CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 1(71)/2010

ZABEZPIECZENIA

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

W NUMERZE:

- Co w normach piszczy?
- Piksel pikselowi wilkiem
- Postanowienia noworoczne
- Bezpieczeństwo danych w Internecie a VPN

WYDANIE SPECJALNE SECUREX 2010

ZNAMY SIĘ ZE SŁYSZENIA

ambient SYSTEM

Profesjonaliści w zakresie kompleksowych systemów nagłośnienia, public address i dźwiękowych systemów ostrzegawczych.

PROFESSIONAL SOUND

W Ambient System zapewniamy najwyższej klasy rozwiązania nagłośnieniowe dla różnorodnych obiektów tj. hale sportowe, stadiony, teatry, filharmonie itp. Nasi specjaliści wykonują dla Państwa projekty systemów nagłośnieniowych poparte wynikami symulacji i ekspertyzami.

PUBLIC ADDRESS

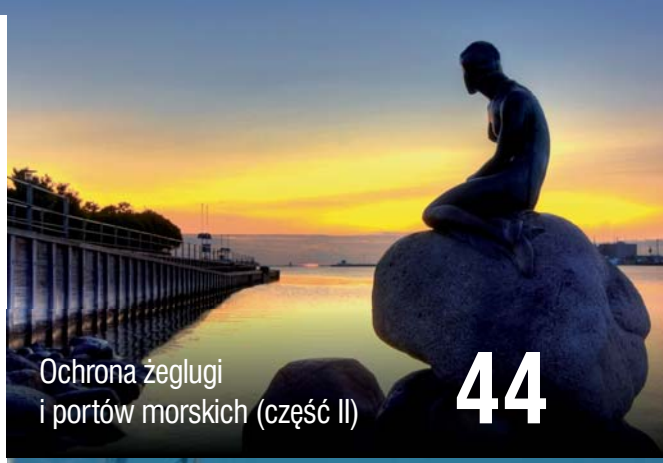
Oferujemy kompleksowe rozwiązania public address wraz z usługami okołosprzedażowymi, począwszy od sporządzenia projektu do stałego serwisu pogwarancyjnego. Proponowane przez nas urządzenia doskonale znajdują zastosowanie w budynkach biurowych, szkołach, szpitalach, portach lotniczych, dworcach itp.

DŹWIĘKOWE SYSTEMY OSTRZEGAWCZE

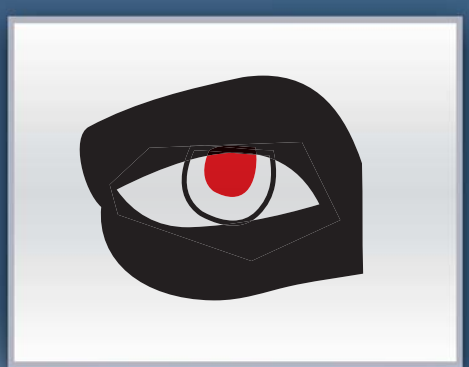
W ciągu ostatnich sześciu lat dostarczamy Państwu nowoczesny i elastyczny w konfiguracji dźwiękowy system ostrzegawczy ABT-Venas wraz z certyfikowanymi głośnikami serii ABT-S. Wspieramy Państwa w zakresie wyboru systemu, technologii, usług projektowych oraz tworzenia symulacji.

ambientsystem.pl

Spis treści



Ośrodek Szkoleniowy Polskiej Izby Systemów Alarmowych zaprasza na kursy i seminaria



OS PISA zaprasza na kursy i seminaria:

– kurs pracownika zabezpieczenia technicznego pierwszego stopnia *Instalowanie i konserwacja systemów zabezpieczeń technicznych* – stopnie 1–4, klasy SA1–SA4,
– kurs pracownika zabezpieczenia technicznego drugiego stopnia *Projektowanie systemów zabezpieczeń technicznych* – stopnie 1–4, klasy SA1–SA4,
– kurs inwestorów systemów zabezpieczeń technicznych,
– kurs pracownika zabezpieczenia technicznego pierwszego stopnia *Montaż, eksploatacja, konserwacja i naprawa urządzeń i środków mechanicznego zabezpieczenia*,
– kurs kosztorysowania systemów zabezpieczeń technicznych,
– kurs ekspertów i doradców w zakresie bezpieczeństwa,
– kursy specjalistyczne,
– seminarium projektowe,
– seminarium instalacyjne.

Seminaria adresowane są do osób, które ukończyły stosowne kursy w innych ośrodkach szkoleniowych.

Absolwenci kursów i seminariów otrzymują dwa dokumenty wystawione **bezterminowo**:

– zaświadczenie o ukończeniu kursu (druk MEN),
– dyplom OS PISA.

Z pełną ofertą szkoleniową Ośrodka PISA można zapoznać się na stronie *www.pisa.org.pl*.

Szczegółowe informacje można uzyskać w OS PISA – tel.: (022) 620 45 57, e-mail: *ospisa@pisa.org.pl*.

Bezpośr. inf. OS PISA

Samsung Techwin Europe dostawcą wszystkich produktów z działu zabezpieczeń Samsung na całą Europę

Od 1 stycznia 2010 r. **Samsung Techwin Europe** przejmuje dostawy i wsparcie techniczne produktów z działu zabezpieczeń Samsung Electronics i Samsung Techwin na terenie całej Europy.

Zmiana ta wchodzi w życie w rezultacie niedawno ogłoszonego transferu aktywów, zasobów ludzkich i zobowiązań pionu zabezpieczeń elektronicznych Samsung Electronics do Samsung Techwin w Korei.

– Decyzja Grupy Samsung o połączeniu tych dwóch działów jest wielkim krokiem w kierunku urzeczywistnienia naszej ambicji stania się czołowym producentem profesjonalnych produktów dla branży security w Europie. Doprowadzi do koncentracji potencjału obu przedsiębiorstw, a w konsekwencji zaowocuje rozwojem bardziej konkurencyjnych urządzeń oraz lepszą obsługą naszych klientów – powiedział **Yong Jun (Jake) Kim**, dyrektor zarządzający w **Samsung Techwin Europe**.

Powyższe działania nie będą miały wpływu na możliwość złożenia przez instalatorów zamówienia na produkty z dotychczasowych asortymentów Samsung Electronics i Samsung Techwin, natomiast istniejące umowy ich dystrybucji zachowają ważność do końca 2010 roku.

– Produkty Samsung Electronics zostaną natychmiast objęte trzyletnią gwarancją Samsung Techwin Europe, a klienci skorzystają z dostępu do jego obsługi technicznej, natomiast inne formy wsparcia zostaną wprowadzone w ciągu najbliższych miesięcy – dodał Kim.

Martin Cottle przeszedł do Samsung Techwin Europe z europejskiego pionu produktów branży security Samsung Electronics i obejmie funkcję kierownika sprzedaży na kraje Europy Północnej i Beneluksu.

Bezpośr. inf. David Solomons
DRS Marketing

securex 2010
program wydarzeń

Międzynarodowa Wystawa Zabezpieczeń SECUREX, której kolejna edycja odbędzie się w dniach od 26 do 29 kwietnia 2010 r. w Poznaniu, jest największą imprezą branży zabezpieczeń w Polsce i w Europie Środkowej.

Podczas targów prezentowane będą najnowsze rozwiązania z dziedziny systemów wykrywania i zwalczania przestępczości, mechanicznych i elektronicznych systemów zabezpieczeń, systemów wizyjnego nadzoru (CCTV) i ochrony mienia.

Nowości

Targi SECUREX są miejscem prezentacji innowacyjnych rozwiązań oraz nowości technologicznych. Podczas ostatniej edycji targów zaprezentowano ponad 180 nowości – produktów debiutujących w ofercie lub po raz pierwszy prezentowanych na targach. Firmy biorące udział w targach już teraz zgłaszają nowe produkty, z którymi można się zapoznać na stronie *www.securex.pl*.

Aktualności branżowe

Na stronie internetowej targów SECUREX będzie można również znaleźć „aktualności branżowe" – informacje o firmach, produktach i wydarzeniach związanych z branżą zabezpieczeń.

Program wydarzeń

Podczas targów nie zabraknie ciekawego programu wydarzeń – konferencji, seminariów i pokazów dla wszystkich chcących poszerzyć swoją wiedzę z dziedziny zabezpieczeń. Ciekawie zapowiada się I Konferencja Zarządzania Bezpieczeństwem Obiektów, organizowana przez Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „POLALARM" oraz Międzynarodowe Targi Poznańskie. Podczas konferencji wybitni specjaliści przedstawią podstawowe pojęcia i definicje z zakresu zarządzania bezpieczeństwem oraz wyjaśnią problemy normalizacji i usług w tej dziedzinie. Omówiona zostanie tematyka zarządzania bezpieczeństwem na rozległych obszarach, w obiektach publicznych specjalnego znaczenia społecznego, w obiektach militarnych. Podkreślone zostaną bezinwestycyjne korzyści wynikające z zarządzania bezpieczeństwem w firmach i zespołach obiektów o szczególnym znaczeniu społecznym, m.in. sportowym, turystycznym, przemysłowym i obronnym. Specjaliści wskażą, w jaki sposób można skorzystać z pomocy fachowców podczas wdrażania systemów zarządzania bezpieczeństwem oraz samodzielnie posługiwać się rozległą wiedzą zawartą w normach europejskich i światowych. Konferencja ma skłonić Polaków do większego zainteresowania się tą tematyką, zwłaszcza w warunkach kryzysu gospodarczego.

Kolejnym interesującym wydarzeniem towarzyszącym tegorocznym targom SECUREX będą Mistrzostwa Polski Instalatorów Systemów Alarmowych organizowane przez Polską Izbę Systemów Alarmowych oraz Międzynarodowe Targi Poznańskie, które mają na celu poszerzenie wiedzy na temat nowych technik i urządzeń służących podwyższaniu poziomu bezpieczeństwa osób i mienia oraz zaprezentowanie sposobów ich wykorzystania w praktyce. Finał mistrzostw będzie miał miejsce na arenie MTP.

Najbliższa edycja targów SECUREX po raz pierwszy odbędzie się w nowoczesnym kompleksie pawilonów 7, 7A, 8, 8A. Dzięki nowej lokalizacji wszystkich wystawców targów SECUREX będzie można znaleźć w jednym miejscu, a zwiedzający dotrą do nich bez konieczności wychodzenia na zewnątrz. Profesjonalnym zwiedzającym ułatwi to rozeznanie się w bogatej ofercie wystawców i odnalezienie w krótkim czasie interesujących ich produktów lub rozwiązań.

W 2008 roku organizowane w cyklu dwuletnim targi SECUREX zgromadziły 220 wystawców z 18 krajów. SECUREX i odbywające się w tym samym czasie targi INSTALACJE i SAWO odwiedziło 28 tys. profesjonalnych zwiedzających.

Program targów SECUREX

- Finał XIII edycji konkursu Polski Mistrz Techniki Alarmowej 2010
  Organizatorzy: Stowarzyszenie POLALARM, Międzynarodowe Targi Poznańskie
- I Konferencja Zarządzania Bezpieczeństwem Obiektów
  Organizatorzy: Stowarzyszenie POLALARM, Międzynarodowe Targi Poznańskie
- Mistrzostwa Polski Instalatorów Systemów Alarmowych
  Organizatorzy: Polska Izba Systemów Alarmowych, Międzynarodowe Targi Poznańskie
- Konferencja dla samorządowców, bankowości oraz dla handlu
  Organizatorzy: Komenda Wojewódzka Policji w Poznaniu, Międzynarodowe Targi Poznańskie

Ponadto w programie:

- Dzień Inwestora
- Dzień Projektanta i Instalatora

Więcej informacji na stronie *www.securex.pl*

Bezpośr. inf. Monika Nawrocka
MTP

Nowy cykl szkoleniowy Bosch Security Systems

Bosch Security Systems posiada bogatą tradycję i doświadczenie w zakresie przeprowadzania szkoleń produktowych. Tylko w 2009 roku zrealizowano ponad 140 szkoleń technicznych i przeszkolono ponad 1300 osób. W lutym firma Bosch rozpoczęła nowy cykl szkoleniowy.

Działalność szkoleniowa Bosch jest skierowana do instalatorów, projektantów, przedstawicieli handlowych, jak również klientów końcowych, którzy są zainteresowani poszerzeniem wiedzy technicznej. Specjalistyczne kursy umożliwiają uzyskanie praktycznych informacji i porad ekspertów dotyczących doboru, instalacji, obsługi i konserwacji produktów oraz systemów firmy Bosch. Szeroka oferta szkoleniowa obejmuje:

– systemy telewizji dozorowej (CCTV), w tym systemy obsługujące protokół IP,
– systemy nagłośnieniowe (PA) i dźwiękowe systemy ostrzegawcze (DSO),
– systemy kongresowe i tłumaczeń symultanicznych,
– systemy sygnalizacji pożarowej,
– systemy sygnalizacji włamania i napadu,
– systemy kontroli dostępu.

Wszystkie kursy są prowadzone przez ekspertów w danej dziedzinie. Katalog szkoleń oraz grafik są dostępne na stronie internetowej www.boschsecurity.pl. Szkolenia odbywają się w wyposażonej w sprzęt demonstracyjny sali szkoleniowej w siedzibie firmy Bosch w Warszawie. Dzięki temu uczestnicy szkoleń mają możliwość praktycznego zapoznania się z obsługą produktów.

W opinii Bosch Security Systems dogłębna techniczna wiedza jest niezbędna, aby prawidłowo oferować, projektować i instalować system zabezpieczeń. Z tego względu kluczowy jest łatwy dostęp do specjalistycznych kursów, a także możliwość uczestniczenia w nich nieodpłatnie. Firma Bosch, jako jedna z nielicznych na rynku systemów zabezpieczeń, oferuje bezpłatne specjalistyczne kursy.

Wiedza teoretyczna oraz praktyczna ekspertów z Bosch Security Systems została doceniona również przez Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej (CNBOP), które zaprosiło firmę do współpracy przy organizacji szkoleń w zakresie systemów sygnalizacji pożarowej oraz dźwiękowych systemów ostrzegawczych. Współdziałając z CNBOP, Bosch przeszkolił ponad 200 osób, natomiast z myślą o tych, którzy pragną poszerzyć wiedzę dotyczącą systemów CCTV wykorzystujących sieci IP, Bosch nawiązał współpracę z firmą ABC Data – Centrum Edukacyjne, jedną z największych i najbardziej doświadczonych firm szkolących w zakresie IT.

Szkolenia Bosch Security Systems są prowadzone zgodnie z systemem zarządzania jakością opartym na normie ISO 9001:2000. Kursy kończą się egzaminem oraz wydaniem certyfikatu. Oprócz możliwości uczestniczenia w szkoleniach, które regularnie odbywają się w siedzibie firmy Bosch, istnieje także możliwość uczestniczenia w prezentacjach i szkoleniach organizowanych przez autoryzowanych partnerów handlowych na terenie całej Polski.

Bezpośr. inf. Bosch Security Systems

Megapikselowe kamery IP Mobotix

wszystko pod kontrolą

Od stycznia 2010 zapraszamy na kolejną edycję szkoleń

Z przyjemnością informujemy, że tegoroczny cykl seminariów poświęcony produktom Mobotix zakończył się sukcesem. W 2009 roku pracownicy spółki Linc przeszkolili blisko 400 osób. W związku z pozytywnym odzewem i żywym zainteresowaniem szkoleniami zdecydowaliśmy się na kontynuację szerzenia wiedzy na temat innowacyjnego monitoringu IP. Od stycznia 2010 r. zapraszamy do uczestnictwa w II edycji cyklu bezpłatnych szkoleń pod hasłem „Megapikselowe kamery IP Mobotix – i wszystko pod kontrolą".

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

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

Sieciowe kamery Mobotix to 6 w 1:

1) rejestrator,
2) transmisja,
3) centrum kontrolne,
4) kamera,
5) obiektyw,
6) obudowa.

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

Wszystkich zainteresowanych uczestnictwem w szkoleniach prosimy o kontakt (*info@mobotix.com.pl* i (lub) 61 839 19 00).

Bezpośr. inf. Linc

Otwarta platforma aplikacyjna
Axis Communications

Axis Communications, lider światowego rynku sieciowych systemów wizyjnych, stworzył platformę pozwalającą na rozwój aplikacji służących do obsługi kamer (Axis Camera Application Platform), dając tym samym początek nowemu poziomowi otwartości w branży bezpieczeństwa. Dzięki otwartej platformie aplikacyjnej każda firma może stworzyć gotowe do pobrania programy, współpracujące z najlepszymi na rynku kamerami sieciowymi i enkoderami wideo marki Axis.

Axis jest pierwszą firmą, która całkowicie otworzyła swoje sieciowe urządzenia wideo na współpracę z zewnętrznymi aplikacjami. – *Mamy tu sytuację zbliżoną do zaistniałej na rynku telekomunikacyjnym, gdzie użytkownicy mają bogatą ofertę aplikacji do pobrania wprost na telefon komórkowy* – powiedział Ray Mauritsson, prezes Axis Communications. – *Jednakże w przypadku rynku zabezpieczeń inny będzie zakres zastosowań aplikacji. Widzimy wielkie zainteresowanie inteligentnym oprogramowaniem wideo, dzięki któremu urządzenia zyskują funkcje związane np. z rozpoznawaniem postaci, śledzeniem, wykrywaniem i zliczaniem obiektów* – dodał Mauritson.

Wizja rozwoju Axis Communications zakłada, że duży asortyment aplikacji zgodnych z urządzeniami Axis będzie łatwo dostępny dla integratorów i użytkowników końcowych. – *Nasza otwarta platforma aplikacyjna pozwoli niezależnym twórcom oprogramowania zaproponować atrakcyjne rozwiązania oferujące dodatkową wartość różnym grupom docelowym. Dzięki temu integratorzy i użytkownicy będą mogli wybrać taką kombinację kamery, enkodera i aplikacji, która najlepiej spełni ich potrzeby wynikające ze specyfiki ich branży, np. transportowej, edukacyjnej lub monitoringu miejskiego* – powiedział Ray Mauritsson.

Tegoroczny raport firmy IMS Research wyraźnie wskazuje na to, że na rynku istnieje duże zapotrzebowanie na oprogramowanie z zakresu analityki wideo. – *Prognozowane roczne tempo wzrostu rynku inteligentnych urządzeń z zakresu bezpieczeństwa i business intelligence wynosi ponad 40% w okresie od 2008 do 2013 r.* – powiedział Niall Jenkins, analityk rynku w IMS Research. – *Udostępnienie przez Axis Communications otwartej platformy aplikacyjnej będzie jednym z najważniejszych czynników wpływających na wzrost i rozwój nowych możliwości w zakresie oprogramowania do analizy materiału wizyjnego na rynku sieciowych kamer i enkoderów wideo* – dodał Jenkins.

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

W sektorze handlu detalicznego niezbędny jest monitoring wizyjny

Bezpieczeństwo, komfort pracy i ograniczenie kradzieży – według sprzedawców detalicznych w Szwecji takie są największe zalety korzystania z monitoringu wizyjnego. 90% właścicieli i pracowników sklepów stwierdza, że wprowadzenie nadzoru wideo przyczyniło się do poprawy bezpieczeństwa obsługi sklepów i spadku liczby kradzieży oraz innych incydentów na terenie obiektów handlowych. Badanie zostało przeprowadzone na zlecenie Szwedzkiego Instytutu Sprzedaży Detalicznej i Szwedzkiej Federacji Handlu przy współudziale firmy **Axis Communications** – światowego eksperta w zakresie systemów monitoringu IP w sektorze handlu.

Wyniki przeprowadzonej ankiety wykazały, że głównym powodem, dla którego właściciele sklepów wdrażają monitoring wizyjny, jest chęć zapobieżenia kradzieżom lub możliwość ich udowodnienia w sytuacji, gdy takie incydenty zaistnieją. Dlatego wielu uczestników badania podkreślało konieczność wykorzystania sprzętu oferującego odpowiednią jakość obrazu i zwracało uwagę na przewagę rozwiązań cyfrowych nad analogowymi.

– *Nadzór wizyjny stał się w ostatnich latach nieodłącznym elementem wyposażenia sklepów, także w Polsce. Nie chodzi tu jedynie o zapobieganie kradzieżom, ale również o inne użyteczne funkcje, które kamery IP mogą zaoferować handlowcom, w tym zliczanie klientów, monitorowanie ich ruchu w sklepie, wskazywanie miejsc, w których się zatrzymują, etc. Takie dane mają istotne przełożenie na wyniki sprzedaży i służą optymalizacji zasobów i procesów. Co więcej, technologia cyfrowej rejestracji obrazu ma tę znaczącą przewagę nad systemami analogowymi, że pozwala łatwo i ekonomicznie gromadzić zarejestrowany materiał o dużej objętości i o jakości umożliwiającej łatwą identyfikację uczestników zajść, a także dokładnie zbadać przebieg zarejestrowanych zdarzeń* – mówi Agata Majkucińska, Key Account Manager w Axis Communications.

Axis Communications ma w ofercie szereg rozwiązań dostosowanych do instalacji w obiektach handlowych. Pod nadzorem kamer IP Axis znajduje się m.in. Douglas Court w Irlandii, uznany w 2008 roku za najlepiej strzeżony obiekt handlowy w Europie.

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

Axis Communications prezentuje nowe modele stałopozycyjnych kamer sieciowych

Firma **Axis Communications** zaprezentowała nową serię stałopozycyjnych kamer sieciowych do instalacji zewnętrznych. Obudowa kamer ma klasę szczelności IP66, co gwarantuje skuteczną ochronę urządzeń przed kurzem, deszczem i śniegiem. Kamery są przystosowane do pracy w ekstremalnie niskich temperaturach, dochodzących do –40°C. Funkcja Arctic Temperature Control pozwoli kamerom uruchomić się nawet w temperaturze poniżej zera. Zasilanie Power over Ethernet znacznie ułatwia instalację i wpływa na obniżenie kosztów.

– *Stałopozycyjne, zewnętrzne kamery sieciowe Axis są wyposażone w specjalną obudowę, dzięki czemu można je zamontować od razu po wyjęciu z pudełka* – mówi Erik Frännlid, dyrektor ds. zarządzania produktami w Axis Communications. – *To bardzo solidne produkty o znakomitych parametrach technicznych, dostosowane do pracy w najbardziej wymagających warunkach, takich jak monitoring na lotniskach, stacjach kolejowych, w nadzorze miejskim i kontroli ruchu ulicznego* – dodał Frännlid.

Nowa seria obejmuje kamery megapikselowe/HDTV, oferujące znakomitą jakość obrazu, obsługę kilku strumieni wideo w formatach H.264 i Motion JPEG, dwukierunkową transmisję dźwięku, inteligentne funkcje wideo, takie jak detekcja ruchu czy dźwięków, funkcję alarmu programowego, ostrzegającą przed próbami modyfikacji ustawień, a także wbudowane gniazda kart pamięci SD/SDHC, pozwalające przechowywać nagrania w samych kamerach. Nowa seria kamer zewnętrznych obejmuje następujące modele:

– kamera sieciowa **AXIS P1343-E**: rozdzielczość SVGA, praca w dzień i w nocy, cyfrowe sterowanie PTZ (obrotem, nachyleniem i przybliżeniem), zdalne ogniskowanie obiektywu;
– kamera sieciowa **AXIS P1344-E**: rozdzielczość 1 MP/HDTV 720 p, praca w dzień i w nocy, cyfrowe sterowanie PTZ (obrotem, nachyleniem i przybliżeniem), zdalne ogniskowanie obiektywu;
– kamera sieciowa **AXIS P1346-E**: rozdzielczość 3 MP/HDTV 1080 p, praca w dzień i w nocy, obiektyw P-Iris (precyzyjne sterowanie przysłoną), cyfrowe sterowanie PTZ (obrotem, nachyleniem i przybliżeniem), równoległe przesyłanie wielu strumieni wideo, zdalne ogniskowanie obiektywu;
– kamera sieciowa **AXIS Q1755-E**: rozdzielczość 2 MB/HDTV 720 p i 1080 i, praca w dzień i w nocy, przybliżenie 10x, autofokus i obsługa głowicy z regulacją obrotu/nachylenia.

Modele AXIS P1344-E, AXIS P1346-E oraz AXIS Q1755-E są zgodne ze standardami SMPTE pod względem rozdzielczości, proporcji obrazu (16:9), odwzorowania kolorów oraz liczby klatek na sekundę.

Dla ułatwienia instalacji kamer w zestawie dostarczany jest od razu uchwyt do montażu na ścianie, osłona przeciwsłoneczna i przewód Ethernet.

Kamery sieciowe AXIS P13-E i AXIS Q1755-E są obsługiwane przez oprogramowanie AXIS Camera Station do zarządzania wideo. Urządzenia są również kompatybilne z wieloma innymi aplikacjami stworzonymi w ramach programu Application Development Partner, prowadzonego przez firmę Axis Communications.

Kamery są dostępne w sprzedaży od stycznia 2010 r.

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

Pierwsza kamera Axis Communications z interfejsem zgodnym z ONVIF

Axis Communications prezentuje **pierwszą kamerę IP z obsługą standardu ONVIF**, czyli ujednoliconego protokołu komunikacyjnego dla sieciowych produktów wizyjnych.

Firma Axis Communications po raz pierwszy udostępniła oprogramowanie w wersji 5.10, umożliwiające obsługę standardu ONVIF, dla stałopozycyjnej, sieciowej kamery kopułkowej AXIS P3301.

– *Wykorzystanie oprogramowania umożliwiającego obsługę standardu ONVIF w kamerze AXIS P3301 to dopiero pierwszy krok zmierzający do zapewnienia otwartości na rynku nadzoru IP. W przyszłości większość sieciowych kamer Axis będzie zgodna ze standardem ONVIF* – mówi Erik Frännlid, dyrektor ds. zarządzania produktami w Axis Communications.

Forum ONVIF zostało powołane w 2008 r. przez firmy Axis Communications, Bosch i Sony w celu stworzenia globalnego standardu interfejsu dla sieciowych produktów wizyjnych. Obecnie ONVIF zrzesza ponad 90 firm, które, według analizy IMS Research, mają pod względem przychodów niemal 60-procentowy udział w rynku sprzętu do sieciowego nadzoru wizyjnego. ONVIF definiuje wspólny protokół wymiany informacji (wykrywanie urządzeń, transmisja wideo, dźwięku, metadanych oraz informacji kontrolnych) między sieciowymi urządzeniami wideo, zapewniając również zgodność operacyjną pomiędzy produktami różnych dostawców. Dzięki forum ONVIF użytkownicy, integratorzy systemów, konsultanci i producenci będą mogli jeszcze lepiej wykorzystać zalety sieciowej transmisji wideo.

– *Dzięki nowej specyfikacji interfejsu użytkownicy i integratorzy projektujący systemy monitoringu zyskają możliwość wyboru spośród najlepszych rozwiązań w danej klasie* – powiedział Erik Frännlid. – *Nasz własny interfejs VAPIX zawsze był otwarty dla zewnętrznych rozwiązań. Dzięki temu sieciowe produkty Axis są dziś kompatybilne z najszerszą na rynku ofertą oprogramowania do zarządzania wideo* – dodał Frännlid.

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

Nowy czytnik **2061 Bluetooth** z serii OMNIKEY

HID Global zakomunikował o wprowadzeniu na rynek nowego czytnika o symbolu **2061 Bluetooth z serii OMNIKEY**. Czytnik pozwala na łatwe i szybkie, ale bardzo bezpieczne zalogowanie użytkownika w sieciach IT agend rządowych, instytucji i firm związanych z ochroną i przechowywaniem tajnych danych w sieciach dzierżawionych.

Obecnie wiele organizacji spotyka się z problemem ochrony danych niejawnych oraz kontroli fizycznego dostępu do tych danych w środowiskach sieci otwartych, bez utrudniania normalnego funkcjonowania pracownikom. Konstrukcja czytnika 2061 Bluetooth z serii OMNIKEY pozwala na łatwe przemieszczanie się osób korzystających z tego systemu i tworzy nową płaszczyznę bezpieczeństwa dla szczególnie mobilnych pracowników.

Nowy czytnik typu *desktop* pozwala na zastosowanie w całym przedsiębiorstwie tych samych kart do logowania się do sieci komputerowych. Poza tym czytnik jest zgodny z ISO 7816-3 oraz EMV 2000 Level 1 i przystosowany do współdziałania z technologiami multikart w dowolnym środowisku Windows.

Bezpośr. inf. Paula Tienza
HID Global
Tłumaczenie: Redakcja

Nowe czytniki HID

przeznaczone do pracy w pomieszczeniach o wysokiej sterylności

HID Global wprowadza do sprzedaży czytniki kart **OMNIKEY 5321 CR USB**. Modele te są wodoodporne, bezkontaktowe, podłączane do komputera poprzez port USB. Dzięki swojej unikatowej konstrukcji umożliwiają zastosowanie ich w kontroli dostępu w środowisku o dużych wymaganiach odnośnie sterylności. Czytnik OMNIKEY 5321 CR USB ma stylową obudowę i jest doskonałym rozszerzeniem asortymentu wyrobów HID, pozwalającym użytkownikom na wykorzystanie bezdotykowych systemów kontroli dostępu do komputerów i sieci IT. Idealnie nadaje się do zastosowania w obiektach produkcyjnych i medycznych (szpitalach). Czytnik spełnia wymagania bezpieczeństwa, takie jak Health Insurance Portability and Accountability Act (HIPAA) w USA dla ośrodków opieki medycznej i szpitali oraz ich dostawców.

Podstawowe cechy czytnika OMNIKEY 5321 CR USB:

– unikatowo zaprojektowana, szczelna obudowa, dostosowana do pomieszczeń o wysokim stopniu czystości i sterylności,
– współdziałanie z kartami HID iCLASS i MIFARE oraz trzema standardami kart zbliżeniowych ISO, łącznie z ISO 14443 A/B, ISO 15693 i Microsoft WHQL,
– standardowe interfejsy do komputerów PC i synchronicznych środowisk API.

Czytnik odczytuje i zapisuje karty zbliżeniowe 13.56 MHz we wszystkich trzech standardach i może wykorzystywać wszystkie używane karty i breloki, takie jak HID iCLASS, NXP MIFARE, DESFire, SMART-MX, ICODE, Texas Instruments TagIT i Infineon my-d. Czytnik odczytuje również karty bezkontaktowe z szybkością do 848 Kbps, zapewniając szybką transmisję danych. Pracuje w systemie HID on the Desktop, zapewniając kontrolę dostępu praktycznie w każdym środowisku.

Bezpośr. inf. Paula Tienza
HID Global
Tłumaczenie: Redakcja

HID Global dostarcza technologię czytnika Multi-ISO, stosowaną w urządzeniach przenośnych Psion Teklogix Ikôn

Technologia czytnika **Multi-ISO** jest obecnie dostępna jako nakładany, bezdotykowy moduł w.cz. dla nabywców nowych komputerów przenośnych (ręcznych) Psion Teklogix Ikôn. Urządzenie zapisu/odczytu integruje przejmowanie danych oraz łączność głosową i danych za pomocą narzędzi bezprzewodowych, włączając w to Wi-Fi, komórkowe 3G HSDPA, Bluetooth i wspomaganą łączność GPS.

Płytki czytników Multi-ISO pozwalają na włączenie tych czytników do dużego asortymentu bezpiecznych rozwiązań bezprzewodowych z **HID Global**, wykorzystywanych w aplikacjach ruchomych płatności bezgotówkowych. Urządzenie Ikôn z płytką czytnika Multi-ISO, dostarczane przez Psion, jest szczególnie przydatne podczas automatycznego pobierania opłat w transporcie, biletowania imprez, w drobnej sprzedaży i w rozwiązaniach mobilnych.

Bardzo bezpieczne urządzenie Ikôn jest wykorzystuje dwa SAM-y, a jego interoperacyjność spełnia wymogi wielu norm przemysłowych, w tym ISO 14443 A/B, ISO 15693, ISO 18000-3 i EPC. Dotyczy to wszystkich etykietek, kart i breloków wg ISO 14443 A/B i ISO 15693. Urządzenie wspomaga również płatności bezdotykowe i jest przygotowane na NFC.

Czytnik Multi-ISO zapewnia również algorytm antykolizyjny do obsługi wielu rodzajów kart.

W celu zapewnienia długotrwałości pracy na baterii w czytnikach Multi-ISO zaimplementowano tryb oszczędzania zasilania. Zwiększa to wygodę użytkownika i minimalizuje czas wyłączenia niezbędny do naładowania baterii.

Ikôn PDA z czytnikiem Multi-ISO był pokazywany na stoisku HID Global (#3H002) na wystawie CARTES & IDentification 2009 w Paryżu w dniach 17–19 listopada 2009 r.

Bezpośr. inf. Paula Tienza
HID Global
Tłumaczenie: Redakcja

Samsung Techwin
wprowadza na rynek nową, wandaloodporną kamerę kopułową

z chipsetem W-5 i funkcją 12-krotnego powiększenia optycznego

Dzięki połączeniu 12-krotnego powiększenia optycznego (oraz 10-krotnego powiększenia cyfrowego), układu DSP W-5, sterowania kamerą przez kabel koncentryczny oraz szeregu zaawansowanych rozwiązań kamera SVD-4700 firmy Samsung Techwin z pewnością zainteresuje instalatorów poszukujących atrakcyjnej cenowo, wandaloodpornej kamery kopułowej.

Kamera SVD-4700 ma klasę szczelności IP66, obudowę z odlewanego ciśnieniowo aluminium i twardą kopułę z poliwęglanu. Została również wyposażona w regulowany, trzyosiowy, dzienno-nocny moduł kamerowy z wbudowanym filtrem podczerwieni, dzięki któremu kamera jest szczególnie użyteczna w warunkach słabego oświetlenia. Urządzenie wyposażono w chipset W-5 Samsung Techwin, czyli nowy, własny układ DSP przeznaczony dla tego typu produktów.

Chipset DSP W-5 sprawia, że kamera SVD-4700 jest bardziej stabilna, a także lepiej realizuje procesy cyfrowej obróbki sygnału. Dzięki temu użytkownicy otrzymują bardzo ostry obraz o wyraźnych kolorach i rozdzielczości 580 TVL. Technologia wydłużonej migawki pozwala kamerze na generowanie obrazów w warunkach oświetleniowych, w których inne dostępne na rynku kamery nie są w stanie ich generować. Ten sam układ wzbogaca kamerę o technologię Samsung Super Noise Reduction trzeciej generacji (SSNRIII), która umożliwia eliminację szumu występującego na obrazie przy niskim oświetleniu, bez efektów zakłóceń lub rozmywania obrazu. Urządzenie wykorzystuje również technologię Samsung Super Dynamic Range (SSDR), która przetwarza ciemne obszary rejestrowane przez kamerę i dopasowuje wzmocnienie w celu wydobycia szczegółów, które normalnie zginęłyby w cieniu.

Użytkownik może obsługiwać funkcję zoomu manualnie lub skorzystać z wbudowanej funkcji wykrywania ruchu. Dzięki niej kamera SVD-4700 automatycznie powiększy określony wcześniej obszar w momencie wykrycia ruchu, a następnie powróci do pozycji początkowej po określonym czasie. Dzięki temu urządzenie sprawdzi się doskonale w zastosowaniach wymagających rozpoznawania poszczególnych ludzi lub pojazdów, a także w obserwacji szerszego obszaru.

Użytkownik może konfigurować wszystkie funkcje zawarte w układzie DSP kamery SVD-4700 poprzez menu ekranowe (dostępne w 14 językach), które można przywoływać i obsługiwać zdalnie, dzięki funkcji sterowania po kablu koncentrycznym. Funkcja ta umożliwia przesyłanie sygnału wizji oraz telemetrii jednym przewodem, dzięki czemu użytkownik może sterować funkcjami PTZ kamery i konfigurować ją za pomocą kompatybilnego rejestratora cyfrowego.

Urządzenie SVD-4700 ma pełną, trzyletnią gwarancję. Może być montowane w sufitach podwieszanych lub bezpośrednio na płaskich powierzchniach sufitów lub ścian. Jest kompatybilne z dużym asortymentem mocowań parapetowych, naściennych, narożnych, słupowych i sufitowych do kamer kopułowych firmy Samsung Techwin.

Bezpośr. inf. David Solomons
DRS Marketing

Nowa kamera kopułkowa firmy Samsung

Pomimo tego, że wyposażona w obiektyw o zmiennej ogniskowej kamera **SID-70** firmy **Samsung Techwin** jest tak mała, że można ją utrzymać w jednej ręce, wyposażono ją w wiele przydatnych funkcji. Ma ona także konkurencyjną cenę. Można ją zamontować praktycznie w dowolnym pomieszczeniu.

– *SID-70 jest kamerą kopułkową do zastosowań wewnątrz obiektów, która spełni oczekiwania najbardziej wymagających klientów* – ocenił Peter Ainsworth, menedżer produktu na Europę firmy Samsung Techwin. – *Naszym konstruktorom udało się wyprodukować kamerę kopułkową, która wykorzystuje najnowsze technologie, a mimo to jest ekonomiczna w każdego rodzaju instalacji CCTV.*

Kamera SID-70 jest wyposażona w zintegrowany filtr odcinający promieniowanie z zakresu podczerwieni i umożliwiający tym samym pracę w trybie całodobowym, trójosiową regulację położenia modułu oraz obiektyw o zmiennej ogniskowej 2,8~10 mm, co zwiększa elastyczność w dostosowywaniu pola widzenia.

Wyposażona w chipset W-5 DSP firmy Samsung Techwin kamera SID-70 wykorzystuje metody redukcji szumów trzeciej generacji – Samsung Super Noise Reduction (SSNRIII). Eliminacja szumów przy słabym oświetleniu nie powoduje „pływania" obrazu oraz jego nieostrości. Technologia Samsung Super Dynamic Range (SSDR) selektywnie rozjaśnia ciemne obszary obrazu w celu uwidocznienia szczegółów. Ponadto kamera posiada funkcję DIS do cyfrowej stabilizacji obrazu oraz eliminacji silnych źródeł światła (np. reflektorów samochodowych) z procesu analizy obrazu.

Chipset W-5 DSP, główny „silnik" asortymentu produktów średniej półki Samsung Techwin, zapewnia kamerze SID-70 większą stabilność i łatwiejsze przetwarzanie obrazu, a w konsekwencji wyraźne, kolorowe obrazy w rozdzielczości 600 TVL. Możliwość 512-krotnego wydłużenia czasu otwarcia migawki umożliwia kamerze generację najwyższej jakości kolorowych obrazów przy minimalnym oświetleniu.

Wszystkie funkcje zawarte w chipsecie SID-70 DSP są dostępne przez menu ekranowe w 14 wersjach językowych. Ustawienia kamery mogą być realizowane także zdalnie, poprzez kabel koncentryczny.

Podobnie jak w przypadku wszystkich innych produktów, firma Samsung Techwin zapewnia bezpłatne zaprojektowanie instalacji, bezpłatną pomoc techniczną i pełną, trzyletnią gwarancję.

Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: Redakcja

Jeszcze większe możliwości rejestratorów firmy Samsung Techwin

Obecnie rejestratory DVR i NVR oraz jednostki rozszerzeń SVS Samsung Techwin zapisują jeszcze więcej materiału wideo.

