/5K, 1/7K, 1/10K, 1/30K, 1/60K, 1/120K
Zasilanie	12 V_{DC}
Pobór prądu	maks. 180 mA
Wymiary (średnica×wys.)	123×95 mm
Temperatura pracy / wilgotność	-10°C~45°C / 30%~80% RH
Masa	366 g

Dystrybucja: &GDE POLSKA

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

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

Kamera VBB-31VF

VBB-31VF to wandaloodporna kamera kopułowa o wysokiej czułości i bardzo wysokiej rozdzielczości (580 TVL w trybie kolorowym, 650 TVL w trybie B/W), wyróżniająca się wiernym odwzorowaniem kolorów. Kolory są żywe i naturalne, a obraz ostry i wyraźny.

Kamera posiada funkcję WDR (szeroki zakres dynamiki) poprawiającą zdolność obserwacji scen o różnym poziomie oświetlenia. W odróżnieniu od tańszych kamer jest to prawdziwy WDR – stosowana jest technika podwójnego skanowania przetwornika.

Kamera dedykowana jest do zastosowań wewnętrznych i zewnętrznych wymagających precyzyjnej regulacji pola widzenia kamery oraz ustawień parametrów pracy kamery, takich jak 3D DNR czy BLC/WDR/Eclipsa. W kamerze zastosowano przetwornik cyfrowej obróbki sygnału DSP Blue-I.

Zalety kamery:

- wbudowany obiektyw o zmiennej ogniskowej 2,8÷10,5 mm z automatyczną przysłoną DC
- dodatkowe wyjście wideo dla instalatora
- regulacja położenia modułu kamery w 3 osiach: pion, poziom oraz obrót wokół własnej osi
- WDR – szeroki zakres dynamiki
- odsuwany mechanicznie filtr IR
- wierne odwzorowanie kolorów
- możliwość pracy w dzień i w nocy, praca z reflektorami podczerwieni
- funkcja DSS x128
- redukcja szumów 3D, redukcja smużenia przemieszczających się obiektów
- cyfrowa stabilizacja DIS

Właściwości:

- kolorowa kamera dzień/noc
- przetwornik 1/3" Double-density scan
- bardzo wysoka rozdzielczość 580 TVL oraz w trybie czarno-białym 650TVL
- wyposażona w mechanicznie odsuwany filtr IR - TDN(ICR),
- czułość 0,1 lx, 0,0002 lx (BW, DSS on)
- obiektyw 2,8÷10,5 mm DC
- OSD
- regulacje jasności oraz koloru
- AGC, WDR, Eclipsa, BLC, AWB, 3D DNR, DIS, Flickerless, D/N, DZ – regulacja przez OSD
- WDR maks. 72 dB
- detekcja ruchu, strefy prywatności, funkcja mirror w pionie i poziomie oraz obrót obrazu, wyostrzanie obrazu
- sterowanie przez RS-485 (Pelco-D)
- zasilanie 12 V_{DC}
- obudowa kopułkowa o średnicy 100 mm, pozwalająca na montaż podwieszany do sufitu oraz w suficie podwieszanym

CNB TECHNOLOGY Inc.

BLUE-i

Dane techniczne	
Model	VBB-31VF
Standard sygnału wideo	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/3" Vertical Double Density CCD
Rozdzielczość efektywna	752(H) x 582(V) 440K
Liczba linii	580 TVL
Wyjście wideo	1,0 V p-p, 75 Ohm
Odstęp sygnał/szum	>52 dB
WDR	maks. 72 dB
Obiektyw	f=2,8~10,5 mm
Tryb dzień/noc	Mechaniczny filtr IR z czujnikiem
Czułość	0,1 lx, 0,0002 lx (B/W, DSS on)
Menu OSD	angielski, chiński, koreański, rosyjski, hiszpański, francuski
Cyfrowa redukcja szumu	63 poziomy/wył.
Balans bieli	automatyczny
Funkcja DSS	do 128 ramek obrazu
Automatyczna regulacja wzmocnienia (AGC)	tak
Kompensacja światła tylnego	BLC, 3 poziomy / wył.
Eclipsa	16 stref
Cyfrowa stabilizacja obrazu	wł./wył.
Cyfrowy zoom	×6,13
Redukcja migotania	wł./wył.
Strefy prywatne	8 programowalnych stref
Detekcja ruchu	4 programowalne strefy
Odbicie lustrzane obrazu	w poziomie, w pionie, obrót
Elektroniczna migawka	1/50~1/120 000 s
Ręczna migawka	1/60, 1/250, 1/700, 1/1K, 1/1.6K, 1/2.5K, 1/5K, 1/7K, 1/10K, 1/30K, 1/60K, 1/120K
Stopień ochrony IP	IP65
Zasilanie	12 V_{DC}
Pobór prądu	maks. 200 mA
Wymiary (średnica×wys.)	100×111 mm
Temperatura pracy / Wilgotność	-10°C ~ 45°C / 30% ~ 80% RH
Masa	844 g

Dystrybucja: &GDE POLSKA

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

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

Kamera WCL-21S

CNB TECHNOLOGY Inc.

WCL-21S to zewnętrzna kamera kompaktowa o bardzo wysokiej czułości i wysokiej rozdzielczości 600 TVL, wyróżniająca się estetyczną obudową.

Kamera przeznaczona jest do zastosowań zewnętrznych. Posiada procesor DSP Monalisa oraz wykorzystuje technologię Intelligent IR. Intelligent IR to nowy rodzaj podświetlenia IR opracowany przez firmę CNB. Eliminuje on efekt przejaskrawienia i rozmycia obrazu w sytuacji, gdy obserwowany obiekt zbliża się do kamery. W standardowym podświetleniu jasność świecenia jest stała, co w praktyce może spowodować prześwietlenie obrazu. Intelligent IR steruje jasnością podświetlenia w zależności od odległości od obserwowanego obiektu.

Zalety kamery:

- wbudowany obiektyw o stałej ogniskowej 6 mm
- możliwość pracy w dzień i w nocy
- wbudowany promiennik podczerwieni o zasięgu 30 m
- Intelligent IR – adaptacyjne podświetlenie w podczerwieni
- Podobną kamerą jest B2310PVF (odsuwany filtr IR, obiektyw 3,8÷9,5 mm DC), a nieco bardziej rozbudowaną B2810PVF (odsuwany filtr IR, funkcja DSS, obiektyw 3,8÷9,5 mm DC)

Właściwości:

- kolorowa kamera dzień/noc
- przetwornik 1/3" Sony Super HAD
- wysoka rozdzielczość 600 TVL (kolor) / 650 TVL (B/W)
- czułość 0,05 lx (kolor), 0,00 lx (IR LED włączone)
- obiektyw 6 mm
- AGC, BLC, AWB – automatyczne
- cyfrowy zoom
- obudowa przystosowana do montażu do ściany i sufitu