Wielkość archiwum rejestratorów *stand-alone* (DVR) i sieciowych (NVR) firmy Samsung Techwin została podwojona dzięki wprowadzeniu dysków twardych 2 TB.

– *Dostępność dysków twardych o pojemności 2 TB umożliwia zbudowanie wewnętrznego archiwum mieszczącego do 8 TB danych, pozwalając na znacznie większą elastyczność rejestracji i archiwizacji materiałów wideo pochodzących z wielu źródeł albo rejestracji materiału z tej samej liczby źródeł, ale ze znacznie lepszą jakością obrazu* – skomentował Peter Ainsworth, kierownik produktu na Europę firmy Samsung Techwin. – *Co więcej, nasze zestawy rozszerzeń serii SVS umożliwią zapis do 24 TB z rejestratorów DVR i do 40 TB z rejestratorów NVR, umacniając naszą pozycję na rynku rozwiązań zapisu obrazu do zastosowań profesjonalnych* – powiedział Peter Ainsworth.

Dostępne są też zestawy aktualizujące, umożliwiające łatwą rozbudowę istniejących instalacji telewizji dozorowej posiadających do 2 TB pamięci pojedynczego dysku.

Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: Redakcja

Model	Wej. wideo	Stacja CD/DVD	Maks. prędkość zapisu w rozdzielczości D1	Maksymalna liczba wewnętrznych dysków twardych	Maksymalna liczba zewnętrznych nośników zapisu danych
SNR-6400 (NVR)	64	N/A	1152	4	4
SNR-3200 (NVR)	32	N/A	480	4	4
SVR-3200	32	√	400	4	2
SVR-1680	16	√	400	4	2
SVR-1660	16	√	100	4	2
SVR-1645	16	√	100	2	1
SVR-960	9	√	100	2	1
SVR-945	9	N/A	100	2	1
SVR-940	9	CD	100	2	N/A
SVR-480	4	√	100	2	1
SVR-450	4	CD	25	1	N/A

Tab. 1. Lista modeli DVR i NVR Samsung Techwin, kompatybilnych z dyskiem twardym 2 TB

Metki Sensormatic
wyjątkowa konstrukcja i funkcjonalność

Oferta zabezpieczeń firmy Sensormatic została poszerzona o pięć nowych metek przeciwkradzieżowych, kompatybilnych z technologią Ultra Max. Metki te, dostępne w ofercie ADT Fire and Security, skutecznie chronią drobne przedmioty przed kradzieżą.

Nowe metki Sensormatic zostały zaprojektowane z myślą o skutecznej ochronie m.in. biżuterii, książek, nośników CD/DVD/Blu-ray, a także opakowań z produktami spożywczymi. Przedmioty narażone na kradzież mogą być jeszcze skuteczniej chronione.

Kompatybilność najnowszych metek Sensormatic z technologią Ultra Max zapewnia z jednej strony skuteczność detekcji prób kradzieży, a z drugiej – łatwość i pewność dezaktywacji przy kasie (dzięki temu nabywca, który już zapłacił za towar, nie zostanie zatrzymany przez służby ochrony w innym sklepie, gdyż po dezaktywacji metki bramki przeciwkradzieżowe nie wygenerują dźwiękowego sygnału alarmowego).

Zabezpieczenia te są niezwykle odporne na działanie warunków zewnętrznych, takich jak zmienna temperatura, wilgoć, działanie wody czy nacisk. Wytrzymała konstrukcja umożliwia stosowanie metek w zróżnicowanych warunkach zewnętrznych. Nowe metki Sensormatic charakteryzują się niewielkim rozmiarem, co sprawia, że mogą pozostać niezauważone i nie psują wyglądu eksponowanych towarów. Są dostępne w różnych wersjach (różne konstrukcje i kształty), więc można chronić za ich pomocą dowolne niewielkie produkty.

UltraStrip III Book to metka przeznaczona m.in. do zabezpieczania książek, czasopism i artykułów papierniczych. Bardzo cienka konstrukcja nie powoduje uszkodzenia stron, a specjalny klej nie pozostawia śladu na powierzchni papieru po odklejeniu metki. Zalety te sprawiają, że jest to idealne rozwiązanie zarówno dla małych i dużych księgarni, jak również dla wielkopowierzchniowych punktów handlowych, oferujących m.in. artykuły papiernicze.

Metka **UltraStrip III Low Profile** jest najcieńsza spośród wszystkich metek marki Sensormatic. Służy przede wszystkim do ochrony płyt CD/DVD/Blu-ray. Metkę można nakleić np. wewnątrz pudełka z płytą DVD, pod nośnikiem. Jej mała grubość sprawi, że nośnik nie ulegnie uszkodzeniu, a silny klej uniemożliwi samoistne odklejenie się metki.

W ofercie produktowej ADT dostępna jest także metka **UltraStrip III Hang Tag**. Jest to zabezpieczenie przywieszane. Ten rodzaj metki pozwala na zabezpieczenie wartościowych przedmiotów o nietypowym kształcie, w przypadku których umieszczenie standardowego zabezpieczenia byłoby trudne. UltraStrip III Hang Tag świetnie sprawdzi się np. w przypadku konieczności ochrony drogich zegarków, markowego sprzętu sportowego czy zabawek. Przywieszona do produktu metka wygląda jak kolejna informacja dotycząca towaru (opis, instrukcja użytkowania, cena). Towary są więc skutecznie chronione, a klienci mogą skupić się na zaletach produktu.

Niezwykle ciekawe rozwiązanie dla właścicieli sklepów spożywczych stanowi **UltraStrip III Microwavable**. Metka ta pozwala na zabezpieczenie przed kradzieżą opakowań z produktami spożywczymi, np. z mięsem lub żywnością mrożoną. Tego typu żywność zakupiona przez klientów bardzo często jest rozmrażana lub podgrzewana w kuchenkach mikrofalowych. Metka, stanowiąca element systemu przeciwkradzieżowego, powinna być przez nich odklejona przed włożeniem żywności do kuchenki mikrofalowej, ale nie wszyscy o tym pamiętają. Specjalna budowa metki UltraStrip III Microwavable zapobiega iskrzeniu w mikrofalówce, chroni urządzenia AGD zapominalskich konsumentów przed zabrudzeniem i zniszczeniem. W przypadku długotrwałego działania mikrofali metka ulega roztopieniu.

Jednym z najnowszych rozwiązań firmy Sensormatic jest **NDL**, czyli metka niedezaktywowalna. Zapewnia ona wysoki poziom detekcji prób kradzieży. NDL sprawdzi się doskonale w przypadku konieczności zabezpieczania elementów ekspozycji lub innych akcesoriów znajdujących się w sklepie i nie będących towarem przeznaczonym do sprzedaży. Brak możliwości dezaktywacji i silny klej sprawiają, że jest to bardzo efektywne zabezpieczenie.

Bezpośr. inf. ADT Fire and Security

Mobotix umacnia swoją pozycję
światowego lidera na rynku cyfrowych kamer megapikselowych

Według ostatnich badań *The Word Market for CCTV & Video Surveillance Equipment – 2009 Edition*, opublikowanych przez IMS Research, w 2009 roku firma MOBOTIX, dostawca sieciowych systemów zabezpieczeń charakteryzujących się wysoką rozdzielczością, kontynuowała umacnianie swojej pozycji globalnego lidera na rynku cyfrowych kamer megapikselowych.

– Mobotix nadal ma dobre wyniki, pomimo kryzysu ekonomicznego. W ujęciu globalnym udział firmy w rynku megapikselowych kamer CCTV jest bliski 40%. Mobotix ma wciąż silną pozycję w Europie i kontynuuje zdobywanie rynku w obu częściach Ameryki – skomentował Alastair Hayfield – Research Manager w IMS Research.

Rynek kamer sieciowych ma tendencję wzrostową

W 2009 r. Mobotix odnotował również wzrost udziału w globalnym rynku kamer IP do 9%. Stał się czwartym na świecie dostawcą w tym segmencie. Udział w rynku EMEA (Europa, Bliski Wschód i Afryka) wzrósł o 3,8%, dając firmie drugie miejsce. W Stanach Zjednoczonych firma Mobotix jest w tej chwili w pierwszej dziesiątce dostawców kamer sieciowych pod względem sprzedaży.

– Przez 10 lat, od momentu założenia firmy, Mobotix dąży do osiągnięcia czołowej pozycji na rynku – powiedział dr Ralf Hinkel, założyciel CEO Mobotix. – Będziemy kontynuować umacnianie tej doskonałej pozycji poprzez oferowanie innowacyjnych produktów głównie w obszarze technologii kamer hemisferycznych.

Bezpośr. inf. Linc

Nowa kamera IP Mobotix
już w sprzedaży

Kamera **Mobotix D24M jest już w sprzedaży**. To kolejny przedstawiciel nowej generacji megapikselowych kamer IP firmy Mobotix. Dzięki zastosowaniu wydajnego procesora możliwe jest generowanie obrazu z prędkością 20 obr/s dla maksymalnej rozdzielczości 3 Mpx, a dla wszystkich niższych rozdzielczości uzyskanie pełnej prędkości 25 obr/s. Do rejestracji lokalnej (DVR w kamerze) można wykorzystać karty microSD (o maks. pojemności 32 GB) lub dowolną pamięć Flash USB (nie ma limitu pojemności). Dzięki dużej wydajności kamera D24M jest ekonomicznym rozwiązaniem, oferującym możliwość zbliżenia wybranego fragmentu obserwowanej sceny przy jednoczesnym zapisie całego obszaru tak, że kamera nie ma martwych stref. Należy podkreślić fakt, że model D24M, tak jak wszystkie kamery Mobotix, pracuje całkowicie autonomicznie dzięki zaimplementowanemu w nim kompletnemu oprogramowaniu realizującemu wszystkie funkcje związane z przetwarzaniem obrazu, a także z działaniem kamery jako rejestratora i urządzenia sieciowego.

Warto też zwrócić uwagę na następujące cechy kamery D24M:

– wysoka rozdzielczość i jakość obrazu (kolorowy przetwornik 3 Mpx – 2048×1536);
– rejestracja lokalna na kartach microSD (w standardzie są 4 GB, a maksymalnie 32 GB, co zapewnia ciągły zapis przez ponad trzy dni);
– konstrukcja umożliwiająca pracę na zewnątrz (klasa szczelności IP65, praca w temperaturze od –30°C do +60°C) przy standardowym zasilaniu PoE.

W Polsce autoryzowanym dystrybutorem Mobotix jest firma Linc.

Bezpośr. inf. Linc

Sprzęt konferencyjny firmy Bosch
wykorzystany podczas konferencji klimatycznej w stolicy Danii

W dniach 7–18 grudnia w Kopenhadze odbył się szczyt klimatyczny Narodów Zjednoczonych (COP15). Miejscem spotkań był budynek Bella Center o powierzchni 77 000 m^2. Już pierwszego dnia poinformowano dziennikarzy o tym, że COP15 jest największym tego typu wydarzeniem w historii ONZ. W jego ramach odbyło się ok. 2500 spotkań.

Na konferencji obecni byli przywódcy i inne osobistości z ponad stu krajów, w tym prezydent Stanów Zjednoczonych Barack Obama, prezydent Francji Nicolas Sarkozy, prezydent Egiptu Hosni Mubarak, premier Izraela Benjamin Netanyahu, a także Connie Hedegaard – duńska minister ds. klimatu i energii oraz przewodnicząca konferencji.

W związku z najwyższą rangą wydarzenia zainstalowano najlepszej jakości **sprzęt konferencyjny**. Jego dostawcą została firma **Bosch Security Systems**.

Instalacja zawierała 2500 mikrofonów dla uczestników, głównie DCN NG, sprzęt DCN NG do tłumaczeń symultanicznych, zainstalowany w dwóch dużych salach plenarnych i pięciu mniejszych pomieszczeniach, jak również odbiorniki Integrus, zapewniające odsłuch tłumaczeń. Dodatkowo zainstalowano 50 modułów sterowania centralnego, zewnętrzne zasilacze oraz ekspandery audio.

vDziennikarze przysłuchiwali się debatom w salach plenarnych w mieszczącym 1100 osób centrum prasowym. Umożliwiły to pracujące w podczerwieni bezprzewodowe odbiorniki Integrus i słuchawki firmy Bosch. W kilku pomieszczeniach zainstalowano system dyskusyjny CCS 800 Ultro.

Instalację sprzętu wykonała firma Teletech Conference Communication A/S – jeden z założycieli Congress Rental Network, zajmujący się wypożyczaniem systemów kongresowych, certyfikowany dealer Bosch Security Systems. Prace przygotowawcze i instalacyjne zajęły dwunastu odpowiedzialnym za nie technikom dziesięć dni. Codziennie nad prawidłowym działaniem sprzętu czuwało 40 techników i pięciu kierowników.

Obecność sprzętu konferencyjnego Bosch na szczycie klimatycznym w Danii jest dużym osiągnięciem firmy – zainteresowanie mediów konferencją było ogromne, a hasło „Kopenhaga" należało w tym czasie do jednych z najczęściej wyszukiwanych w największej wyszukiwarce internetowej.

Bezpośr. inf. Bosch Security Systems

System obserwacji w podczerwieni o zasięgu jednego kilometra

GVS1000 – nowa oferta firmy Bosch do ekstremalnych zastosowań

Firma **Bosch Security Systems** wprowadza do sprzedaży GVS1000 – system obserwacji w podczerwieni o najdłuższym dostępnym zasięgu. GVS1000 stanowi zintegrowane rozwiązanie dozorowe, które zapewnia sterowanie obrotem, pochyleniem i zoomem w najbardziej wymagających zastosowaniach oraz dostarcza wysokiej jakości obraz w dzień i w nocy.

System GVS1000 oferuje pełne wykrywanie, klasyfikację, rozpoznanie i identyfikację (DCRI) w całkowitej ciemności oraz najwyższe parametry dozoru nocnego. Dzięki możliwości rozpoznania z odległości jednego kilometra oraz klasyfikacji z odległości 1,2 km GVS1000 zapewnia, nawet w całkowitej ciemności, reprodukcję detali sceny, np. ubrania, numerów czy liczb koniecznych do określenia, czy obserwowana osoba lub obiekt stanowi zagrożenie. Taka jakość obserwacji dostarcza użytkownikowi informacji niezbędnych do podjęcia decyzji dotyczących bezpieczeństwa. Systemy GVS1000 szczególnie sprawdzają się w monitorowaniu portów i nabrzeży, transportu kołowego i lotniczego oraz granic i rozległych obszarów, w których obserwacja na dużą odległość odbywa się przez okrągłą dobę.

System GVS1000 jest wyposażony w zaawansowaną optykę. Obiektywy dalekiego zasięgu z korekcją podczerwieni zapewniają 60-krotny zoom optyczny oraz możliwość obserwacji w nocy na odległość przekraczającą 1,2 km. Dzięki ogniskowej w zakresie 12,5–750 mm lub 25–1500 mm (z włączoną funkcją podwajania) obiektyw współpracuje z przetwornikiem obrazu Dinion XF o wysokich parametrach i zapewnia najwyższej jakości obraz

z dużych odległości zarówno w dzień, jak i w nocy. Zastosowanie innych technologii dozoru nocnego, np. obrazowania termowizyjnego, nie pozwala na uzyskanie takiego poziomu szczegółowości sceny.

System GVS1000 wykorzystuje dwa zestawy aktywnych oświetlaczy podczerwieni do obrazowania dalekiego oraz średniego i (lub) krótkiego zasięgu. Eliminuje tym samym ewentualne zagrożenia związane z systemami podczerwieni opartymi na laserach. Oświetleniem podczerwienią można sterować ręcznie lub automatycznie – przez fotokomórkę.

Dzięki precyzyjnemu mechanizmowi obrotu i pochylenia oraz wytrzymałej, odpornej na warunki atmosferyczne konstrukcji, w skład której wchodzą obudowa do zastosowań zewnętrznych i wycieraczka, system GVS1000 doskonale nadaje się do szczegółowego odwzorowania obrazu w ekstremalnie trudnych warunkach środowiskowych.

Bezpośr. inf. Bosch Security Systems

Nowa seria monitorów LCD z podświetleniem LED w ofercie firmy Bosch

Bosch Security Systems rozszerza swoją ofertę o serię **wysokiej rozdzielczości monitorów LCD z podświetleniem LED**, które współpracują z analogowymi urządzeniami wizyjnymi, cyfrowymi rejestratorami wizyjnymi oraz komputerami PC. Nowa seria, wraz z serią zwykłych monitorów LCD, zastąpi monitory kineskopowe.

Monitory kolorowe, wyposażone w podświetlenie LED, są dostępne w wersjach o przekątnych widocznego obszaru obrazu 8,4" i 10,4". Zapewniają jaskrawość o wartości 400 i 450 cd/m^2, a także bardzo precyzyjną reprodukcję kolorów i wysoki współczynnik kontrastu 600:1 i 700:1. Czas reakcji matrycy czyli czas przejścia pojedynczego piksela matrycy ciekłokrystalicznej ze stanu zapalonego (biały) do stanu zgaszonego (czarny) a następnie ponownie do stanu zapalonego (biały) wynosi odpowiednio 10 i 20 ms. Dzięki temu obrazy są dynamiczne i wyraźne, a efekt smużenia i poświaty dla szybko przemieszczających się obiektów jest zredukowany. Monitory odznaczają się również szerokim kątami widzenia w poziomie i pionie.

Panele z podświetleniem LED eliminują zjawisko pogarszania się jaskrawości w długim okresie eksploatacji monitorów.

Stały poziom jaskrawości umożliwia większy komfort pracy i dłuższą obserwację ekranu bez zmęczenia wzroku. Monitory LED mają ponadto mniejszą masę, są cieńsze i pobierają od 15 do 50% mniej energii niż zwykłe monitory LCD o porównywalnej przekątnej ekranu.

Monitory posiadają dwa wejścia BNC całkowitego sygnału wizyjnego z wyjściami przelotowymi, wejście Y/C (S-video) oraz VGA do współpracy z cyfrowymi rejestratorami wizyjnymi i komputerami PC. Dodatkowo monitor posiada dwa wejścia audio oraz wbudowane głośniki.

Bezpośr. inf. Bosch Security Systems

INBUS 2009
krótka refleksja uczestnika

To było kolejne spotkanie seminaryjne ludzi pracujących na rzecz doskonalenia funkcjonowania automatyki w budynku pod wspólnym hasłem:

5th International Congress on
INTELLIGENT BUILDING SYSTEMS
InBuS 2009
Systemy automatycznego zarządzania
w budynkach inteligentnych

Dwa dni (22 i 23 października 2009 roku), poświęcone odpowiednio systemom automatyki budynkowej (czwartek) oraz rozwojowi inteligentnych budynków i rezydencji (piątek), wypełnione były referatami teoretycznymi, a także prezentacjami realizowanych i już funkcjonujących rozwiązań.

Co mogło i powinno w INBUS-ie najbardziej zainteresować (zdaniem piszącego te słowa):

1) Prezentacja Wydziału Architektury Politechniki Śląskiej, poświęcona metodom oceny sprawności działania inteligentnego budynku w całym okresie jego rozwoju przy odniesieniu się do zmieniającej się koncepcji budynku:
   – zautomatyzowanego (*automated building* – do roku 1985);
   – odpowiadającego na potrzeby (*responsive building* – lata 1986–1991);
   – efektywnego (*effective building* – od roku 1992).

   Choć ostateczne stwierdzenie było następujące: „(…) obiektywna ocena całościowej sprawności działania budynków inteligentnych jest obecnie niemożliwa (…)", wskazano i omówiono szereg metod cząstkowych, pozwalających na miarodajną ocenę poziomu tej inteligencji.

   Szereg pytań uczestników konferencji i żywa dyskusja w kuluarach świadczą najlepiej o ważkości zagadnień poruszonych przez prof. dr hab. inż. arch. E. Niezabitowską i dra inż. arch. D. Masły, a także o potrzebach rynku związanych z jakością i sprawnością wprowadzanych rozwiązań praktycznych.
2) Prezentacja Andrzeja Kołodyńskiego z firmy DeltaCenter, pokazująca teorię sieci BACnet oraz obiekty jej bezpośredniego zastosowania – to dla tych wciąż wątpiących w BMS. Andrzej Kołodyński przypomniał, że funkcjonujemy w społeczeństwie informacyjnym (III fali – wg H. i A. Tofflerów).
3) Prezentacja interfejsu „człowiek – budynek" dla funkcjonującego kompleksowego rozwiązania EIB/KNX, dokonana przez p. Krzysztofa Sasina z firmy ABB i będąca niejako uzupełnieniem prezentacji Andrzeja Kołodyńskiego. Sterownik realizujący menu składające się z ośmiu grup głównych (po 15 pozycji każda) oraz wyświetlający dodatkowe komunikaty ostrzegawcze (wg pozycji) i alarmowe (wspólne i w każdej grupie) jest przykładem przemyślanego i funkcjonalnego łącza „system – użytkownik". Użycie prostych i oczywistych piktogramów, przyporządkowanie grupom odrębnych kolorów (przy zachowaniu czerwieni dla ostrzeżeń i alarmów) oraz możliwość doboru koloru ekranu (czarny/niebieski/szary) składa się na efektywny i przyjazny dla użytkownika panel komunikacyjny.
4) Prezentacja przygotowana przez Uniwersytet Ekonomiczny w Poznaniu, dająca istotną podbudowę teoretyczną dla przewidywanego rozwoju samego interfejsu „człowiek – maszyna". Dr inż. Jacek Chmielewski z Katedry Technologii Informacyjnych w sposób prosty i przystępny opisał teorię zjawisk wynikających z potrzeby automatycznego generowania zintegrowanego interfejsu „człowiek – maszyna" na potrzeby inteligentnego budynku. Elementy odpowiadające tym teoretycznym rozważaniom już funkcjonują w prototypowych instalacjach najnowszych systemów budynkowych.
5) Prezentacja prac zespołu AGH WEAIiE, dokonana przez dra Andrzeja Ożadowicza i pokazująca praktyczne wdrożenie standardów sterowania automatyką budynków dla potrzeb BMS w warunkach realizacji klastra technologii energooszczędnych, poprzez wykorzystanie wdrażanych standardów ISO (tabela poniżej) w połączeniu z nowoczesnymi technologiami.

Protokół	Standard/Certyfikat	Data
BACnet	ISO/IEC 14543-3	Listopad 2006
KNX	ISO/IEC 14543-3	Listopad 2006
Lon-Works	ISO/IEC 14908-1	Listopad 2008

6) Referat Moniki Haduch, przystępnie wyjaśniająca kwestie certyfikatów energetycznych budynków i dająca lepsze zrozumienie problematyki poruszanej w prezentacji Andrzeja Ożarowicza. Zgodnie ze swoim głównym hasłem („najtańszą formą energii jest energia zaoszczędzona") nie tylko objaśniła celowość i potrzebę wprowadzenia w UE certyfikatów energetycznych budynków, ale pokazała wynikające z niego praktyczne korzyści, już osiągnięte w warunkach polskich.

Ponadto godne uwagi były specjalistyczne prezentacje z zakresu bezpieczeństwa (5. panel):

1) Referat Piotra Januszewicza pt. „Wykorzystanie analiz niezawodnościowych w optymalizacji kosztów eksploatacji systemów bezpieczeństwa" dotyczyła wykorzystania parametrów niezawodnościowych urządzeń dla potrzeb obniżenia kosztów eksploatacji inteligentnych budynków.
2) Referat Andrzeja Ryczera pt. „Metoda oceny stopnia bezpieczeństwa inteligentnego budynku", opisujący wykorzystanie metod z zakresu POE (Post-Occupancy Evaluation) oraz istniejące rozwiązania normatywne (normy i specyfikacje techniczne) z zakresu bezpieczeństwa i analizy ryzyka, a także wprowadzający pojęcie stopnia zabezpieczenia inteligentnego budynku (SZIB).

Jak można podsumować całość? To było na pewno potrzebne i interesujące spotkanie. Dzięki niemu uczestnicy mogli nie tylko pogłębić swoją wiedzę teoretyczną, ale także zapoznać się z realizacjami praktycznymi – prototypowymi oraz już wdrożonymi do codziennej praktyki. Ponadto odniesiono się na nim do bieżących zagadnień (certyfikaty energetyczne, problematyka energooszczędności budynków), dając uczestnikom podstawy do własnych przemyśleń i działań.

Opracował: dr inż. Marek Blim
Redakcja

System radarowo-termowizyjny
w ofercie firmy CBC Poland

15 grudnia 2009 r., na terenie konferencyjnym FSO w Warszawie, firma **CBC Poland** zaprezentowała **system radarowo-termowizyjny GANZ Radar Vision**, przeznaczony do wykrywania i śledzenia osób i pojazdów na terenach rozległych. Uczestnicy spotkania mieli możliwość obserwacji działania systemu zainstalowanego na terenie pobliskiego placu manewrowego. System radarowy skutecznie wykrywał i śledził poruszające się na placu osoby i samochody oraz kierował sprzężoną z nim dualną kamerą uchylno-obrotową C-ALLVIEW THERMAL w taki sposób, że widoczny był zwykły i termowizyjny obraz intruza. Po zadymieniu placu świecami dymnymi ujawniła się fantastyczna skuteczność techniki termowizyjnej.

System GANZ Radar Vision może być zastosowany w każdych warunkach pogodowych. Umożliwia detekcję intruza w odległości do 800 m od miejsca instalacji radaru. Przestrzeń skanowana jest z szybkością 360°/s. Poruszające się obiekty są bardzo szybko wizualizowane na mapie. System nadzorujący radar pozwala eliminować fałszywe alarmy, na przykład wywołane przez zwierzęta, oraz tworzyć na mapie terenu strefy, w których wykrycie ruchu nie powoduje alarmu. Jeden radar może obsługiwać pięć kamer C-ALLVIEW THERMAL. Rozległe obszary mogą być nadzorowane przez wiele radarów.

System jest bardzo prosty w montażu i obsłudze. W Polsce system działa na lotniskach w Balicach i w Łodzi. Więcej informacji o systemie GANZ Radar Vision znajdą Państwo na stronie internetowej *http://www.ganzradarvision.pl/*.

Bezpośr. inf. Redakcja

Kolejni absolwenci i… kolejni studenci

21 listopada 2009 r., w Sali Rady Wydziału Mechatroniki (WMT) Wojskowej Akademii Technicznej, odbyło się uroczyste zakończenie VIII edycji niestacjonarnych studiów podyplomowych pn. **Ochrona osób i mienia oraz Bezpieczeństwo lokalne i zarządzanie kryzysowe**, połączone z inauguracją ich IX edycji. Organizatorami studiów są Instytut Techniki Uzbrojenia Wydziału Mechatroniki oraz Studium Ochrony Osób, Mienia i Usług Detektywistycznych CRIMEN II.

Podczas uroczystości dziekan WMT prof. dr hab. inż. Radosław Trębiński i dyrektor Instytutu Techniki Uzbrojenia WMT prof. dr hab. inż. Józef Gacek, w obecności prezesa Zarządu Polskiej Izby Ochrony Sławomira Wagnera, prezesa firmy CRIMEN II mgr. inż. pil. Eugeniusza Zduńskiego oraz wykładowców, wręczyli nowym studentom symboliczne indeksy, a absolwentom – świadectwa ukończenia studiów, a także uhonorowali nagrodami najlepszych. Prymusem VIII edycji studiów podyplomowych został mgr Sebastian Żelisko (średnia ocen 4,82), który wykonał pracę końcową nt. **Ochrona imprez masowych przed terrorystycznym zamachem bombowym**. Ponadto studia ukończyli z wyróżnieniem: mjr mgr Robert Kłonica, mgr inż. Marcin Uliasz, mgr Małgorzata Kiełek, mgr Grzegorz Kowalik, ppłk dypl. inż. Waldemar Szynkowski, inż. Andrzej Wróblewski i mjr mgr Adam Borkowski. VIII edycję studiów ukończyło 24 absolwentów. Gratulujemy!

Bezpośr. inf. Ryszard Woźniak

Przełom czy kompromis?

Podsumowanie konferencji PISA

„Ochrona wartości pieniężnych i bezpieczeństwo banków w świetle nowych wymagań normatywnych dla systemów alarmowych. Przełom czy kompromis?" – pod takim hasłem w dniu 25 listopada 2009 r. odbyła się **konferencja** zorganizowana przez **Polską Izbę Systemów Alarmowych (PISA)**. Miejscem spotkania była siedziba banku Pekao SA – współorganizatora konferencji – przy ul. Żwirki i Wigury 31 w Warszawie.

Prelegentami byli przedstawiciele Grupy UniCredit, Ministerstwa Spraw Wewnętrznych i Administracji, Komendy Głównej Policji, Związku Banków Polskich, Polskiego Komitetu Normalizacyjnego oraz PISA. Słuchaczami były osoby reprezentujące sektor bankowy, firmy świadczące usługi z zakresu bezpieczeństwa fizycznego i technicznego, członkowie organizacji i stowarzyszeń oraz pasjonaci, a więc wszyscy ci, którym nieobce są zagadnienia z branży szeroko rozumianego bezpieczeństwa technicznego.

Kilka minut po godzinie jedenastej (godzina rozpoczęcia konferencji) niemal wszystkie miejsca siedzące przygotowane przez organizatorów zostały zajęte, wobec czego Janusz Szymków – dyrektor Zarządzający Departamentu Bezpieczeństwa Banku Pekao SA – dokonał oficjalnego rozpoczęcia konferencji. Witając gości, zwrócił uwagę na fakt, iż wstąpienie Polski do Unii Europejskiej pociąga za sobą konieczność stosowania się do wytycznych unijnych, standaryzujących rozwiązania i produkty, a rekomendacje płynące z międzynarodowych organizacji normalizacyjnych nie mogą być przez nas ignorowane.

Roberto Pongiluppi – dyrektor Zarządzający Departamentu Bezpieczeństwa Grupy Kapitałowej UniCredit, do której należy m.in. bank Pekao SA – przybliżył uczestnikom spotkania Grupę Kapitałową, jej strategię i cele. Ta globalna korporacja zatrudnia przeszło 166 tysięcy pracowników, ma około 10 tysięcy oddziałów w 23 krajach, którym zaufało już około 10 milionów klientów. Jednym z priorytetów organizacji – w tym Departamentu Bezpieczeństwa – jest integracja pomysłów i rozwiązań występujących we wszystkich lokalnych korporacjach, stworzenie „rodzinnej" grupy.

Kolejna przesłanka, jaką kieruje się Departament, to zintegrowanie z biznesem – wypracowanie wspólnego minimalnego standardu modelu dla procesów bezpieczeństwa produktów i usług, dostosowanych do potrzeb klientów. Bezpieczeństwo ma być bliższe określonemu środowisku biznesowemu dzięki utworzeniu Pionu ds. Wsparcia biznesu w ramach bezpieczeństwa. Grupa nie ma nadmiernie rozbudowanej struktury obszaru bezpieczeństwa – organizacja tożsama jest we wszystkich oddziałach i spółkach Grupy, co powoduje swoiste „zbliżenie terytorialne".

Kluczem do sukcesu jest jedna grupa (ta sama wizja, wartości, cele), jedna marka, jeden Departament Bezpieczeństwa – strategiczny partner dla całej grupy.

Następnie głos zabrał Henryk Dąbrowski – dyrektor Biura PISA, który pokrótce odniósł się do regulacji prawnych i normatywnych w zakresie bezpieczeństwa, a także skierował podziękowania do kierownictwa Banku Pekao SA za stworzenie możliwości współpracy, czego efektem była m.in. konferencja. Zwrócił uwagę na fakt, iż rok 2009 jest rokiem szczególnym, gdyż po pięciu latach obecności Polski w UE zostało przyjęte polskie tłumaczenie normy EN 50131-1:2006 (PN-EN 50131-1:2009). Poprosił kolejnego prelegenta, by odpowiedział na istotne dla branży bezpieczeństwa pytania: „Czy warto dostosowywać normy europejskie do naszych warunków? Jaki jest tego cel? Kto odnosi korzyści?"

Ryszard Grabiec – dyrektor Zespołu ds. Obronności i Bezpieczeństwa Powszechnego (PKN) podjął się udzielenia odpowiedzi na te pytania. Rozpoczął od przedstawienia genezy powstania regulacji normatywnych wspólnych członków Unii Europejskiej, cofając się do czasów Traktatu Rzymskiego ustanawiającego Europejską Wspólnotę Gospodarczą, z której później wyłoniła się UE z jednolitym rynkiem towarów i usług. Wprowadzenie jednolitych norm stało się kluczowym elementem umożliwiającym standaryzację rozwiązań i produktów. Prelegent zwrócił uwagę, iż kraje członkowskie są zobligowane do stosowania się do wytycznych wynikających z dyrektyw unijnych – stosowanie się do zapisów norm jest dobrowolne. Rynek wymusza jednak dostosowanie się do ich zapisów. Każdy szanujący się producent i usługodawca, który dba o swój wizerunek, stara się iść z duchem czasu. Wolna konkurencja sprawia, iż interesariusze – tacy jak producenci towarów, dostawcy usług, użytkownicy, konsumenci, władze publiczne – zwracają się do instytucji normalizacyjnych (w Polsce do PKN), które umożliwiają im opracowanie norm. Wspólne normy to swobodny przepływ towarów i usług na rynku unijnym.

Polska, wstępując do UE, zobowiązała się do stosowania się do dyrektyw unijnych, a co za tym idzie – do konieczności harmonizacji norm. Ryszard Grabiec omówił drogę, jaką trzeba pokonać od momentu ogłoszenia normy europejskiej do czasu wdrożenia jej polskiego odpowiednika.

Przedstawiciel MSWiA Cezary Gawlas – dyrektor Departamentu Zezwoleń i Koncesji – omówił stan prac nad zmianami w Ustawie z dnia 22 sierpnia 1997 r. o ochronie osób i mienia. Poinformował, że już kilkakrotnie dokonywano prób przygotowania projektu nowej ustawy w tym zakresie, ale z powodów organizacyjno-politycznych nie udało się tego planu zrealizować. Obecnie prowadzone są prace zmierzające do wprowadzenia zmian do przepisów wykonawczych, które zdaniem MSWiA najbardziej tego wymagają.

Nadkomisarz Katarzyna Olejnik – naczelnik Wydziału Nadzoru nad Specjalistycznymi Uzbrojonymi Formacjami Ochronnymi Biura Prewencji KGP – omówiła szczegółowo projekt zmian w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie szczegółowych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne.

Z kolei Ryszard Woźniak – doradca prezesa Związku Banków Polskich, sekretarz prezydium Komitetu ds. Bezpieczeństwa Banków przy ZBP – omówił zagadnienia, jakimi zajmuje się ZBP, w zakresie bezpieczeństwa banków w korelacji z nowymi trendami ujawniającymi się w statystykach zdarzeń przestępczych. Rozwijający się rynek operacji bezgotówkowych powoduje, iż coraz mniejsze wartości pieniężne znajdują się w oddziałach banków. Potencjalni napastnicy muszą liczyć się z tym, że, napadając na placówkę banku, mogą nie zaspokoić swoich apetytów. Poszukują oni innych dróg do spełnienia swoich celów.

Andrzej Tomczak i Maksymilian Majerski z PISA podjęli się dokonania porównania zapisów norm PN-93/E-08390 i PN EN 50131. Swoją prezentację rozpoczęli od przedstawienia europejskich i krajowych instytucji normalizujących oraz normalizacji krajowej i europejskiej na przykładzie PN EN 50131. Zdaniem prelegentów nowe normy są korzystne dla użytkowników systemów alarmowych, gdyż pozwalają na bardziej precyzyjny dobór urządzeń do konkretnych wymagań i potrzeb. Podstawowe różnice pomiędzy zapisami norm ujawniają się w klasyfikacji urządzeń i systemów alarmowych: w „nowych" normach klasyfikacja użytkowa pomieszczeń została odseparowana od klasyfikacji klimatycznej. Następnie szczegółowo omówiono różnice pomiędzy zapisami obu norm w zakresie klasyfikacji zagrożeń oraz wymagań dla parametrów technicznych urządzeń w zależności od danej klasyfikacji. Ostatnim elementem prezentacji było porównanie czujników ruchu o różnych parametrach w oparciu o własne testy. Szczególne zainteresowanie wzbudziły pokazy filmowe z zapisami przebiegu testów.

Konferencja nie tylko umożliwiła wysłuchanie prelekcji oraz obejrzenie prezentacji przygotowanych przez mówców – była także wspaniałą okazją do kuluarowych rozmów, nawiązania kontaktów pomiędzy przedstawicielami różnych firm z branży bezpieczeństwa, odświeżenia dawnych znajomości. Tematem przewodnim, który poruszano podczas przerw, były obawy o wzrost kosztów rozwiązań, do których będą musieli dostosować się producenci urządzeń i systemów w kontekście zapisów nowych norm. Z drugiej jednak strony uznano, iż długotrwały okres przejściowy pomiędzy pojawieniem się projektów norm a ich wdrożeniem pozwolił na dokonanie niezbędnych zmian. W szczególności nowe normy nie rewolucjonizują podejścia do budowy urządzeń i systemów bezpieczeństwa, a jedynie uszczegóławiają zapisy w zakresie wcześniej już przyjętych dobrych praktyk, stosowanych przez wielu producentów i projektantów. Pojawiły się również wątpliwości, czy projekt zmian w zapisie „Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie szczegółowych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne" oraz zapisy nowych norm nie wpłyną znacząco na zmianę dotychczasowego podejścia do sposobu zabezpieczenia obiektów. Z jednej strony zasady zabezpieczenia obiektów zostały trochę zliberalizowane. Na drugim końcu szali jest jednak obowiązująca metodyka uzgadniania planów ochrony obiektów, pozostawiająca decydentom – komendantom wojewódzkim policji, z których pełnomocnikami należy uzgadniać plany ochrony obiektów – duże pole do własnych interpretacji i narzucania własnych rozwiązań w zakresie bezpieczeństwa. Każdy z nich może mieć własny pogląd na aspekty zabezpieczenia obiektów. Bez szczegółowych i standaryzujących przepisów w tym zakresie metodyka uzgadniania planów ochrony może być różna, zależna od podejścia każdego z nich...

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

Krzysztof Białek
Redakcja

Warsztaty SAMURAI 2009

na temat wymagań użytkowników Inteligentnych Systemów Wizyjnych

W dniach 5–6 listopada 2009 r. zaproszony przez firmę **ESAProjekt** przedstawiciel stowarzyszenia **POLALARM** Krzysztof Ciesielski (wiceprezes POLALARM) oraz Teresa Karczmarzyk (redaktor naczelny czasopisma *Zabezpieczenia*) wzięli udział w organizowanej przez konsorcjum projektu **SAMURAI** konferencji, która miała miejsce w Londynie. W spotkaniu uczestniczyli także przedstawiciele ESAProjekt – Rafał Dunal (dyrektor handlowy w ESAProjekt) i Maciej Kotok (kierownik projektu w ESAProjekt).

Firma ESAProjekt od lat należy do grona czołowych na rynku polskim firm informatycznych zajmujących się produkcją oprogramowania oraz integracją systemów informatycznych. W swojej ofercie ESAProjekt posiada m.in. nowatorskie rozwiązania służące do inteligentnego monitoringu wizyjnego i autorski system do automatycznego rozpoznawania numerów tablic rejestracyjnych – CARBER. Od kilku lat firma czynnie uczestniczy w programach badawczych Komisji Europejskiej, w ramach których współpracuje z wiodącymi europejskimi ośrodkami naukowo-technicznymi oraz innymi nowatorskimi firmami z branży IT.

Efektem tej współpracy jest obecnie realizowany w ramach 7. Programu Ramowego Komisji Europejskiej projekt SAMURAI (ang. *Suspicious and Abnormal Behaviour Monitoring Using a Network of Cameras for Situation Awareness Enhancement*). SAMURAI ma na celu opracowanie innowacyjnej technologii do ciągłego monitoringu krytycznej infrastruktury obiektów, takich jak lotniska, stacje metra, dworce kolejowe, centra handlowe, szpitale itp., pod kątem podejrzanego i nienormalnego zachowania osób w nich przebywających. Jednym z głównych założeń projektu SAMURAI jest stworzenie inteligentnego systemu nadzoru wizyjnego opartego na sieci rozproszonych sensorów różnego typu, kamer statycznych i ruchomych, odbiorników GPS oraz nasobnych (czyli noszonych „na sobie" przez personel dozorowy) sensorów audio/wideo. Projekt jest realizowany przy współpracy przedsiębiorstw i instytucji naukowych z Europy:

– Queen Mary University of London (Wielka Brytania) – lider projektu,
– University di Vero (Włochy),
– Elsag Datamat (Włochy),
– Waterfall Solutions (Wielka Brytania),
– Borthwick Pignon Solutions (Estonia),
– ESAProjekt (Polska),
– Syndicat Mixte des Transports pour le Phone et l'Agglomeration Lyonnaise (Francja),
– BAA Limited (Wielka Brytania).

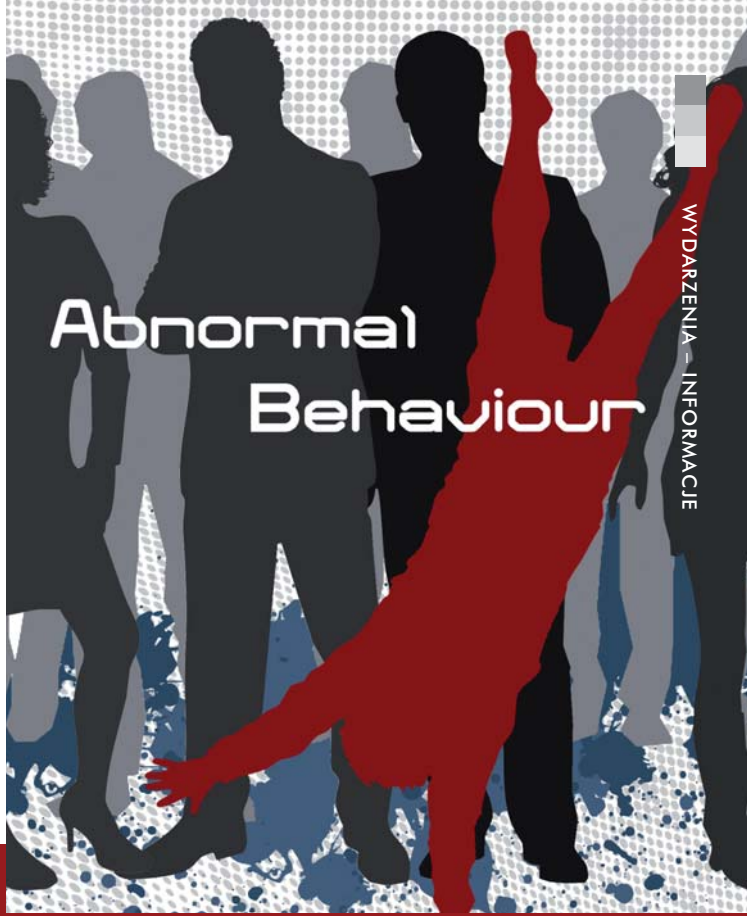
W ramach konsorcjum firma ESAProjekt jest odpowiedzialna za część prac związanych z integracją systemów dostarczanych przez pozostałych członków konsorcjum oraz stworzenie graficznego interfejsu użytkownika, zawierającego m.in. wizualizację 3D monitorowanego obiektu.

Podczas wizyty w Londynie uczestnicy konferencji odwiedzili Queen Mary University of London oraz lotnisko Heathrow należące do BAA (British Airport Authority) – gospodarza całego wydarzenia. Pierwszego dnia odbyły się ciekawe prezentacje

i wykłady. Uczestnicy mieli także jedyną w swoim rodzaju okazję do odwiedzenia laboratoriów QMUL, w których opracowywane są nowatorskie rozwiązania związane z inteligentnym monitoringiem wizyjnym. Drugiego dnia spotkanie miało miejsce na lotnisku Heathrow, gdzie zaprezentowano wybrane rozwiązania z dziedziny zabezpieczeń, które są na nim stosowane, oraz oprowadzono uczestników po otwartej części jednego z terminali pasażerskich.

Po powrocie z Londynu odbyła się prezentacja technologii rozwijanych w ramach projektu SAMURAI podczas XII Forum Monitoringu Polskiego organizowanego przez stowarzyszenie POLALARM. Stowarzyszenie blisko współpracuje z firmą ESAProjekt w ramach projektu SAMURAI i będzie na bieżąco informować o postępach związanych z nim prac.

Rafał Dunal
ESAProjekt



W kilku zdaniach postaram się przybliżyć Czytelnikom sam projekt. Zadanie przede mną niełatwe, bo trudno jest pokrótce opisać to, nad czym pracuje sztab naukowców, ekspertów i specjalistów z różnych dziedzin i co nawet dla inżynierów zajmujących się na co dzień telewizją dozorową czy monitoringiem nie jest proste.

Celem projektu **SAMURAI** jest rozwinięcie i zintegrowanie innowacyjnych, inteligentnych systemów dozoru przeznaczonych do monitorowania aktywności (działań i zachowań) ludzi i pojazdów, zarówno w obrębie ważnych obszarów publicznej infrastruktury, jak i wokół nich. Konsorcjum, które tworzy projekt SAMURAI, składa się z ośmiu przedsiębiorstw („partnerów"), pochodzących z różnych miejsc w Europie, a jego przewodniczącym i koordynatorem projektu jest profesor Shaogang Gong. W celu zapewnienia skutecznego monitoringu wizyjnego projekt SAMURAI oferuje istotne innowacje, które wyróżniają go na tle innych tego typu projektów nie tylko w Unii Europejskiej, ale i na całym świecie.

Do monitorowania podejrzanych i odbiegających od normy, potencjalnie niebezpiecznych zachowań SAMURAI wykorzystuje nie tylko sieć kamer, rozpatrywanych jako sensory stałe, ale i komplementarne źródła informacji, którymi są sensory mobilne. Są to sensory, w które jest wyposażony poruszający się na chronionym terenie personel dozorowy i które dostarczają rozmaitych sygnałów wizyjnych i dźwiękowych. Wszystkie te sygnały – zarówno z sensorów stałych, jak i mobilnych – są przesyłane do centrum operacyjnego w celu dalszej analizy, która przewiduje nie tylko automatyczne rozpoznanie podejrzanego obiektu na podstawie opracowanych z wykorzystaniem zdobyczy różnych dziedzin nauki modeli behawioralnych, ale i działania operatora centrum dozoru, który podejmuje bardziej efektywne decyzje na podstawie różnych źródeł informacji. Jest to przykład synergicznego zbierania danych oraz ich analizowania „w locie", co odróżnia projekt SAMURAI od funkcjonujących dotychczas systemów dozoru, które bazują na przetwarzaniu sygnałów z sensorów.

Zastosowanie połączonych w sieć heterogenicznych sensorów zamiast samych pojedynczych kamer CCTV i połączenie różnych źródeł informacji gwarantuje uzyskanie lepszej wizualizacji chronionych obszarów użyteczności publicznej. Inne istniejące systemy, koncentrujące się na analizie zarejestrowanego obrazu wideo, często niejednoznacznego, używają z góry określonych, sztywnych reguł/norm, nierzadko generując fałszywe alarmy. SAMURAI ma rozwinąć charakteryzowanie zachowań w czasie rzeczywistym i adaptacyjny system detekcji zachowań odbiegających od normy w celu ostrzegania przed zdarzeniami alarmowymi i przewidywania rozwoju zagrożenia, przy znacznym zmniejszeniu liczby fałszywych alarmów.

W imieniu redakcji czasopisma *Zabezpieczenia* dziękuję firmie **ESAProjekt** za możliwość uczestniczenia w konferencji. Dla mnie osobiście była ona doskonałą okazją do poznania kulis tak dużego projektu i ludzi, którzy posiadają ogromną wiedzę i chęć dokonania czegoś szczególnego w dziedzinie bezpieczeństwa, są otwarci na nowe wyzwania, kreatywni, a przy tym niezwykle skromni i sympatyczni. Przyznaję, że ogrom przedsięwzięcia i liczba uczestniczących w nim firm, uczelni i osób jest naprawdę imponująca. Warto podkreślić, że bierze w nim udział także polska firma.

W imieniu swoim i całej redakcji życzę wszystkim zaangażowanym w projekt wielu sukcesów.

Teresa Karczmarzyk

Zapraszam do obejrzenia fotoreportażu
www.zabezpieczenia.com.pl

XII Forum Monitoringu Polskiego

relacja

Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem POLALARM było organizatorem XII edycji Forum Monitoringu Polskiego. W dniach 19–20 listopada, w Centrum Szkoleń i Konferencji GEOVITA w Jadwisinie, licznie przybyli goście mieli okazję zapoznać się z tematyką normalizacji branżowej, monitorowania sygnałów alarmowych i technicznych oraz obiektów ruchomych, z najnowszymi zastosowaniami monitoringu alarmowego i – przede wszystkim – z systemami służącymi do monitorowania infrastruktury IT (co było nowością na tegorocznym forum)

Świat nie stoi w miejscu, dynamicznie rozwijają się nowe technologie, dlatego też organizatorzy, chcąc iść z duchem czasu, dostosowują tematykę forum do oczekiwań słuchaczy. Do wygłoszenia referatów organizatorzy zaprosili najlepszych specjalistów z dziedziny monitoringu, którzy przedstawili najnowsze trendy rozwojowe i najciekawsze problemy pojawiające się w ich pracy zawodowej. Obrady podzielono na dwa bloki tematyczne. Po każdym z nich odbyły się ciekawe, merytoryczne dyskusje. W programie były też prezentacje kilku interesujących rozwiązań technicznych. Do udziału w forum organizatorzy zaprosili przedstawicieli departamentów bezpieczeństwa największych banków, przedstawicieli największych firm ochrony osób i mienia oraz różnych innych branż korzystających z usług monitorowania.

Moderatorami seminarium byli wiceprezesi POLALARM – Andrzej Ryczer oraz Krzysztof Ciesielski, którzy powitali przybyłych gości, a następnie przedstawili program konferencji. Bardzo aktywny był Jerzy Sobstel z Nomy2 – pracujący w komitecie TC 79 w CENELEC[1]. Jego udział w seminarium podniósł jego poziom. Celne riposty i właściwie zadawane pytania doskonale uzupełniały materiał prelegentów. Dzięki temu stał się on doskonałym trzecim moderatorem.

Moim subiektywnym zdaniem moderatorzy tego typu konferencji powinni być znakomicie przygotowani i obeznani z tematem, co niewątpliwie dodaje konferencjom splendoru i przyczynia się do tego, że słuchacze stają się bardziej aktywni. Będąc na wielu podobnych konferencjach (niekoniecznie branżowych), zauważyłam taką oto prawidłowość – im moderator bardziej przygotowany, profesjonalny, tym spotkanie ciekawsze, a uczestnicy aktywniejsi. Wiadomo przecież, że trud włożony w przygotowanie tego typu imprezy powinien zaowocować dużą liczbą słuchaczy, co w rezultacie powinno przełożyć się na spodziewane zyski, bo przecież taki, w efekcie końcowym, jest cel organizatorów. Słuchacze natomiast powinni otrzymać od prelegentów stosowną do wyłożonych środków wiedzę, która w efekcie przełoży się na zwiększenie zysków przedsiębiorstwa. Jeżeli te założenia zostaną spełnione, to można powiedzieć, że cel takich spotkań został osiągnięty.

Konferencję podzielono na dwa panele:

I panel: zagadnienia prawno-organizacyjne

II panel: zagadnienia techniczne w monitoringu alarmowym i wizyjnym

Na wstępie **Krzysztof Ciesielski** wprowadził zebranych w tematykę nowych norm i specyfikacji technicznych w branży technicznej ochrony osób i mienia. Poinformował o wynikach ogłoszonego przez POLALARM konkursu na opracowanie i złożenie uwag do opracowanej przez stowarzyszenie specyfikacji technicznej. Nagrodą było darmowe uczestnictwo w forum. Zdobywcą nagrody za *rzetelne i merytoryczne podejście do tematu* był Włodzimierz Cieślak. Krzysztof Ciesielski przekazał okolicznościowy dyplom i podziękował za cenne, merytoryczne uwagi. Nagrodę w imieniu Wlodzimierza Cieślaka odebrał kolega z firmy Konsalnet, Maciej Nowak.

Następnie Krzysztof Ciesielski omówił kwestie prawno-organizacyjne. Dotyczyły one najważniejszych spraw, jakie dzieją się w naszej branży. Przypomniał, że w tym roku przestała funkcjonować stara norma, tzw. „14", a zaczęła funkcjonować nowa PN-EN50131-1:2009. Mówił także o tym, że aktualnie tłumaczone są nowe arkusze tej normy.

Wyjaśnił, że stowarzyszenie opracowało Specyfikację Techniczną POLALARM, niezależny od normy branżowy dokument, opracowany po to, aby lepiej zrozumieć nową normę. Poinformował, że specyfikacja jest już w końcowej fazie przygotowania i że powstała przy bardzo dużym wkładzie pracy Andrzeja Ryczera oraz innych członków stowarzyszenia. Dokument był omawiany w szerszym gronie, a także przekazany do zaopiniowania Polskiemu Komitetowi Normalizacyjnemu.

Andrzej Ryczer wyjaśnił m.in., że są pewne żelazne prawa, które rządzą tłumaczeniem norm na język polski, np. to, że skrótów angielskich się nie tłumaczy, stosujemy skróty angielskie – takie reguły obowiązują powszechnie w polskiej normalizacji. Cykl opracowywania normy w języku polskim składa się z kilku etapów. Na posiedzeniach Komitetu Technicznego dyskutowana jest treść polskiego tłumaczenia normy i jego zgodność z oryginałem. Zwykle bierze w tym aktywny udział kilka osób. Ustalenie odpowiednich terminów polskich jest wynikiem konsensusu. Istnieje bowiem wiele trudnych pojęć w języku angielskim, nie znanych w języku polskim. Zdarza się, że trzeba stworzyć nowe polskie terminy i, aby zachować maksymalną wierność, sięga się często np. do oryginału normy w języku francuskim lub niemieckim.

Oryginalne normy „Systemy Alarmowe" są opracowywane w Komitecie Technicznym CENELEC TC 79. W ich opracowywaniu bierze udział Komitet Techniczny KT 52,

1) CENELEC to Europejski Komitet Normalizacyjny Elektrotechniki. CENELEC powstał w 1973 roku w wyniku połączenia dwóch wcześniej istniejących organizacji europejskich – CENELCOM i CENEL. Obecnie jest prywatnym stowarzyszeniem technicznym typu „non-profit", działającym w ramach prawa belgijskiego. Siedzibą jest Bruksela. Misją CENELEC jest opracowywanie dobrowolnych norm z zakresu elektrotechniki i elektroniki w celu wspierania rozwoju Jednolitego Rynku Europejskiego/ Europejskiego Obszaru Gospodarczego w sektorze dóbr i usług elektrotechnicznych i elektronicznych. Członkami są Krajowe Komitety Elektrotechniki państw UE i EFTA. W Polsce rolę Komitetu Krajowego pełni Polski Komitet Normalizacyjny – PKN (jest członkiem CENELEC od 1 stycznia 2004 r.). Komitety Krajowe z krajów sąsiadujących z UE, będące członkami lub członkami stowarzyszonymi Międzynarodowej Komisji Elektrotechnicznej IEC, mogą ubiegać się o status afilianta.

Obecnie członkami CENELEC są: Austria, Belgia, Bułgaria, Cypr, Czechy, Dania, Estonia, Finlandia, Francja, Niemcy, Grecja, Węgry, Islandia, Irlandia, Włochy, Litwa, Łotwa, Luksemburg, Malta, Holandia, Norwegia, Polska, Portugalia, Rumunia, Hiszpania, Słowacja, Słowenia, Szwecja, Szwajcaria i Wielka Brytania.

Albania, Bośnia i Hercegowina, Chorwacja, Republika Macedonii, Serbia, Czarnogóra, Tunezja, Turcja oraz Ukraina są obecnie członkami stowarzyszonymi, z perspektywą zostania pełnoprawnymi członkami (afiliantami).

CENELEC, tak samo jak CEN i ETSI, jest uznawany przez władze UE i EFTA za europejską organizację normalizacyjną. Źródło: Wikipedia

przez co możemy mieć wpływ na treść przyszłej normy. Polsce, jako jednemu z najludniejszych i największych krajów Unii (szóste miejsce pod obydwoma względami), przyznaje się w trakcie głosowań 27 głosów, tak jak Hiszpanii (Francji, Niemcom, Włochom i Wielkiej Brytanii – 29, pozostałym państwom – nie więcej niż 13 głosów), zatem możemy mieć znaczący wpływ na wyniki głosowań w procesie opracowywania norm oryginalnych.

W praktyce głosujemy korespondencyjnie, natomiast mamy dość skromny udział w „fizycznym" uczestnictwie w posiedzeniach TC 79 i w pracach jego Grup Roboczych – głównie z przyczyny finansowej (w praktyce bierze w tym czynny udział tylko jeden z członków KT 52, którego uczestnictwo jest finansowane przez jego instytucję macierzystą).

– *Aktywny udział Polaków w normalizacji europejskiej może być możliwy dzięki jego finansowaniu przez instytucje bądź przez nich samych, a takich „bogatych osób", które miałyby ponadto czas i wolę częstych wyjazdów na spotkania grup roboczych i posiedzenia plenarne, jest na razie niewiele* – wyjaśnił Andrzej Ryczer.

Następnie przedstawił prezentację *Znaczenie wymagań normy PN-EN 0131-1:2009 dotyczących systemów alarmowych sygnalizacji włamania i napadu oraz transmisji alarmu – aspekty klasyfikacyjne*. Wykład dotyczył, jak to obrazowo określił, „jakby «zanurzenia» wymagań wynikających z tej normy w ogólnym środowisku normalizacyjnym «Systemów Alarmowych» ze zwróceniem uwagi na pewne szczegółowe aspekty". O tym, że tłumaczenie normy się pojawi, było wiadomo od dawna (norma ta, zgodnie z obowiązującymi zasadami, została przyjęta w Polsce w języku oryginału, zaraz po jej ustanowieniu w TC 79, i miała od razu taki sam status, jak norma przetłumaczona – tzn. można było się na nią powoływać i z niej korzystać). Tłumaczenie pojawiło się zbyt późno, ale, jak powiedział A. Ryczer, „wynikało to z różnych przyczyn, może nawet z dość długiego, ze względu na znaczenie normy, opracowywania tekstu polskiego i zatwierdzania tłumaczenia".

Jednym z celów prezentacji było przedstawienie przyjętych w PN EN 50131-1 zasad klasyfikacji systemów alarmowych na tle innych wymagań normalizacyjnych, tzn. wymagań norm pokrewnych z grupy norm „Systemy Alarmowe". Drugim celem było wskazanie na konieczność opracowania tłumaczenia interpretacji tych zasad. Pojawiły się bowiem trzy ważne dokumenty:

– interpretacje odnoszące się do całej grupy norm „Systemy Alarmowe", I&HAS (*Intruder&Hold-Up Systems*), ACC (*Access Control*), CCTV oraz innych systemów,
– interpretacje dotyczące wyłącznie normy PN EN 50131-1 (o objętości blisko połowy tekstu dokumentu głównego; termin zatwierdzenia nowej wersji przez TC 79 wyznaczono na lipiec 2010 r.),
– poprawki do tekstu oryginalnego PN EN 50131-1.

Zdaniem Andrzeja Ryczera najlepiej byłoby wydać dokument jednolity, który zawierałby wszystkie te trzy dokumenty: normę PN EN 50131-1, poprawki i interpretacje. Nie ma takiego dokumentu międzynarodowego. Być może KT 52 (jeden z największych komitetów w PKN) wystąpi z taką inicjatywą. Interpretacje będą opracowane w języku polskim w pierwszej połowie 2010 roku i zatwierdzone równolegle z zatwierdzeniem ich wersji międzynarodowej.

Po długim wprowadzeniu dokonano prezentacji składającej się z dwóch części:

Część I

1) Wprowadzenie – miejsce normy PN EN 50131-1 w grupie norm „Systemy Alarmowe".
2) Zasady przyjętej klasyfikacji na tle innych wymagań normalizacyjnych.

Część II

3) Omówienie treści normy.
4) Wybrane wymagania dot. zasad monitorowania systemu alarmowego.
5) Transmisja alarmu według normy.
6) Pilna konieczność opracowania zasad oceny ryzyka.
7) Podsumowanie – problemy interpretacyjne.

Prelegent przedstawił zasady klasyfikacji przyjęte w normach „Systemy Alarmowe":

– stopień zabezpieczenia I&HAS (obecnie, zgodnie z normą, zaleca się stosować termin „stopień zabezpieczenia", a nie „klasa ochrony"),
– klasa rozpoznania SKD,
– stopień zabezpieczenia systemu CCTV (w TC 79 został przygotowany projekt nowej normy europejskiej),
– typ konfiguracji systemu łączonego i zintegrowanego.

W normie PN-EN 50131-1:2009 I&HAS – Część 1: Wymagania systemowe zależnie od poziomu ryzyka (który ma być redukowany przez zastosowanie systemu) mówi się o czterech stopniach zabezpieczenia:

– 1 – ryzyko małe – włamywacze niedoświadczeni,
– 2 – ryzyko małe do średniego – włamywacze z ograniczoną znajomością I&HAS (ang. *Intruder and Hold Up Alarm Systems*),
– 3 – ryzyko średnie do dużego – włamywacze biegli,
– 4 – ryzyko wysokie – bezpieczeństwo jest najważniejsze, możliwe jest szczegółowe zaplanowanie włamania/napadu i zamiana elementów systemu.

W normie dotyczącej systemów kontroli dostępu (PN-EN 50133-1:1996 + AC:1998 + A1 2002: Systemy alarmowe – Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia – Część 1: Wymagania systemowe) stosuje się „klasy rozpoznania" i „klasy dostępu":

– klasa rozpoznania 0 – brak rozpoznania pozytywnego – rozpoznanie opiera się na prostym zapytaniu o dostęp bez podania tożsamości (przycisk, styk, detektor ruchu),
– klasa rozpoznania 1 – informacja zapamiętana – rozpoznanie opiera się na haśle, osobistym numerze identyfikacyjnym PIN itp.,
– klasa rozpoznania 2 – identyfikator lub biometryka – rozpoznanie opiera się na danych z identyfikatora lub biometrycznych (karty, klucze, odciski palców, siatkówka oka itp.),
– klasa rozpoznania 3 – identyfikator lub biometryka oraz informacja zapamiętana.

Klasy dostępu w PN-EN 50133-1:1996 dotyczą zależności praw dostępu od siatki czasu:

– klasa dostępu A – ani nie stosuje się siatki czasu, ani nie rejestruje się transakcji uzyskiwania dostępu,
– klasa dostępu B – wykorzystuje się funkcje siatki czasu oraz rejestruje się zdarzenia,
– klasa B zawiera podklasę Ba z funkcją siatki czasu, bez rejestracji zdarzeń.

Projekt normy dotyczącej systemów CCTV

TC 79 przygotowuje projekt normy dotyczący wymagań systemowych CCTV prEN 50132-1:2007 *Alarm systems – CCTV surveillance systems for use in security applications – Part 1: Systems requirements*, na którą wielu projektantów i instalatorów czeka od dawna. Jest to dość obszerny dokument, w którym zawarto dużo definicji dotyczących systemów CCTV (ok. 50% objętości). Trudno powiedzieć, jak długo będzie trwało ustanowienie normy.

W normie wprowadzono (po raz pierwszy w normalizacji systemów alarmowych!) cztery stopnie zabezpieczenia systemu CCTV, tzn. starano się dostosować ich strukturę do poziomu ryzyka:

– stopień 1 – ryzyko małe – nadzór CCTV sytuacji o małym ryzyku; system CCTV nie ma zabezpieczenia przed sabotażem i nie wymaga się, aby podstawowe funkcje były monitorowane;
– stopień 2 – ryzyko małe do średniego – system CCTV ma proste zabezpieczenia przed sabotażem i nie wymaga się, aby podstawowe funkcje były monitorowane;
– stopień 3 – ryzyko średnie do wysokiego – system CCTV ma proste zabezpieczenia przed sabotażem i wymaga się, aby podstawowe funkcje były monitorowane w prosty sposób;
– stopień 4 – ryzyko wysokie – system CCTV ma mocne zabezpieczenia przed sabotażem i wymaga się, aby podstawowe funkcje były monitorowane w sposób ciągły.

Ostatnim z omawianych przez Andrzeja Ryczera dokumentów była Specyfikacja Techniczna CLC/TS 50398:2009 *Alarm systems – Combined and integrated alarm systems – General requiments.* Zwrócił on uwagę na „stopnie zabezpieczenia" opisane w tym dokumencie.

Jest to nowy dokument (z roku 2009), który dotyczy łączonych i zintegrowanych systemów alarmowych. Klasyfikacja wynika w pewnym sensie ze skutków łączenia i integrowania aplikacji (w dokumencie nie mówi się wprost o „stopniach zabezpieczenia").

Jak aplikacje wpływają na siebie? Czy w przypadku sabotażu np. w I&HAS uszkodzony zostanie również połączony z nim system CCTV? Analizowane są szkodliwe wpływy jednych systemów (aplikacji) na inne. Wyróżniono trzy podstawowe typy konfiguracji zintegrowanych systemów alarmowych:

1) typ 1 – bezwzględny brak szkodliwych wpływów – dołączenie do wspólnych środków,
2) typ 2A – brak szkodliwych wpływów – wspólne łącza transmisyjne, wspólne środki, redundancja,
3) typ 2B – wspólne łącza transmisyjne, wspólne urządzenia i wspólne środki – pojedyncze uszkodzenie w jednej aplikacji może mieć szkodliwy wpływ na aplikacje alarmowe.

Jak dobrać stopień zabezpieczenia systemu alarmowego? Bez dokładnej interpretacji norm europejskich jest to trudne – brakuje jednolitej klasyfikacji. W podsumowaniu swojego wykładu Andrzej Ryczer wykazał, że tylko w dwóch z czterech norm (jedna jest w stadium projektu) zastosowano taką samą klasyfikację stopni zabezpieczenia (I&HAS i CCTV). Ponadto zwrócił uwagę na fundamentalny problem – nie można poprawnie dobrać stopnia zabezpieczenia systemu alarmowego, jeżeli uprzednio nie przeprowadzi się oceny ryzyka – struktura systemu musi

być zawsze dostosowana do poziomu ryzyka – i to jest ideą klasyfikacji w rozważanych normach.

Jak to zrobić? Są pewne metody tablicowe (które były i są stosowane, np. w VDS i innych normach europejskich, gdzie stopień zabezpieczenia przypisano określonemu typowi działalności w danym obiekcie). KT 52 będzie się starał o ewentualną publikację zasad podanych w tych dokumentach. Komitet może podjąć działania wspomagające i opracować np. bazującą na pewnych formalnych wymaganiach Specyfikację Techniczną, która pomoże dobierać stopnie zabezpieczenia adekwatne do poziomu ryzyka. Aby uzasadnić potrzebę takich działań, Andrzej Ryczer przedstawił w prezentacji ważniejsze zagadnienia związane nie tylko z ostatnio przetłumaczoną normą PN EN 50131-1, ale także z jej „siostrzanymi" normami dotyczącymi telewizji i kontroli dostępu oraz systemów zintegrowanych i łączonych.

Wdrożenie systemu bezpieczeństwa informacji ISO 27001 w ACO to temat kolejnego referatu, który wygłosił **Andrzej Wójcik**. Stwierdził on, że aby funkcjonować w nowoczesnym biznesie Europy lub podjąć działania z firmami, które pewne standardy uznają, np. z jednostkami budżetowymi, gdzie ISO27001 jest już zalecane, konieczne jest wdrożenie systemu bezpieczeństwa informacji ISO 27001. W Europie system ten jest już standardem. Przypomniał, że „informacja jest obecnie niezwykle cennym i pożądanym dobrem, a jej wartość zależy od tego, kto, kiedy i w jakim celu jej potrzebuje". Prelegent starał się uświadomić słuchaczom, że zbyt rzadko rozpatrujemy ją w kategoriach towaru i nie pamiętamy, że to właśnie ją najłatwiej jest upłynnić. Dlatego należy dołożyć wszelkich starań, aby ją chronić.

Oto kilka podanych przez Andrzeja Wójcika przykładów organizacji szczególnie narażonych na ryzyko związane z utratą informacji:

– banki, zwłaszcza internetowe, i inne instytucje finansowe,
– firmy ubezpieczeniowe,
– firmy świadczące usługi outsourcingowe i firmy z nich korzystające,
– firmy które technologicznie sterują procesami technologicznymi,
– firmy stosujące rozległe sieci teleinformacyjne,
– firmy o dużym znaczeniu dla gospodarki narodowej,
– firmy i instytucje silnie zależne od społecznej akceptacji,
– centra przetwarzania danych,
– centra zarządzania kryzysowego i alarmowe, np. ACO.

Andrzej Wójcik przypomniał o wymaganiach prawnych, wynikających z odpowiednich ustaw, rozporządzeń i wymagań kontraktowych, nakładających na kierownictwo organizacji obowiązek podjęcia działań o charakterze organizacyjno-technicznym w zakresie ochrony informacji.

Zaznaczył, że system bezpieczeństwa jest jednym z narzędzi kierowania firmą, które ma wspierać, a nie utrudniać działanie przedsiębiorstwa. Przypomniał, jak ważna jest ocena ryzyka, a także to, że ryzykiem trzeba zarządzać, czyli eliminować pewne niebezpieczeństwa z zachowaniem akceptowalnego poziomu kosztów. System bezpieczeństwa informacji uwiarygodnia nas w oczach naszych klientów. Obecnie już wiele firm i korporacji nie podpisze umowy z inną firmą, jeżeli jedna z nich nie wdrożyła ISO27001. Decyzja o wdrożeniu systemu powinna być strategiczna, bo wpływa on na funkcjonowanie całej organizacji, jest jednym z narzędzi w procesie zarządzania firmą. W procesie

biznesowym ma on wspierać zarządzanie firmą, a nie utrudniać je, powodować ograniczenia. Norma znajduje zastosowanie we wszystkich organizacjach, nawet tych, które nie mają systemów teleinformatycznych. Można ją zastosować na przykład tylko w jednym dziale przedsiębiorstwa. System i jego funkcjonowanie trzeba ciągle doskonalić i sprawdzać, np. poprzez audyt. Należy planować, wdrażać i rozwijać systemy zarządzania bezpieczeństwem informacji (ZSBI), aby odpowiednio i skutecznie zabezpieczać realizowane procesy biznesowe. Proces wdrażania, a później certyfikacji, może trwać od pół roku do około trzech lat, zależnie od zakresu i obszaru wdrożenia, jak twierdzi Andrzej Wójcik, a cena, jak sam powiedział, „nie kładzie przedsiębiorstwa na łopatki". Korzyści to przede wszystkim usprawnienie biznesu, wzrost konkurencyjności firmy oraz jej wizerunek jako zaufanego partnera w biznesie.

Andrzej Starnawski – kolejny prelegent – omówił uwarunkowania Specyfikacji Technicznej POLALARM. Przedstawił w skrócie burzliwą historię powstawania tego dokumentu oraz jego stan obecny.

Omówił także kilka ważniejszych kwestii związanych z normalizacją. W aktach prawnych (rozporządzeniach) nie powinno się przytaczać nazw norm, co wynika z ogólnej zasady dobrowolności stosowania norm. Poza tym treści norm zmieniają się – są różne w różnych wydaniach – lub normy są uchylane. W praktyce legislacyjnej wygląda to różnie.

Mamy do czynienia z regulowanym obszarem oceny, który wyznaczają wymagania dyrektyw UE oraz krajowe regulacje prawne.

Drugim obszarem jest obszar oceny dobrowolnej, na którym mogą funkcjonować różnego rodzaju dokumenty potwierdzające dobrowolną ocenę wyrobu. Jednostki akredytowane mogą wystawiać dokumenty na równi z jednostkami, które akredytacji nie mają.

W obszarze dobrowolnym można dokonać oceny zgodności wyrobów z normami, a także z innymi wymaganiami, takimi jak kryteria, wymagania branżowe itp.

Andrzej Starnawski przypomniał, że wymagań branżowych nie można nazywać dokumentami normatywnymi, gdyż nie mają z tymi dokumentami nic wspólnego. Branża reguluje pewne sprawy według własnej dobrej praktyki, a rynek to akceptuje lub nie (albo akceptuje to część rynku). Jest w tym temacie całkowita dobrowolność. W naszej branży nie było chętnych do zajęcia się stworzeniem takiego dokumentu, bo wymaga to włożenia weń pewnego wysiłku intelektualnego, a ludzi chcących zrobić coś więcej dla wszystkich jest niewielu. Trzeba mieć duszę społecznika, a o to zawsze było trudno w naszym środowisku. Dopiero fakt uchylenia „14" spowodował energiczne działania. Podjął je POLALARM. W przeszłości mówiło się o tym, że nad takimi wymaganiami można by popracować wspólnie, bez względu na podziały, ale do takiej współpracy nie doszło, dlatego opracowano je pod patronatem POLALARMU. W ten sposób powstała Specyfikacja Techniczna POLALARM.

Andrzej Starnawski wyjaśnił, że nie można mówić „Specyfikacja Techniczna", odrzucając słowo „POLALARM", bo wtedy sugeruje się, że jest to dokument normatywny o charakterze specyfikacji technicznej, opracowany przez CEN czy CENELEC, gdyż organizacje te oprócz norm wydają również tego typu dokumenty. Projekt normy, który nie uzyska akceptacji, a jest zbiorem wartościowych wymagań, staje się specyfikacją techniczną – czy to CEN, czy CENELEC.

Oczywiście los takiej specyfikacji za jakiś czas się odmienia, gdyż następuje kolejne podejście i robi się z niej normę.

Specyfikacja Techniczna POLALARM to po prostu wymagania branżowe POLALARM. Andrzej Starnawski poinformował, że na stronach WWW stowarzyszenia POLALARM zostanie zamieszczona „wyczyszczona" Specyfikacja Techniczna POLALARM z naniesionymi zmianami uzgodnionymi z PKN. Rynek i instytucje zdecydują, czy ta specyfikacja się przyjmie. Wymagania odnoszące się do systemów SWiN jako całości, a także do stosowanych w tych systemach urządzeń, obecnie są zawarte w:

– stosownych normach europejskich PN-EN,
– Specyfikacji Technicznej POLALARM,
– uchylonej/zastąpionej (ale możliwej do stosowania) poczciwej „14".

To rynek, jaki tworzą zleceniodawcy i zleceniobiorcy, dokona selekcji i zadecyduje, które z wymienionych wymagań będzie dominować jako punkt odniesienia w realizowanych systemach SWiN. Na wybór będzie miała wpływ ogólna sytuacja ekonomiczna.

W tej sprawie głos zabrał Krzysztof Serafin, który wyraził swoje ubolewanie, że specyfikacja w ogóle nie opisuje systemów dozoru telewizyjnego i kontroli dostępu. Stwierdził między innymi, że stracona została kolejna okazja do wprowadzenia szerszej definicji systemów alarmowych do specyfikacji. Zwłaszcza przy określaniu klasy SA3 warto było poświęcić więcej uwagi tym systemom, a nie tylko systemom sygnalizacji włamania i napadu. Klasa SA3 zniknęła z nowej, aktualnej normy, a została w rozporządzeniu, które jest nadal obowiązujące. Specyfikacja powinna określić, jaki kompleksowy system alarmowy należy zastosować, aby odpowiadał on określonej w rozporządzeniu klasie SA3. Krzysztof Serafin wyraził nadzieję, że opracowywana specyfikacja techniczna zostanie zmodyfikowana przed jej końcową publikacją.

Andrzej Ryczer stwierdził, że mając do dyspozycji odpowiednie narzędzia i grupę specjalistów, można takie dokumenty opracować.

Następnie wypowiedział się Jerzy Sobstel (przedstawiciel Polski w CENELEC), który radził, żeby nie spieszyć się ze zmianą wymagań dotyczących systemów transmisji alarmów, gdyż to, co zostało na ten temat napisane w EN 50131-1:2006, jest niespójne z EN 50136 i będą wprowadzane zmiany. Trzeba to również uwzględniać w Specyfikacji Technicznej POLALARM – nie przepisywać bezpośrednio z normy 131.

– Bardzo dobrze, że wreszcie coś w zakresie tworzenia wymagań branżowych się dzieje, bo w ostatnich latach mieliśmy okres totalnej martwoty. Polski Komitet Normalizacyjny zajmuje się tylko publikacją tłumaczenia norm europejskich. Wprowadzony w PKN system ISO nie zawiera nawet odpowiednich procedur pozwalających na formalne zainicjowanie opracowania nowych norm europejskich – powiedział Jerzy Sobstel. *– Mamy pełne prawo tworzyć normy, jak inne kraje. Musi powstawać cały szereg dokumentów uzupełniających do norm europejskich. Muszą mieć one różną rangę. Muszą mieć rangę różnych poradników, specyfikacji branżowych, norm środowiskowych. Istnieje również konieczność wydawania norm krajowych, ale pod warunkiem, że są one niesprzeczne z normami europejskimi. Również powstające nowe specyfikacje i poradniki powinny co najmniej unikać sprzeczności lub wykluczać sprzeczność z normami europejskimi.* Jerzy Sobstel przypomniał o istnieniu dyrektywy usługowej: *– Coraz więcej polskich firm działa na rynku europejskim. Nagle może się okazać, że ludzie wykształceni w Polsce*

znają tylko wymagania sprzeczne ze stosowanymi w innych krajach europejskich.

W **panelu dyskusyjnym** po pierwszej części konferencji wywiązała się ożywiona dyskusja. Na koniec Krzysztof Ciesielski zaprosił do współtworzenia Specyfikacji Technicznej POLALARM.

Aleksander M. Woronow z **Softex Data** wygłosił referat zatytułowany *Inteligentne systemy nadzoru wizyjnego na przykładzie rozwiązań firmy Milestone*. Przedstawił rozwiązania systemowe związane z zarządzaniem ruchem pakietów danych w sieciowych systemach telewizyjnych, czyli systemy monitorowania wizyjnego w technologii IP. Prezentacja miała na celu „pokazanie, w jakim miejscu jesteśmy i czego możemy obecnie od tych systemów oczekiwać". Przypomniał w skrócie, czym zajmuje się firma Softex Data. Wraz z partnerami dostarcza ona kompletnych rozwiązań oraz pojedynczych elementów służących do stworzenia sieciowego monitoringu wizyjnego. Ma do zaoferowania najlepsze światowe rozwiązania – kamery i wideoserwery Axis Communications oraz oprogramowanie Milestone Xprotect. Milestone System to powstała w 1998 roku duńska firma programistyczna, która jest światowym liderem w branży oprogramowania do zarządzania otwartą platformą wideo IP.