Dane techniczne	
Model	WCL-21S
Standard sygnału wideo	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/3" SONY Super HAD CCD
Rozdzielczość efektywna	752(H)×582(V) 440K
Liczba linii	550 TVL
Wyjście wideo	1,0 V p-p, 75 Ohm
Odstęp sygnał/szum	>50 dB (wył. AGC)
Obiektyw	f = 6 mm
Tryb dzień/noc	auto
Czułość	0,05 lx (kolor) / 0,00 lx (IR LED włączone)
Promiennik IR	Intelligent IR LED 36EA (850nm, 30°), czujnik 1EA
Zasięg promiennika IR	maks. 30 m
Balans bieli	automatyczny
Automatyczna regulacja wzmocnienia (AGC)	tak
Kompensacja tylnego oświetlenia	SBLC, automatyczna
Elektroniczna migawka	1/50~1/120 000 s
Stopień ochrony IP	IP66
Zasilanie	12 V_{DC}
Pobór prądu	maks. 0,5 A
Wymiary (szer.×wys.×gł.)	78×150 mm
Temperatura pracy / Wilgotność	-10°C ~ 45°C / 30% ~ 80% RH
Masa	800 g

Dystrybucja: &GDE POLSKA

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

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

Monitor wideodomofonowy CDV-71AM firmy Commax

Monitor Commax CDV-71AM uzupełnia ofertę firmy w grupie analogowych systemów wideodomofonowych. Przeznaczony jest do użytku w domach jedno- lub kilkurodzinnych. Ze względu na zastosowanie zaawansowanego technologicznie 7-calowego wyświetlacza LCD wyróżnia się bardzo dobrą jakością wyświetlanego obrazu.

Monitor CDV-71AM obsługuje dwa panele wejściowe, dzięki czemu możliwy jest kontakt audiowizualny np. z dwoma furtkami (wraz z funkcją otwarcia obu wejść) oraz dodatkowo dwie zewnętrzne kamery CCTV - umożliwiające np. obserwację większego obszaru podczas rozmowy z odwiedzającym (funkcja PIP – *picture-in-picture*). Zestaw wideodomofonowy 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 (automatycznie lub ręcznie) wraz z datą i godziną. 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:

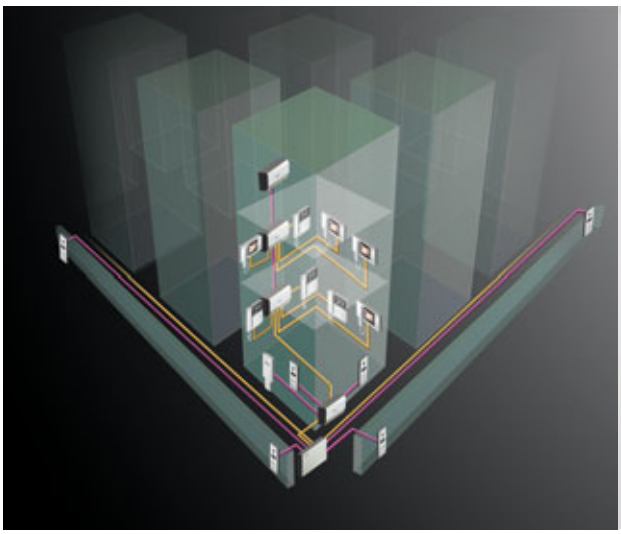
- monitor kolorowy
- wyświetlacz 7" Color TFT-LCD 16:9
- standard sygnału wideo PAL/NTSC
- obsługuje dwa wejścia (dwa panele wejściowe)
- obsługa kamer CCTV (wyświetlanie PIP – picture-in-picture)
- wbudowany moduł pamięci 128 obrazów
- możliwość podłączenia dodatkowego monitora
- współpraca z unifonami DP-4VR, DP-4VH
- paging pomiędzy stacjami
- instalacja czteroprzewodowa + obwód elektrozamka
- współpracuje z kamerami analogowymi czteroprzewodowymi
- zasilanie 230 V
- wymiary: 243×168×35 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

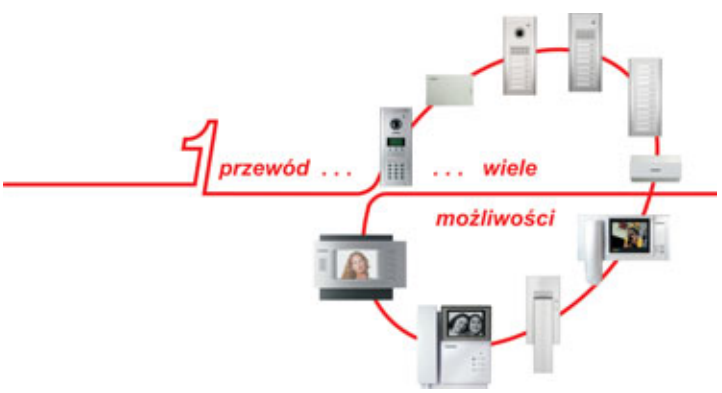
System wieloabonentowy serii 2400

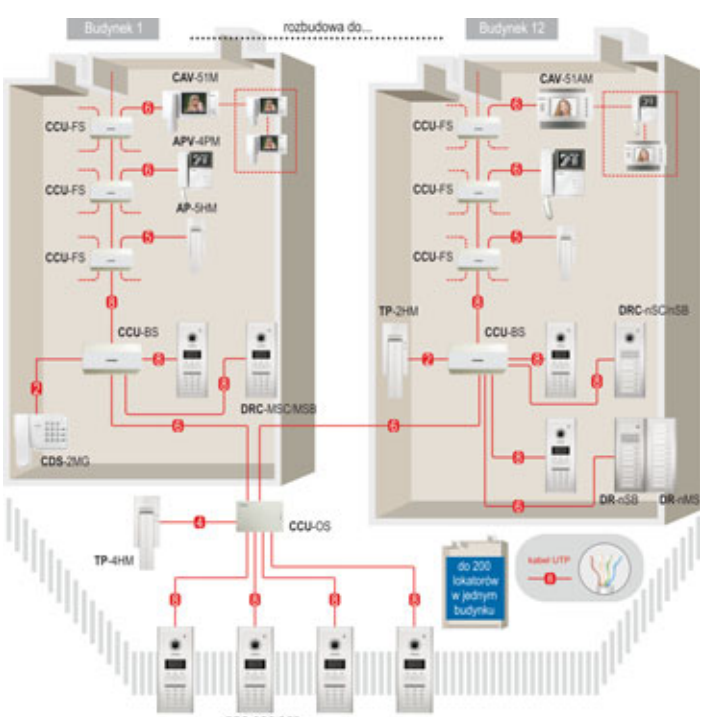


System wieloabonentowy serii 2400 przeznaczony jest do instalacji zarówno w prostych, jak i w bardzo rozbudowanych aplikacjach - maksymalna liczbę obsługiwanych przez system abonentów wynosi 2400. U każdego lokatora może być zainstalowane do 3 urządzeń (jedno urządzenie typu Master i dwa urządzenia typu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