Paweł Szczepanowski z firmy **BETACOM** wygłosił referat pt. *Monitoring IT – centralne zarządzanie dostępnością elektronicznych zasobów firmy*. Firma BETACOM należy do największych integratorów systemów informatycznych polskiego rynku. Jedną z mocniejszych stron firmy jest projektowanie i wdrażanie systemów określających dostępność do systemów informatycznych. Firma działa na rynku od kilkunastu lat, od 2004 roku jest notowana na Giełdzie Papierów Wartościowych w Warszawie. Jej działalność skupia się m.in. na integracji systemów informatycznych, produkcji oprogramowania na zamówienie, kompleksowej obsłudze informatycznej, oferowaniu systemów zarządzania wiedzą i kapitałem ludzkim, integrowaniu usług sieciowych, budowie systemów bezpieczeństwa i archiwizacji danych.

– W związku z rozwojem naszej aplikacji trwają obecnie rozmowy z firmą Axis Communications. Chcemy zbliżyć się do technologii i kamer tak, aby również w naszym portalu umieścić te rozwiązania w ramach centralizacji zarządzania bezpieczeństwem – poinformował Paweł Szczepanowski.

Wystąpienie **Agaty Majkucińskiej** z **Axis Communications** stanowiło prezentację nowych technologii. Agata Majkucińska przypomniała zebranym, że firma Axis Communications obchodzi w tym roku 25-lecie swojego istnienia, a na rynku nadzoru wizyjnego jest od 13 lat. W roku 1996 stworzono i wprowadzono na rynek pierwszą na świecie kamerę IP. Firma jest twórcą technologii nadzoru wizyjnego opartej na IP – pionierem tej technologii. Od 2009 roku koncentruje się tylko i wyłącznie na tego typu rozwiązaniach. Agata Majkucińska powiedziała, że jej zdaniem „technologia IP będzie standardem przyszłości. Systemy IP mają coraz więcej zwolenników, coraz więcej klientów jest nimi zainteresowanych". Porównała kamery analogowe z kamerami sieciowymi. Opisała wiele ciekawych funkcji kamer IP. Zwróciła również uwagę na zintegrowanie kamer z odpowiedniego rodzaju oprogramowaniem. Wspomniała o wprowadzonych do sprzedaży nowych rozwiązaniach, o seriach kamer P13 oraz P1346, które dopiero mają się ukazać. Opowiedziała o najmłodszym dziecku firmy – kamerze P5534, a także o tym, że Axis współpracuje z Pentaxem, producentem najlepszych obiektywów.

Witold Faber, pracownik firmy **Linc** (Linc jest dystrybutorem produktów firmy Mobotix), wygłosił referat pt. *Systemy wizyjne o wysokiej rozdzielczości obrazu pod kątem monitorowania zagrożeń oraz zachowań publiczności w obiektach sportowych.*

– Telewizja obserwacyjna nie jest elementem kluczowym w żadnym obiekcie, nie przesądza o faktycznym bezpieczeństwie danego obiektu. Ma tylko wspierać bezpieczeństwo. Na to, czy dany obiekt jest bezpieczny, czy nie, składa się wiele czynników. Telewizja dozorowa dokumentuje i może ułatwić uzyskanie danych operacyjnych – powiedział Witold Faber.

Krótko przedstawił niemiecką firmę Mobotix, której produkty są dostępne w wielu krajach na wszystkich kontynentach. Nadmienił, że Mobotix jest spółką notowaną na giełdzie i produkuje wyłącznie megapikselowe kamery IP. Opowiedział o ich możliwościach i funkcjach. Ich cechą charakterystyczną jest to, że mają wbudowane oprogramowanie. Kamery Mobotix nie mają żadnych części ruchomych, potrafią pracować w każdych warunkach, również w warunkach zewnętrznych – bez konieczności stosowania dodatkowego zasilania. Witold Faber powiedział też, że program Milestone w pełni obsługuje kamery Mobotix.

Zintegrowany system obsługi monitoringu ESOMWIN-SQL we współpracy z systemem zarządzania agencją ochrony ESOMSQL to temat wystąpienia **Zenona Janiaka** z firmy **EKOTRADE**, który zaprezentował między innymi najnowszą wersję oprogramowania.

– Najnowszy system informatyczny zaspokaja potrzeby firm działających w branży security. Pracuje w oparciu o bazę danych w standardzie SQL, zarówno w sieci lokalnej, jak i rozległej. Zaawansowane technologie w połączeniu z prostotą instalacji i nadzoru gwarantują, że nie będzie potrzebne zatrudnianie specjalistów z branży IT, jak również opłacanie drogiego abonamentu usług serwisowych, tak jak w przypadku niektórych rozwiązań istniejących na rynku. Elastyczność systemu umożliwia jego sprawne wdrożenie w każdej wielkości przedsiębiorstwie. Proces adaptacji systemu do aktualnych oczekiwań użytkownika będzie podążał za rosnącymi potrzebami rozwijającego się przedsiębiorstwa – powiedział Zenon Janiak.

Kolejnym punktem programu konferencji była prezentacja systemu transmisji danych, związanych z alarmami w infrastrukturze IT. System został omówiony przez **Fransa Hermesa** z Holandii, przedstawiciela firmy **Spectator Video Technology**, w referacie zatytułowanym *Rozwiązania transmisji audio i wideo zoptymalizowane pod kątem transmisji w infrastrukturze IP*. Frans Hermes omówił zastosowania systemu transmisji IP w sieci komputerowej w rozwiązaniach monitoringu. Wspomniał o praktycznych rozwiązaniach zaimplementowanych między innymi w Niemczech. Wystąpienie Fransa Hermesa zakończyło pierwszy dzień forum.

Na zakończenie uczestnicy i prelegenci I panelu wzięli udział w dyskusji.

Drugiego dnia odbyło się siedem prezentacji, z czego trzy poświęcono monitorowaniu z wykorzystaniem GPS. **Pierwsza** z nich, autorstwa Roberta Rymarza, zatytułowana *Przegląd europejskich trendów w systemach zarządzania flotą z wykorzystaniem urządzeń monitoringu GPS*, dotyczyła dwóch zagadnień – systemu zarządzania flotą oraz systemu, który jest z nim nierozerwalnie powiązany, a mianowicie systemu automatycznej lokalizacji pojazdów.

Systemy automatycznej lokalizacji pojazdów to rozwiązania bazujące na zainstalowanym w samochodzie odbiorniku satelitarnym, który odbiera sygnały z satelitów krążących wokół ziemi. Moduł transmisji danych przekazuje informacje do centrów obliczeniowych. Informacje te są przetwarzane na wiele różnych sposobów. Omówiwszy je pokrótce, Robert Rymarz przeszedł do głównej części swego wystąpienia, czyli szczegółowego omówienia systemów zarządzania flotą, które mają pomóc przedsiębiorstwom w zarządzaniu zasobami związanymi z transportem, czyli w prowadzeniu pełnej ewidencji pojazdu. Podkreślił, że obecnie w Polsce zauważa się wzrost zainteresowania przedsiębiorców tymi systemami. Wymienił największe firmy, które są liderami na rynku europejskim.

– *Rozwój systemów zależy od specjalizacji rozwiązań. Nie należy szukać rozwiązań uniwersalnych, trzeba je dostosowywać do indywidualnych potrzeb klientów* – stwierdził Robert Rymarz w podsumowaniu.

Prelekcję Roberta Rymarza uzupełnił **Jerzy Sobstel**, wspominając o Europejskim Systemie Wspomagania Satelitarnego – EGNOS[2].

Następna w kolejności była prezentacja **Krzysztofa Ciesielskiego** zatytułowana *Przegląd możliwości systemów GPS pod kątem zastosowania w systemach zarządzania flotą, systemach informowania o wypadkach drogowych oraz do kształtowania nowoczesnych produktów ubezpieczeń komunikacyjnych*.

Krzysztof Ciesielski dokonał przeglądu systemów GPS w węższym zakresie, nie omawiając systemów zarządzania flotą, gdyż temat ten dość szczegółowo omówił Robert Rymarz. Uświadomił raz jeszcze słuchaczom, że systemy GPS trafiają pod strzechy. Stosowane są np. w naszych samochodach, telefonach komórkowych, komputerach PC. Są mapy, do których jest szybki i łatwy dostęp i których szczegółowość jest ciągle zwiększana. Producenci wymyślają kolejne rozwiązania. Krzysztof Ciesielski opowiedział o nowych produktach wykorzystujących GPS (np. dostarczających informacji o utrudnieniach w ruchu lub o awarii pojazdów), które wkrótce się pojawią i na pewno będą bardzo popularne w Polsce, tak jak w innych krajach. Przedstawił korzyści wynikające z wykorzystania tych produktów. Powiedział też o produktach ubezpieczeniowych,

2) Europejski system EGNOS (European Geostationary Navigation Overlay Service) wspomaga działanie istniejących systemów nawigacji satelitarnej (głównie sieci Navstar). Do odbiorników GPS współpracujących z EGNOS wysyłane są sygnały korekcyjne pochodzące z satelitów geostacjonarnych znajdujących się nad Europą. Sygnały te zawierają korekty pozycji podawanych przez sieć Navstar, co kilkukrotnie zwiększa ich dokładność. Przede wszystkim jednak, EGNOS weryfikuje dane pochodzące z sieci Navstar, sprawdzając, czy nie doszło do awarii tych satelitów lub błędów podczas transmisji. Dzięki temu dane z sieci Navstar/EGNOS mogą być zastosowane tam, gdzie ze względów bezpieczeństwa muszą być w pełni wiarygodne. Są to tzw. aplikacje typu „Safety of Life", np. precyzyjna nawigacja samolotów, sterowanie ruchem pociągów czy niektóre akcje ratunkowe. EGNOS opiera się na trzech satelitach geostacjonarnych (15,5°W, 21,5°E i 25°E). Na Ziemi znajdują się stacje pomiarowe i kontrolne, które prowadzą ciągłe testy sieci Navstar i satelitów EGNOS. Obliczają poprawki danych GPS, wykrywają nieprawidłowości w transmisji i sprawdzają, czy nie doszło do awarii któregoś z satelitów. Poprawki i dane o stanie sieci GPS są transmitowane do satelitów EGNOS, które z kolei wysyłają je do odbiorników GPS. Jedna ze stacji kontrolnych sieci EGNOS znajduje się w Warszawie, w Centrum Badań Kosmicznych.

Źródło: http://www.kt.agh.edu.pl/~brus/satelity/navi.html#europa

które wkrótce pojawią się w Polsce i które bazują na systemach GPS. Nie ma jeszcze ubezpieczeń komunikacyjnych możliwych dzięki tym systemom, ale na pewno pojawią się – to tylko kwestia czasu.

Daniel Kamiński przedstawił najczęściej występujące w ACO (Alarmowych Centrach Odbiorczych) rodzaje problemów. Wiedzę na ich temat zaczerpnął ze swojej wieloletniej praktyki zawodowej. Omówił sytuacje kryzysowe, które mogą być następstwem braku kontroli działalności centrum monitorowania, błędów ludzkich, niepodejmowania decyzji, awarii technicznych, czynników losowych wywołanych siłą wyższą, działań terrorystycznych. Następnie omówił fazy zarządzania kryzysowego (zapobieganie, przygotowanie, reagowanie, odbudowa), etapy zarządzania ciągłością działania (analiza zagrożeń, analiza procesów biznesowych, identyfikacja kluczowych procesów, utworzenie planów ciągłości działania, wdrożenie PCD (BCP), testy wdrożonych rozwiązań i procedur, szkolenia), a potem podjął się charakterystyki ACO (liczba i rodzaj obsługiwanych obiektów, liczba połączeń przychodzących i wychodzących, liczba stosowanych systemów transmisji, liczba stanowisk pracy, liczba serwerów, funkcjonalność oprogramowania biznesowego, korzystanie z nowoczesnych usług), omówił procedury ACO (weryfikacja alarmów, reakcja na sygnał o alarmie, reakcja na sygnał o usterce, instrukcja ochrony centrum oraz działania w sytuacjach kryzysowych, instrukcja współpracy z innymi działami, np. z księgowością), problemy ciągłości pracy ACO (długi czas oczekiwania na połączenie, duża liczba braków łączności, długi czas reakcji, duża liczba sygnałów w godzinach szczytu, koszty związane z obsługą fałszywych alarmów, koszty związane z zagwarantowaniem ciągłości pracy) i wspomniał o możliwych awariach podczas pracy ACO (awarie urządzeń odbiorczych, przyłączy telekomunikacyjnych, zasilania i klimatyzacji, urządzeń transmisyjnych na dużym obszarze, sieci komputerowej, programu monitoringu i inne).

Prelekcja miała dynamiczny charakter, słuchacze mieli możliwość weryfikacji swoich doświadczeń z praktycznymi doświadczeniami prelegenta, który poprzez ćwiczenia zachęcał słuchaczy do aktywnego udziału w jego wystąpieniu.

Daniel Kamiński zachęcał również do organizowania mniej formalnych spotkań i wymieniania się doświadczeniami. Jego zdaniem mogłoby to przyczynić się do wzrostu świadomości pracowników ACO, a dzięki temu do zwiększenia poziomu bezpieczeństwa klientów. Można było zauważyć duże doświadczenie prelegenta. Wystąpienie było ciekawe, a jego forma (czyli ukazanie problemów, z jakimi pracownicy ACO mogą się spotkać) rzadko spotykana. Nie każdy mówi o problemach, z jakimi przyszło mu się zmierzyć w swojej pracy. Na forum publicznym mówi się raczej o sukcesach, i to nie o wszystkich, bo nie każdy lubi dzielić się z innymi wiedzą, do której sam z trudem doszedł, a która jest niewątpliwie bardzo przydatna dla innych.

Taki styl prelekcji jest bardzo przydatny, bo może uchronić słuchaczy przed ewentualnym powielaniem błędów w przyszłości. Po co „otwierać otwarte drzwi"? Warto skorzystać z doświadczeń innych.

Doskonałym uzupełnieniem prezentacji Daniela Kamińskiego była prezentacja **Rafała Dunala** z firmy **EsaProjekt** pt. *Przegląd inteligentnych systemów wizyjnych z algorytmami rozpoznawania obrazów, osób, tablic rejestracyjnych*

i nietypowych zachowań. Rafał Dunal stwierdził między innymi, że uzupełnienie monitoringu tradycyjnego o monitoring inteligentny może sprawić, że wykrywalność zdarzeń wzrośnie kilkakrotnie. Wskazał szereg wad monitoringu tradycyjnego (człowiek jest jego najsłabszym ogniwem, liczba kamer/monitorów jest ograniczona, poziom analizy zdarzeń zmienia się w czasie, jest dużo błędów, są duże koszty, brakuje skutecznej kontroli nad pracą służb, narzędzi do działań automatycznych, narzędzi do analizy koincydencji zdarzeń i analiz statystycznych, funkcje archiwalno-dokumentacyjne przeważają nad prewencyjnymi).

– *Obserwujący dwa monitory operator po 10 minutach pracy nie wychwytuje około 45% informacji dostarczanych przez obraz, a po 22 minutach aż 95%, natomiast sztuczna inteligencja zawarta w oprogramowaniu analizy obrazu wykorzystuje algorytmy heurystyczne najnowszej generacji, co oznacza, że system myśli jak człowiek, ale nie zasypia, nie traci koncentracji* – mówił Rafał Dunal. Inteligentny system może monitorować tysiące obrazów pochodzących z kamer wizyjnych. Prelegent podał kilka przykładów inteligentnego monitoringu, takich jak śledzenie obiektu, klasyfikacja obiektu, nadzór nad obszarem, wykrywanie kradzieży, wykrywanie pozostawionego bagażu/przedmiotu, detekcja podejrzanego zachowania, detekcja aktów wandalizmu/graffiti, wykrywanie powstania tłoku, zliczanie obiektów/statystyka, kontrola kierunku poruszania się, wielopoziomowe alerty, koincydencja zdarzeń itp.

Wspomniał o technologii *Automatic Number Plater Recognition*, umożliwiającej odczytywanie numerów tablic rejestracyjnych na podstawie analizy obrazów ruchomych i statycznych, wykorzystującej kamery obserwujące drogę oraz system komputerowy przetwarzający obraz z tych kamer. Analiza obrazu polega na zlokalizowaniu pojazdu, odnalezieniu tablicy rejestracyjnej, odczytaniu jej i odpowiedniej kwalifikacji. System rozpoznaje numery tablic krajowych i zagranicznych o różnych kolorach (białych, czarnych, żółtych, niebieskich), akceptuje różne wielkości i kroje znaków.

Jak podał Rafał Dunal, pierwsze systemy rozpoznawania tablic były zastosowane na jednym z mostów w Wielkiej Brytanii, prawdopodobnie w roku 1976.

Prelegent zaprezentował system CARBER (który jest w ofercie firmy EsaProjekt) oraz jego wybrane zastosowania.

Wspomniał też o projekcie SAMURAI (więcej informacji na jego temat znajdą państwo na stronach 20-21 niniejszego numeru *Zabezpieczeń*).

W podsumowaniu pokazał nowe możliwości inteligentnych systemów wizyjnych, jakie obecnie coraz częściej się pojawiają. Stwierdził, że zbyt często skupiamy się tylko na rozwiązaniach sprzętowych, a nie software'owych. Wykazał, że przedstawione najnowsze rozwiązania i technologie mają przyszłość i że należy poważnie brać je pod uwagę, gdyż są łatwo skalowalne i łatwo je rozbudowywać, nie ponosząc kosztów wymiany całości – wymieniamy tylko komponenty software'owe.

Warto dodać, że firma EsaProjekt jest zainteresowana współpracą z innymi firmami podczas realizacji projektów komercyjnych, a także badawczo-rozwojowych.

Drugiego dnia, w ostatniej części konferencji, **Piotr Błaszczyk**, główny konstruktor firmy EBS, wygłosił prelekcję pt. *Nowe możliwości wykorzystania urządzeń monitoringu alarmowego*. Był to pokaz klasycznego wykorzystania infrastruktury monitorowania alarmów. Piotr Błaszczyk omówił rozwój transmiterów – media transmisyjne, moduły, typy zdarzeń. Do

typowych usług zaliczył: przesyłanie stanów wejść cyfrowych, przesyłanie zdarzeń w formatach ContactID oraz SIA, przesyłanie testów okresowych, monitorowanie napięcia sieciowego i zasilania awaryjnego. Do usług dodanych zaliczył: monitorowanie obecności urządzeń, monitorowanie sabotażu urządzeń, monitorowanie stanów urządzeń zewnętrznych (wskazania liczników energii elektrycznej, wskazania liczników energii cieplnej, ilość towaru w zasobnikach maszyn sprzedających, ilość gotówki w maszynie grającej/sprzedającej, aktywność urządzenia, zdalna diagnostyka i konfiguracja).

Następnie omówił typy zdarzeń, jakie można odczytać zdalnie z liczników energii elektrycznej, maszyn sprzedających, bramek antykradzieżowych oraz automatów do gier o niskich wygranych, i wynikające z tego korzyści.

– *Przyszłość jest w integracji systemów. Dzięki niej można byłoby ograniczyć do minimum liczbę urządzeń* – powiedział Piotr Błaszczyk i ustosunkował się do nadal raczkującej automatyki domowej. – *Poprzez telefon komórkowy moglibyśmy sprawdzać, czy ktoś włamuje się do domu albo czy temperatura w lodówce jest dostatecznie niska.*

Prezentacja **Witolda Strzeleckiego** z **ISM EuroCenter** nosiła tytuł *Nowe technologie w systemach monitoringu wizyjnego* i zawierała wiele elementów obecnych w wystąpieniach przedmówców, jednakże Witold Strzelecki omówił także wiele innych, ciekawych rozwiązań, nawiązując do swoich własnych doświadczeń związanych między innymi z monitorowaniem imprez masowych, szczególnie zachowań ludzi podczas meczu piłki nożnej.

Zademonstrował również, jak wyglądają przykładowe obrazy z kamery mutimegapikselowej, ukazujące fragment miasta, drogi i ulice oraz port morski.

Kamery multimegapikselowe to przykład nowych trendów w systemach CCTV. Kamery te charakteryzują się bardzo dobrą jakością obrazu. Ich wykorzystanie może być rozwiązaniem alternatywnym wobec stosowania dotychczas popularnych kamer o rozdzielczości 720×576 pikseli. Nowoczesne kamery megapikselowe mają rozdzielczość o wiele wyższą, co pozwala na monitorowanie zdecydowanie większych obszarów. Dodatkowym atutem tego typu urządzeń jest możliwość powiększania dowolnych fragmentów obrazu. Największą ich zaletą jest to, że mimo powiększenia i obserwacji powiększonego wycinka obrazu na ekranie monitora nagrywany jest cały obszar. Kamery te idealnie nadają się do systemów CCTV, w których duży nacisk kładzie się na doskonałe odwzorowanie najmniejszych szczegółów monitorowanego obiektu.

Ostatnie wystąpienie – *O inteligentnych kamerach na przykładzie rozwiązań firmy Sony* – to wykład **Andrzeja Walczyka**, który przedstawił typowy system monitorowania IP bazujący na kamerach sieciowych zawierających interfejsy Fast Ethernet, które umożliwiają bezpośrednie podłączenie kamer do sieci IP. Andrzej Walczyk przypomniał, że kamery SONY stanowią integralną całość i jakiekolwiek serwery zewnętrzne nie są potrzebne. Jeżeli jednak wystąpi konieczność włączenia do systemu niesieciowych, analogowych kamer CCTV, to oczywiście istnieje możliwość ich włączania w sieć IP, co wiąże się z zastosowaniem dodatkowych koderów. Należy wówczas posłużyć się serwerami wizyjnymi SONY (które zostały krótko opisane). Następnie prelegent zapoznał zebranych z asortymentem urządzeń przeznaczonych do pracy w systemach monitorowania firmy SONY na przykładzie typowego systemu

spełniającego wymogi ochrony imprez masowych (ze szczególnym naciskiem na rozdzielczość obrazu, liczbę klatek na sekundę i wandaloodporność).

– *Urządzenia produkowane przez SONY oraz zaproponowane sposoby wykorzystania tych urządzeń pozwalają na tworzenie zautomatyzowanych systemów monitoringu wizyjnego, wspomagających pracowników ochrony przez generację odpowiednich ostrzeżeń w sytuacjach uznawanych za krytyczne oraz podejmujących samodzielne działania w ramach zaimplementowanego programu. Wszystko to pozwala nazywać te systemy monitoringu wizyjnego inteligentnymi* – stwierdził Andrzej Walczyk w podsumowaniu.

Ośrodek GEOVITA, położony nad brzegiem Zalewu Zegrzyńskiego, zaledwie 35 kilometrów od centrum Warszawy, oraz zamówiona przez organizatorów dobra pogoda sprzyjały uczestnikom forum. Uroczysta kolacja oraz widowiskowe popisy barmanów przygotowujących drinki w rytm muzyki to pomysł organizatorów na zakończenie pierwszego dnia forum. Atmosfera sprzyjała zacieśnianiu więzi koleżeńskich, nawiązywaniu nowych znajomości, wymianie doświadczeń i spostrzeżeń. Jak zauważyłam, rozmowy kuluarowe są nieformalną, ale bardzo potrzebną i lubianą formą kontaktów.

Dobrze się stało, że stowarzyszenie zrezygnowało ze sztywnych ram forum i wprowadziło nowe tematy – stara się nadążać za zmianami, jakie przynosi rynek, na którym pojawia się coraz więcej nowych urządzeń, systemów i technologii. Ze względu na dużą liczbę podobnych konferencji trzeba mieć pomysł na ciekawą prezentację, aby nie tylko utrzymać, ale przede wszystkim zainteresować stałych i wiernych uczestników tego typu imprez, a także przyciągnąć uczestników nowych, młodych i ciekawych nowych rozwiązań. Moim zdaniem formuła polegająca na pokazie slajdów w programie PowerPoint powinna być uzupełniana o nowe, dynamiczne pokazy, może na przykładzie działających już systemów, programów itp. Oczekujemy ciekawych prezentacji, pokazów i merytorycznych dyskusji, dobrze przygotowanych moderatorów i ekspertów. Takim pozytywem na Forum Monitoringu Polskiego, a może już nie polskiego, bo niektóre prezentacje wykraczały poza obręb naszego kraju (m.in. prezentacja Rafała Dunala, który wraz ze swoja firmą EsaProjekt bierze udział w europejskim projekcie SAMURAI, oraz prezentacja Fransa Hermesa – przedstawiciela holenderskiej firmy Spectator), była, moim zdaniem, obecność współautorów dokumentów normalizacyjnych, którzy podjęli trud, aby unowocześnić obowiązujące w kraju przepisy prawne i doprowadzić do uzgodnienia ich z normami i przepisami międzynarodowymi, i którzy w sposób możliwie jasny podzielili się swoimi bogatymi doświadczeniami nabytymi podczas ich opracowywania. Kompetencje i wiedza tych osób (bardzo nielicznych, wbrew pozorom) pozwoliły już teraz na istotne uporządkowanie istniejącego bałaganu normalizacyjnego.

Zapraszam do obejrzenia fotoreportażu *www.zabezpieczenia.com.pl*

Opracowała: Teresa Karczmarzyk

Autopoprawka do artykułu zamieszczonego na łamach **Zabezpieczeń nr 6/2009**

W artykule pt. *Nagłaśnianie stref na przykładzie głośników pożarowych serii UNISPEAKER*, zamieszczonym w *Zabezpieczeniach* w numerze 6/2009, na stronie 65 jest błąd we wzorze do obliczania liczby głośników **LG**.

Opublikowany wzór ma postać:

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

Nie jest on prawidłowy, gdyż liczba głośników powinna być ilorazem powierzchni nagłaśnianej i kwadratu odległości pomiędzy głośnikami, a zatem powinien przyjąć następującą postać:

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

gdzie:

LG – liczba głośników,

P – nagłaśniana powierzchnia w [m^2]

O^2 – odległość pomiędzy głośnikami podniesiona do kwadratu.

Jak widać, po zastosowaniu prawidłowej postaci wzoru w efekcie końcowym znacznie zmniejszy się liczba potrzebnych głośników, a zatem i koszt instalacji.

Należy jednak pamiętać o tym, że są to jedynie wartości przybliżone, a ostateczną liczbę głośników należy dobrać w zależności od warunków panujących w nagłaśnianej strefie.

Rafał Kowal
AAT Holding

Versa
wszechstronne centrale alarmowe

Nowoczesne centrale VERSA to połączenie intuicyjnej i prostej obsługi z zaawansowanymi możliwościami rozbudowy i wszechstronnymi funkcjami komunikacyjnymi. Dzięki temu są idealnym rozwiązaniem dla zabezpieczania mieszkań, domów i małych obiektów handlowo-biurowych.

Satel®

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

Co w normach piszczy?

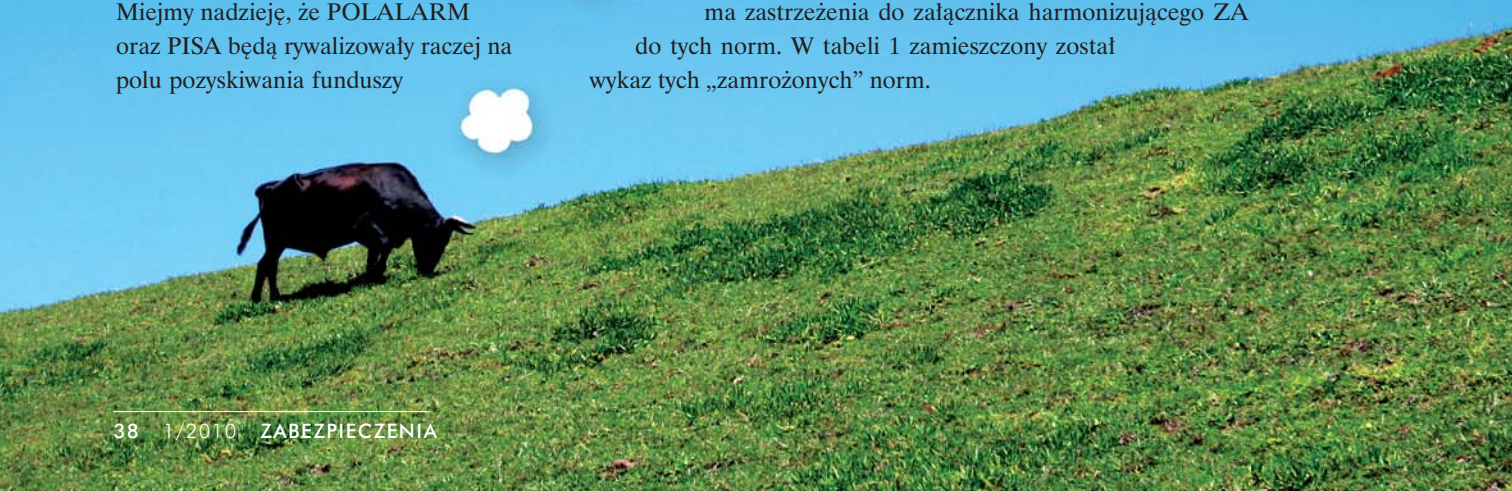
Jerzy W. Sobstel

Czasami piszczy i zgrzyta. Oczywiście nie w samych normach, w których co najwyżej różne byki i byczki porykują, lecz w całym procesie tworzenia norm i ich publikacji. Wbrew obiegowym opiniom normy nie powstają w laboratoriach naukowców pracujących bezinteresownie dla dobra ludzkości ani w gabinetach brukselskich biurokratów. Teoretycznie powinny być wynikiem konsensusu osiągniętego przez wszystkich interesariuszy, którzy zechcieli wziąć udział w pracach normalizacyjnych. W praktyce proces ten bywa bardzo burzliwy i zawiły

Na naszym krajowym podwórku dotyczy to na przykład problemów z publikacją polskiej wersji normy europejskiej EN 50131-1:2006 oraz promowaniem przez POLALARM niezgodnej z nią specyfikacji technicznej. Miejmy nadzieję, że POLALARM nie poprzestanie na tej pierwszej próbie oryginalnych prac normalizacyjnych i że kolejne, bardzo zresztą potrzebne, produkty okażą się mniej kontrowersyjne.

Nowa formuła funkcjonowania Polskiego Komitetu Normalizacyjnego umożliwia bezpośredni udział w pracach normalizacyjnych wszystkim podmiotom zainteresowanym opracowywaniem i stosowaniem norm. Można się cieszyć, że podstawowy dla branży zabezpieczeń Komitet Techniczny 52 liczy już 30 członków i to zarówno producentów, organizacje branżowe, uczelnie, jak i instytucje państwowe. Pierwsze posiedzenia tego komitetu były dosyć burzliwe i wskazywały na przenoszenie się starych animozji na nowe pole konfrontacji. Miejmy nadzieję, że POLALARM oraz PISA będą rywalizowały raczej na polu pozyskiwania funduszy na tłumaczenia norm europejskich niż w rozgrywkach personalnych. Ciekawe również, jaką aktywnością w pracach normalizacyjnych wykażą się nowi członkowie KT 52, gdy zorientują się, na czym te prace polegają, na co w rzeczywistości będą mieli wpływ. Czy będą zainteresowani żmudną analizą projektów norm, które ich bezpośrednio nie dotyczą? Czy będą skłonni płacić za przywilej uczestniczenia w pracach normalizacyjnych, co przewidywał na przykład projekt ustawy o normalizacji?

Cieszy rosnące zainteresowanie normami. Warto jednak pamiętać, że polskie tłumaczenia norm europejskich są publikowane przez PKN zwykle po trzech latach od ich publikacji w języku oryginału, czyli po czterech latach od zakończenia prac przez odpowiedni komitet techniczny. Projekty norm znane są jeszcze wcześniej. Jeżeli chcemy konkurować na rynku europejskim, powinniśmy wiedzieć, co się na nim dzieje, jakie normy powstają, a jakie nie i dlaczego. Informacji o tym może (i powinna) dostarczać prasa branżowa. Dla przykładu – zainteresowani systemami sygnalizacji pożarowej zapewne zauważyli wyraźny przestój w publikacji europejskich norm zharmonizowanych z tej dziedziny. Nie wynika to bynajmniej z opieszałości poszczególnych grup roboczych. Szereg norm zostało opracowanych i zatwierdzonych w formalnym głosowaniu, jednak ich publikacja została wstrzymana przez konsultanta CEN, który ma zastrzeżenia do załącznika harmonizującego ZA do tych norm. W tabeli 1 zamieszczony został wykaz tych „zamrożonych” norm.



Numer projektu normy	Tytuł	Stan prac
EN 54-2	*Control and indicating equipment*	Skonsolidowana wersja przekazana do głosowania i odrzucona przez konsultanta CEN. Projekt usunięty i ponownie zarejestrowany.
EN 54-4	*Power supply equipment*	Skonsolidowana wersja przekazana do głosowania i odrzucona przez konsultanta CEN. Projekt usunięty i ponownie zarejestrowany.
EN 54-10	*Flame detectors – Point detectors*	Zarejestrowana przez CEN do weryfikacji. Procedurę zatwierdzania zmieniono na ankietę powszechną plus formalne głosowanie. Projekt usunięty i ponownie zarejestrowany.
EN 54-11	*Manual call points*	Zmiana przekazana do głosowania i odrzucona przez konsultanta. Zweryfikowana wersja przesłana ponownie 2008-10-03 i ponownie odrzucona. Projekt usunięty, wymaga ponownego zarejestrowania.
EN 54-17	*Short-circuit isolators*	Zmiana przesłana do głosowania i odrzucona przez konsultanta. Projekt usunięty i ponownie zarejestrowany.
EN 54-18	*Input/output devices*	Zmiana przesłana do głosowania i odrzucona przez konsultanta. Projekt usunięty i ponownie zarejestrowany.
EN 54-20	*Aspirating smoke detectors*	Zmiana przesłana do głosowania i odrzucona przez konsultanta. Projekt usunięty i ponownie zarejestrowany.
EN 54-22	*Line type heat detectors*	Projekt normy przesłany do głosowania i odrzucony przez konsultanta. Usunięty z planu prac i ponownie zarejestrowany.
EN 54-23	*Fire alarm devices - Visual alarms*	Projekt normy przesłany do formalnego głosowania (2008-01). Odrzucony przez konsultanta. Poprawiony, przesłany ponownie do CEN (2008-09-03) i ponownie odrzucony. Przesłany po raz kolejny do CEN (2009-07) i zaakceptowany przez konsultanta CEN.

Tab. 1. Wykaz „zamrożonych" norm

Jak widać, ostatni z projektów został zaakceptowany prze konsultanta CEN, a formalne głosowanie nad nim zakończono 22 grudnia 2009 r. i zapewne nowa norma niebawem zostanie opublikowana.

Nie oznacza to jednak końca kłopotów. Komitet Techniczny CEN/TC72 uważa, że Załącznik ZA zastosowany w normie EN 54-23: 2010 nie jest odpowiedni dla pozostałych norm i na swoim posiedzeniu plenarnym w Madrycie w październiku 2009 r. powołał grupę zadaniową do opracowania kolejnej wersji tego załącznika. Oznacza to, że na pozostałe normy z serii EN 54 jeszcze poczekamy.

Na tym samym posiedzeniu CEN/TC72 zainicjowane zostały prace nad normą EN 54-32: *Fire detection and fire alarm systems – Part 32: Planning, design, installation, commissioning, use and maintenance of voice alarm systems*.

Nie został natomiast wyjaśniony los normy EN 60849:1998 (PN-EN 60849:2001 *Dźwiękowe systemy ostrzegawcze*). Jest ona identyczna z liczącą sobie już ponad dziesięć lat normą IEC 60849:1998, która została wycofana ze zbioru norm IEC i zastąpiona przez normy ISO 7240-16:2007 oraz ISO 7240-19:2007.

Norma PN-EN 60849:2001, jako niezgodna z EN 54-16:2008 (PN-EN 54-16:2008 *Systemy sygnalizacji pożarowej – Część 16: Dźwiękowe systemy ostrzegawcze – Centrale*), musi być wycofana do marca 2011 r.

„Oj, będzie się działo!"

dr inż. Jerzy W. Sobstel

Postanowienia noworoczne

Grzegorz Ćwiek

Początek roku to doskonały moment, by podsumować to, co wydarzyło się w poprzednim roku, wyciągnąć odpowiednie wnioski na przyszłość i postanowić poprawę. Niemal każdy z nas to robi i… niewiele z tego wynika. Korzystając z okazji, składam wszystkim życzenia jak najlepszego wypełniania noworocznych postanowień – i to od początku do końca, a nie wybiórczo, jak to zwykle mamy w zwyczaju. A dlaczego? Hm… Bo zawsze jest tak, że jak się nie podejdzie do czegoś w sposób rzetelny i konkretny, precyzyjnie zaplanowawszy, jak nasze przedsięwzięcie ma się zakończyć, to można trwać w przeświadczeniu, że jest dobrze – albo nieźle – a w rzeczywistości jest mizernie i dość niebezpiecznie…

Spójrzmy, drodzy przyjaciele, na naszą branżę – branżę systemów bezpieczeństwa. Wszystko jest już niby bardzo dobrze przygotowane – i przepisy lokalne (polskie), i tłumaczenia, i interpretacje rozmaitych norm europejskich, mamy normy zharmonizowane i certyfikaty, zaświadczenia, aprobaty, dopuszczenia. Czego zatem brakuje? Co jest nie tak? Zdaniem wielu kolegów z branży (tych świadomych i rzetelnych) brakuje przede wszystkim **spójności między teorią a praktyką (rzeczywistością)**.

Weźmy za przykład branżę bezpieczeństwa pożarowego, a konkretnie systemy wykrywania zagrożeń pożarowych. O możliwości wprowadzenia urządzeń do sprzedaży i użytkowania decyduje spełnienie przez producentów szeregu wymagań stawianych przez rozmaite ustawy i normy. Na straży poprawności produkcji i sprawności urządzeń stoją certyfikaty, dopuszczenia, aprobaty oraz lepiej lub gorzej przetłumaczone oświadczenia producentów, za które sami ponoszą odpowiedzialność. I to jest oczywiście dobre – z jednej strony ustawodawca kontroluje rynek, broniąc go przed napływem taniego sprzętu o marnej jakości, z drugiej strony nie robi jednak tego, co najważniejsze zdaniem wielu z „nas" – ludzi z branży, mianowicie nie kontroluje w należyty sposób tego, w jaki sposób systemy oparte na tych urządzeniach są projektowane i instalowane w obiektach. Ktoś mógłby powiedzieć, że mamy w tej mierze pewne unormowania i wytyczne. Jasne, że tak, ale normy nie są obligatoryjne, a wytyczne zapisane w formie małych książeczek lub porad internetowych mogą być traktowane jak zbiór ciekawych tekstów, a nie jak jasna i klarowna instrukcja, jak należy, a jak nie należy postępować. Nie ma także żadnej kary za niezastosowanie się do większości wytycznych, chyba że za karę uznać należy reprymendę rzeczoznawcy ds. zabezpieczeń przeciwpożarowych lub konieczność poświęcenia czasu na forsowanie odstępstw lub uzgadnianie interpretacji przepisów. Ponadto rzeczoznawcy czasem nawzajem podważają podejmowane przez siebie decyzje, a będąc zupełnie obiektywnym i uczciwym, trzeba uznać, że w wielu przypadkach obie strony mają rację. Istnieje zbyt duża dowolność interpretacji przepisów istniejących i zbyt duża luka prawna, która nie jest zapełniona żadnymi jednoznacznymi zapisami o charakterze wymagalności.