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

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





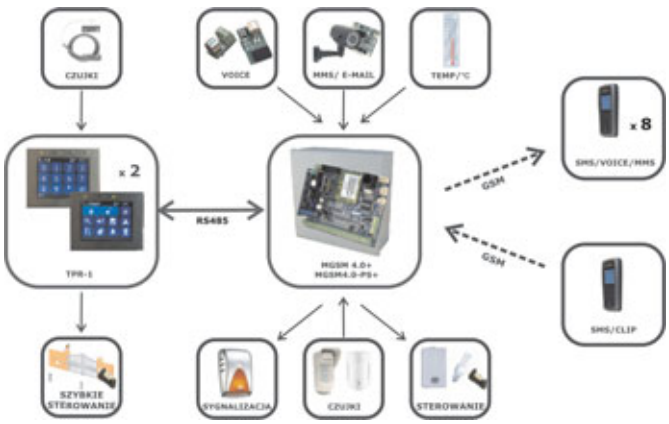
Dystrybucja:

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

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

MGSM 4.0+/4.0-PS+ & TPR-1
Centrala alarmowa z komunikacją GSM sterowana panelem dotykowym (klawiaturą dotykową)

Centrala alarmowa MGSM 4.0+/4.0-PS+ wraz z panelem dotykowym TPR-1 i pozostałymi dedykowanymi urządzeniami to nowoczesna konstrukcja spełniająca wymagania najbardziej wymagających klientów. Wbudowany komunikator GSM pozwala na bezpośrednie przesyłanie informacji na telefony użytkowników i (lub) stacji monitorowania. Ponadto zintegrowany moduł GSM pozwala na zdalne sterowanie systemem (czuwaniem) poprzez SMS-y. System pozwala także na sterowania urządzeniami (wyjściami) poprzez SMS-y lub sygnały CLIP. Centrala MGSM 4.0+ wyposażona jest w automatyczne funkcje monitorujące stan systemu.



Centrala dodatkowo może być rozbudowana o następujące urządzenia:

- panel dotykowy TPR-1, nowoczesna klawiatura do kontroli systemu „TouchPanel", z unikalnymi funkcjami i eleganckim wyglądzie
- moduł FGR-4 do przesyłania wiadomości MMS/E-MAIL ze zdjęciami z kamer przemysłowych, pozwalające na weryfikacje wideo stanu obiektu
- syntezer mowy VSR-2, pozwalający na przesłanie 16 komunikatów głosowych zawierających unikalne informacje o zdarzeniu (VOICE),
- syntezer mowy VSR-1, pozwalający na przesłanie komunikatu głosowego (VOICE),
- moduł audio AMR-1 (mikrofon), pozwalający na podsłuch obiektu (weryfikacja audio),
- czujnik temperatury TSR-1, służący do kontroli temperatury i funkcji termostatu,
- zasilacz systemowy PSR z mikroprocesorową kontrolą parametrów i akumulatora,
- zasilacz systemowy z wbudowanym sterownikiem radiowym PSR-RF, pozwala na sterowanie czuwaniem systemu i wyjściami przekaźnikowymi poprzez piloty radiowe.

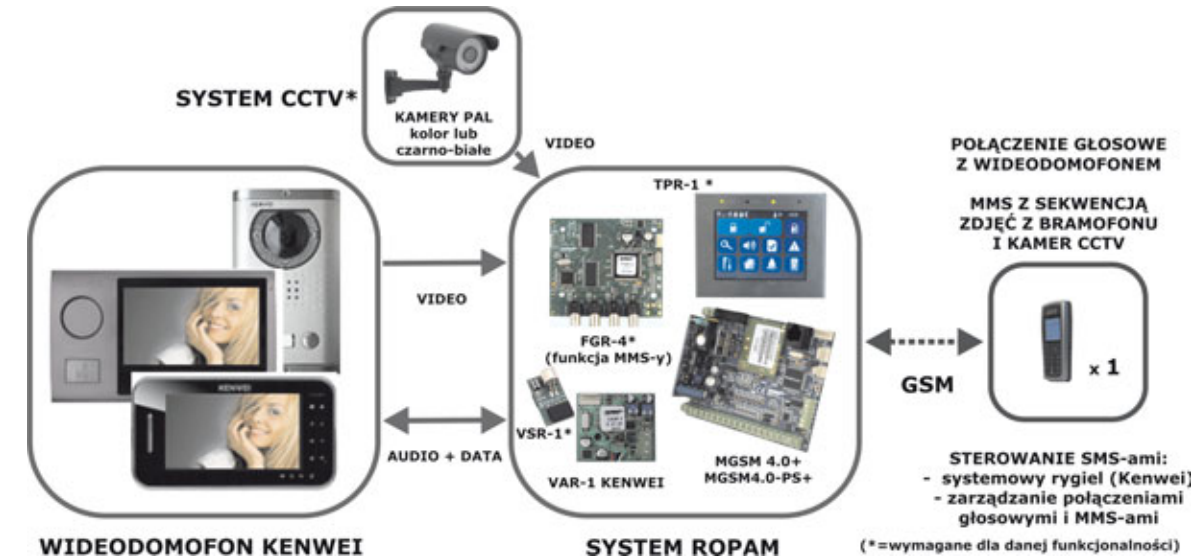
System alarmowy zbudowany z centrali alarmowej serii MGSM 4.0+/4.0-PS+, panelu dotykowego z kolorowym wyświetlaczem TPR-1 oraz innych urządzeń dodatkowych to idealne rozwiązanie dla obiektów mieszkalnych i małych obiektów komercyjnych. Intuicyjny i przejrzysty interfejs, powoduje, że sterowanie systemem alarmowym jest intuicyjne i wyjątkowo proste. Panel dotykowy w połączeniu z modułami MGSM 4.0+/4.0-PS+ pozwala na zbudowanie w pełni funkcjonalnego systemu alarmowego. Przy połączeniu dwóch paneli otrzymujemy następującą konfigurację: 12 wejść, 10 wyjść, jedna strefa z czuwaniem nocnym oraz z wbudowaną komunikacją i sterowaniem GSM. Centrala MGSM 4.0+/4.0-PS+ pozwala ponadto na stworzenie prostych aplikacji automatyki domowej ze zdalną kontrolą poprzez sygnały SMS/CLIP. Elastyczne funkcje pozwalają ponadto na stosowanie centrali alarmowej w systemach, w których wykorzystuje się kontrolę sygnałów binarnych, temperaturę, wymagana jest weryfikacja wizualna, a przesyłanie informacji jest w standardach SMS, VOICE, MMS, e-mail.

Z podstawowych właściwości systemu należy wyróżnić:

- 8 do 12 wejść do podłączenia czujek, urządzeń wyzwalających,
- 8 do 12 wyjść sterowanych, dedykowanych do sygnalizacji lub sterowania,
- wbudowany komunikator GSM z transmisją na 8 numerów telefonu,
- przesyłanie informacji o stanie systemu poprzez SMS,
- przesyłanie informacji głosowej (VOICE),
- przesyłanie wiadomości multimedialnej (MMS/E-MAIL),
- funkcja pomiaru temperatury i termostatu,
- funkcje kontroli połączenia,
- funkcje ograniczenia i kontroli kosztów.