Ale to oczywiście tylko wierzchołek góry lodowej. Za wykryte nieprawidłowości w projekcie hali targowej w Katowicach (po słynnej tragedii sprzed kilku lat) projektanci usłyszeli zarzuty prokuratora. Takie sprawy, jak ta, ciągną się latami i – w zależności od branży, której to dotyczy – istnieje mniejsza lub większa możliwość udowodnienia nieprawidłowości działania projektanta, jego ignorancji lub niewiedzy. Jak wygląda sytuacja w przypadku projektantów systemów sygnalizacji pożarowej? Chyba najgorzej w branży. Podlegają bowiem wszelkim restrykcjom ze strony prokuratury w momencie wystąpienia nieprawidłowości, ale, z drugiej strony, nie mają żadnego wsparcia ze strony ustawodawcy czy administracji państwowej – ani w zakresie jasności przepisów i wytycznych dotyczących projektowania (o czym była mowa wcześniej), ani w zakresie szkoleń i podnoszenia kwalifikacji (mogą dobrowolnie wziąć udział tylko w szkoleniach organizowanych przez stowarzyszenia, instytucje, takie jak np. Instytut Techniki Budowlanej czy Centrum Naukowo Badawcze Ochrony Przeciwpożarowej, lub też firmy prywatne). Nie istnieje oficjalny, jedyny słuszny test sprawdzający w sposób obiektywny znajomość zasad projektowania systemów bezpieczeństwa pożarowego. Nie istnieje certyfikat potwierdzający jakość pracy projektanta. Nie ma – tak jak w przypadku produktów – audytów, testów kontrolnych i procedur recertyfikacyjnych dla usługodawcy, którym w tym zakresie jest właśnie projektant. Z tego powodu w szeregach projektantów obecni są farmaceuci, technicy weterynarii, filologowie, spawacze, ślusarze i specjaliści z innych branż – w tym elektrycy, domorośli elektronicy – którzy nie mają zielonego pojęcia o ryzyku i odpowiedzialności za prace, które wykonują. Oczywiście nie mamy nic przeciwko ogrodnikom w branży – i mamy nadzieję, że zostanie to dobrze zrozumiane – jednak bez gruntownego, ustawowo lub za pomocą odpowiedniego rozporządzenia, uregulowanego poziomu jakości wykształcenia, wiedzy i doświadczenia projektantów nie możemy spać spokojnie. To jeden z ważniejszych przykładów braku spójności norm i przepisów na naszym rynku, którym jak najszybciej powinni zająć się wszyscy mający wpływ na kształt branży bezpieczeństwa w Polsce. Chwała wszystkim projektantom – o wszelakim wykształceniu – za to, że próbują we własnym zakresie i na własny koszt podnosić swoje kwalifikacje, jednak tysiące projektów powstających każdego roku w Polsce nie pozostawiają złudzeń – **istnieje konieczność ujednolicenia procesu kształcenia fachowców**, określenia przynajmniej minimalnych wymagań dotyczących ich umiejętności i wprowadzenia obowiązku odnawiania tych wymagań najrzadziej co trzy lata. Postęp technologiczny jest dzisiaj bowiem tak szybki, że nie można prowadzić prawidłowych prac projektowych bez ciągłego uzupełniania wiedzy. Z kolei młodzi projektanci potrzebują wiedzy praktycznej, doświadczenia, „żywych" przykładów od starszych i bardziej doświadczonych kolegów. Szkolenia mogliby przeprowadzać także strażacy – prezentując trudności, jakie napotykają podczas akcji ratunkowych w przypadku źle zaprojektowanego systemu sygnalizacji pożarowej czy ewakuacji (DSO, architektura i inne).

W tym miejscu koniecznie należy wspomnieć o podobnym problemie, który dręczy wykonawców. Jakość wykonywanych przez nich prac także nie podlega jakimkolwiek uregulowaniom. Rzetelność wykonawców – szczególnie w czasach kryzysu, kiedy na wszystko brakuje pieniędzy – jest szczególnie istotna. O ile o jakość instalacji wykonywanych w Niemczech, Stanach Zjednoczonych, Austrii czy w innych rozwiniętych krajach dbają także ubezpieczyciele, o tyle w Polsce często nie dba o nią nawet sam inwestor, nie zdając sobie sprawy z tego, jak wielki błąd popełnia. Zatrudniając do instalacji systemu bezpieczeństwa pożarowego firmę nieprzygotowaną, nieprzeszkoloną w tym zakresie, ryzykuje bowiem całym swoim majątkiem, a także naraża się na konsekwencje karne w przypadku jakiegokolwiek tragicznego wypadku zaistniałego wskutek błędnie wykonanej instalacji bezpieczeństwa. W Polsce występuje także zjawisko „zmowy" inwestora z firmą wykonawczą,

świadczącą usługi wykonawcze w zakresie wyżej wymienionych instalacji. Takiego zjawiska nie spotyka się na zachodzie Europy. Dochodzi u nas do kuriozalnych sytuacji, kiedy to inwestor, powiadomiony przez producenta i rzeczoznawcę do spraw zabezpieczeń przeciwpożarowych o tym, że wybrany przez niego wykonawca nie ma żadnej wiedzy fachowej, przygotowania merytorycznego ani sprzętowego do wykonywania projektów czy samych instalacji, ze względu na niską cenę pozostaje przy swoim wyborze i w sposób świadomy naraża osoby trzecie na utratę życia lub zdrowia(!).

Wiele lat temu, z inicjatywy Stowarzyszenia Inżynierów i Techników Pożarnictwa, powstała idea dobrowolnej certyfikacji usług. Oczywiście tematykę tę podjęły także inne stowarzyszenia i do dziś zostało przeszkolonych już wiele firm. Z uwagi na brak jakiejkolwiek obligatoryjności takiego procesu certyfikacji po latach niemal nikt nie zwraca już na to uwagi, a na konferencjach i spotkaniach branżowych w zasadzie przestało się o tym głośno mówić. Inwestorzy z zadziwieniem wysłuchują opowieści o podobnych pomysłach i praktykach, po czym zadają bardzo konkretne pytanie: jakie korzyści odniosę, zatrudniając taką, a nie inną firmę? Kiedy jednak poza wysoką jakością usług (dla wielu trudno mierzalną) nie pojawia się żadna korzyść w postaci np. zniżek ubezpieczeniowych lub innych zachęt ze strony administracji publicznej, rzadko decydują się na taki wybór. Dopiero po jakimś czasie trwania procesu inwestycyjnego okazuje się, że koszty związane z zatrudnieniem firmy „tańszej" znacznie przekraczają ceny ofert firm wprawdzie droższych, ale doskonale przygotowanych technicznie, sprzętowo i osobowo do rzetelnej pracy. Powodem tego jest konieczność dokonania wielu zmian i poprawek w błędnie wykonanych projektach i instalacjach, a czasem zwiększenie lub zmiana zakresu zamówienia z uwagi na całkowicie błędne rozwiązania wybrane przez nierzetelnego wykonawcę. Ponadto kosztowne procesy i spory o odszkodowania lub odzyskanie należności ciągną się latami.

Wracając zatem do życzeń noworocznych – życzmy sobie w nowym roku, by wszelkie możliwe instytucje publiczne, stowarzyszenia, centra naukowe oraz firmy prywatne zjednoczyły się w roku 2010, zakończyły wieloletnie debaty i spory na tematy mało istotne i zajęły się wspólnie stworzeniem dla nas wszystkich tak przejrzystych, jasnych i konkretnych warunków pracy, by była ona coraz ciekawsza i bezpieczniejsza dla usługodawców i usługobiorców, a także byśmy wszyscy mogli skupić się na dobrej robocie, a nie traceniu czasu na udowadnianie sobie racji w tych przypadkach, w których jest to bardzo trudne. Czekamy na impuls ze strony MSWiA lub innych organów publicznych i zaproszenie do rozmów na temat tego, jak ułatwić pracę nam, pracownikom branży zabezpieczeń, a także ludziom korzystającym z naszych produktów i usług. Konieczne wydaje się uzupełnienie istniejących rozporządzeń o zapisy bardziej klarowne i szczegółowe. Niezbędne jest wprowadzenie obligatoryjnych szkoleń dla projektantów wraz z konkretnymi zasadami ich certyfikacji oraz weryfikacji wiedzy w kilkuletnich odstępach. Spowodowałoby to automatycznie konieczność przyjęcia przez środowisko konkretnych wytycznych zarówno w zakresie projektowania, jak i wykonywania instalacji systemów bezpieczeństwa. Należałoby zatem koniecznie(!) włączyć do procesu legislacyjnego większe grono specjalistów, uznanych ekspertów oraz polskich i zagranicznych (obecnych na krajowym rynku) producentów, jako konsultantów posiadających ogromną wiedzę nie tylko teoretyczną, ale i praktyczną – tak niezbędną do tworzenia przepisów mądrych i potrzebnych. Powinno się jak najszybciej zadbać o zachęty dla firm ubezpieczeniowych (finansowe, podatkowe, inne), by mocniej zaangażowały się w ocenę jakości instalacji systemów bezpieczeństwa oraz kontrolę firm wykonawczych i samych inwestorów. Taki impuls ze strony administracji publicznej musiałby z kolei przełożyć się na znacznie lepsze warunki ubezpieczenia dla inwestorów, którzy lepiej zabezpieczaliby swoje obiekty oraz wykonawców, świadczących usługi lepszej jakości. Na znaczeniu zyskałaby certyfikacja usług. Koszty poniesione przez wszystkich uczestników rynku w początkowej fazie takiego procesu zmian z pewnością przełożyłyby się na większe przychody i mniejsze straty dla wszystkich w długim okresie. Rynek byłby bardziej uporządkowany, a kary za „grzechy" większe. Kto wie drodzy przyjaciele… Może nawet uda się w tym roku skończyć z praktyką tworzenia przepisów nie mających żadnego sensu?[1] To byłby naprawdę udany rok…

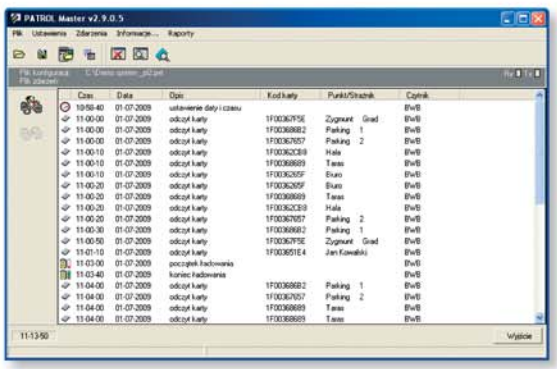
Grzegorz Ćwiek

1) Autor celowo nie wymienia tu przykładów, których jest aż nadto i każdy mógłby wymienić ich wiele.

PATROL II *LCD*

Dokumentuje rzetelność pracy

PATROL II LCD to uniwersalny, przenośny czytnik transponderów zbliżeniowych, przeznaczony do rejestracji obecności wartownika w wyznaczonych miejscach i określonych porach.



Patrol Master

Oprogramowanie zarządzające systemem rejestracji pracy wartowników. Udostępniane **bezpłatnie** na stronie www.roger.pl

PATROL II LCD to nowa wersja dobrze znanego rejestratora Patrol II wyposażona w szereg nowych funkcji podnoszących niezawodność działania urządzenia oraz dokładność weryfikacji rzetelności pracy wartowników.

rejestracja
pracy
wartowników

roger®

www.roger.pl

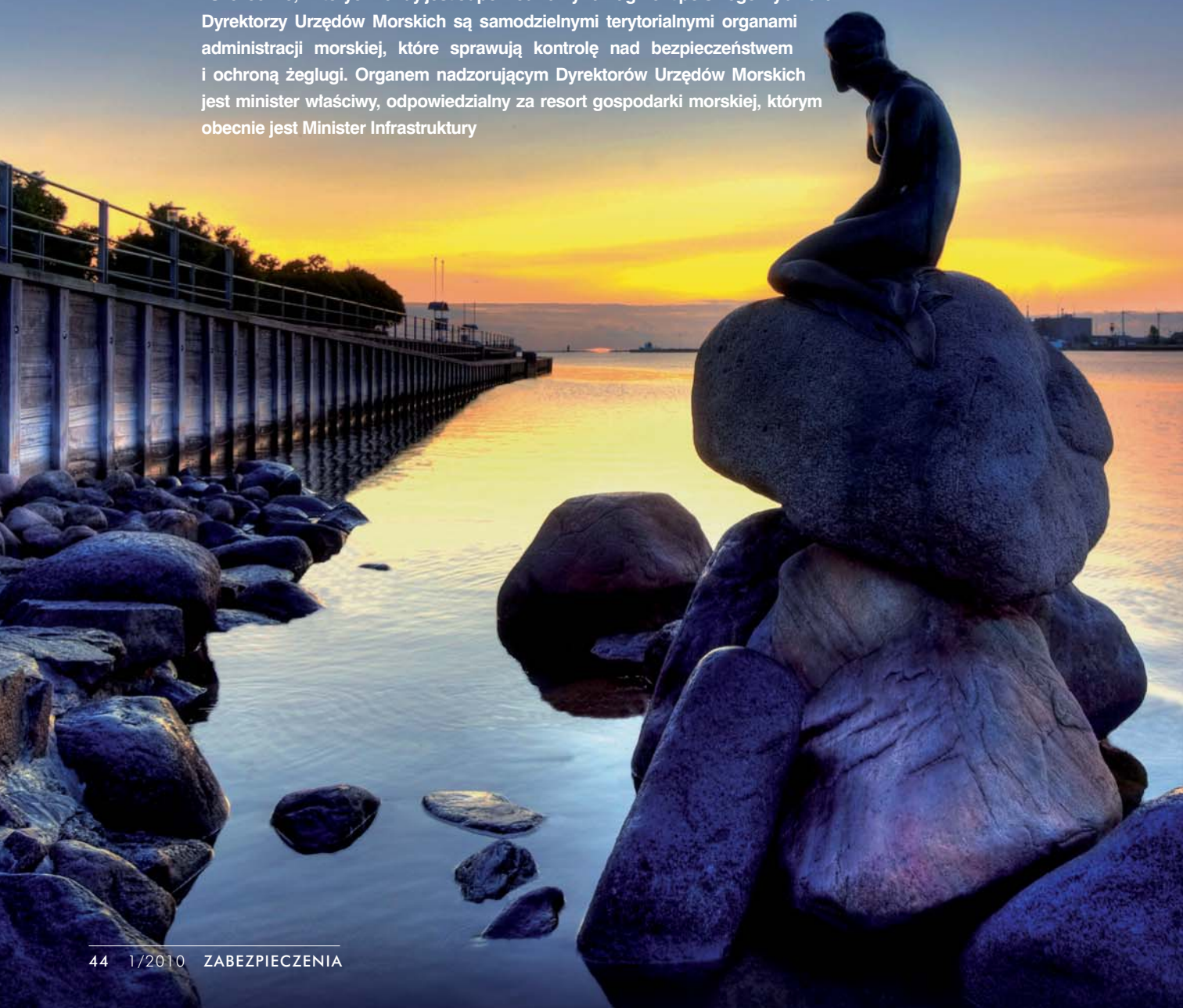
Wojciech Zdanowicz

Ochrona żeglugi i portów morskich

część 2

Pozostając przy tematyce ochrony żeglugi i portów, która w numerze 6/2009 *Zabezpieczeń* została ujęta z perspektywy międzynarodowej, niniejszy artykuł skupi się jedynie na wspomnianej wcześniej krajowej regulacji, tj. na ustawie z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz.U. Nr 171, poz. 1055). W tej ustawie przyjęto koncepcję ochrony żeglugi i portów przez organy administracji morskiej. Całość koordynacji zadań i nadzoru na szczeblu centralnym spoczywa na ministrze właściwym do spraw gospodarki morskiej, natomiast na szczeblu regionalnym za sprawy ochrony odpowiadają przede wszystkim dyrektorzy urzędów morskich. System ochrony żeglugi i portów morskich przewiduje ochronę portu jako całości, ochronę poszczególnych obiektów portowych oraz ochronę statków zawijających do portów. Dla wyjaśnienia należy zaznaczyć, że w Polsce funkcjonują trzy Urzędy Morskie, w Gdyni, Słupsku i Szczecinie, z których każdy jest odpowiedzialny za fragment polskiego wybrzeża.

Dyrektorzy Urzędów Morskich są samodzielnymi terytorialnymi organami administracji morskiej, które sprawują kontrolę nad bezpieczeństwem i ochroną żeglugi. Organem nadzorującym Dyrektorów Urzędów Morskich jest minister właściwy, odpowiedzialny za resort gospodarki morskiej, którym obecnie jest Minister Infrastruktury



W rozdziale pierwszym ustawa wprowadza podstawowe definicje oraz obowiązujące dokumenty odniesienia, które zawierają międzynarodowe przepisy w zakresie ochrony żeglugi i portów morskich lub które są wdrażane do polskiego prawa. Mowa tu o wspomnianych w poprzednim artykule[1] dokumentach[2].

Rozdział drugi określa organizację systemu ochrony żeglugi i portów morskich, wyznaczając organy i podmioty odpowiedzialne za ochronę, zakres tej odpowiedzialności oraz zadania, jakie będą przez nie realizowane. W dalszej części ustawy przedstawione zostały merytoryczne wymagania dla systemu ochrony żeglugi i portów morskich[3].

Ochrona portu

Zgodnie z definicją ustawy port obejmuje akweny i grunty oraz związaną z nimi infrastrukturę portową, na jego obszarze znajduje się jeden lub więcej obiektów portowych objętych postanowieniami Kodeksu ISPS.

Ustawa wprowadza pojęcie organu ochrony portu, którym jest dyrektor właściwego urzędu morskiego. Powierzenie dyrektorom urzędów morskich funkcji organu ochrony portu umożliwia realizowanie zadań ochrony na wszystkich obszarach portowych, zarówno tych administrowanych przez zarządy portów, jak i tych zarządzanych przez podmioty prywatne. Organ ochrony portu jest odpowiedzialny za przeprowadzenie oceny stanu ochrony portu oraz przygotowanie planu ochrony portu. Ocena stanu ochrony portu ma na celu zidentyfikowanie kluczowej infrastruktury na obszarze portu oraz ocenę ryzyka i zagrożeń w odniesieniu do tej infrastruktury. Plan ochrony portu ma określać sposób reakcji na zidentyfikowane zagrożenia i metodę ich neutralizacji. Obydwa wymienione dokumenty dotyczące ochrony portu podlegają odpowiednim uzgodnieniom na szczeblu lokalnym (z wojewodą i służbami mu podległymi) i muszą być zatwierdzone przez ministra właściwego do spraw gospodarki morskiej w porozumieniu z ministrem właściwym do spraw wewnętrznych.

Podobnie jak w przypadku obiektu portowego, dla całego portu wyznaczona zostaje osoba odpowiedzialna za koordynację ochrony w porcie. Jest nią oficer ochrony portu (PSO – *Port Security Officer*). Funkcja ta została powierzona kapitanowi portu jako osobie, w której jurysdykcji znajdują się wszystkie obiekty portowe i która najlepiej wie, jaka sytuacja w porcie jest w danym momencie.

Organ ochrony portu oraz oficer ochrony portu współdziałają w zakresie ochrony portu z podmiotem zarządzającym portem w sposób określony w ustawie oraz w planie ochrony portu. Oznacza to, że za praktyczne wdrożenie postanowień opracowanego przez administrację morską planu ochrony portu, a więc również za poniesienie związanych z tym kosztów, odpowiada podmiot zarządzający portem wraz z podmiotami zarządzającymi poszczególnymi obiektami portowymi.

Dotychczas wstępnie określono, że na terenie Polski znajduje się dziesięć portów, które w związku z faktem, że na ich obszarze znajdują się obiekty portowe, w rozumieniu Kodeksu ISPS, podlegać będą przepisom ustawy (porty w Gdańsku, Gdyni, Szczecinie, Świnoujściu, Policach, Władysławowie, Darłowie, Kołobrzegu, Ustce i Elblągu).

Ostateczna lista portów chronionych zgodnie z przepisami ustawy zostanie ogłoszona w obwieszczeniu Ministra Infrastruktury, które prawdopodobnie zostanie wydane do połowy 2010 r.

Należy zauważyć, że w praktyce wyszczególnienie portów w obwieszczeniu Ministra Infrastruktury nie musi oznaczać zamknięcia całych portów dla ruchu publicznego, co mogłoby być szczególnie uciążliwe, mieć negatywny wpływ na lokalną gospodarkę lub być dla niej niebezpieczne (zmniejszenie ruchu turystycznego). Identyfikacja obszarów szczególnie wrażliwych oraz zastosowanie środków ochrony będzie wynikało z oceny ryzyka przeprowadzanej w ramach opracowania ocen stanu ochrony portów.

Ochrona obiektu portowego

Za ochronę obiektu portowego odpowiedzialny jest zarządzający obiektem portowym. Podmiot ten ma obowiązek wyznaczenia oficera ochrony obiektu portowego (PFSO) oraz współdziałania z organami administracji morskiej, Strażą Graniczną, policją oraz Państwową Strażą Pożarną, a także Służbą Celną w celu realizacji ochrony w obiekcie portowym. Podmiot zarządzający obiektem portowym jest również zobowiązany do zapewnienia technicznych i finansowych środków związanych z realizacją ochrony konkretnego obiektu portowego.

Ochrona obiektu portowego opiera się na planie ochrony obiektu portowego. Z kolei jego sporządzenie opiera się na dokonanej wcześniej ocenie stanu ochrony obiektu portowego, przygotowanej przez dyrektora właściwego urzędu morskiego. Ocena ochrony obiektu portowego, po uzgodnieniu na szczeblu lokalnym (z wojewodą i podległymi mu służbami), podlega zatwierdzeniu przez ministra właściwego do spraw gospodarki morskiej.

Na podstawie tej oceny plan ochrony obiektu portowego jest przygotowywany przez PFSO, a następnie podlega zatwierdzeniu przez organ, który sporządził ocenę stanu ochrony obiektu portowego – dyrektora właściwego terytorialnie urzędu morskiego.

Obecnie w Polsce operuje ok. 70 obiektów portowych. Listy obiektów portowych są ogłaszane przez dyrektorów właściwych urzędów morskich w drodze zarządzeń porządkowych. Podobnie jak w przypadku portów, środki, które muszą być zastosowane w celu ochrony obiektu portowego, będą wynikać z oceny ryzyka przeprowadzanej w ramach oceny stanu ochrony obiektu portowego.

---

1) Zabezpieczenia nr 6(70)/2009.

2) Są to:
– międzynarodowa konwencja o bezpieczeństwie życia na morzu (Konwencja SOLAS),
– międzynarodowy kodeks dla ochrony statków i obiektów portowych (Kodeks ISPS),
– rozporządzenie (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie wzmocnienia ochrony statków i obiektów portowych,
– dyrektywa 2005/65/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie wzmocnienia ochrony portów.

3) W związku z szerokim zakresem regulacji, które dotyczą w równie szerokim stopniu statków, obiektów portowych i portów, dla potrzeb niniejszego artykułu oraz w związku z faktem, że problematyką ochrony statku zajmują się głównie przedsiębiorstwa armatorskie, instytucje klasyfikacyjne oraz administracja morska, omówione zostaną jedynie wymagania odnośnie portów i obiektów portowych.

Weryfikacja i kontrola

Ochrona portów oraz obiektów portowych podlega weryfikacjom na zgodność z postanowieniami ustawy oraz wspomnianych przepisów międzynarodowych. Weryfikacje portów są przeprowadzane co najmniej raz na pięć lat przez zespół powoływany przez ministra właściwego do spraw gospodarki morskiej. Obiekty portowe są kontrolowane co najmniej raz do roku przez zespoły powoływane do tego celu przez dyrektora właściwego urzędu morskiego. Wspomniane zespoły mogą również dokonywać kontroli doraźnych w okresie pomiędzy weryfikacjami.

Uznana organizacja ochrony (RSO)

Minister właściwy do spraw gospodarki morskiej może upoważnić uznaną organizację ochrony do prowadzenia działalności w zakresie oceny i weryfikacji, zatwierdzania lub certyfikacji, zgodnie z wymaganiami określonymi w Kodeksie ISPS oraz rozporządzeniu (WE) nr 725/2004.

Upoważnienie RSO następuje w drodze decyzji ministra właściwego do spraw gospodarki morskiej, w uzgodnieniu z ministrem właściwym do spraw wewnętrznych.

Podmiot ubiegający się o upoważnienie powinien złożyć wniosek z proponowanym zakresem upoważnienia oraz dokumentacją stwierdzającą spełnienie kryteriów określonych w załącznikach do ustawy. Organizacja, która uzyskała upoważnienie, podlega kontroli przeprowadzanej przez ministra właściwego do spraw gospodarki morskiej co najmniej raz na dwa lata. W tym miejscu należy zaznaczyć, że zakres upoważnienia RSO został w ustawie ograniczony w porównaniu do możliwości, jakie zostały przewidziane w przepisach międzynarodowych. W praktyce oznacza to, że w Polsce RSO może zostać upoważniona do:

- sporządzania oceny stanu ochrony portu, konkretnego obiektu portowego lub więcej niż jednego obiektu portowego oraz wprowadzania poprawek do tej oceny,
- sporządzania, na podstawie ocen stanu ochrony portu lub obiektu portowego, planu ochrony portu lub obiektu portowego oraz wprowadzania poprawek do tego planu,
- doradzania lub udzielania pomocy zarządzającym portami lub obiektami portowymi w sprawach ochrony.

Poziomy ochrony

W ślad za obowiązującym prawodawstwem międzynarodowym i europejskim projektowana ustawa przyjmuje koncepcję trzech poziomów ochrony w odniesieniu do statków, obiektów portowych i portów.

Wyznaczenie trzeciego poziomu ochrony jest środkiem wyjątkowym, stosowanym jedynie wtedy, gdy istnieją wiarygodne informacje, że zdarzenie naruszające ochronę jest prawdopodobne lub powoduje bezpośrednie zagrożenie. Poziom ochrony 3 powinien być wyznaczany jedynie na czas zidentyfikowanego zagrożenia lub rzeczywistego zdarzenia naruszającego ochronę, ponieważ środki zapobiegawcze przewidziane dla tego poziomu ochrony mogą powodować bardzo duże utrudnienia w normalnych operacjach przebiegających na terenie obiektu portowego lub na statku, np. wstrzymanie załadunku/wyładunku statków.

W celu zapewnienia ciągłości zadań i odpowiedzialności za podejmowanie decyzji w sytuacji, gdy zostanie wprowadzony poziom ochrony 3 oraz dojdzie do naruszenia ochrony, przepisy ustawy zostały powiązane z ustawą z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. Nr 89, poz. 5 z późn. zm.).

Szkolenia w zakresie ochrony statku, obiektu portowego i portu

Zgodnie z ustawą o bezpieczeństwie morskim szkolenia w zakresie ochrony są prowadzone przez uznawane i nadzorowane przez ministra właściwego do spraw gospodarki morskiej wyższe szkoły morskie oraz uznawane i nadzorowane przez dyrektora właściwego urzędu morskiego ośrodki szkoleniowe. Szkolenia odbywają się zgodnie z modelowym programem przygotowanym przez Międzynarodową Organizacje Morską (IMO) oraz rozporządzeniem Ministra Infrastruktury. Obecnie do szkolenia z zakresu obowiązków PFSO upoważnionych jest dwanaście ośrodków.

Kontrola osób, bagażu i ładunku

Przewiduje się, że obowiązki przeprowadzania kontroli osób udających się na teren portu, obiektu portowego lub na statek będą spoczywały na jednostce ochrony portu lub obiektu portowego, która będzie współpracować w tym zakresie z policją. Zakres współpracy będzie wynikać z planu ochrony portu lub obiektu portowego.

Jednostkę ochrony portu lub obiektu portowego będzie stanowić specjalistyczna uzbrojona formacja ochronna wykonująca zadania w zakresie ochrony żeglugi i portów morskich, działająca na podstawie przepisów ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. Nr 145 z 2005 r., poz. 1221 z późn. zm.) i zgodnie z tymi przepisami. Ponadto działania i uprawnienia jednostki ochrony portu lub obiektu portowego zostały rozszerzone przepisami ustawy o ochronie żeglugi i portów morskich i należą do nich:

- niedopuszczenie do wejścia osoby nieposiadającej wymaganych uprawnień na obszar lub do obiektu podlegającego ochronie,
- kontrola manualna i przeglądanie zawartości bagażu,
- stosowanie urządzeń technicznych do wykrywania przedmiotów lub substancji.

W związku z posiadaniem dodatkowych obowiązków i uprawnień kierownik jednostki będzie musiał zapewnić, że pracownicy jednostki ochrony posiadają odpowiednie przeszkolenie. Nadzór nad służbą ochrony portu lub obiektu portowego będzie wykonywać policja.

Jednostka ochrony portu lub obiektu portowego będzie dokonywać również kontroli ładunków przeznaczonych do transportu na teren portu. W tym przypadku będzie ona współdziałać ze Służbą Celną lub Strażą Graniczną, ponieważ właśnie te służby mają odpowiednie uprawnienia wynikające z ich ustaw kompetencyjnych.

Katalog przedmiotów i substancji, których posiadanie i transport są zabronione, zostanie określony rozporządzeniem ministra właściwego do spraw gospodarki morskiej w porozumieniu z ministrem właściwym do spraw wewnętrznych. Szczegółowe metody i środki kontroli i ochrony zostaną natomiast określone przez Radę Ministrów.

Wojciech Zdanowicz

Sygnalizatory z komunikatami głosowymi

światło i dźwięk dla bezpieczeństwa

SG-Pgw

- montowane przez puszkę PIP-3A

SGO-Pgz

- lampa ksenonowa z podwójnym błyskiem
- montowane przez puszkę PIP-4A

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

Wewnętrzne i zewnętrzne **sygnalizatory z komunikatami głosowymi** firmy W2 jako jedyne tego typu urządzenia na rynku **uzyskały certyfikaty i świadectwa dopuszczenia CNBOP**. Wyróżniają je cechy takie jak możliwość wgrywania **do 4 dowolnych komunikatów**, synchroniczna praca w sieci. Sygnalizatory SGO-Pgz i SG-Pgw umożliwiają ponadto **proste adresowanie komunikatów** i współpracę z wyłącznikiem sygnału dźwiękowego WSD-1. Posiadają również przydatne funkcje takie jak ustalenie priorytetu komunikatów i zabezpieczenie przed utratą synchronizacji.

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

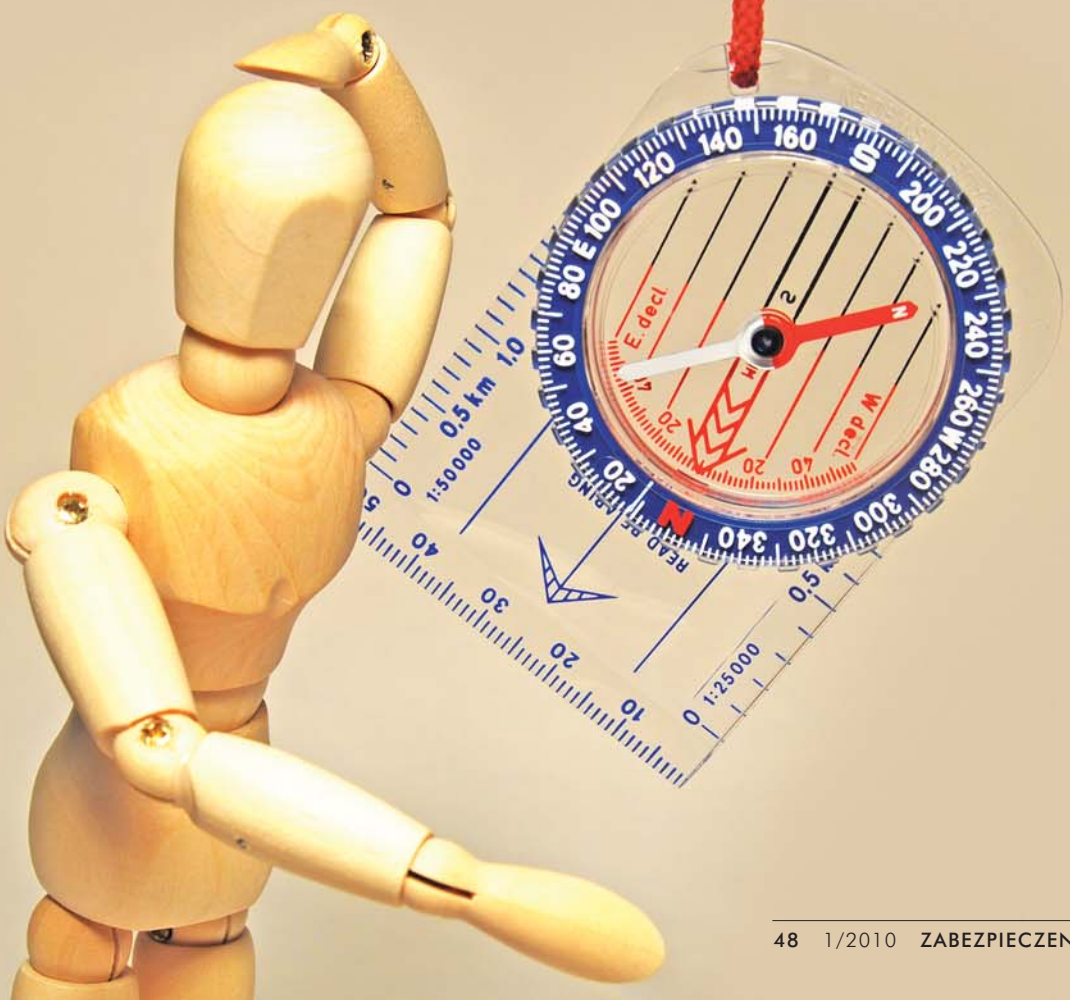
Technologie Potrzeby Wybory

Sławomir Piela

Sytuacja, w której pojawia się możliwość lub konieczność implementacji nowych rozwiązań informatycznych jest częstsza niż mogłoby się z pozoru wydawać. Z systemami komunikacji e-mail, usługami hostingowymi, systemami księgowymi, systemami zarządzania relacjami z klientami i specyficznymi dla branży security systemami monitorowania stykamy się co jakiś czas, weryfikując choćby przelotnie ich przydatność dla funkcjonowania naszej organizacji

Szczególną rolę pośród systemów informatycznych zajmują systemy księgowe, zarządzania relacjami z klientami oraz specjalizowane systemy monitorowania. Coraz częściej pomiędzy tymi systemami pojawiają się różnego rodzaju sprzężenia. Postępuje także ich integracja. Niemożność podjęcia decyzji o zastosowaniu pewnych rozwiązań jest często spowodowana brakiem uporządkowanej i spójnej wizji potrzeb i potencjalnych rozwiązań.

Niestety często decydującym elementem w procesie decyzyjnym jest przypadek, błędny rachunek kosztów i zysków oraz brak systematycznej analizy napotkanych rozwiązań pod kątem stosowanych technologii. Skupianie się na powierzchownych elementach oferty marketingowej powoduje często błędny wybór rozwiązania skutkujący zablokowaniem możliwości rozwoju, uzyskaniem korzyści niższych od spodziewanych lub utratą czy też zablokowaniem możliwości uzyskiwania przewagi konkurencyjnej i dodatkowych dochodów. Jednym z możliwych efektów błędnego wyboru jest także zwiększenie ryzyka



biznesowego. Należy zatem zastanowić się, jakie są właściwe metody oceny i mechanizmy wyboru rozwiązań informatycznych. Wydaje się, że jest kilka elementów kluczowych, które często są pomijane.

Pierwszy z nich to solidna identyfikacja potrzeb, która powinna obejmować także prognozę rozwoju firmy w kontekście tego, w jakim segmencie rynku i jak chcemy ją pozycjonować. Rzetelne określenie miejsca i perspektyw rozwoju pozwoli określić narzędzia, za pomocą których możemy zrealizować cel. Błąd na tym etapie może spowodować, iż potencjał firmy nie zostanie wykorzystany właściwie i zmarnowane zostaną szanse na rozwój.

Ważne jest okresowe badanie potrzeb klientów i sprawdzanie zdolności obecnej infrastruktury firmy do ich zaspokajania. Zrealizowanie pozornie przeciwstawnych celów (np. obniżenie cen a zarazem zwiększenie liczby dostępnych usług) nie musi być niemożliwe. Istnieją rozwiązania systemowe, które pozwalają na jednoczesne obniżenie kosztów działania firmy (np. poprzez usprawnienie procesu obiegu informacji wewnętrznej, ograniczenie nakładów finansowych i czasowych na obsługę klienta) i podwyższenie poziomu świadczonych usług.

Kolejny element to rzetelna weryfikacja jakości systemu, którego wdrożenie planujemy. Poświęcenie czasu na pełne testy wydajności, stabilności i funkcjonalności systemu gwarantuje redukcję ryzyka przy przejściu na nowe rozwiązanie. Testy te powinny obejmować także zapoznanie się ze sposobem działania serwisu i wsparcia dla nowego rozwiązania oraz kontakt z firmami podobnymi do naszej, które już korzystają z tego systemu[1].

Ostatni etap jest trudny, szczególnie w kontekście oceny technologii proponowanych przez nowego partnera. Ocena proponowanych rozwiązań technologicznych wymaga zasięgnięcia opinii z zewnątrz, jeśli nie mamy własnych służb technicznych zdolnych do prawidłowej oceny tych rozwiązań.

Proponowane technologie powinny gwarantować skalowalność i zdolność do rozbudowy danego systemu tak, aby w perspektywie kilku lat nie stanąć przed koniecznością kolejnej jego zmiany.

Przedmiotem oceny powinna być między innymi wykorzystywana technologia komunikacji z bazami danych. Systemy pracujące bezpośrednio na bazach danych obarczone są szeregiem problemów (bezpieczeństwo, zasobożerność, interakcja z innymi systemami), których unika się dzięki stosowaniu nowoczesnej technologii trójwarstwowej. Technologia ta traktuje bazę danych jako repozytorium informacji przetwarzanych przez moduł główny. Jej wykorzystanie wymaga wiedzy i jest pracochłonne, za to pozwala na rozbudowę oraz zapewnia wyższy poziom bezpieczeństwa niż starsze rozwiązania, które pracują bezpośrednio na bazach danych. Kolejną ważną zaletą, szczególnie w przypadku dużych rozwiązań, jest możliwość przejścia na większy silnik bazodanowy w relatywnie krótkim czasie. Struktura taka daje także ogromną elastyczność zarówno producentowi, jak i użytkownikowi, który może samodzielnie uzyskiwać dostęp do baz danych i tworzyć autorskie elementy rozwiązania. Niebagatelne znaczenie ma także fakt, iż stosowanie tej technologii umożliwia pełną integrację z innymi systemami w sposób naturalny i bez konieczności bezpośredniego dostępu do baz danych. Protokoły komunikacji w tej technologii pozwalają na wynoszenie elementów systemu (np. do podwykonawców, kluczowych klientów, innych oddziałów itp.) w sposób naturalny i nie wymagają one łączy o dużej przepustowości – potrafią pracować nawet na łączach GPRS.