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

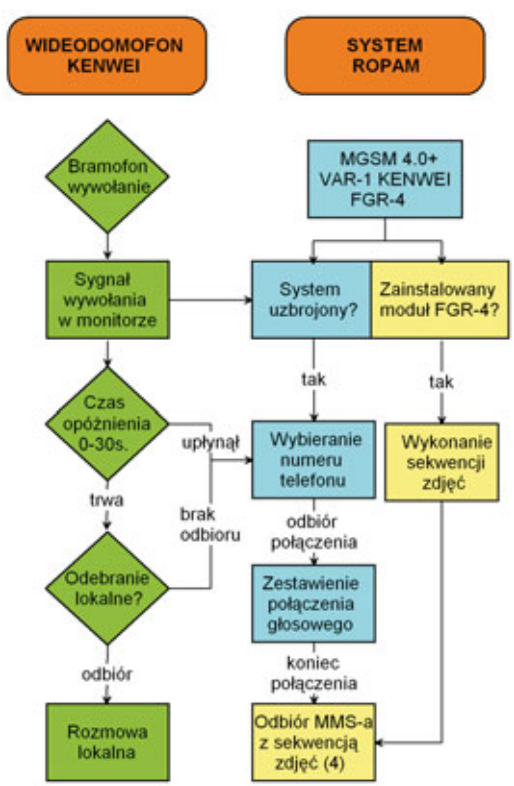
Integracja systemu Ropam z wideodomofonem z wykorzystaniem bramki VAR-1 KENWEI i modułu FGR-4



VAR-1 KENWEI jest bramką integrującą system alarmowy MGSM 4.0+/4.0-PS+ z wideodomofonen Kenwei poprzez magistralę cyfrową.

Podstawowe właściwości zintegrowanego systemu:

- dwukierunkowa komunikacja głosowa, pomiędzy wideodomofonem a telefonem komórkowym poprzez sieć GSM
- inteligentny algorytm przekazu połączenia z detekcją lokalnego odbioru rozmowy
- transmisja MMS-ów z sekwencją zdjęć z kamery bramofonu i (lub) systemu CCTV
- przekazywanie połączeń tylko podczas nieobecności właściciela (czuwanie systemu)
- głosowa lub ukryta informacja o przekierowaniu połączenia
- regulowany czas opóźnienia przekierowania połączenia
- kontrola i zmiana przekazów przez użytkownika (niezależne komendy SMS: AUDIO, MMS-y)
- zdalne sterowanie (komendą SMS) systemowym przekaźnikiem wideodomofonu (rygiel)
- zdalne pobranie zdjęć z kamery bramofonu i/lub systemu CCTV, poprzez MMS-a „na życzenie”
- łatwa integracja: 3-przewodowa magistrala + sygnał wizyjny
- regulacja poziomu dźwięku w bramofonie i telefonie komórkowym,
- system nie ogranicza innych funkcji systemów, a podnosi ich funkcjonalność
- funkcje ograniczenia ilości przekazów (kosztów)
- współpraca z wybranymi modelami wideodomofonów Kenwei



Wymagane elementy systemu ROPAM:

- MGSM 4.0+/4.0-PS+ centrala alarmowa z komunikacją GSM
- VAR-1 Kenwei bramka wideodomofonu, 3-przewodowa magistrala
- FGR-4 moduł przetwarzania sygnału wideo z kamer na MMS-y

Opcjonalne elementy systemu:

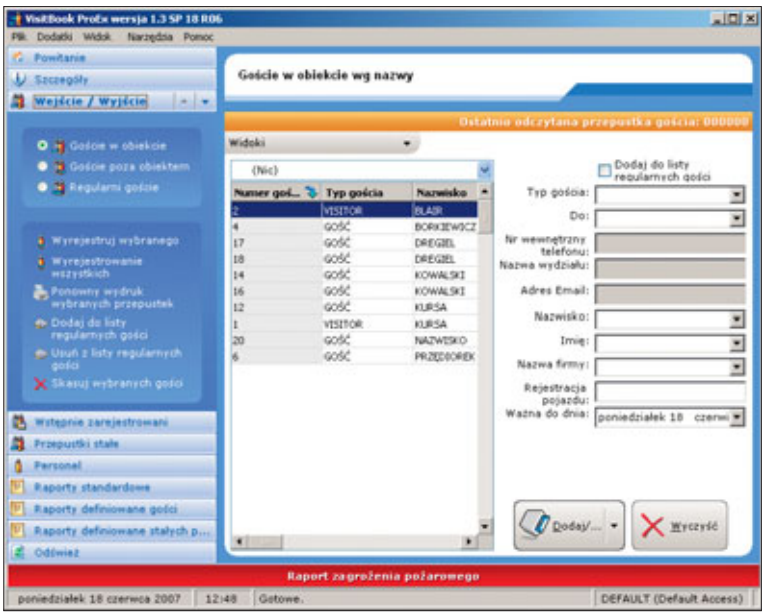
- VSR-1 syntezer mowy, komunikat o przekazie połączenia
- TPR-1 panel dotykowy , nowoczesna klawiatura do kontroli systemu
- TSR-1 czujnik temperatury, służący do kontroli temperatury i funkcji termostatu
- pozostałe elementy systemu Ropam Elektronik

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

System rejestracji gości VisitBook



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

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

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

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

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

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

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

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

GOLD-PLUS inteligentny tester akumulatorów z ręczną kalibracją

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

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

Cechy charakterystyczne

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

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

Dystrybucja: alarmnet®

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

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

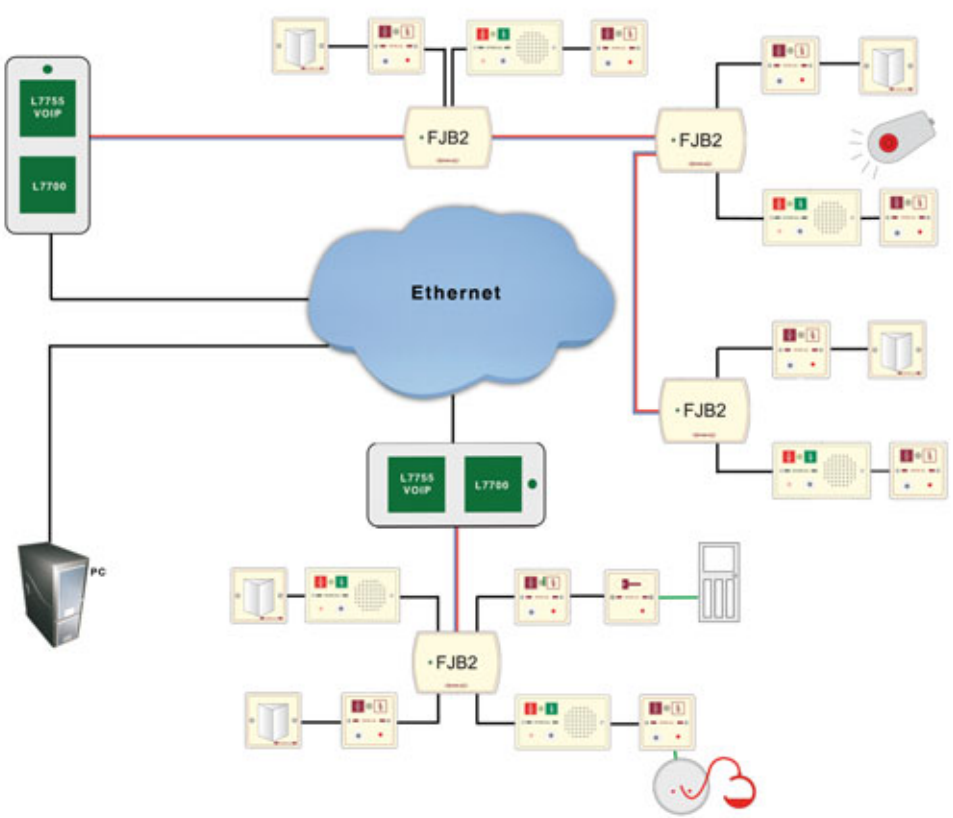
Intercall – szpitalny system przywoławczy

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

Monitor głośnomówiący kolorowy MT320C-CK2 do systemu wideodomofonowego

Monitor głośnomówiący MT320C-CK2 charakteryzuje się nowoczesnym wzornictwem i różnorodnymi możliwościami rozbudowy. Posiada 7" kolorowy panoramiczny wyświetlacz TFT LCD.

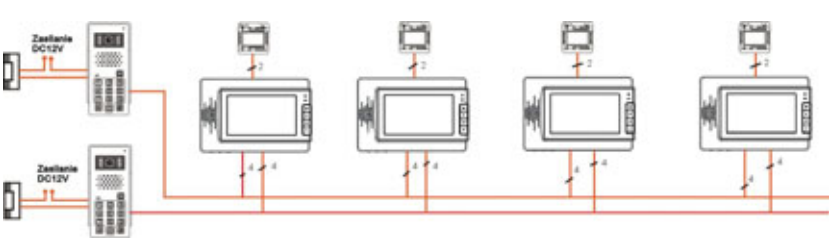
Monitor zapewnia pełną regulację parametrów takich jak: głośność, jasność i kolor. Urządzenie umożliwia podłączenia 2 stacji bramowych i rozbudowę o dodatkowe 3 monitory lub unifony w pełni zaspokajając potrzeby indywidualnego użytkownika. Alternatywnie możliwe jest podłączenie zamiast drugiej stacji bramowej, kamery CCTV.

Funkcja podglądu zapewnia możliwość obejrzenia obszaru w polu widzenia kamery stacji bramowej, jak również obrazu z dołączonej zewnętrznej kamery CCTV. Dzięki takiemu rozwiązaniu otrzymujemy stworzony niskim kosztem prywatny mini-monitoring.

Monitor MT320-CK2 może pracować w systemach jednoabonentowych, jak i wieloabonentowych, obsługujących do 8 użytkowników.

Obudowa monitora MT320-CK2 jest wykonana z estetycznego i trwałego tworzywa. Jej grubość wynosi tylko 18 mm, zatem zmieści się na każdej ścianie. Obudowa monitora występuje w dwóch wersjach kolorystycznych, czarnej lub białej.

Dane techniczne	
Zasilanie	14,5 V_{DC}
Pobór prądu	300 mA
Ekran	7" LCD TFT
Wymiary	160×240×18 mm



Dystrybutor:

Firma Handlowa Wena
Al. Prymasa Tysiąclecia 66
01-424 Warszawa

tel. (22) 817 40 08 tel./faks: (22) 837 02 86
e-mail: wena@wena.biz
http://www.wena.biz

Stacja bramowa SAC50C-CK do systemu wideodomofonowego

Stacja bramowa SAC50C-CK wyposażona jest w kolorową kamerę z przetwornikiem 1/3" CCD. Stacja ma wbudowany szyfrator umożliwiający otwarcie drzwi za pomocą indywidualnego kodu PIN, zamiast tradycyjnego klucza. Jest to bardzo wygodne rozwiązanie szczególnie w zimie, gdy nie musimy „wydobywać" kluczy z kieszeni.

Stacja posiada opcję otwierania drzwi ze środka posesji za pomocą zwykłego włącznika. W tym przypadku nie ma konieczności montowania klamki do otwierania drzwi. Urządzenie umożliwia sterowanie czasem zwolnienia elektrozaczepu. Podtrzymanie czasowe można ustawić w przedziale od 1 aż do 99 sekund.

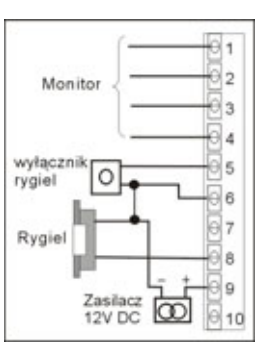
Obiektyw kamery można regulować w pionie i poziomie, umożliwia nam to dostosowanie stacji do naszych indywidualnych oczekiwań.

Obiekt obserwowany przez kamerę jest oświetlony 6 diodami LED, dzięki temu możliwe jest rozpoznanie osób także w nocy. Również korzystanie z klawiatury w nocy jest możliwe dzięki podświetleniu każdego znaku na klawiaturze.

Stacja dedykowana jest do montażu natynkowego. Współpracuje z 4-przewodowymi monitorami serii CK2. Istnieje także wersja 2-przewodowa o symbolu SAC50C-K2.

Obudowa stacji jest odporna na akty wandalizmu, ponieważ wykonano ją z utwardzonego stopu aluminium.

Dane techniczne	
Zasilanie	12 V_{DC}
Przetwornik obrazu	1/3" CCD
Minimalne oświetlenie	0,05 lx
Kąt obiektywu	80°
Podświetlenie	LED światło białe
Wymiary	180×75×45 mm



Dystrybutor:
wena
Firma Handlowa Wena
Al. Prymasa Tysiąclecia 66
01-424 Warszawa
tel. (22) 817 40 08 tel./faks: (22) 837 02 86
e-mail: wena@wena.biz
http://www.wena.biz

Drukarka Fargo HDP5000

Innowacyjna technologia pozwalająca na nanoszenie obrazu na kartę, bez kontaktu karty z głowicą sprawia, że eliminuje się wszelkie niedoskonałości druku występujące w tradycyjnych drukarkach

Fargo HDP5000 jest drukarką retransferową (High definition Printing) gwarantującą najwyższą jakość wydruku na kartach plastikowych. Technologia retransferowa polega na wykonaniu nadruku na nośniku pośrednim (folia transportowa), a następnie naniesieniu obrazu na powierzchnię karty plastikowej. Dzięki tej technologii można drukować całą powierzchnię karty w sposób precyzyjny, uzyskując jakość wydruku niemal porównywalną z metodą offsetową. Dodatkowym atutem technologii retransferowej jest brak jakiegokolwiek kontaktu z głowicą drukarki. HDP 5000 może drukować karty elektroniczne również z naniesionym chipem (układem stykowym) bez pogorszenia jakości. HDP5000 jest obecnie uznawana za jedną z najbardziej zaawansowanych drukarek do kart plastikowych na świecie. Drukarki HDP5000 mają zastosowanie m.in. w instytucjach publicznych, agencjach rządowych, centralach banków, wyższych uczelniach.