Cenną zaletą systemu, na którą warto zwrócić uwagę, jest sposób, w jaki zachowuje się on w przypadku konieczności obsługi dużych ilości danych czy też sytuacji nietypowych. Nowoczesny system powinien mieć mechanizmy pakowania danych i synchronizacji buforów. O ile bezpośrednia weryfikacja tego, czy takie mechanizmy zostały zaimplementowane czy nie, jest w zasadzie niemożliwa bez wglądu do kodu źródłowego, o tyle można przetestować ich działanie poprzez przeciążenie systemu istotnie nadmiarową liczbą alarmów lub sygnałów oraz wykonanie zestawienia na bardzo dużej liczbie danych. Na przykład jednoczesne uderzenie 10 000 sygnałów w system, czy też wykonanie przekrojowego zestawienia z długiego okresu, nie powinno spowodować zatrzymania pracy systemu. Sytuacje te, chociaż nie są typowe, mogą się pojawić np. w przypadku chwilowej utraty komunikacji z kanałem transmisji (np. utraty łączności z siecią GSM) lub błędnie wybranego zakresu danych do raportu. System posiadający wyżej wspomniane mechanizmy pozwoli na zatrzymanie raportu w dowolnym momencie, przetworzy cały pakiet sygnałów i nie będzie wykazywał spowolnienia przy obsłudze nawet tysięcy jednocześnie otwartych alarmów.

Trudnym do sprawdzenia elementem są zdolności integracyjne systemu. Poza stacjami bazowymi, które można podłączyć równolegle, pozostaje tylko kontakt z firmami korzystającymi ze sprzętu innego niż ten, który jest dostępny dla nas, i zasięgnięcie ich opinii.

Innymi nowoczesnymi technikami są praca grupowa i automatyzacja. O ile ta ostatnia istnieje już od jakiegoś czasu na rynku w różnych formach, to praca grupowa, będąca daleko idącym rozwinięciem automatyzacji, jest nową jakością. Technika ta pozwala na zlecanie i przyjmowanie obsługi zdarzeń alarmowych ze współpracujących firm. Przy tej wymianie zachowana jest poufność danych, kontrola dotarcia sygnałów oraz kontrola tempa przyjęcia zlecanych do obsługi zadań. W obliczu istniejących w branży ochrony trendów ta funkcjonalność, wraz z techniczną zdolnością i systemu, i producenta do wykonywania sprzęgów z dowolnymi systemami, jest elementem, którego nie można pominąć podczas oceny systemu. Warto także zwrócić uwagę na wymagania sprzętowe systemu. Niższe wymagania sprzętowe to niższe koszty i większa wydajność systemu.

Reasumując, ocena istniejących systemów powinna podlegać audytowi w zadanych odstępach czasowych pod kątem przydatności do zaspokajania bieżących i przyszłych potrzeb klientów, a ocena pojawiających się rozwiązań wymaga zaangażowania, wkładu pracy i wiedzy. Jednym z podstawowych elementów oceny powinny być stosowane technologie, które warunkują zdolność systemu do adaptowania się do wciąż zmieniających się warunków rynkowych. Ważny jest też sposób dostępu do danych. Aby nie narażać się na uzależnienie od jednego dostawcy, należy każdorazowo upewnić się, czy będzie istniała możliwość konwersji gromadzonych przez nas danych w przypadku przejścia na inny system.

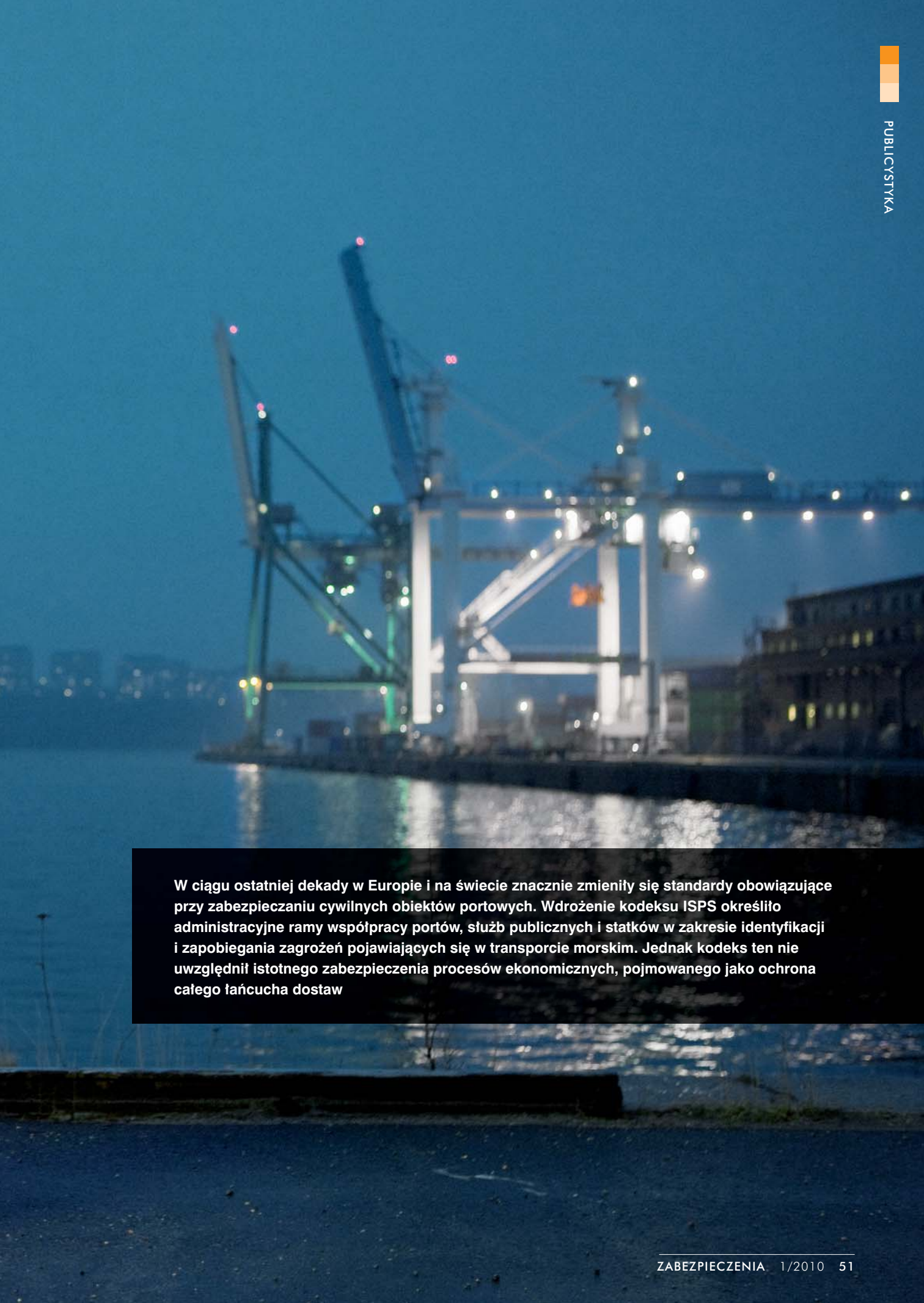
Sławomir Piela
Next!

1) Lub „już wykorzystują ten system”.

AEO

Nowe standardy bezpieczeństwa w sektorze techniki morskiej

Tomasz Warejko-Rowdo



W ciągu ostatniej dekady w Europie i na świecie znacznie zmieniły się standardy obowiązujące przy zabezpieczaniu cywilnych obiektów portowych. Wdrożenie kodeksu ISPS określiło administracyjne ramy współpracy portów, służb publicznych i statków w zakresie identyfikacji i zapobiegania zagrożeń pojawiających się w transporcie morskim. Jednak kodeks ten nie uwzględnił istotnego zabezpieczenia procesów ekonomicznych, pojmowanego jako ochrona całego łańcucha dostaw

Firmy zajmujące się obrotem międzynarodowym, które chcą uzyskać status Uprzywilejowanego Podmiotu Gospodarczego (AEO – ang. *Authorized Economic Operator*), muszą spełnić zupełnie nowe wymagania. Od roku 2008 na terenie państw UE zaczęto wdrażać program AEO promujący firmy mające skodyfikowany i kompleksowy wkład w system bezpieczeństwa procesów ekonomicznych. Status AEO nie jest obligatoryjny, lecz daje szereg ułatwień firmie, która go uzyska. W krajach europejskich szczególnie zainteresowane nim są firmy logistyczne, armatorzy oraz porty. Jest to związane przede wszystkim z tym, że posiadacz świadectwa AEO podlega mniejszej liczbie kontroli fizycznych i kontroli dokumentów. Ponadto może podawać mniej danych na potrzeby przywozowej/wywozowej deklaracji skróconej. Dodatkowe korzyści obejmują priorytetową obsługę zgłoszeń celnych oraz priorytetową obsługę wszelkich wniosków o wydanie pozwoleń czy zaświadczeń.

Uzyskanie certyfikatu AEO jest wynikiem spełnienia ścisłych i rygorystycznych wymagań w zakresie bezpieczeństwa i ochrony. Stanowią one zespół norm opartych na standardzie ISO 28000 i dotyczą takich elementów, jak organizacja wewnętrzna środków bezpieczeństwa, zabezpieczenie wstępu na teren obiektu, ochrona fizyczna, ochrona jednostek cargo i procesów logistycznych. Struktura takiego systemu zbudowana jest z szeregu bardzo precyzyjnych procedur mających na celu minimalizację ryzyka wystąpienia negatywnych incydentów, które mogą zagrozić bezpieczeństwu łańcucha dostaw.

Takie podejście do zasad bezpieczeństwa jest dużym wyzwaniem dla firm zajmujących się usługami ochrony. Wymaga coraz większej profesjonalizacji, także przy opracowywaniu i wdrażaniu poszczególnych procedur. Wobec zmieniających się uwarunkowań podmioty gospodarcze zostają zmuszone do przeniesienia części odpowiedzialności za zabezpieczenie procesów ekonomicznych na wyspecjalizowanego operatora ochrony. Jest to więc szansa na zastosowanie i wypróbowanie najnowszych rozwiązań technicznych i systemowych.

Do tej pory ochronę postrzegano jako element, który wymaga najmniej inwestycji i modernizacji. Kalkulowano przede wszystkim bezpośrednie koszty i wybierano warianty najtańsze i najprostsze. Efektywność działania miała znaczenie drugorzędne.

Korzyści, jakie daje status AEO, spowodowały reorientację w spojrzeniu na zasady bezpieczeństwa i, co za tym idzie, na dostawcę usług ochrony. Bezpieczeństwo stało się wymierną wartością dodaną, a kwestie merytoryczne stały się pierwszoplanowe. Inwestowanie w rozwój sektora ochrony zaczęło się po prostu opłacać. Zaowocowało to opracowaniem zaawansowanych technologicznie systemów wykorzystujących rozwiązania sieciowe.

Bardzo ciekawe są rozwiązania tego typu zastosowane w ochronie obiektów portowych starających się o uzyskanie świadectwa AEO. Warto przyjrzeć się szczególnie opracowanym przez Securitas systemom zabezpieczeń dla portu w Rotterdamie oraz portu Kotka w Finlandii. Stanowią one doskonały przykład odejścia od tradycyjnych usług dozorowych, stosowanych w ochronie fizycznej.

Uniport w Rotterdamie nazywany jest wrotami Europy. Jest to największy terminal kontenerowy w Holandii. Obsługuje 40% całego przeładunku kontenerów przesyłanych na kontynent europejski. Pod koniec 2009 roku uzyskał certyfikat AEO. Kwestie bezpieczeństwa są w nim traktowane absolutnie priorytetowo. Securitas opracował i wdrożył tam sieciowy system bezpieczeństwa, który obejmuje systemy CCTV i biometryczne karty dostępu. Obszar Uniportu jest podzielony na trzy strefy bezpieczeństwa. Każda z nich jest objęta innym kodem dostępu. Ponadto znajdują się tam specjalne strefy, wydzielone dla towarów objętych szczególnym nadzorem. Warto zwrócić uwagę na zintegrowany system kontroli przepływu kontenerów i odpraw samochodów ciężarowych. Zastosowano w nim tzw. Visual Gate. Jest to całkowicie automatyczny terminal odpraw ciężarówek i kontenerów, wyposażony w specjalny zestaw kamer wraz z podświetlaczami. Kamery skanują dane kontenera, zabezpieczeń i plomb oraz tablic rejestracyjnych i stanu pojazdu. Następnie przesyłają całość danych do weryfikującego je serwera bazy odpraw. Wystarczy, że pracownik ochrony wpisze do komputera dane kierowcy podjeżdżającego do odprawy, a system natychmiast sprawdzi zgodność stanu pojazdu z dokumentami przewozowymi i pozwolenie na przejazd zostanie udzielone automatycznie. Visual Gate jest zintegrowana z bramą wykrywającą materiały radioaktywne. Całość systemu ochrony Uniportu jest obsługiwana przez jednego(sic!) operatora ochrony.

Nasycenie Uniportu zaawansowaną techniką i zastosowanie w nim rozwiązań sieciowych pozwoliło zredukować czynnik ludzki do absolutnego minimum. Całkowicie zrezygnowano z wykonywania przez pracowników ochrony żmudnych i powtarzalnych czynności kontrolnych. Zminimalizowano tym samym potencjalne ryzyko błędu ludzkiego, które jest istotnym zagrożeniem dla tego typu operacji. Tam, gdzie duża liczba restrykcyjnych procedur wymaga dokładnej i stałej kontroli, pojawia się groźba rutyny, obniżającej czujność i dokładność. Wartością dodaną całego sytemu jest znaczne przyspieszenie odpraw i kontroli. Przy natężeniu ruchu, jaki występuje w Uniporcie, dokładne kontrolowanie każdego pojazdu przez zespół ludzi szybko doprowadziłyby do zatoru i wstrzymania ciągłości przepływu. W efekcie doszłoby do strat finansowych. Zastosowane rozwiązanie umożliwia stałą, błyskawiczną odprawę, a jednocześnie zachowanie niezbędnych procedur.

Port Kotka w Finlandii jest największym obszarem portowym w tym kraju. Podzielony jest na trzy regiony, które łącznie mają powierzchnię ponad 800 hektarów. Wyjątkowo trudny, rozległy teren, obfitujący w gęste lasy i sieć zbiorników wodnych, sprawił, że wymagana przez kodeks ISPS kontrola i ochrona portu była dużym wyzwaniem. Tradycyjne sposoby patrolowania wymagałyby bardzo licznego zespołu ochrony, aby sprostać standardom narzuconym przez ISPS. Dlatego Securitas opracował i wdrożył koncepcję wykorzystania specjalnych patroli mobilnych.

Cały obszar portu Kotka jest nasycony nowoczesną techniką telewizyjną. Jednostka patrolowa dysponuje pojazdami wyposażonymi w notebooki połączone bezprzewodowo z siecią kamer. Patrol odbiera bieżące obrazy ze wszystkich

kamer nadzorujących obszar portowy. Zastosowanie inteligentnych kamer z detekcją ruchu daje natychmiastową informację o naruszeniu obserwowanego obszaru. Czas reakcji patrolu ochrony na wszelkie zdarzenia na strzeżonym terenie zostaje skrócony do minimum. Mobilna jednostka patrolowa ma podgląd całego portu w trybie on-line i może w każdej chwili elastycznie reagować na zdarzenia na dowolnym odcinku. Zintegrowany system wyjątkowo efektywnie wykorzystuje załogi ochrony do zabezpieczania bardzo rozległego obszaru. Stanowi połączenie ruchomego centrum monitoringu z grupą interwencyjną.

Takie inicjatywy, jak AEO na pewno zmienią sposób pojmowania bezpieczeństwa. Myśląc o ochronie i zabezpieczeniach, ludzie nie będą już wyobrażać sobie tylko dozorcy w budce, ewentualnie wspomaganego przez najprostsze kamery CCTV. Coraz więcej zadań dozorowych przejmie bardziej wyrafinowana technologia. Zamiast słabo przeszkolonych pracowników pilnujących terenu, potrzebne staną się wykwalifikowane i wyspecjalizowane zespoły. Wykwalifikowani specjaliści będą opracowywać indywidualne rozwiązania dla każdego typu obiektu oraz nadzorować właściwe funkcjonowanie kompleksowego systemu bezpieczeństwa. Wiąże się to oczywiście z innymi wynagrodzeniami za usługi ochrony, lecz korzyści płynące z dostosowania się do standardów ISO 28000 i AEO spowodują, że inwestowanie w bezpieczeństwo stanie się opłacalne.

W Polsce program AEO jest mało popularny. Dla wielu przedsiębiorców stosunek korzyści z uzyskania tego statusu do sił i środków, jakie należy w tym celu zaangażować, jeszcze nie jest jasny. Dotychczas stosunkowo niewiele podmiotów podjęło starania, aby uzyskać certyfikat AEO; do tej pory nie uzyskał go żaden z największych portowych terminali kontenerowych. Mimo to integracja ekonomiczna wymusi także u nas dostosowanie się do europejskich norm bezpieczeństwa biznesu. Tym samym zmieni to sposób postrzegania dostawców usług ochrony i wykorzystania ich wiedzy, technologii i kompetencji. Jest to duża szansa rozwoju dla tych firm, które posiadają właściwy potencjał ludzki i techniczny oraz doświadczenie w pracach nad najnowszymi rozwiązaniami technicznymi i proceduralnymi w obszarze zabezpieczeń.

Tomasz Warejko-Rowdo
Securitas Polska

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

NOWE kamery IP serii T1

kamery kolorowe i dzień/noc

- praca w trybie dwustrumieniowym
- sprzętowa detekcja ruchu
- funkcje przed-alarmu i po-alarmu - nagrywanie wideo w formacie AVI
- w zestawie oprogramowanie NMS (NOVUS MANAGEMENT SYSTEM) - do rejestracji wideo, podglądu "na żywo", odtwarzania oraz zdalnej konfiguracji urządzeń wideo IP

Kamera kompaktowa NVIP-TC5400C
- kontrola połączenia sieciowego oraz funkcja sprawdzania adresu IP
- możliwość zapisu plików na karcie SD/SDHC

Kamera megapikselowa kopułkowa NVIP-TC2400D/MPX1.3
- wysoka rozdzielczość megapikselowa SXGA - 1280x1024
- obiektyw asferyczny, f=3.7~12 mm
- kontrola połączenia sieciowego oraz funkcja sprawdzania adresu IP
- możliwość zapisu plików na karcie SD/SDHC

Kamera w obudowie z oświetlaczem IR NVIP-TDN3400H/IR-3
- mechaniczny filtr podczerwieni, oświetlacz IR - 42 diody LED
- obiektyw asferyczny, f=3.7~12 mm

NMS Compatible

Wyłączny dystrybutor produktów NOVUS® w Polsce:

AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 022 546 05 46, faks 022 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Wykorzystanie telefonii mobilnej i Internetu

w procesie przekazywania informacji w systemach nadzorujących stan chronionego obiektu

Marcin Buczaj

Prawidłowe działanie systemu nadzoru polega na szybkim procesie neutralizacji występujących zagrożeń. Aby ten proces przebiegał szybko i skutecznie, muszą istnieć sprawne i niezawodne systemy komunikacyjne, przekazujące informację o stanie obiektu między poszczególnymi komórkami systemu. Do najnowszych takich układów należą systemy zabezpieczające, współpracujące z siecią telefonii mobilnej GSM i siecią internetową. W artykule zwrócono uwagę na możliwości wykorzystania struktur sieci GSM i Internetu do budowy mobilnych systemów kontrolujących i sterujących pracą poszczególnych elementów w zintegrowanych systemach zarządzających. Przedstawiono również analizę czynników wpływających na proces przekazywania informacji oraz ich wpływ na czas neutralizacji zagrożenia

1. Wstęp

Im krótszy jest czas pomiędzy chwilą wykrycia zagrożenia a reakcją użytkownika systemu na dane zagrożenie, tym większa jest szansa na ograniczenie szkód wywołanych tym zagrożeniem [2]. Aby spełnić powyższe kryterium, konieczne jest wykorzystanie takich technologii, które są autonomiczne i ogólnie dostępne, mają wystarczającą przepustowość łączy oraz gwarantują odpowiedni poziom zachowania poufności przesyłanej informacji. Obecnie takie możliwości daje zastosowanie w systemach nadzorujących stan obiektu elementów umożliwiających współpracę tych systemów z infrastrukturą sieci telefonii mobilnej GSM i sieci internetowej. Wykorzystanie tych dwóch mediów informacyjnych daje dodatkowo możliwość uproszczenia procesów związanych z przekazywaniem informacji na drodze obiekt – użytkownik oraz ograniczenia kosztów użytkowania systemu.

W artykule zostanie przedstawiony wpływ zastosowania technologii GSM i Internetu na przebieg procesu neutralizacji zagrożenia. Poprzez przedstawienie różnych sytuacji, które mogą się urzeczywistnić podczas normalnej pracy systemu, dokonana będzie analiza wpływu zastosowanego rozwiązania technicznego na:

– funkcjonowanie systemu,
– zwiększenie możliwości systemu,
– przebieg poszczególnych etapów procesu neutralizacji zagrożenia,
– czas procesu neutralizacji zagrożenia.

W artykule zwrócona zostanie również uwaga na możliwości wynikające z zastosowania infrastruktury GSM i Internetu jako czynników wpływających na charakterystykę i możliwości budowanego systemu nadzoru nad stanem chronionego obiektu. Zasygnalizowany zostanie również zarys możliwości systemu nadzoru, za pomocą którego możliwe jest przejęcie roli i funkcji realizowanych przez wyspecjalizowane stacje monitorujące stan chronionego obiektu przez użytkownika wyposażonego w telefon komórkowy i komputer z dostępem do sieci internetowej. Może to być szczególnie ważne w systemach instalowanych w obiektach małych, o stosunkowo niewielkiej wartości, w których koszty nadzoru mogą być stosunkowo duże w porównaniu z wartością zabezpieczanego mienia. Ponadto użytkownik systemu, który ma bieżącą informację o stanie obiektu i informację o wykrytych zagrożeniach, może wychodzić przy podejmowaniu decyzji poza sztywne schematy działania, jakie obowiązują przy działaniu służb zewnętrznych, i dopasowywanie za każdym razem decyzji do zaistniałej sytuacji.

2. Charakterystyka i ocena możliwości wykorzystania infrastruktury GSM i Internetu w systemach nadzoru nad stanem chronionego obiektu

Sieć GSM

Sieć GSM jest zespołem współpracujących ze sobą elementów, których podstawowym zadaniem jest dostarczenie usług telekomunikacyjnych dla ruchomych abonentów sieci. W tym celu elementy sieciowe komunikują się ze sobą za pomocą ściśle zdefiniowanych interfejsów, z których najbardziej charakterystyczny jest interfejs radiowy, realizowany w oparciu o pasmo częstotliwości GSM [1].

Standardowa infrastruktura sieci GSM składa się z następujących elementów:

– komórki (ang. *cells*),
– stacje bazowe – BTS (ang. *Base Transceiver Stations*),
– sterowniki stacji bazowych – BSC (ang. *Base Station Controllers*),
– cyfrowe centrale telefoniczne – MSC (ang. *Mobile Switching Centres*),
– centrale dostępowe – GMSC (ang. *Gateway Mobile Services Switching Centres*),
– rejestr abonentów macierzystych – HLR (ang. *Home Location Register*),
– rejestr abonentów wizytujących – VLR (ang. *Visitor Location Register*),
– centrum zarządzające wiadomościami SMS – SMSC (ang. *Short Message Service Center*).

Najważniejsze zalety zastosowania sieci GSM w systemach nadzorujących stan obiektu:

– ogólna dostępność i praktycznie nieograniczony zasięg,
– powszechność występowania urządzeń GSM,
– kompatybilność urządzeń ze standardem,
– brak procesu instalacji urządzeń do sieci (o ile nie zainstalowano funkcji SIM lock),
– brak konieczności logowania się do sieci,
– możliwość sprawdzania stanu systemu w sposób zdalny,
– możliwość zmian stanu systemu i poszczególnych jego elementów w sposób zdalny,
– możliwość archiwizowania zdarzeń w postaci tekstowej w pamięci telefonu,
– łatwa obsługa w standardzie.

Najważniejsze wady zastosowania sieci GSM w systemach nadzorujących stan obiektu:

– ograniczona przepustowość łącza,
– konieczność posiadania aktywnego numeru,
– przesyłanie tylko wybranych, odpowiednio spreparowanych i przetworzonych, informacji w formie SMS,
– nadzór nad obiektem w trybie on-line może przebiegać tylko na podstawie informacji dostarczanej w formie tekstowej (ewentualnie głosowej, po nawiązaniu połączenia telefonicznego).

Internet

Internet to międzynarodowa, połączona logicznie w jednolitą sieć adresową opartą na protokole IP sieć komputerowa, która służy do przesyłania informacji. Sieć ta dostarcza lub wykorzystuje usługi wyższego poziomu, które oparte są na funkcjonowaniu telekomunikacji i związanej z nią infrastrukturze [7].

Najważniejsze zalety zastosowania sieci Internet w systemach nadzorujących stan obiektu:

– duża przepustowość łącza,
– łatwy dostęp do informacji o stanie obiektu,
– możliwość tworzenia mobilnych systemów zarządzania,
– możliwość przesyłania informacji przetworzonej w postaci tekstowej lub graficznej,
– możliwość przesyłania informacji nieprzetworzonych w postaci obrazu i dźwięku,
– możliwość tworzenia zaawansowanych procedur związanych z nadzorem nad obiektem i sterowania poszczególnymi elementami systemu.

Najważniejsze wady zastosowania sieci Internet w systemach nadzorujących stan obiektu:

– problemy z dostępem do sieci mimo ogólnoświatowego zasięgu,
– konieczność uzyskania autoryzacji przy łączeniu się z siecią,
– brak możliwości ciągłego i pewnego monitorowania chronionego obiektu w przypadku mobilnych systemów zarządzania,
– konieczność posiadania odpowiedniego sprzętu komputerowego i infrastruktury sieciowej zarówno w chronionym obiekcie, jak i w miejscu zdalnego nadzoru.

3. Wykorzystanie infrastruktury sieci GSM i Internetu w procesie nadzoru nad stanem chronionego obiektu

Każde zastosowanie nowej technologii przeważnie ma na celu poprawę funkcjonowania danego systemu lub uzyskanie nowych możliwości, niedostępnych dla starej infrastruktury. W tej części artykułu zostaną przedstawione możliwości, jakie daje zastosowanie elementów wykorzystujących infrastrukturę sieci GSM i Internetu w systemach nadzoru nad stanem kontrolowanego obiektu. Analiza zostanie przeprowadzona pod kątem nowych możliwości oraz ich wpływu na działanie całego systemu i na czas przebiegu poszczególnych, występujących w systemach nadzorujących stan chronionego obiektu, procesów.

Proces wykrywania zagrożeń przez system nadzorujący

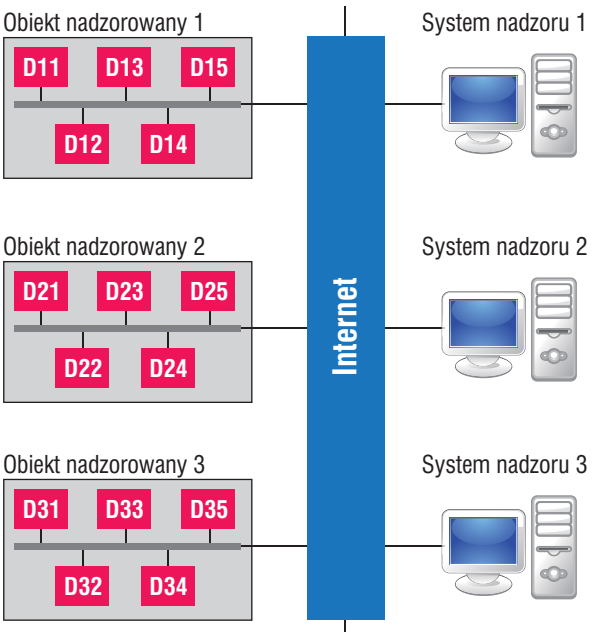
W procesie wykrywania zagrożeń przez system wykorzystuje się technologię GSM i Internet w celu komunikacji między poszczególnymi elementami systemu (szczególnie w przypadku systemów w obiektach rozproszonych). Można wyróżnić następujące zadania, jakie mogą być realizowane przez układy wyposażone w dostęp do Internetu lub wykorzystujące sieć GSM do komunikowania się:

A1) Zastosowanie elementów współpracujących z siecią internetową w części odpowiedzialnej za detekcję zagrożenia. Umożliwia to budowę systemu nadzoru dla obiektów o znacznym stopniu rozproszenia (Rys. 1).

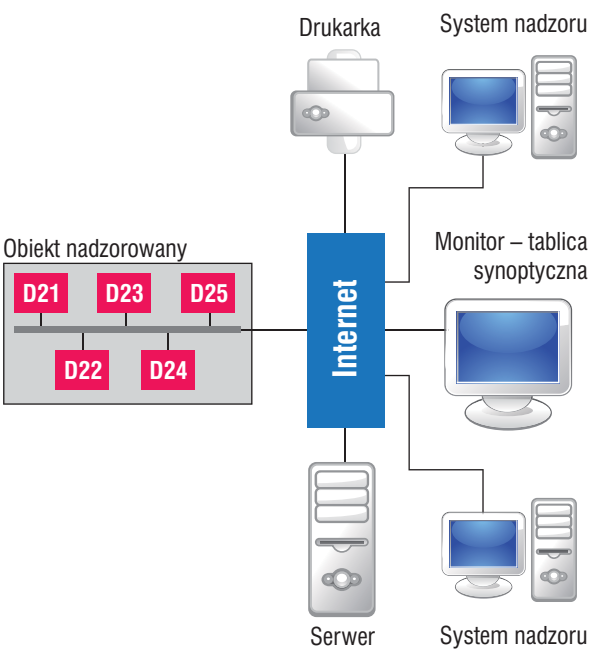
A2) Zastąpienie klasycznych (sprzętowych) układów służących do zbierania i analizy informacji układami wirtualnymi (programowymi) – rys. 1. Umożliwia to budowę rozproszonych układów analizująco-decyzyjnych o dowolnym stopniu powielenia, co utrudnia proces sabotażu i praktyczne eliminuje możliwość ingerencji w proces działania rejestratora zdarzeń.

A3) Tworzenie wirtualnych komputerowych systemów pomiarowych, czasami pracujących niezależnie, ukierunkowanych na różne podejścia do rejestrowanego przez układy detekcyjne sygnału (Rys. 2). Przesył całego, nieprzetworzonego strumienia informacji źródłowej i jego zdalna analiza umożliwia opracowanie adaptacyjnych algorytmów wykrywania zagrożenia, w których parametry oceny mogą się zmieniać w zależności od rejestrowanych parametrów innych elementów detekcyjnych.

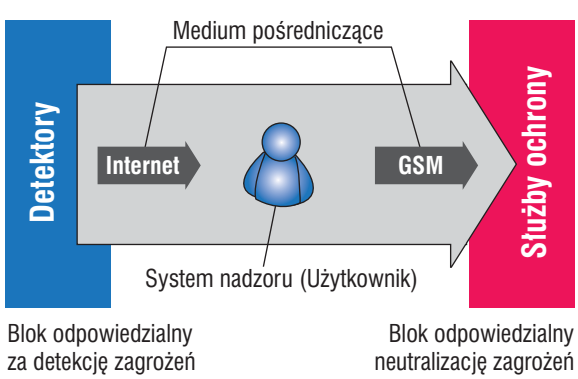
A4) Zdalne uwierzytelnianie użytkowników systemu na podstawie otrzymywanego za pośrednictwem Internetu obrazu z kamer w chronionym obiekcie oraz przyznawanie dostępu do chronionego obiektu w sposób zdalny, za pomocą sieci GSM lub Internet [4].



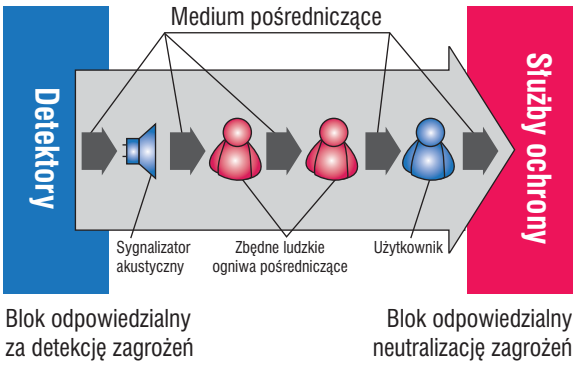
Rys. 1. Topologia systemu nadzoru wykorzystującego sieć Internet
D – detektory



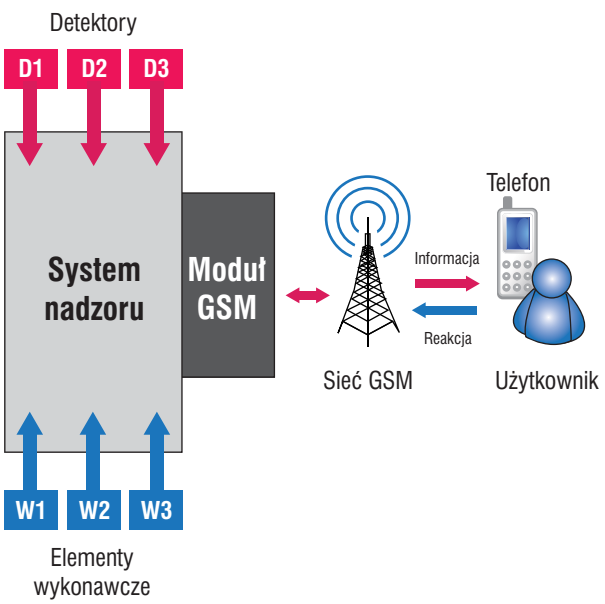
Rys. 2. Wirtualny system nadzorujący stan chronionego obiektu
D – detektory



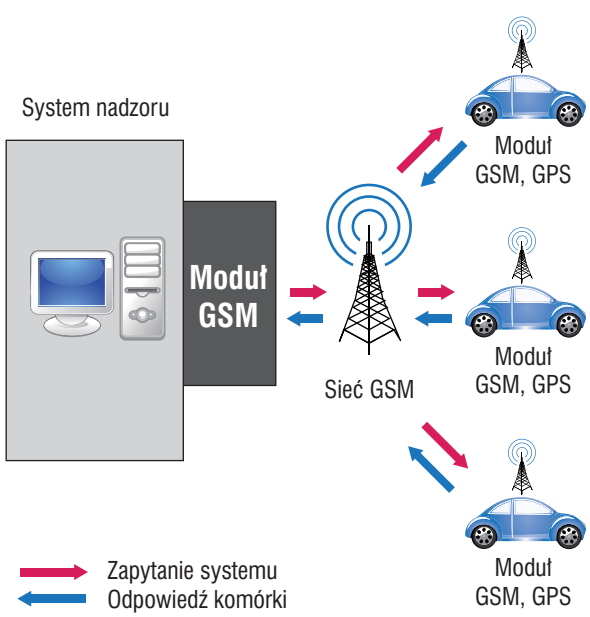
Rys. 3. Zoptymalizowanie procesu przekazywania informacji



Rys. 4. Zbędne ogniwa ludzkie w procesie przekazywania informacji o systemie



Rys. 5. Model systemu umożliwiającego użytkownikowi zdalne sterowanie elementami wyposażenia obiektu



Rys. 6. Zarządzanie flotą pojazdów za pomocą sieci GSM

A5) Dostęp do strumienia informacji generowanego przez urządzenia detekcyjne (szczególnie urządzenia rejestrujące obraz) a przez to dostęp do danych, które niekoniecznie powinny być udostępniane osobom postronnym.

Proces przekazywania informacji o wystąpieniu zagrożenia

Zastosowanie układów współpracujących z siecią GSM i Internetem w procesie przekazywania informacji o wykryciu zagrożenia służbom odpowiedzialnym za jego neutralizację daje nowe, niedostępne wcześniej funkcje i ogranicza czas tego procesu.

B1) W procesie przekazywania informacji o wystąpieniu zdarzenia zostają wyeliminowane zbędne etapy (Rys. 3). Informacja dochodzi do użytkownika praktycznie bezzwłocznie i niezależnie od miejsca jego przebywania. Nie muszą występować etapy pośrednie. W sposób istotny skracany jest czas reakcji użytkownika – osoby zarządzającej przepływem informacji, która może bezzwłocznie przystąpić do neutralizacji zagrożenia.

Obecnie często zdarza się, że o skuteczności działań zmierzających do neutralizacji zagrożenia decydują osoby postronne. O włączeniu się alarmu informowane jest za pomocą sygnalizatorów optyczno-akustycznych otoczenie obiektu, a nie użytkownik.

Zastosowanie technologii GSM charakteryzuje się dodatkowo tym, że użytkownik jest fizycznie informowany o zajściu zdarzenia. W przypadku Internetu w systemie (na serwerze, komputerze) występuje tylko zapis polegający na zarejestrowaniu zmiany stanów. Oczywiście można wygenerować programowo pewne działanie polegające na poinformowaniu użytkownika.

B2) Z procesu decyzyjnego zostaje wyeliminowany zbędny czynnik ludzki (Rys. 4). Dzięki temu czas reakcji na dane zdarzenie jest powtarzalny. Praktycznie nie występuje niewyznaczalny, zmienny losowo czynnik w postaci czasu działania człowieka. Po zarejestrowaniu zdarzenia przez system automatycznie następuje (według przewidzianego algorytmu działania) przekazanie informacji bezpośrednio do odpowiednich komórek odpowiedzialnych za neutralizację zagrożenia.

B3) Dzięki zastosowaniu modułów GSM w urządzeniach przenośnych i pojazdach istnieje możliwość bezpośredniego zabezpieczania nieruchomości. Odpowiednio wyposażony system zabezpieczający generuje sygnał alarmowy i przesyła go bezprzewodowo za pośrednictwem ogólnodostępnej sieci telefonicznej.

Przykładem praktycznego zastosowania takiego rozwiązania jest użycie modułów GSM w autoalarmach [5]. W przypadku zajścia zdarzenia użytkownik pojazdu jest o nim niezwłocznie powiadamiany za pomocą wiadomości tekstowej (SMS) i nie musi liczyć na życzliwość osób postronnych.

B4) Podczas przesyłania informacji o stanie obiektu do sieci Internet możliwy jest równoległy dostęp do aktualnych danych. Dzięki temu proces przekazywania informacji może przebiegać wielowątkowo i niezależnie. Ponadto istnieje możliwość tworzenia procedur polegających na potwierdzaniu otrzymanych informacji i przekazywaniu informacji o aktualnie podejmowanych decyzjach i działaniach przez poszczególne ośrodki (węzły) decyzyjne.