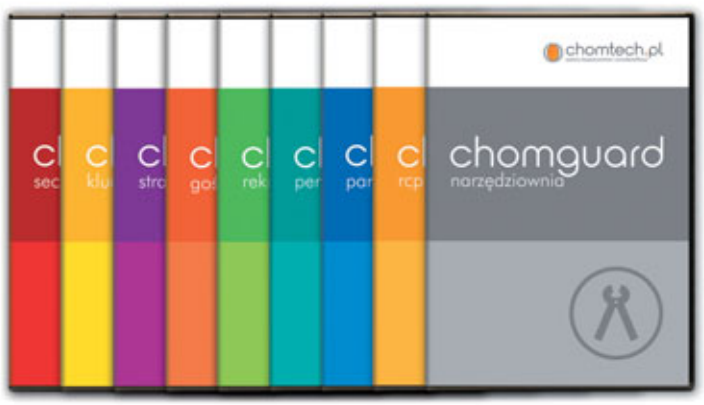
Podstawowe cechy drukarki	
Technologia nadruku	kolor retransferowy
Obszar wydruku	od krawędzi do krawędzi (nadruk całej powierzchni karty)
Komunikacja	port USB, Ethernet
Gwarancja	dożywotnia na głowicę
Rodzaj nadruku	jednostronny lub obustronny
Kodery kart	HID Prox, iCLASS, Mifare, DESFire, HICO, LOCO, ISO7816-1/2/3/4
Druk na kartach	ABS, PVC, PET, PETG, chipowe, magnetyczne
Pamięć wewnętrzna podstawowa	16 MB RAM
Praca w sieci	TAK. Wbudowany serwer wydruków, zarządzanie z dowolnego miejsca w sieci LAN
Oprogramowanie	Chomguard Personalizacja, ASURE ID
Sterownik	Windows XP/Serwer/Vista
Wyświetlacz	LCD z komunikatami w języku polskim
Zabezpieczenia	możliwość drukowania hologramów, znaki wodne, nadruk UV
Materiał do druku	taśma z wałkiem czyszczącym
Prędkość wydruku	38 sekund/karta (wydruk seryjny przy zastosowaniu taśmy YMC)
Napięcie	100-240 V_{AC}, 3,8 A
Gwarancja	2 lata (dotyczy sieci sprzedaży chomtech.pl)
Serwis	chomtech.pl

chomtech.pl®
systemy bezpieczeństwa i autoidentyfikacji

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

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

Chomguard – rodzina aplikacji przeznaczonych do wspomagania systemów bezpieczeństwa



chomguard®

Programy Chomguard są specjalistycznymi aplikacjami dedykowanymi do wspomagania zarządzania systemami bezpieczeństwa w obiektach dowolnego typu.

Aplikacje współpracują z kontrolerami, czytnikami kontroli dostępu, drukarkami do kart plastikowych, kamerami IP, wideorejestratorami, tripodami, furtami stadionowymi, centralami alarmowymi, rejestratorami czasu pracy, urządzeniami biometrycznymi, drukarkami fiskalnymi oraz innymi aplikacjami typu: MRP, CRM, HR stosowanymi do wspomagania zarządzania przedsiębiorstwem.

Programy Chomguard są podzielone na osobne tematycznie moduły które można łączyć w zależności od potrzeb użytkownika (rozwoju firmy) w bardzo zaawansowane systemy wykorzystujące sieci LAN, WAN, przeglądarki internetowe (praca rozproszona). Pracują na jednej bazie danych co oznacza, że wprowadzenie osoby do systemu w jednym module będzie równoznaczne z aktualizacją w pozostałych modułach Chomguard (dostępne silniki baz: Oracle, MSSQL, MySQL, PostgreSQL, Firebird).

- **Chomguard Security:** aplikacja przeznaczona do sterowania i wizualizacji systemów kontroli dostępu, telewizji dozorowej, alarmu, włamania i napadu – w zależności od wersji
- **Chomguard Klucze:** aplikacja przeznaczona do procesu zarządzania kluczami na terenie obiektu w którym występuje duża liczba pomieszczeń
- **Chomguard Strażnik:** aplikacja przeznaczona do weryfikacji osób wchodzących na teren zakładu pracy lub innych miejsc, gdzie występuje konieczność potwierdzenia tożsamości
- **Chomguard Goście:** aplikacja przeznaczona do kontroli obecności osób (gości) przebywających czasowo na terenie przedsiębiorstwa
- **Chomguard Rekreacja:** aplikacja przeznaczona do obsługi klientów obiektów rekreacyjnych z pełnym rozliczaniem usług np. basen, sauna, siłownia, catering itp.
- **Chomguard Personalizacja:** aplikacja przeznaczona do tworzenia projektów kart identyfikacyjnych oraz wydruków
- **Chomguard Parking:** aplikacja przeznaczona do zarządzania parkingiem komercyjnym lub zamkniętym, współpraca z biletерką, czytnikami, szlabanami itp.
- **Chomguard RCP:** aplikacja służąca do rejestrowania i automatycznego rozliczania czasu pracy
- **Chomguard Narzędziownia:** aplikacja służąca do ewidencji i nadzoru nad cennymi zasobami przedsiębiorstwa

chomtech.pl®
systemy bezpieczeństwa i autoidentyfikacji

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ALPOL Sp. z o.o.
ul. Ks. F. Ścigały 10
40-208 Katowice
tel. (32) 790 76 56
Infolinia 0 801 77 77 90
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.
ul. Jutrzenki 105
02-231 Warszawa
tel. (22) 715 41 00/01
faks (22) 715 41 05/06
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 0 801 133 084
faks (22) 843 94 51
e-mail: info@legrand.com.pl
www.legrandgroup.pl

CAMSAT
ul. Ogrodowa 2a
86-050 Solec Kujawski /k. Bydgoszczy
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

Centrum Monitorowania Alarmów Sp. z o.o.
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. (0) 665 380 677
faks (12) 260 13 95

ul. Palacza 127, 60-279 **Poznań**
tel./faks (61) 861 40 51
tel. kom. (0) 601 203 664
e-mail: poznan@cma.com.pl

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

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

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

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

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

DPK System
ul. Piłsudskiego 41
32-020 Wieliczka
tel. (12) 288 14 26 , 288 23 75
faks (12) 278 48 91
e-mail: jablotron@jablotron.pl; biuro@dpksystem.pl
www.jablotron.pl

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

DYSKRET Sp. z o.o.
ul. Mazowiecka 131
30-023 Kraków
tel. (12) 423 31 00
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) 518 84 00
faks (22) 812 62 12
e-mail: sales@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
Adam Piotrowski
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

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

ELTCRAC
Mirosław Gabzdyl, Marek Miękina Sp. J.
ul. Ruciana 3
30-803 Kraków
tel. (12) 292 48 60
faks (12) 292 48 65
e-mail: biuro@eltcrac.com.pl
www.eltcrac.com.pl

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

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

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

EUREKA SOFT & HARDWARE
ul. Rynek 13
62-300 Września
tel. (61) 437 90 15
e-mail: biuro@eureka.com.pl
www.eureka.com.pl

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

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

Przedstawicielstwo we Wrocławiu
tel. kom. 0 693 195 009
e- mail: factor.wr@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
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. (58) 553 67 59
faks (58) 553 48 67
e-mail: info@kolektor.pl
www.kolektor.pl

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

NAPCO POLSKA
ul. Pszona 2
31-462 Kraków
tel. (12) 410 05 10, 410 05 11
faks (12) 412 13 12
e-mail: napco@napco.pl
www.napco.pl

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

OBIS CICHOCKI ŚLĄZAK Sp. J.
ul. Rybnicka 64
52-016 Wrocław
tel. (71) 343 16 76, 341 98 54, 340 01 25
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
Zakład Urządzeń Dozymetrycznych Sp. z o.o.
ul. Glinki 155
85-861 Bydgoszcz
tel. (52) 363 92 61
faks (52) 363 92 64
e-mail: polonalfa@polon-alfa.com.pl
www.polon-alfa.pl

PROFICCTV Sp. z o.o.
ul. Obornicka 276
60-693 Poznań
tel. (61) 842 29 62
faks (61) 842 29 62
e-mail: biuro@proficctv.pl
www.proficctv.pl

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

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

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

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

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

SAWEL
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

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

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

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

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

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

S.M.A.
System Monitorowania Alarmów Sp. z o.o.
ul. Rzymowskiego 30
02-697 Warszawa
tel. (22) 651 88 61
faks (22) 651 88 76
e-mail: sma@sma.biz.pl
www.sma.biz.pl

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

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

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

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

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

ul. Rysia 1A
53-656 **Wrocław**
tel. (71) 711 09 19
faks (71) 711 09 20

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

SONY POLAND Sp. z o.o.
ul. Ogrodowa 58
00-876 Warszawa
tel. (22) 520 25 73
tel. kom. (0) 600 206 173
faks (22) 520 25 77
e-mail: marcin.witkowski@eu.sony.com
www.sonybiz.net

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

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

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

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

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

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

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

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

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

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

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

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

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

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

TAP- Systemy Alarmowe Sp. z o.o.
Os. Armii Krajowej 125
61-381 Poznań
tel. (61) 876 70 88
faks (61) 875 03 03
e-mail: 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 Sp. J.
ul. Słoneczna 4
40-135 Katowice
tel. (32) 258 22 89, 357 19 10, 357 19 20
faks (32) 357 19 11, 357 19 21
e-mail: biuro@tayama.com.pl
www.tayama.com.pl

TECHNOKABEL S.A.
ul. Nasielska 55
04-343 Warszawa
tel. (22) 516 97 97
faks (22) 516 97 91
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
3D	TAK	TAK	–	–	TAK
AAT Holding	–	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	–
ADT Fire and Security	TAK	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	–
Alarmnet	–	TAK	TAK	–	TAK
Alarmtech Polska	TAK	TAK	TAK	–	TAK
Alkam System	TAK	TAK	TAK	TAK	–
Alpol	–	–	TAK	–	TAK
Ambient System	TAK	TAK	TAK	TAK	TAK
Anma	–	TAK	–	TAK	TAK
ASSA ABLOY	–	–	TAK	–	–
Atline	–	TAK	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	–	–	TAK
CBC Poland	TAK	TAK	TAK	–	TAK
CMA	–	–	–	TAK	–
CONTROL SYSTEM FMN	–	TAK	TAK	TAK	TAK
D-2	–	TAK	TAK	TAK	–
D-MAX	–	TAK	TAK	–	TAK
D+H Polska	TAK	TAK	TAK	TAK	TAK
DANTOM	TAK	–	TAK	–	–
DG Elpro	–	TAK	TAK	TAK	–
DOM Polska	TAK	TAK	TAK	–	–
DPK System	–	–	TAK	TAK	TAK
Dyskam	TAK	TAK	–	TAK	TAK
Dyskret	–	TAK	TAK	TAK	TAK
EBS	TAK	TAK	TAK	–	–
ela-compil	TAK	–	TAK	–	TAK
El-Mont	TAK	–	–	TAK	–
Elproma	–	TAK	TAK	TAK	–
Eltcrac	TAK	TAK	TAK	TAK	TAK
Elza Elektrosystemy	–	TAK	–	TAK	TAK
Emu	–	–	TAK	–	–
Eureka	–	TAK	–	TAK	–
Factor Polska	–	TAK	TAK	–	TAK
FES	TAK	TAK	TAK	TAK	TAK
GDE Polska	–	–	TAK	–	TAK
HSA	–	–	TAK	–	–

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Insap	–	TAK	TAK	TAK	TAK
ISM EuroCenter	–	–	TAK	–	–
Janex International	–	TAK	TAK	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK
KATON	–	–	TAK	–	TAK
Kolektor MR	–	TAK	TAK	TAK	–
Laskomex	TAK	TAK	TAK	–	TAK
Legrand Polska	TAK	TAK	TAK	–	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	TAK	TAK	TAK	–
NAPCO	–	TAK	TAK	TAK	TAK
Nuuxe – Radioton	–	–	TAK	–	–
OBIS	–	TAK	–	TAK	–
OMC INDUSTRIAL	–	–	TAK	–	TAK
Petrosin	–	TAK	–	TAK	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	TAK	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	–	–	–
Ramar	–	–	TAK	TAK	TAK
RISCO	TAK	–	TAK	–	TAK
ROPAM Elektronik	TAK	–	TAK	–	–
Satel	TAK	–	–	–	TAK
SATIE	TAK	–	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	–	–
Sony	TAK	–	TAK	–	–
Sprint	–	TAK	TAK	TAK	–
S.P.S. Trading	TAK	–	TAK	–	TAK
STRATUS	–	TAK	TAK	–	TAK
SYSTEM 7	TAK	TAK	TAK	–	TAK
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Tayama	–	–	TAK	–	–
Technokabel	TAK	TAK	–	–	–
UNICARD	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	–	–
Vision Polska	–	TAK	TAK	–	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
3D	–	TAK	–	–	–	–	–	–	–
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, systemy rejestracji gości, karty magnetyczne i zbliżeniowe								
ADT Fire and Security	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Alarm System	TAK	TAK	TAK	–	–	–	–	–	–
Alarmnet	TAK	TAK	TAK	–	–	TAK	–	TAK	–
Alarmtech Polska	TAK	–	–	–	–	–	–	–	–
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Ambient System	TAK	TAK	–	TAK	–	–	–	–	TAK
Anma	TAK	TAK	TAK	TAK	–	TAK	–	–	–
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
ATLine	–	TAK	–	–	TAK	–	TAK	–	–
BOSCH	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
bt electronics	–	–	TAK	–	–	TAK	–	TAK	–
CAMSAT	–	TAK	–	–	–	–	TAK	–	–
CBC Poland	–	TAK	–	–	–	–	TAK	–	–
CMA	TAK	–	TAK	TAK	TAK	TAK	TAK	TAK	–
Control System FMN	TAK	TAK	TAK	–	–	TAK	–	TAK	–
D-2	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
D-MAX	–	TAK	–	–	–	–	–	–	–
D+H Polska	–	–	–	TAK	–	–	–	TAK	TAK
DANTOM	TAK	TAK	TAK	TAK	–	–	–	TAK	–
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
DOM Polska	–	–	TAK	–	–	–	–	TAK	–
DPK System	TAK	TAK	TAK	–	TAK	–	–	–	–
Dyskam	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
Dyskret	TAK	TAK	TAK	TAK	–	TAK	–	TAK	TAK
EBS	TAK	–	TAK	–	–	–	–	–	–
ela-compil	–	–	–	–	–	TAK	–	–	–
El-Mont	TAK	TAK	TAK	–	–	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Eltcrac	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Elza Elektrosystemy	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Emu	akumulatory bezobsługowe do zasilania awaryjnego urządzeń alarmowych								
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
Factor Polska	TAK	TAK	TAK	TAK	TAK	–	–	TAK	–
FES	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
GDE Polska	–	TAK	TAK	–	–	–	TAK	–	–
HSA	TAK	TAK	TAK	TAK	–	–	–	TAK	–