Proces	Sytuacja	Zastosowana technologia		Wpływ zastosowanego rozwiązania na:			
		GSM	Internet	funkcjonowanie systemu	możliwości systemu	przebieg procesu neutralizacji zagrożenia	czas procesu neutralizacji zagrożenia
1	A1	-	+	bardzo duży	bardzo duży	korzystny	średni
	A2	-	+	bardzo duży	bardzo duży	korzystny	duży
	A3	-	+	bardzo duży	bardzo duży	korzystny	duży
	A4	±	+	duży	duży	korzystny	duży
	A5	±	+	średni	średni	niekorzystny	duży
2	B1	+	+	bardzo duży	bardzo duży	korzystny	bardzo duży
	B2	+	+	bardzo duży	duży	korzystny	bardzo duży
	B3	+	-	duży	średni	korzystny	bardzo duży
	B4	-	+	duży	bardzo duży	korzystny	średni
	B5	+	+	bardzo duży	bardzo duży	korzystny	duży
3	C1	+	-	duży	średni	korzystny	bardzo duży
	C2	+	+	bardzo duży	bardzo duży	korzystny	bardzo duży
	C3	+	-	duży	duży	korzystny	duży

Tab. 1. Ocena wpływu zastosowania technologii GSM i Internetu w systemach nadzorujących stan chronionego obiektu
1 – proces detekcji zagrożenia, 2 – proces przekazywania informacji miedzy ogniwami systemu, 3 – proces neutralizacji zagrożenia

B5) Nowoczesne systemy realizujące i nadzorujące przepływ informacji oraz zarządzające nim kształtują w dowolny sposób dostępność danych w poszczególnych węzłach systemu nadzorującego. Nadawanie użytkownikom priorytetów dotyczących dostępności do danych daje możliwość sprawnego prowadzenia procesu nadzorowania.

Proces fizycznej neutralizacji zagrożenia

W przypadku procesu fizycznej neutralizacji zagrożenia rola systemów GSM i Internetu nie jest tak istotna, jak w przypadku procesu przekazywania informacji, jednak i w tym procesie zastosowanie tych technologii może mieć wpływ na skuteczność podejmowanych decyzji i skrócenie czasu potrzebnego do neutralizacji zagrożenia.

C1) Wyposażenie mobilnych jednostek służb odpowiedzialnych za neutralizację zagrożeń w telefony komórkowe umożliwia szybkie połączenie się z nimi przez centrum zarządzające. Ponadto zastosowanie technologii GSM pozwala na zachowanie większego poziomu poufności przekazywanych informacji niż w systemach krótkofalówek i radia CB.

C2) Wyposażenie elementów wykonawczych w chronionych obiektach w moduły umożliwiające zdalne sterowanie tymi elementami umożliwia wykonanie operacji mających na celu bezzwłoczną neutralizację zagrożenia (Rys. 5). W praktyce system nadzorujący jest wyposażany w dwufunkcyjne moduły, które umożliwiają wysyłanie informacji o stanie obiektu i mogą zmieniać stan urządzeń, które znajdują się w nim, na podstawie informacji dochodzących do systemu z zewnątrz.

Przykładem takiego rozwiązania jest system umożliwiający użytkownikowi zmianę stanu pracy pojazdu (wyłączenie silnika, odcięcie dopływu paliwa) w sposób zdalny, za pomocą telefonu komórkowego, po otrzymaniu informacji o nieautoryzowanym dostępie i uruchomieniu pojazdu [5].

C3) Wyposażenie mobilnych jednostek w systemy GSM i GPS, które przekazują informacje o aktualnym położeniu tych jednostek centrali nadzorującej, umożliwia przydzielenie jednostek, które znajdują się najbliżej obiektu lub mogą do niego najszybciej dotrzeć, do wykonania danej akcji [6]. Oprócz przekazywania informacji o położeniu pojazdu systemy takie umożliwiają również informowanie o stanie pojazdu i elementach jego wyposażenia (jest to ważne w przypadku pojazdów służb ratunkowych i pojazdów wojskowych) – Rys. 6.

4. Wpływ zastosowania technologii GSM i Internetu na działanie systemów nadzoru

W tabeli 1 przedstawiona została analiza wpływu zastosowania technologii GSM i Internetu w systemach nadzorujących stan chronionego obiektu i zarządzających pracą poszczególnych układów (komórek systemu). W analizie zostały uwzględnione sytuacje opisane w rozdziale 3.

5. Podsumowanie

Wykorzystanie telefonii mobilnej GSM i Internetu w systemach nadzorujących stan chronionego obiektu może w sposób istotny wpływać na pracę takich systemów. Może to być oddziaływanie pozytywne, poprawiające działanie systemu poprzez zwiększenie skuteczności wykrywania i neutralizowania występujących zagrożeń oraz skracające czas reakcji na występujące zagrożenie. Może mieć również negatywny wpływ na działanie systemu. Ryzyko ma związek z wykorzystaniem ogólnodostępnych mediów do przesyłu informacji.

Wydaje się, że zagrożenia wynikające z wykorzystania ogólnodostępnych kanałów informacyjnych nie mogą przysłonić związanych z nim zalet (podobne analizy były przeprowadzane w przypadku wprowadzania bankowości internetowej). Trzeba jednak przyznać, że w obiektach strategicznych powinno się przykładać szczególną wagę do nieupubliczniania strumienia informacji. W przypadku tych obiektów rozwiązaniem może być budowa wydzielonych sieci komputerowych o zasięgu lokalnym. Dzięki tym sieciom można skorzystać – chociaż dużym kosztem – z dobrodziejstw nowych technologii.

Rozwój systemów nadzorowania opartych na przesyle informacji za pomocą sieci internetowej wprowadza nowe, dotychczas nieznane możliwości. Można na przykład tworzyć wirtualne narzędzia (systemy) umożliwiające realizację funkcji i zadań spełnianych obecnie przez elementy fizyczne (np. centralę alarmową). Jedynymi elementami rzeczywistymi w takich systemach będą detektory i elementy wykonawcze. Proces akwizycji, analizy i rejestracji sygnału będzie wykonywany programowo przez jednostki komputerowe.

Dzięki bezpośredniemu przesyłaniu informacji o stanie obiektu do zainteresowanego użytkownika technologie GSM i Internet umożliwiły eliminację zbędnych ogniw procesu przekazywania informacji (szczególnie czynników ludzkich). Ograniczenie roli osób postronnych i ograniczenie czynnika ludzkiego do osób czynnie zaangażowanych w proces przekazywania informacji spowodowało, że informacja krąży w sposób przemyślany, a to powoduje zmniejszenie czasu reakcji i czasu podejmowania decyzji, jaki mija od momentu wykrycia przez system zdarzenia do początku akcji neutralizacji zagrożenia.

Wykorzystanie technologii GSM i Internetu (szczególnie bezprzewodowego) zapewniło mobilność elementów systemu nadzorującego. Użytkownik może mieć dostęp do informacji o stanie chronionego obiektu na bieżąco (o ile jest w zasięgu sieci). Ponadto możliwe jest zdalne nadzorowanie stanu obiektów przenośnych i pojazdów.

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

Bibliografia:

1. Simon A., *Sieci komórkowe GSM/GPRS*, Wydawnictwo Xylab, Kraków 2002.
2. Buczaj M., *Czas jako kryterium skuteczności przebiegu procesu neutralizacji zagrożeń w systemach nadzorujących stan chronionego obiektu*, w: *Zabezpieczenia* nr 6/2009.
3. Szulc W., Rosiński A., *Systemy sygnalizacji włamania*, część I, w: *Zabezpieczenia* nr 2/2009.
4. Kargul D., *Tendencje rozwoju współczesnych technik zabezpieczenia mienia stosowanych w budownictwie*, praca dyplomowa, Politechnika Lubelska, Lublin 2009.
5. Daniluk M., *Tendencje rozwoju nowoczesnych technik zabezpieczenia mienia w motoryzacji*, praca dyplomowa, Politechnika Lubelska, Lublin 2007.
6. Ożga B., *Wykorzystanie systemów GSM i GPS do monitorowania położenia obiektu*, praca dyplomowa, Politechnika Lubelska, Lublin 2007.
7. *www.wikipedia.org*

SZKOŁA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ TECHOM w WARSZAWIE
inż. Bogdana Tatarowskiego

Wpis do Ewidencji Niepublicznych Placówek Oświatowych Starostwa Powiatu Warszawskiego pod nr 363K/2001

zaprasza na:

KURSY ZAWODOWE

w zakresie

INSTALOWANIA SYSTEMÓW ALARMOWYCH
Dla przyszłych wykonawców prac instalatorskich i konserwacyjnych oraz dla użytkowników systemów, inwestorów i administratorów obiektów chronionych

PROJEKTOWANIA SYSTEMÓW ALARMOWYCH
Dla obiektów cywilnych i wojskowych oraz z tzw. „Listy Wojewody"

ZARZĄDZANIA BEZPIECZEŃSTWEM OBIEKTU
Bezpieczeństwo teleinformatyczne
Wymagania prawne i normatywne

RZECZOZNAWSTWA SYSTEMÓW TECHNICZNEGO
Systemy Technicznego Zabezpieczenia Osób i Mienia
Zarządzanie Bezpieczeństwem Obiektu

SEMINARIUM AUTORYZACYJNE
Dla Absolwentów Kursów
Przydatne dla Inwestorów i Towarzystw Ubezpieczeniowych

INFORMACJA ORAZ PRZYJMOWANIE ZGŁOSZEŃ:

tel. (022) 625 32 96
tel. (022) 625 34 00
fax.(022) 625 26 75
00-545 Warszawa, ul. Marszałkowska 60
www.techom.com
e-mail: techom@techom.com

TECHOM

Bezpieczeństwo danych w Internecie a **VPN**

Jacek Gawrych

Wyobraź sobie świat, w którym przestępcy są niemal bezkarni. Twój samochód ukradł właśnie Rosjanin wynajęty przez Argentyńczyka, którego opłacił Somalijczyk zatrudniony przez twojego sąsiada. Temu ostatniemu po prostu nie spodobała się twoja praca w firmie wspierającej rząd amerykański w walce z terroryzmem. Ów Rosjanin nawet nie ruszył się z domu, aby ukraść ci samochód. Stworzył do tego zadania niewidzialnego robota, który przybył do Polski i zrobił to za niego. Jeżeli polska policja miałaby ująć twojego sąsiada – głównego zleceniodawcę, musiałaby skutecznie współpracować z policją w Rosji, Argentynie i Somalii (sytuacja niewyobrażalna przy takiej szkodliwości czynu). Czy podany przykład jest według ciebie opisem nieprawdopodobnych zdarzeń w nierealnym świecie? A co powiesz na to, że podobnym światem jest Internet, w którym twoja firma z pewnością funkcjonuje?

Z niniejszego artykułu dowiesz się, jakiego typu zagrożenia dla twojej firmy czyhają w Internecie, ile mogłyby kosztować skutki udanego ataku na twoją firmę i jakie problemy mogłyby być rozwiązane dzięki technologii Wirtualnych Sieci Prywatnych (ang. *Virtual Private Network* – VPN).

Co zagraża mojej firmie w Internecie?

Na początku wyjaśnienie – na twoją firmę będziemy tu patrzeć tak, jak na zbiór wszelkich informacji, które się w niej znajdują i *de facto* stanowią jej główną wartość. Bądź co bądź, żyjemy w świecie, w którym biznes opiera się na wykorzystywaniu informacji, które sam wytwarza lub czerpie z zewnątrz. Nawet firmy wydobywające złoża naturalne i handlujące nimi mają swoje pilnie strzeżone tajemnice. Przez bezpieczeństwo twojej firmy w Internecie będziemy więc rozumieli bezpieczeństwo informacji, które są w niej przetwarzane. Istnieją trzy podstawowe atrybuty informacji, które mogą być zaatakowane z Internetu:

– poufność (ktoś nieuprawniony wchodzi w posiadanie twoich danych),
– integralność (ktoś modyfikuje twoje dane),
– dostępność (ktoś sprawia, że przez określony czas nie masz dostępu do swoich danych).

Warto dobrze zapamiętać te trzy słowa – na nich opiera się niemal cała teoria bezpieczeństwa informacji. Być może łatwiej będzie po angielsku: *Confidentiality, Integrity i Availability* to w skrócie CIA. Przyjrzyjmy się przykładowym atakom na poufność informacji w firmie. Przede wszystkim ten atrybut może być lepiej zabezpieczony technologią VPN.

1) Serwer e-mail twojej firmy jest dostępny z każdego miejsca w Internecie, aby pracownicy mogli sprawdzać pocztę nawet przez telefony komórkowe, kiedy są w swoich samochodach. Mówiąc dokładniej, usługa POP3 lub IMAP na tym serwerze jest dostępna z każdego zakątka świata. Załóżmy, że komuś bardzo zależy na czytaniu waszej korespondencji e-mail. Wynajmuje więc człowieka, który od dziecka pasjonował się szukaniem błędów programistycznych w serwerach pocztowych. Tak się złożyło, że ów człowiek, pogłębiając swoje pasje, znalazł pewien błąd w dokładnie tej wersji serwera pocztowego, z której korzysta twoja firma. Błąd ten umożliwia przejęcie pełnej kontroli nad całym systemem operacyjnym, na którym zainstalowana jest aplikacja serwerowa. O tym błędzie nie poinformował on programistów, którzy ją stworzyli, więc nie wydadzą oni w najbliższym czasie tzw. łatki, usuwającej błąd. Do czasu wydania łatki wasz serwer będzie miał lukę, dzię-

ki której ciągle będzie można czytać waszą korespondencję e-mail. Co gorsze, będzie to możliwe również po jej wydaniu, bo wspomniany pasjonat z pewnością stworzy sobie wiele tylnych furtek (ang. *backdoor*) do waszego serwera. Atakujący zadbał również o swoją anonimowość i dostał się do waszego serwera za pośrednictwem wielu innych komputerów, rozproszonych na całej kuli ziemskiej.

2) Twoja firma wdrożyła nowe rozwiązanie CRM (*Customer Relationship Management*) w postaci aplikacji WWW, do której logują się pracownicy z zewnątrz przez protokół HTTP. Łącze internetowe w twojej firmie jest dzierżawione od administratora biurowca, w którym macie siedzibę. Wystarczy przejąć kontrolę nad bramą internetową administratora budynku (najczęściej jest nią ruter), aby podsłuchiwać wszelką komunikację pomiędzy zewnętrznymi pracownikami a aplikacją CRM w twojej firmie.

Ile może kosztować moją firmę incydent związany z bezpieczeństwem?

To bardzo prosta matematyka. Załóżmy, że wyceniacie informacje w bazie danych wspomnianej aplikacji CRM na jeden milion złotych. Wynajęty przez was audytor bezpieczeństwa stwierdza, że przy obecnych zabezpieczeniach aplikacji prawdopodobieństwo przechwycenia jej bazy danych w ciągu najbliższego roku wynosi 10%. Oznacza to, że w najbliższym roku ryzykujesz 100 000 złotych w związku z samą bazą danych aplikacji CRM. Do tej kwoty należy dodać ryzyka związane ze wszystkimi innymi aktywami informacyjnymi i już znamy odpowiedź na zadane pytanie. Jak wobec tego zadbać o bezpieczeństwo? Co zrobić? Dokładnie to samo, co robisz, aby zmniejszyć ryzyko kradzieży swojego samochodu. Wdrażasz zabezpieczenia. W przypadku samochodu jest to autoalarm, immobilizer lub lokalizator samochodu. Dodatkowo ubezpieczasz pojazd od kradzieży na kwotę równą jego wartości.

Jak dobierać zabezpieczenia dla mojej firmy?

Zdroworozsądkowo i opłacalnie. Dokładnie tak, jak robisz to w przypadku swojego samochodu. Jeśli jest wart 100 000 zł, a prawdopodobieństwo jego kradzieży wynosi 5%, nie warto wydawać na jego zabezpieczenia więcej niż 5000 zł. Jeśli jednak wydamy 1000 zł na zabezpieczenie, które zmniejszy prawdopodobieństwo kradzieży o 3%, zrobimy świetny interes – za 1000 zł zmniejszymy ryzyko o 3000 zł. Powróćmy do bezpieczeństwa danych w firmie. Jeśli przeanalizujemy wartość wszystkich informacji w naszej firmie i znajdziemy prawdopodobieństwa udanych ataków na nie, dostaniemy listę ryzyk mierzonych w PLN. Wystarczy posortować tę listę malejąco i już wiemy, co zabezpieczać w pierwszej kolejności. W pewnym miejscu tej listy należy postawić grubą kreskę, która oddzieli ryzyka akceptowalne (odpowiednio niskie) od nieakceptowalnych. Potem należy już tylko sprawić, aby ryzyka znad kreski znalazły się pod nią. Robimy to dokładnie tak, jak w przypadku zabezpieczenia dla samochodu. Weźmy technologię VPN. Załóżmy, że wdrożenie jej w twojej firmie kosztowałoby 30 000 zł w ciągu najbliższych dwóch lat. Technologia ta zmniejszyłaby prawdopodobieństwo wystąpienia incydentów związanych z bezpieczeństwem twoich aktywów informacyjnych, dzięki czemu suma zmniejszonych ryzyk wyniosłaby 200 000 zł. Znowu robisz świetny interes – zarabiasz 170 000 zł.

Przed czym obroni nas VPN?

Czym jest VPN, czyli Wirtualna Sieć Prywatna? To programistyczny twór, który sprawi, że twoi zdalni pracownicy lub inne lokalizacje twojej firmy logicznie stworzą jedną odseparowaną sieć prywatną. Na bazie sieci absolutnie publicznej, jaką jest Internet, można więc stworzyć sieć prywatną. Dzięki VPN użytkownik nie dostrzeże różnicy między pracą przy biurku w sieci wewnętrznej firmy a pracą na laptopie w swoim domu. Tak, jeśli myślisz o telepracownikach, VPN jest niemal koniecznością. Ta technologia daje dwie ogromne korzyści:

– pozwala na odseparowanie od publicznej sieci usług, które muszą być w niej dostępne, ale tylko dla twoich pracowników (np. serwera poczty przychodzącej),
– pozwala na szyfrowanie komunikacji między zdalnymi punktami (pracownik firmy, inna lokalizacja firmy), dzięki czemu dane przesyłane przez Internet są niezrozumiałe dla osób postronnych.

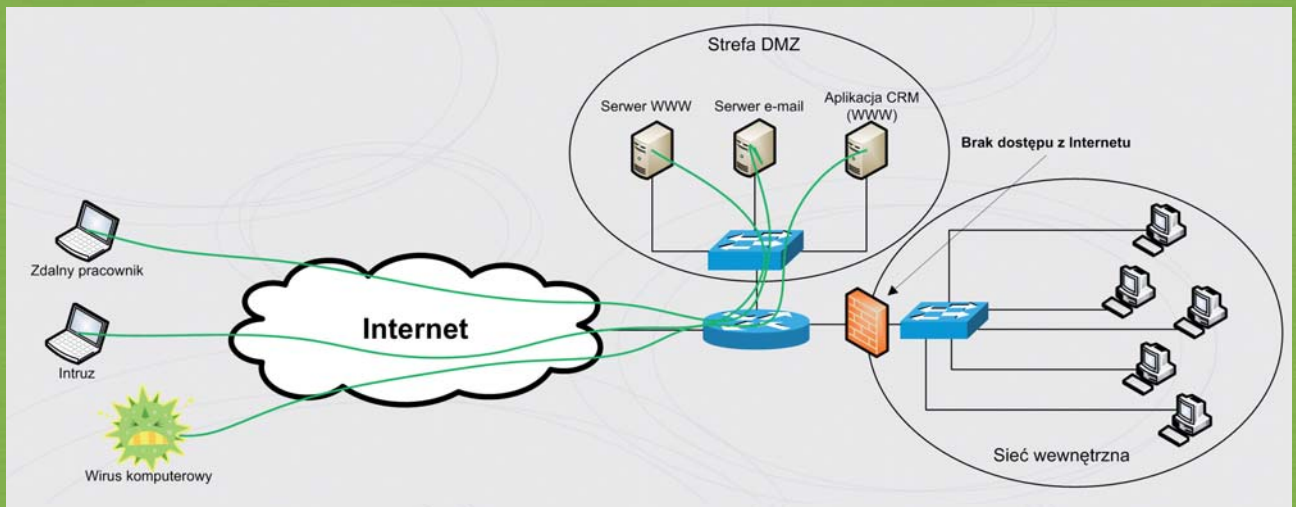
Wdrażając VPN, budujemy niejako dodatkowe ogrodzenie wokół firmy z jedną furtką, przez którą zostaną wpuszczeni tylko nasi pracownicy. Dopiero za tym ogrodzeniem umieszczamy serwery, które udostępniamy dla pracowników/lokalizacji zewnętrznych. Jakie są korzyści?

Wiele naszych aplikacji staje się niedostępnymi z sieci publicznej dla osób nieautoryzowanych, wciąż pozostając dostępnymi dla naszych zewnętrznych pracowników. One po prostu przestają być wystawiane na ostrzał dokonywany przez ludzi mających złe zamiary względem naszej firmy.

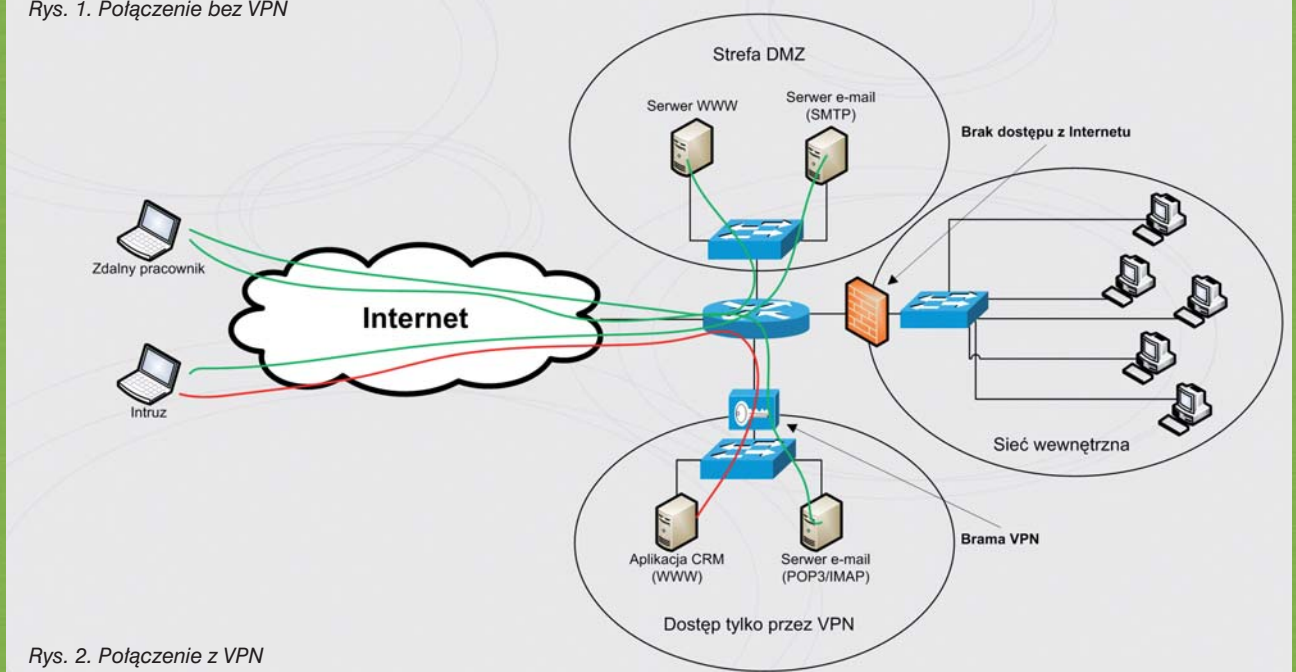
Komunikacja zdalnych pracowników z zasobami firmy może być wielokrotnie trudniejsza do podsłuchania dzięki zastosowaniu szyfrowania. Jest to szczególnie istotne, kiedy pracownicy łączą się z zasobami firmy przez sieci bezprzewodowe. Jeśli nie szyfrujemy danych przesyłanych przez sieci bezprzewodowe, mogą one trafić do atakującego nas człowieka w czystej formie – gotowe do przeczytania.

Przed czym NIE obroni nas VPN?

Jeśli wdrożymy VPN jako pojedynczą i jedyną koncepcję bezpieczeństwa, po prostu zmniejszymy prawdopodobieństwo wystąpienia pewnych incydentów. Absolutnie nie możemy myśleć, że dzięki jej wdrożeniu mamy zapewnioną poufność wszystkich danych w firmie. Wyobraźmy sobie chociażby, że intruzowi uda się przejąć kontrolę nad komputerem naszego pracownika. Może on zrobić to na bardzo wiele różnych sposobów i jeśli tylko jeden z nich okaże się skuteczny, uzyska dostęp do naszych usług. Skoro ma do nich dostęp pracownik korzystający ze służbowego laptopa, ma go też intruz, który przejął pełną kontrolę nad jego komputerem. Zauważmy też inną rzecz. VPN jest usługą publicznie dostępną w Internecie. Działa na tej samej zasadzie, na której wcześniej działały inne usługi, teraz za nią schowane – a więc można próbować atakować także usługę VPN, co może doprowadzić do przejęcia kontroli nad kolejnymi systemami w naszej sieci. Mimo to warto inwestować w tę technologię. Dzięki niej wiele dostępnych publicznie usług zastępujemy jedną. Istnieje znacznie mniejsze prawdopodobieństwo tego, że atakujący wie, jak złamać/zhakować usługę VPN, niż tego, że wie, jak złamać którąkolwiek z aplikacji, którą VPN zasłania. Weźmy też po uwagę to, że aplikacje VPN są projektowane i programowane przez ludzi orientujących się w zagadnieniach bezpieczeństwa z reguły o wiele bardziej niż



Rys. 1. Połączenie bez VPN



Rys. 2. Połączenie z VPN

ludzie tworzący aplikacje CRM lub POP3. Zwykle ci ostatni niejako zwalniają się z obowiązku tworzenia bezpiecznych aplikacji, sugerując ich umieszczenie za bramą VPN.

Jak działa VPN?

Koncepcje VPN można podzielić na dwie różne gałęzie:

1) VPN dla pracowników (*client-server* VPN), którzy „wdzwaniają się" do zasobów firmy (podając PIN/hasło, przedstawiając wiarygodny certyfikat, generując hasło przez token),
2) VPN między lokalizacjami firmy (*site-to-site* VPN). Jego zadaniem jest utrzymywanie stałego szyfrowanego łącza pomiędzy naszymi siedzibami – oczywiście na bazie Internetu. Ta technologia nie wymaga interwencji człowieka przy zestawianiu połączenia. Ono musi ustanawiać i wznawiać się automatycznie. Poza tym koncepcje te są niemal identyczne.

VPN można zrealizować według kilku różnych podejść. Najpopularniejsze z nich (i nie będące zarazem własnością żadnej firmy) to SSL VPN i IPSec VPN. Rozwiązania te można zaimplementować na bezpłatnym oprogramowaniu typu *open source* lub na komercyjnych aplikacjach czy dedykowanych urządzeniach. SSL VPN bazuje na certyfikatach X.509 i na uwierzytelnieniu między stronami na ich podstawie. Certyfikaty te można wygenerować samodzielnie (jest to mniej bezpieczne) lub wykupić w profesjonalnym centrum certyfikacyjnym. Szczegóły działania technologii VPN poznasz najlepiej, po prostu ją konfigurując. Jeśli myślisz o wdrożeniu usługi na oprogramowaniu *open source* lub o pogłębieniu swojej wiedzy, polecam książkę *Sieci VPN. Zdalna praca i bezpieczeństwo danych. Wydanie II rozszerzone* Marka Serafina. Jeśli myślisz o wdrożeniu komercyjnym, poproś producenta o wyjaśnienie szczegółów technologii, którą ci zaproponuje.

Podsumowanie

Wiesz już, przed czym pomoże ci obronić się technologia VPN. Wiesz również, że nie jest ona jedynym sposobem zabezpieczenia danych w twojej firmie. Jeśli jednak chcesz udostępniać tajne dane swojej firmy pracownikom przez Internet, możesz wdrożyć VPN bez żadnych kalkulacji, czy to się na pewno opłaca. Opłaca się! Jest niemal niemożliwe, aby obecne ceny tej technologii (przy rozwiązaniach *open source* jej koszty są powiązane wyłącznie z instalacją i utrzymaniem usługi) przerosły oszczędności, jakie dzięki niej zyskamy.

Jacek Gawrych

GO MEGA

Przedstawiamy nową rodzinę megapikselowych kamer Sony

ZAPROJEKTOWANE Z MYŚLĄ O BEZPIECZEŃSTWIE

Sony and 'IPELA' are registered trademarks of the Sony Corporation, Japan.

SONY

IPELA

Inteligentna analiza obrazu... bezpieczeństwo dla Ciebie

ALTRAM

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

www.sonybiz.pl

Piksel pikselowi wilkiem

Andrzej Walczyk

Pojęcie piksela pojawiło się w słownictwie związanym z telewizją dość późno. Zostało zapożyczone z techniki komputerowej, gdzie znacznie wcześniej, na długo przed upowszechnieniem się elementów CCD i monitorów LCD, wprowadzony został podział ekranu na dające się osobno opisać miniaturowe elementy o określonej barwie i jaskrawości. Powodem była potrzeba zapamiętywania i obróbki treści obrazu. To z kolei wymagało kwantyzacji sygnału analogowego i przejścia na opis cyfrowy

Obraz ciągły czy podzielony?

Kwantyzacja dotyczyła zamiany sygnału analogowego na odpowiadający mu ciąg liczb i odbywała się poprzez próbkowanie sygnału analogowego i pomiar wartości próbek (tak jak na przykład podczas kodowania metodą PCM). Kwantyzacji uległ także sam obraz, a dokładnie jego powierzchnia, która straciła ciągłość i została podzielona na setki tysięcy pól zwanych pikselami. Stało się tak pomimo powszechnego stosowania monitorów kineskopowych, działających na zasadach analogowych.

Właśnie w tym, że monitory kineskopowe były urządzeniami analogowymi, tkwiło źródło ówczesnego sukcesu. Wyświetlany obraz mógł mieć dowolny kształt i rozmiary, gdyż powierzchnia ekranu miała charakter ciągły, nie zawierała żadnych wyróżnionych punktów, była w stanie zaakceptować każdy rozkład pikseli[1]. W przypadku komputerów, których karty graficzne wytwarzały obrazy o wysokiej rozdzielczości, oznaczało to odejście od dotychczasowych częstotliwości odchylania ramki i linii. Było to możliwe, gdyż ekran kineskopu miał budowę ciągłą, akceptował dowolne formaty obrazu i częstotliwości odświeżania.

Pierwsze problemy – monitory LCD w telewizji analogowej

Pierwsze zwiastuny problemu wystąpiły w momencie pojawienia się monitorów LCD, których ekrany nie miały budowy ciągłej, lecz były podzielone na pojedyncze elementy świecące, czyli piksele, ułożone w rzędy i kolumny, tworzące jednoznacznie zdefiniowany raster telewizyjny. Tym razem nie było już mowy o dowolności. Na przykład nie można było wyświetlić elementu obrazu, który znajdował się na granicy pomiędzy sąsiednimi pikselami, co dla stosowanego dotychczas klasycznego kineskopu nie stanowiło problemu.

Podczas wyświetlania obrazów analogowych dobrą praktykę stanowiło stosowanie monitorów LCD z rastrem dopasowanym do standardu PAL czy VGA, czyli posiadających relatywnie niską rozdzielczość. Tendencja ta była powodem licznych nieporozumień, gdyż machina marketingowa chętnie zapożyczała pojęcia z rynku komputerowego i bezkrytycznie wprowadzała je do systemów CCTV, twierdząc, że na monitorze o wyższej rozdzielczości uzyska się obraz o lepszej jakości. Trudno odmówić logiki tej prostej w odbiorze, jednakże z gruntu fałszywej argumentacji.

Jak wygląda obraz telewizyjny o rozdzielczości zwanej umownie PAL-owską, czyli o rozmiarach rastra obrazowego 768×576 pikseli, lub o rozdzielczości VGA, czyli 640×480 pikseli, oglądany na monitorze komputerowym o dużo wyższej rozdzielczości? Zasadniczo są dwie możliwości, obie mają swoje wady i zalety i są uzależnione od działania oprogramowania graficznego oraz od mechanizmów obróbki sygnału wizyjnego zaszytych w samym monitorze.

Rozwiązaniem korzystniejszym dla obserwatora, aczkolwiek mało efektownym, jest wyświetlanie obrazu z zachowaniem zgodności liczby i rozkładu pikseli ze standardem PAL lub VGA, jednakże wyświetlany w ten sposób obraz zajmuje jedynie część powierzchni ekranu. Zaletą jest uzyskanie ostrego, wyrazistego obrazu o dobrej reprodukcji barw.

Inną możliwością jest wyświetlanie obrazu na dużym fragmencie lub na całej powierzchni ekranu monitora, co pociąga za sobą konieczność przekształcenia oryginalnego obrazu. I tu czeka nas ogromne rozczarowanie, gdyż pomimo wysokiej rozdzielczości monitora wyświetlany na nim obraz nie będzie robił dobrego wrażenia wzrokowego. Najdotkliwiej będzie można odczuć to podczas oglądania znaków alfanumerycznych, czyli, mówiąc prościej, napisów. Kształt liter będzie się zmieniał w zależności od ich pozycji na ekranie. Na podobnej zasadzie grubość linii tworzącej litery też będzie zmienna. Obraz jako całość będzie sprawiał wrażenie nieostrego, pozbawionego szczegółów.

Przyczyną tego zjawiska jest konieczność aproksymacji barwy i jaskrawości pikseli docelowych, fizycznie umieszczonych na ekranie monitora, przy czym dysponuje się danymi dotyczącymi pikseli źródłowych o innym rozkładzie, stanowiących obraz z kamery. Jeśli te dwie grupy pikseli nie pokrywają się wzajemnie, obraz nie może być ani wyraźny, ani ostry. Treść obrazu wyświetlanego na ekranie monitora stanowi efekt przekształcenia dążącego do możliwie najlepszego upodobnienia tego obrazu do oryginału, co nie może dawać dobrych efektów.

Tak więc „piksel pikselowi wilkiem", dlatego bezpośrednie wykorzystanie tanich, komputerowych monitorów LCD do wyświetlania obrazów w standardzie PAL lub VGA natrafia na poważne problemy. Dla uzyskania poprawnych efektów konieczne jest stosowanie specjalnych monitorów LCD, przystosowanych do pracy w systemach analogowych. Przykładem takiego analogowego monitora LCD, odznaczającego się wyjątkowo plastyczną reprodukcją obrazów, jest przedstawiony na zdjęciu model SONY LMD 1410SC o rozmiarach matrycy równych 640×480 pikseli.

Dość charakterystyczną reakcją klientów na ten monitor było podejrzenie, że ktoś próbuje pozbyć się zalegających rezerw magazynowych, bo przecież wiadomo, że dostępne są monitory o znacznie wyższej rozdzielczości. Z kolei konfrontacja innych monitorów z LMD 1410SC, który wyświetla doskonały obraz, wywoływała zdziwienie i niedowierzanie. Podsumowując – wysoka rozdzielczość monitora analogowego nie stanowi gwarancji wysokiej jakości obrazu; można nawet powiedzieć, że jest odwrotnie, czyli oceniana wzrokowo wypadkowa rozdzielczość obrazu jest gorsza niż w przypadku monitora analogowego o mniejszej liczbie pikseli.

Linie telewizyjne jako miara rozdzielczości poziomej

We współczesnych, cyfrowych systemach telewizji dozorowej zwykło się określać rozdzielczość obrazu przez podanie rozmiarów rastra obrazowego, mierzonych liczbą pikseli w rzędach i w kolumnach. Przykładowo – w standardzie PAL można to opisać jako 768×576 pikseli. Jest to niezbyt precyzyjne, gdyż przez rozdzielczość rozumie się zdolność do reprodukcji małych szczegółów obrazu, zaś duża liczba pikseli jest jedynie narzędziem stwarzającym taką możliwość, dlatego te pojęcia są

1) Mówiąc ściślej, ciągły charakter miał jedynie ekran kineskopu monochromatycznego. W przypadku kineskopów kolorowych ekran był podzielony na triady, czyli trójelementowe fragmenty pozwalające na reprodukcję barw, jednakże nie miało to nic wspólnego z pikselami, których rozkład mógł być dowolny.

często utożsamiane. Tego typu rozumowanie niesie ze sobą ryzyko popełnienia pewnych błędów, jednakże wysoka jakość nowoczesnych obiektywów oraz zastosowanie cyfrowej techniki obróbki i transmisji danych pozwoliło na takie ograniczenie czynników pogarszających jakość obrazu, że w warunkach praktycznych można przyjąć, że liczba pikseli przetwornika zastosowanego w kamerze jest miarą maksymalnej rozdzielczości, dostępnej dla całego systemu.

Jednakże w wielu przypadkach, chociażby podczas rozstrzygania przetargów publicznych, wymagane jest podanie rozdzielczości mierzonej w tak zwanych liniach telewizyjnych (TVL). Sposób określenia rozdzielczości w TVL opisuje polska norma EN 50132-7. Polega on na określeniu maksymalnej liczby pionowych pasów, na przemian czarnych i białych, które można rozróżnić na wycinku obrazu telewizyjnego, którego szerokość jest równa wysokości ekranu. Jak łatwo zauważyć, taka definicja oznacza, że maksymalna dostępna rozdzielczość obrazu rastrowego wyrażona w liniach telewizyjnych jest równa liczbie pikseli w dowolnej z kolumn tego rastra, czyli w przypadku standardu PAL może dochodzić do 576 linii telewizyjnych. Ze względów praktycznych, a także ze względu na to, że do tworzenia ostatecznego obrazu nie zawsze wykorzystywane są wszystkie piksele rastra (mówi się o tak zwanych pikselach aktywnych), przyjmuje się maksymalną wartość rozdzielczości kamer analogowych pracujących w standardzie PAL równą 540 TVL.

Fot. 1. Monitor SONY LMD 1410SC

W zasadzie problem pomiaru faktycznej rozdzielczości kamer występuje tylko w przypadku konstrukcji hybrydowych, to znaczy kamer, które wytwarzają w swoim wnętrzu analogowy sygnał wizyjny, a następnie zamieniają ten sygnał na postać cyfrową. Takie kamery są cyfrowe tylko w nazwie, a w rzeczywistości niczym nie różnią się od dwuczłonowego zestawu, w skład którego wchodzi kamera analogowa połączona z koderem IP. Tego typu konstrukcje są nadal oferowane przez niektórych producentów. Trudno się dziwić niskiej jakości obrazu wytwarzanego przez takie hybrydy, gdyż jest on zupełnie niepotrzebnie przetwarzany z jednej postaci w drugą, zaś rozdzielczości nie da się określić inaczej, jak za pomocą liczby linii telewizyjnych (TVL). Na wartość rozdzielczości mają wpływ parametry wszystkich układów wzmacniających, filtrujących, próbkujących oraz przetwornika analogowo-cyfrowego. Dlatego też w kamerach hybrydowych nie da się oszacować rozdzielczości obrazu na podstawie rozmiarów przetwornika, trzeba ją zmierzyć za pomocą tablicy testowej, tak jak robiło się to jeszcze w latach pięćdziesiątych zeszłego stulecia. Kamery o takiej konstrukcji są drogie i obarczone licznymi wadami, z których główną jest brak możliwości wytworzenia obrazu megapikselowego, gdyż nie istnieje nic takiego, jak megapikselowy, analogowy, zespolony sygnał wizyjny.