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
ISM EuroCenter	–	TAK	–	–	–	–	TAK	–	–
Janex International	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
Laskomex	–	TAK	TAK	–	–	–	–	TAK	–
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	–	–	–	–	TAK	–
NAPCO	TAK	TAK	TAK	–	TAK	–	–	–	–
Nuuxe – Radioton	–	TAK	–	TAK	–	–	–	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	–	–	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	TAK	–	–	–	TAK	–
Petrosin	TAK	TAK	TAK	–	–	–	–	–	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	konserwacja i serwis zabezpieczeń mechanicznych								
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	TAK	–	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	TAK	TAK	–	–	–	–
RISCO	TAK	–	TAK	–	–	TAK	TAK	–	–
ROPAM Elektronik	TAK	TAK	TAK	TAK	–	–	TAK	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
SATIE	–	–	TAK	–	–	–	–	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
S.M.A.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Schneider Electric Buildings Polska	–	TAK	TAK	–	–	TAK	–	–	–
Sony	–	TAK	–	–	–	–	TAK	–	–
Sprint	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	–	TAK	TAK	TAK	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
SYSTEM 7	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	TAK	–	TAK	–	TAK	–	–	–	–
Tayama	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Technokabel	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
Marek Bladoszewski

Korekta
Paweł Karczmarzyk

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

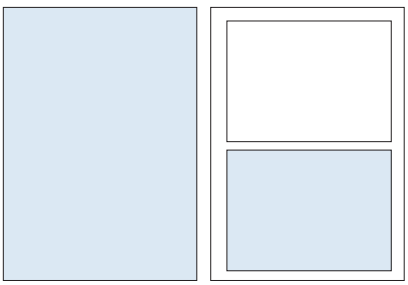
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. (22) 546 0 546
faks (22) 546 0 501

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

Cennik reklam

Reklama wewnątrz czasopisma:

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



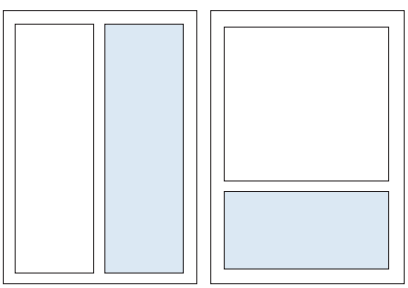
cała strona (200 x 282 mm + 3mm spad)

1/2 strony (170 x 125 mm)

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

Reklama na okładkach:

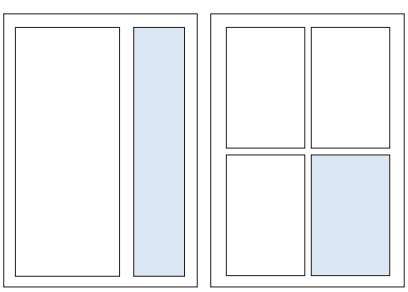
pierwsza strona	indywidualne negocjacje
druga strona	5000 zł
przedostatnia strona	5000 zł
ostatnia strona	5000 zł



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 (22%)

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

Spis reklam

COMMAX
Blooming Life, Home Network

KOMFORT & BEZPIECZENSTWO

Monitor **CDV-71AM**

CDV-71AM

Monitor CDV-71AM

- monitor 7" LCD z podświetleniem LED
- głośnomówiący
- obsługa dwóch wejść
- możliwość podłączenia dodatkowych kamer CCTV
- funkcja PIP (picture-in-picture)
- wbudowany moduł pamięci 128 obrazów
- współpraca z kamerami PAL, NTSC
- możliwość podłączenia dodatkowych unifonów
- menu ekranowe
- zasilanie 230V

DP-4VH

Kamery współpracujące :

DRC-4CG

DRC-4CP

DRC-4CP black

DRC-4CAN

DRC-4CH

CNB TECHNOLOGY Inc.

INTELIGENTNE DOŚWIETLENIE

Kamera box **CCM-21VF**

Kamera box CCM-21VF

- kolorowa kamera dzień/noc
- nowoczesny procesor DSP Monalisa
- przetwornik 1/3" Super HAD II
- bardzo wysoka rozdzielczość 600 TVL w trybie kolorowym
- odsuwany filtr IR – TDN (ICR)
- adaptacyjne podświetlenie Intelligent IR o zasięgu do 25m, 2 diody SR LED (Single Reflective LED), czas bezawaryjnej pracy diod dłuższy nawet o 50%, brak efektu przejaskrawienia i rozmycia obrazu
- czułość 0,05 lx (kolor), 0,005 lx (B/W), 0,00 lx (włączone podświetlenie)
- wbudowany obiektyw o zmiennej ogniskowej 3,8÷9,5 mm DC
- bardzo wygodna regulacja obiektywu
- AGC, SBLC, AWB, DNR, Flickerless, Motion det., Private zone, D/N – regulacja przez OSD
- estetyczną i niebanalna obudowa typu box
- zasilanie 12VDC
- sterowanie po RS-485 pozwala na zdalną zmianę ustawień kamery

Intelligent IR to nowy rodzaj podświetlenia w IR opracowany przez firmę CNB. Eliminuje on efekt przejaskrawienia i rozmycia obrazu gdy obserwowany obiekt zbliża się do kamery. W standardowym podświetleniu jasność świecenia jest stała, dlatego bliskie obiekty są doświetlone tak samo mocnym światłem jak dalekie, co w praktyce może spowodować prześwietlenie obrazu. Intelligent IR steruje jasnością podświetlenia w zależności od odległości od obserwowanego obiektu.

COMMAX

Importer i dystrybutor:

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

CNB TECHNOLOGY Inc.


Potrzebuję
bezpieczeństwa
całej firmy, które
jest niezawodne i
najnowocześniejsze.
HID oferuje rozwiązania
na których możesz polegać. Łączą one bezpieczeństwo
i wygodę użycia
GENUINE
HID
SECURE IDENTITY
HID Global oferuje klientom dodatkowe usługi zapewniające bezpieczną dostawę i niezawodne funkcjonowanie wszystkich produktów już od momentu ich rozpakowania. Ze względu na dożywotnie gwarancje udzielane klientom i funkcje zaawansowanego zarządzania kontrolą dostępu HID Global jest firmą cieszącą się największym zaufaniem w branży. Bliska współpraca z klientami umożliwia spełnienie nawet najwyższych wymagań w zakresie bezpieczeństwa — obecnych i przyszłych.
HID
Odwiedź naszą stronę hidglobal.com/corporatesolutions/Zab