Tej i innych wad nie mają kamery cyfrowe, w których od przetwornika obrazowego aż po wyjściowe gniazdo RJ-45 obraz ma postać strumienia danych cyfrowych. W takiej sytuacji rozdzielczość może być wyrażana liczbą pikseli i jest zbliżona do rozdzielczości przetwornika obrazowego użytego w kamerze. Warto podkreślić, że w przypadku kamer cyfrowych, które są wyposażone w pomocnicze wyjście wizyjne, powstający na tym wyjściu analogowy sygnał wizyjny jest elementem wtórnym, wytwarzanym ze strumienia danych cyfrowych, a nie pobieranym z wyjścia części analogowej, jak to ma miejsce w przypadku kamer hybrydowych. Jest to obraz przeznaczony wyłącznie do celów serwisowych i jego rozdzielczość ma się nijak do parametrów samej kamery, które mogą być zdecydowanie lepsze.

W tym momencie dochodzimy do kolejnego istotnego punktu. Osoby sceptyczne wobec technologii cyfrowej twierdzą, że kamery analogowe dawały obraz lepszy niż kamery cyfrowe. Trudno odmówić im racji – w przypadku archaicznych kamer

hybrydowych rzeczywiście tak było, obraz na wyjściu analogowym był wolny od wad pojawiających się podczas próbkowania i zamiany na postać cyfrową i miał większą rozdzielczość od wynikowego obrazu cyfrowego na wyjściu sieciowym. Tego typu problemy nie występują w kamerach cyfrowych, w których sygnał analogowy w ogóle nie powstaje, a końcowa rozdzielczość nie różni się od pierwotnej, określanej przez parametry przetwornika.

Rozdzielczość rejestratora cyfrowego

W przypadku cyfrowych systemów telewizji dozorowej trudno jest uznawać rozdzielczość rejestratora za jeden z parametrów tego urządzenia. Tego typu podejście jest reliktem z epoki systemów analogowych i hybrydowych, w której rejestrator, w zależności od swoich parametrów, w mniejszym lub większym stopniu pogarszał jakość zapisywanego obrazu. W systemach cyfrowych rejestrator nie dokonuje żadnej zmiany treści obrazu, jest jedynie narzędziem rejestrującym, zapisującym strumień danych dochodzący poprzez sieć IP. Dlatego o rozdzielczości i o innych parametrach obrazu nie decyduje rejestrator, tylko przetwornik obrazowy i oprogramowanie kodujące użyte w kamerze. Co prawda część producentów oferuje rejestratory transkodujące, to znaczy zapisujące obrazy w innym formacie niż obrazy przychodzące z sieci IP, ale ma to związek z poprawą kompresji, z dążeniem do efektywnego wykorzystania przestrzeni pamięciowych etc. i w efekcie ubocznym może mieć nieznaczny wpływ na rozdzielczość obrazu. Tego typu działania są raczej sporadyczne.

Sytuacja wygląda inaczej w systemach hybrydowych, w których do rejestratora dostarczany jest analogowy sygnał wizyjny, który podlega próbkowaniu i zamianie na postać cyfrową. Rozwiązanie to ma wszystkie wady wymienione w opisie kamer hybrydowych, to znaczy transmisja sygnału poprzez kabel koncentryczny, późniejsze jego wzmacnianie, filtracja, próbkowanie etc. mają na tyle duży wpływ na jakość obrazu, że jego wynikowa rozdzielczość ma jedynie pośredni związek z liczbą pikseli w przetworniku kamery i może być określona wyłącznie metodą pomiaru. Na szczęście rejestratory hybrydowe są stosowane coraz rzadziej, przeważnie podczas modernizacji starych instalacji analogowych, z tego względu nie będą dokładniej omawiane.

Rozdzielczość obrazu na stacji roboczej

We współczesnych, cyfrowych systemach telewizji dozorowej obrazy są wyświetlane na stacjach roboczych, czyli stanowiskach zawierających między innymi wyspecjalizowany komputer wyposażony w odpowiednią kartę graficzną i specjalistyczne oprogramowanie, pozwalające na tworzenie stosownych zobrazowań, oraz monitor o wysokiej rozdzielczości. Stwarza to zupełnie nową jakość funkcjonalną i eliminuje ograniczenia rozdzielczości obrazów wynikające z aproksymacji pikseli opisanej na początku tego artykułu. W tym przypadku niezgodność układu pikseli źródłowych, odwzorowujących rozkład pikseli w przetworniku kamery z rozkładem pikseli na monitorze stacji roboczej, nie jest już tak istotna, czyli powiedzenie „piksel pikselowi wilkiem" przestaje być aktualne.

Z czego wynika tak wysoka jakość obrazu uzyskiwana na współczesnych stacjach roboczych? Dlaczego ograniczenia

wynikające z różnic w rozdzielczości kamer i monitorów nie są tu aż tak istotne? Powodem jest duża moc obliczeniowa komputerów oraz kart graficznych, które składają się na stacje robocze. Co prawda rozkład pikseli w obrazie wyświetlanym na ekranie monitora z całą pewnością odbiega od źródłowego rozkładu pikseli w przetworniku kamery, jednakże tym razem nieunikniona aproksymacja treści poszczególnych pikseli, to znaczy ich barwy i jaskrawości, jest dokonywana w dużo doskonalszy sposób. Proces ten odbywa się dynamicznie i zachodzi nawet wtedy, gdy rozmiary wyświetlanego obrazu ulegają zmianie, na przykład wtedy, gdy operator systemu powiększa obraz do rozmiaru całego ekranu monitora lub zmniejsza go do rozmiarów wynikających z podziału. W każdej z tych sytuacji obraz będzie zachowywał najwyższą możliwą do uzyskania rozdzielczość i dobrą reprodukcję barw.

Wspomniane stacje robocze mogą być wyposażane w monitory o różnej rozdzielczości i różnych rozmiarach. Wobec braku ograniczeń systemowych można sobie pozwolić na dużą różnorodność rozwiązań, wynikającą z założeń funkcjonalnych oraz konkretnych potrzeb użytkowników końcowych. W przypadku niewielkich systemów dozorowych stosuje się kilka małych monitorów o standardowej rozdzielczości, zajmujących niewielką powierzchnię i nie stwarzających problemów ergonomicznych podczas aranżacji pomieszczeń ochrony. W dużych i bardzo dużych systemach dozorowych sytuacja wygląda inaczej. Tradycyjne podejście, sprowadzające się do stosowania wielu małych monitorów, stwarza poważne problemy ergonomiczne i utrudnia aranżację pomieszczeń ochrony.

Najnowszą tendencją jest stosowanie niewielkiej liczby bardzo dużych monitorów o przekątnej ekranu rzędu 32", 40" lub nawet 60" i tworzenie tak zwanych monitorów wirtualnych, czyli wydzielonych fragmentów ekranu, stanowiących oddzielne pola obrazowe. Monitory wirtualne nie muszą być cały czas widoczne na ekranie i to odróżnia je od fizycznych, istniejących realnie małych monitorów podglądowych, stosowanych w archaicznych systemach hybrydowych. Małe monitory podglądowe zawsze musiały zajmować przestrzeń w pomieszczeniu ochrony, zaś były wykorzystywane sporadycznie, tylko w sytuacjach alarmowych. Monitory wirtualne mogą pojawiać się na żądanie, na przykład w chwili wykrycia sytuacji wymagającej interwencji operatora, mogą być powiększane na całą powierzchnię ekranu jednym kliknięciem myszy, a także mogą znikać, gdy już nie są potrzebne. Warto zauważyć, że rozdzielczość monitorów wirtualnych nie jest stała i może być dynamicznie dostosowywana do pełnionych przez nie funkcji, ulegać modyfikacji wraz ze zmianą rozmiarów pola obrazowego.

Z pozoru występuje tu podobieństwo do monitorów analogowych, opisanych we wstępie artykułu, jednakże, pomimo zbieżności celu, zastosowane metody są całkowicie różne i na stacjach roboczych wyświetlany jest obraz zachowujący wysoką jakość, niezależnie od jego aktualnego formatu.

Nie wszyscy producenci systemów monitoringu wizyjnego mają tak nowoczesne podejście. Na rynku nadal dostępne są systemy hybrydowe mające w nazwie słowo „cyfrowe", w których wykorzystywane są zwykłe monitory analogowe, sterowane poprzez kable koncentryczne, i które otrzymują zespolony sygnał wizyjny od odwrotnych koderów IP, czyli urządzeń zamieniających strumień danych cyfrowych na postać analogową. Jak na ironię stanowi to kolejne przetwarzanie tego samego sygnału, gdyż pochodzi on zazwyczaj z kamer analogowych, gdzie w koderach IP zespolony sygnał wizyjny był już raz przetwarzany na postać cyfrową. By tak dziwaczny system mógł w ogóle funkcjonować, nadzór nad pracą wszystkich wymienionych koderów jest sprawowany przez specjalny serwer zarządzający, zaś o sieciowości takiego systemu można mówić jedynie w obrębie serwerowni. Na temat walorów funkcjonalnych tej klasy systemów oraz jakości uzyskiwanych przez nie obrazów lepiej w ogóle się nie wypowiadać. Co prawda w przeszłości systemy hybrydowe odegrały pewną rolę w rozwoju telewizji przemysłowej, jednak obecnie stanowią jedynie ślepą uliczkę ewolucji i tak należy je traktować.

Tendencje na najbliższe lata

Tyle dygresji na tematy historyczne, wróćmy do rozwiązań współczesnych. Tendencją, którą można zaobserwować na współczesnym rynku CCTV jest stopniowy wzrost rozdzielczości. Dotyczy to zarówno kamer, jak i monitorów. W procesie tym widać jednak wyraźną granicę, która przebiega na poziomie nazywanym umownie *Full HD*. Chodzi o wielkość matrycy równą 1920×1080 pikseli, stosowaną w telewizji programowej, a także w sprzęcie domowym. Ten sam format zaczyna być coraz liczniej reprezentowany w urządzeniach do monitoringu telewizyjnego.

Przyczyn tej sytuacji jest wiele. Zauważany do niedawna pęd do bardzo dużych liczb pikseli, sięgających 16 mln, pomału ustępuje zdroworozsądkowym wymaganiom użytkowym, związanym z parametrami kamer, przepływnością typowych sieci IP oraz koniecznością ograniczenia przestrzeni dyskowej rejestratorów. Jakość obrazów uzyskiwanych z kamer wysokomegapikselowych jest relatywnie niska. Ich jedynym atutem są duże rozmiary matrycy, poza tym mają same wady. Odznaczają się bardzo niską czułością, niską poklatkowością, wymagają bardzo dobrze skorygowanych, drogich obiektywów, nie nadają się do pracy w typowych obudowach stosowanych w CCTV, gdyż przednie szybki tych obudów powodują utratę rozdzielczości układu kamera – obudowa – obiektyw. Takie kamery bardziej przypominają wyspecjalizowane aparaty fotograficzne niż urządzenia telewizyjne. Na przykład typowe kamery z przetwornikiem 16 Mpix, generują najwyżej trzy klatki obrazowe na sekundę przy pełnej rozdzielczości. Czy to w ogóle można nazwać telewizją?

Podobnie jak kilkadziesiąt lat temu, o rozwoju profesjonalnych systemów telewizyjnych zadecydował masowy rynek konsumencki. Obecnie zauważa się dążność do dorównania formatowi *Full HD* w sprzęcie CCTV.

Dążności tej sprzyja dostępność tanich monitorów, którymi mogą być konsumenckie odbiorniki telewizyjne. Przykładem mogą być monitory z rodziny Sony Bravia, które są dostępne w wersjach o różnych rozmiarach ekranu, akceptują wiele formatów i sposobów kodowania obrazów. W zasadzie należałoby je nazwać monitorami z możliwością odbioru programu telewizyjnego. Wszystko to sprzyja projektowaniu i instalacji systemów bezpieczeństwa pracujących w formacie *Full HD*, które z dużym prawdopodobieństwem wkrótce staną się standardem.

Andrzej Walczyk

Odmień swój system ochrony, zastosuj inteligentne kodery wizyjne.

Hybrydowe rozwiązania dla profesjonalistów pozwalają na niezauważalną integrację starych i nowych, obecnych i przyszłych rozwiązań, w całym zakresie profesjonalnych produktów monitoringu wideo Sony, oraz produktów innych firm.

Najnowsza linia wideoserwerów Sony pozwala na niezauważalne przejście od istniejących systemów, zbudowanych w oparciu o kamery analogowe, do rozwiązań bazujących na sieciach IP. Zbudowane w oparciu o najnowsze zdobycze sieciowych technologii wizyjnych osiągają wysoki stopień funkcjonalności, zapewniając maksymalny poziom bezpieczeństwa wynikający z zaawansowanych funkcji inteligencji, pozwalając równocześnie na redukcję kosztów instalacji.

Wybierz wideoserwer na miarę twoich potrzeb spośród urządzeń jednowejściowych lub czterowejściowych. Przejdź do świata nieograniczonych możliwości, bez wymiany całej instalacji! Zastosuj kodery wizyjne Sony, już zainstalowane kamery analogowe i wykorzystuj detekcję ruchu, przedmiotów, zliczanie obiektów i inne funkcje zaawansowanej inteligencji znajdujące się w wideoserwerach Sony. Od tej pory inteligencja systemu dostępna jest za rozsądną cenę, nawet w przypadku kamer analogowych!

Zapoznaj się ze wszystkimi rozwiązaniami dla profesjonalistów oferowanymi przez Sony w postaci inteligentnych wideoserwerów, kamer sieciowych i oprogramowania. Odwiedź **www.sonybiz.pl**

Unikalna hybrydowa technologia zaprojektowana z myślą o bezpieczeństwie

SONY

GO CONVERT

MIGRACJA → ROZWÓJ → ZAPIS → PODGLĄD → OBRAZ

KAMERY ANALOGOWE
GO HYBRID
KAMERY IP

www.sonybiz.pl

Przyszłość należy do inteligentnych systemów nadzoru IP

Agata Majkucińska

Zgodnie z prognozami IMS Research, zawartymi w raporcie *Światowy rynek urządzeń CCTV i wideo służących do monitoringu – wydanie 2008*, do 2012 roku światowy rynek kamer sieciowych osiągnie wartość ponad 2,5 miliarda USD. Również w Polsce nasila się trend migracji z analogowych systemów monitoringu wizyjnego do nowych rozwiązań IP. Wynika to nie tylko z globalnej tendencji upowszechniania się rozwiązań sieciowych, ale również z planowanych w Polsce licznych inwestycji w infrastrukturę, które związane są m.in. z organizacją Euro 2012. Wyzwania, jakie obecnie są stawiane przed systemami nadzoru wizyjnego, nie pozostawiają wątpliwości, że coraz częściej wykorzystywana będzie technologia zobrazowania cyfrowego i wkrótce wyprze ona instalacje analogowe. Od 1996 roku, kiedy firma Axis Communications stworzyła i wprowadziła na rynek pierwszą kamerę sieciową, właśnie ten segment rynku monitoringu wizyjnego rozwija się najbardziej dynamicznie, a w ciągu najbliższych pięciu lat będzie rósł w tempie 35% rocznie

Od H.264 do HDTV

Obraz w wysokiej rozdzielczości nie jest już tylko domeną stacji telewizyjnych. Kamery HDTV coraz powszechniej wykorzystuje się także w sektorze nadzoru wizyjnego. Transfer do technologii HD nie byłby jednak możliwy bez optymalizacji wykorzystania pasma sieciowego i stworzenia możliwości transmisji wielu skompresowanych, niezależnie skonfigurowanych strumieni wideo o bardzo wysokiej jakości. Dlatego H.264 – najnowszy standard kompresji wideo – stanie się, prawdopodobnie w ciągu najbliższych lat, preferowaną metodą transmisji obrazu. W systemach nadzoru wizyjnego wykorzystujących kodowanie H.264 zmniejszają się koszty pamięci masowej oraz poprawia się wykorzystanie pasma sieciowego – nawet o 80% w porównaniu z kodowaniem Motion JPEG i o 50% w porównaniu z tradycyjnym formatem MPEG-4 Part 2. Jedna sekunda nieskompresowanego obrazu telewizyjnego zajmuje 165 MB. Oznacza to, że w przypadku braku kompresji jedna minuta przekazu telewizyjnego zajmowałaby 9,9 GB przestrzeni dyskowej, jedna godzina – 594 GB, a 24 godziny – 14 246 GB (jest to odpowiednik 14 dysków twardych o pojemności 80 GB). Taka ilość danych nie mogłaby zostać przesłana przez sieć w rozsądnym czasie, ponadto większość systemów monitoringu wizyjnego musi współdzielić sieć z innymi aplikacjami. Naturalne wydaje się więc wykorzystanie najefektywniejszej metody kompresji materiału wizyjnego, zapewniającej transfer obrazu o wysokiej jakości przy znacznie mniejszych wymaganiach dotyczących szerokości pasma, mniejszej stopie błędów i niższej latencji (czasie potrzebnym na kompresję, przesłanie, dekompresję i wyświetlenie pliku).

Telewizja wysokiej rozdzielczości

Upowszechnienie się standardu H.264 ma jeszcze jedną ważną zaletę – przyczyniło się do spopularyzowania kamer megapikselowych i HDTV w sektorze monitoringu wizyjnego. Dzięki efektywnej kompresji można łatwo zredukować rozmiary plików bez uszczerbku dla jakości obrazu, która w przypadku takich modeli kamer, jak np. AXIS P1346, jest niemal fotograficzna. Zastosowanie kamery AXIS P1346 HDTV z przetwornikiem 3 Mpx, wykorzystującej nowatorską metodę sterowania przysłoną, tzw. P-Iris (kombinacja oprogramowania Axis i sterowania obiektywem firmy KOWA), gwarantuje wysoki kontrast, głębię i ostrość obrazu, a jednocześnie niweluje efekt rozmywania się obrazu spowodowany dyfrakcją światła na krawędziach zbyt małego otworu przesłony. Cechy te mają szczególne znaczenie przy obserwacji długich korytarzy, przestrzeni parkingowych, dużych powierzchni i oddalonych obiektów.

Materiał wizyjny materiałem dowodowym

Dzięki zastosowaniu najnowszych technologii, gwarantujących uzyskanie ostrego, klarownego obrazu, materiał wizyjny zarejestrowany przez kamery cyfrowe może służyć jako nieoceniony dowód w postępowaniach sądowych. Odróżnia to kamery cyfrowe od modeli analogowych, które nawet przy najwyższej z możliwych w ich przypadku rozdzielczości (4CIF) nie były w stanie dostarczać wiarygodnego obrazu scen o dużym natężeniu ruchu. Wynika to z charakteru obrazu analogowego, który powstaje w wyniku skanowania z przeplotem, tzn. obrazy tworzone są z dwóch pól linii parzystych i nieparzystych – ich nałożenie tworzy pełną klatkę. Ta cecha obrazu analogowego

Fot. 1. Nowoczesne kamery sieciowe sprawdzają się w każdych warunkach

sprawia, że podczas obserwacji obiektu znajdującego się w ruchu występuje duże prawdopodobieństwo rozmycia się obrazu, co często uniemożliwia identyfikację osób lub pojazdów.

Uniwersalne zastosowania

Realizowany w technologii IP monitoring wizyjny znajduje dziś zastosowanie w wielu środowiskach, zarówno w niewielkich zakładach pracy czy sklepach, jak i w olbrzymich obiektach użyteczności publicznej. Niemal wszystkie obiekty olimpijskie na świecie objęte są nadzorem bazującym na technologii IP, wykorzystującym kamery i wideoserwery sieciowe, w tym także między innymi sprzęt produkowany przez firmę Axis Communications. Rozwiązania IP znajdują też szczególne zastosowanie w systemach monitoringu miejskiego. Wykorzystanie kamer o dużej rozdzielczości i szerokim kącie obserwacji pozwala na instalację znacznie mniejszej ich liczby niż w przypadku urządzeń o mniejszej rozdzielczości. Funkcje inteligentnej analizy obrazu umożliwiają znacznie mniejsze zaangażowanie personelu odpowiedzialnego za monitoring oraz wydajne przyspieszenie reakcji służb w razie wystąpienia sytuacji niestandardowych. Dodatkowo, dzięki funkcji PoE (*Power over Ethernet*) instalacja systemów IP nie wymaga dodatkowego okablowania służącego do zasilania urządzeń.

Fot. 2. Kamera termowizyjna AXIS Q1910

Monitoring do zadań specjalnych

Rozwój systemów nadzoru wizyjnego zmierza w kierunku opracowywania urządzeń do coraz bardziej rozbudowanych instalacji zewnętrznych, stwarzających coraz wyższe wymagania użytkowe. Na rynku pojawiły się już systemy wykorzystujące kamery termowizyjne, które umożliwiają niezawodne wykrywanie ludzi i zdarzeń nawet w całkowitych ciemnościach lub w trudnych warunkach pogodowych, np. podczas silnej mgły czy zadymienia. Kamery te tworzą obraz w reakcji na ciepło emitowane przez pojazdy z silnikami cieplnymi lub przez ludzi i zwierzęta. Model AXIS Q1910-E spełnia wymagania IP66, dzięki czemu przystosowany jest do pracy na zewnątrz. Znakomicie sprawdza się w systemach monitoringu granic państwowych, na autostradach, drogach szybkiego ruchu, peronach stacji kolejowych, mostach i w tunelach. Kamera ta dostarcza obraz o rozdzielczości 160 x 128 pikseli, dysponuje kątem widzenia równym 17 stopni, wytwarza maksymalnie 8,33 klatek na sekundę. Kamera AXIS Q1910-E ma wbudowane funkcje inteligentnej analizy obrazu telewizyjnego, dzięki którym jest w stanie generować alarmy ostrzegające o próbach manipulacji, jest wyposażona w czujnik ruchu i ma możliwość transmisji sygnałów fonicznych. Wprowadzenie inteligentnych kamer termowizyjnych do oferty Axis Communications to posunięcie, które z pewnością wyznaczy kierunek rozwoju firmy na najbliższe lata.

Agata Majkucińska
Axis Communications

Fot. 3. Kamera HDTV/3 MP AXIS P1346 z P-Iris

GODZINA 1:16
Trwa kradzież samochodu.

Efektywny system zewnętrznego nadzoru wizyjnego chroni to co cenimy najbardziej, ostrzega o niespodziewanych zdarzeniach a nawet uaktywnia konkretne działania. Ale kamery, które są w stanie to osiągnąć muszą wytrzymywać ciężkie opady śniegu, intensywne opady deszczu lub silne wiatry- i ciągle dostarczać użyteczny obraz.

Kamery do zastosowań zewnętrznych Axis są wyjątkowo proste do zainstalowania, co oszczędza cenny czas i minimalizuje koszty utrzymania. Wytrzymują one ekstremalne warunki pogodowe i zapewniają wyjątkową jakość obrazu. Ponieważ system nadzoru wizyjnego musi dostarczać niepodważalne dowody w formie przejrzystego, wyraźnego materiału wizyjnego- nawet w najcięższych warunkach.

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

Seria kamer sieciowych Axis P33: obudowa klasy IP66, praca w trybie dzień/noc, funkcja wide dynamic range, H.264, zasilanie PoE, jakość obrazu HDTV, zdalny zoom, ogniskowanie i wiele innych.

AXIS COMMUNICATIONS

Niech ochrona gra czysto

Videotec

Firma Videotec oferuje głowice uchylno-obrotowe ULISSE, cechujące się zarówno stylowym wyglądem, jak i solidnym wykonaniem. Włoski producent Videotec, którego produkty odznaczają się niezawodnością, potwierdzoną przez ponad dwadzieścia lat praktyki, ma w swojej ofercie wiele systemów CCTV do zastosowań zewnętrznych oraz łączy innowacyjne technologie z niebanalnym wzornictwem, uzyskując niedościgniony poziom jakościowy swoich wyrobów

Firma produkuje profesjonalne i certyfikowane elementy wyposażenia systemów monitoringu wizyjnego, takie jak obudowy ochronne i systemy pozycjonowania kamer, przeznaczone do użycia w warunkach zewnętrznych oraz w szczególnie agresywnych warunkach środowiskowych, a także klawiatury sterujące i systemy zarządzające instalacjami wizyjnymi, w tym urządzenia do cyfrowej analizy sygnałów wizyjnych.

Produkty firmy Videotec są z powodzeniem wykorzystywane w tysiącach telewizyjnych systemów obserwacyjnych na obszarze całego świata.

Wystarczy wspomnieć o produkowanej przez firmę Videotec uchylno-obrotowej głowicy ULISSE, na którą padł ostatnio wybór podczas realizacji systemu nadzoru wizyjnego na terenie jednego z ważniejszych stadionów w Madrycie.

W przypadku stadionów szeroko i powszechnie dyskutowany jest problem bezpieczeństwa, zwłaszcza po pełnych przemocy incydentach, zakończonych tragicznie, zaistniałych podczas imprez sportowych. Szczególnie dotyczy to świata piłki nożnej.

Podczas rozmowy z wieloma menedżerami ds. bezpieczeństwa przedstawiciele firmy Videotec stwierdzili, że rozwiązania związane z bezpieczeństwem stadionów sprowadzają się do:

– dobrego rozplanowania obiektu, który powinien być otoczony rozległą przestrzenią parkingową i doskonałym systemem dróg dojazdowych, pozwalających na łatwe dotarcie do stadionu i na łatwe jego opuszczenie, a także umożliwiać szybką ewakuację, o ile będzie ona konieczna;
– zatrudnienia wyspecjalizowanych pracowników, nie stosujących środków represyjnych, pozostających w stałym kontakcie z policją stacjonującą poza terenem obiektu;
– zapewnienia biernego zabezpieczenia w postaci ogrodzenia o wysokości co najmniej trzech metrów;

– zastosowanie skutecznego systemu nadzoru wizyjnego, zarówno w obrębie obiektu, jak i poza jego terenem.

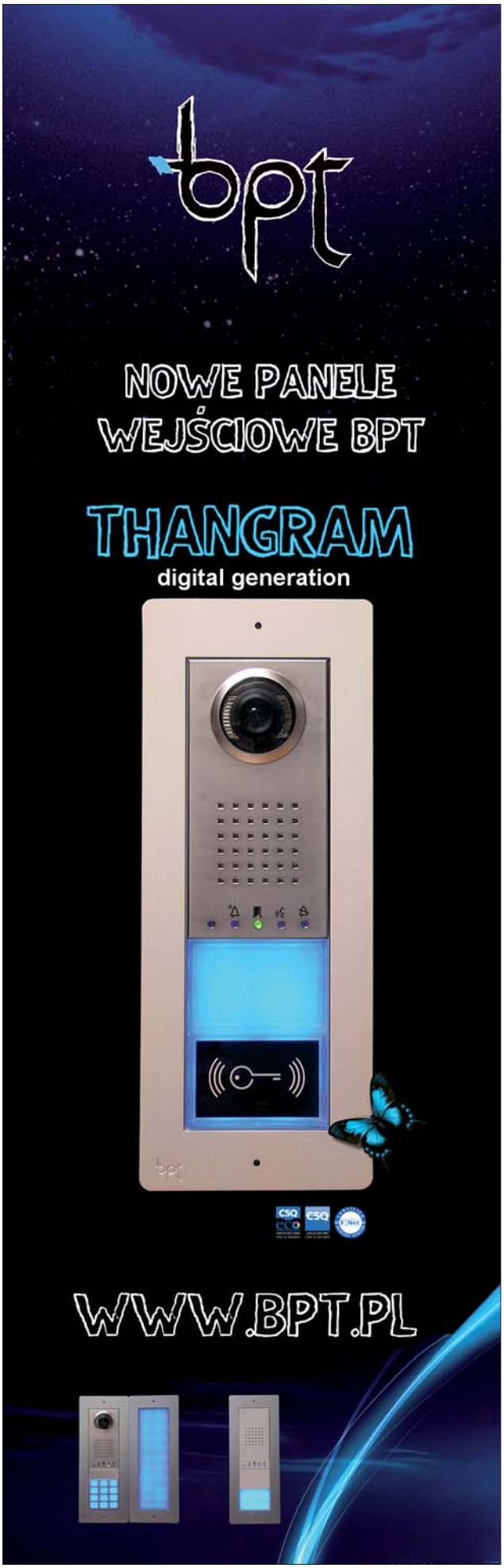
Ankietowani menedżerowie ds. bezpieczeństwa potwierdzili istotne znaczenie systemu monitoringu wizyjnego, pracującego w czasie rzeczywistym, zdolnego do dostarczania przydatnych informacji.

Większość widzów ma przychylny stosunek do tego rodzaju nadzoru i nie odczuwa niepokoju w jego obecności, zarówno wewnątrz obiektu, jak i poza jego obrębem, tak więc można obserwować zachowania publiczności podczas przebiegu całej imprezy sportowej, a także pozyskiwać bieżące obrazy, które pokazują zachowania widzów zakłócających porządek. Co więcej, operator odpowiedzialny za obsługę systemu dozorowego musi dysponować możliwością pełnego, natychmiastowego sterowania każdą pojedynczą kamerą. W celu uzyskania możliwie najpełniejszego obrazu operator musi mieć możliwość nadzorowania pracy tych kamer, z których obrazy są aktualnie wyświetlane na monitorach kontrolnych, poprzez zdalne sterowanie nimi z wykorzystaniem głowic uchylno-obrotowych. W trakcie tych czynności obrazy pochodzące ze wszystkich kamer muszą być rejestrowane.

Wizyjne urządzenia dozorowe, używane do rejestracji obrazu widzów podczas ich wchodzenia na stadion, pobytu na jego terenie oraz w trakcie jego opuszczania, powinny być chronione przed uszkodzeniem lub wszelką inną ingerencją i zastosowane w liczbie pozwalającej na bezproblemową rejestrację obrazów z wszystkich wejść i wyjść, wszystkich sektorów zarezerwowanych dla publiczności, obszarów wewnętrznych dostępnych dla publiczności (z wyjątkiem toalet), a także obszarów zewnętrznych, wykorzystywanych do wstępnej selekcji widzów.

Kamery powinny być rozmieszczone głównie wewnątrz ciągów komunikacyjnych, w taki sposób, by mogły obserwować twarze widzów ujmowane *an face*. Ponadto powinny być umieszczane ponad tłumem, aby widzowie znajdujący się z przodu nie zasłaniali osób stojących za nimi.

Podsumowując, monitoring wizyjny odgrywa fundamentalną rolę w zapewnieniu efektywnej i skutecznej ochrony stadionów, która jest niezbędna do tego, by każdy z widzów mógł na nowo odkryć przyjemność płynącą ze zdrowej i wolnej od przemocy formy rozrywki.



Biorąc to wszystko pod uwagę, można stwierdzić, że duży asortyment głowic uchylno-obrotowych ULISSE i ULISSE COMPACT firmy Videotec doskonale sprawdzi się w instalacjach monitoringu o wysokich wymaganiach użytkowych, takich jak systemy obserwacyjne na stadionach sportowych. Te zaawansowane technologicznie urządzenia pozycjonujące integrują w jedną całość głowicę uchylno-obrotową, obudowę kamery i odbiornik telemetryczny.

Obecnie produkty z rodziny ULISSE są dobrze znane na rynku CCTV, zdobywają uznanie i znaczące nagrody. To dlatego, że stanowią zaawansowane technologicznie rozwiązania, łączące w sobie zalety konstrukcyjne i wytrzymałość tradycyjnych urządzeń uchylno-obrotowych z elastycznością i szybkością działania typowych szybkoobrotowych kamer kopułowych.

Głowice uchylno-obrotowe ULISSE oferują sprawdzoną niezawodność. Mogą pracować przez całą dobę w najcięższych warunkach środowiskowych, przy silnym wietrze niosącym kurz lub piasek, w bardzo wysokich lub bardzo niskich temperaturach, a koszty ich konserwacji są niskie.

Urządzenia uchylno-obrotowe ULISSE wyróżniają się zarówno w stosunku do szybkoobrotowych kamer kopułowych, jak i konkurencyjnych głowic uchylno-obrotowych, dysponując zdolnością do ciągłego ruchu obrotowego o dużej prędkości, zapewniając bardzo precyzyjne pozycjonowanie, dysponując funkcjami automatycznej panoramy oraz możliwościami tworzenia sekwencji patrolowych, przewyższając technologię PTZ możliwością obserwacji obszarów znajdujących się ponad horyzontem, a także uproszczoną instalacją.

Ponadto prezentowana rodzina produktów pozwala na tworzenie różnorodnych rozwiązań dzięki:

– możliwości wyboru dowolnego typu kamer (od kamer standardowych poprzez zestawy kamer i obiektywów o znacznych rozmiarach do kamer termowizyjnych), dowolnego typu obiektywów, a także kamer zintegrowanych;
– wbudowanemu, stanowiącemu fabryczne wyposażenie oświetlaczowi IR-LED, a także, w przypadku głowicy ULISSE COMPACT, dzięki specjalnemu wysięgnikowi sufitowemu do montażu urządzenia w pozycji odwróconej, która sprawdza się w przypadku instalacji wewnątrz pomieszczeń lub pod zadaszeniem ochronnym, np. na stadionie;
– opcji wycieraczki ze spryskiwaczem;
– zdolności do ruchu obrotowego w pionie, w zakresie od +90° do - 90°, z maksymalną prędkością 200°/s (dla głowicy ULISSE COMPACT).

Operatorzy mogą z łatwością sterować wszystkimi urządzeniami uchylno-obrotowymi ULISSE, robiąc to zdalnie, z pokoju kontrolnego, w trybie analogowym lub w trybie IP.

Ze względu na szeroki zakres oferowanych rozwiązań, wyjątkowe cechy użytkowe, elastyczność i solidną konstrukcję głowica ULISSE jest jednym z najbardziej udanych produktów firmy Videotec.

Więcej informacji można uzyskać na stronie *www.videotec.com.*

Videotec

Szybki, Skuteczny i Konkurencyjny

ULISSE COMPACT

ULISSE COMPACT jest najnowszym rozwiązaniem przeznaczonym dla absorbujących zastosowań zabezpieczających i monitorowania na zewnątrz budynków.

Dzięki swojej zwartej i zdecydowanej sylwetce ULISSE COMPACT umożliwia ciągły obrót z dużą prędkością, bezwzględną dokładność ustawienia i większą jakość obrazu oraz ekstremalną wytrzymałość i uproszczoną konfigurację systemu.

VIDEOTEC

CCTV PRODUCTS

www.videotec.com

System IP Internec

kamery megapikselowe
kamery PTZ IP
wideoserwery IP

Mariusz Jastrząbek

Od kilku lat obserwuje się dynamiczny wzrost zainteresowania urządzeniami IP w systemach telewizji dozorowej, a potentaci w branży prognozują stopniowe odejście od analogowej CCTV. O korzyściach oraz wadach stosowania obu technologii napisano już „gigabajty" tekstu, zatem nie będziemy się dziś spierać na ten temat. Mimo to żywię nadzieję, że dzięki przedstawieniu zalet systemu bazującego na urządzeniach Internec IP uda się przeciągnąć kilku dotychczasowych przeciwników IP na stronę zwolenników tej technologii

Rodzina produktów IP Internec obejmuje wiele modeli kamer stałopozycyjnych IP o rozdzielczościach D1, 1,3 Mpx oraz 2 Mpx, sieciowych, obrotowych kamer PTZ oraz wideoserwerów IP. Kamery IP Internec są dostępne w różnych wersjach, jako kamery kopułowe wewnętrzne lub zewnętrzne z wbudowanym obiektywem zmiennoogniskowym oraz kamery typu *box* z obiektywem dobieranym w zależności od potrzeb.

W ofercie firmy Internec IP nowość stanowi zewnętrzny, zintegrowany, megapikselowy punkt kamerowy PTZ w obudowie kopułowej. Model ten łączy wysoką jakość obrazu o rozdzielczości 1,3 Mpx (1280×960 px) z możliwościami sterowania położeniem kamery w poziomie i pionie oraz 10-krotnej zmiany powiększenia optycznego.

Często niechęć do rozwiązań bazujących na technologii IP, z którą można się spotkać wśród instalatorów, wynika z wcześniejszych złych doświadczeń związanych ze sprzętem IP. Poniżej przedstawione zostaną wybrane właściwości urządzeń Internec IP.

Jakość obrazu uzyskiwanego w warunkach nocnych

Sprawa dotyczy kamer megapikselowych, które zwykle bazują na przetwornikach obrazowych typu CMOS, charakteryzujących się dużymi wymaganiami co do oświetlenia, jednakże modele megapikselowe IP Internec 1,3 Mpx wykorzystują przetworniki typu CCD. Kamery te wyróżniają się wyjątkowo wysoką czułością, równą 0,1 lx przy F = 1,2 w trybie dziennym oraz 0,01 lx przy F = 1,2 w trybie nocnym. W połączeniu z poklatkowością 25 kl./s, zapewniającą uzyskanie płynnego obrazu o rozdzielczości HD720, kamery IP Internec 1,3 Mpx stanowią rozwiązanie idealnie sprawdzające się w systemach monitoringu przestrzeni otwartych, również w warunkach słabego oświetlenia. Kamery IP Internec z przetwornikiem CCD 1,3 Mpx są dostępne w wersji *box*, bez obiektywu (model 862MF-E), w wersji kopułowej, wandaloodpornej, zewnętrznej (762MF-FB). Dostępny jest także wspomniany wcześniej model obrotowy PTZ (2DF1-671).

Wykorzystanie pasma sieciowego oraz przestrzeni dyskowej

Wiele modeli megapikselowych kamer IP bazuje na kompresji MJPEG. Po podłączeniu takiej kamery do systemu monitoringu okazuje się, że generowany przez nią strumień danych przekracza 20 Mb/s. Charakterystyczną cechą kamer IP Internec jest kompresja MPEG4 lub H.264 we wszystkich dostępnych rozdzielczościach, dzięki której strumienie danych generowane przez te kamery wahają się w granicach od 1 do 4 Mb/s. W praktyce taka redukcja pasma ma kolosalne znaczenie. Nawet kilkanaście kamer megapikselowych IP Internec nie przeciąży sieci LAN 100 Mbps, a czasy archiwizacji nagrań mogą być liczone w tygodniach przy obecnych pojemnościach dysków twardych.

Podgląd w sieci Internet

Problemy związane z ograniczoną przepływnością połączeń z Internetem (np. w przypadku usługi Neostrada 512 przepływność dla danych wychodzących jest ograniczona do 128 kb/s) dają się niwelować dzięki dwustrumieniowości urządzeń IP Internec. Podczas konfiguracji urządzeń IP Internec parametry kompresji dla głównego strumienia danych oraz dla strumienia pomocniczego definiuje się oddzielnie. Urządzenia IP Internec pozwalają na jednoczesne wykorzystywanie obu wspomnianych strumieni przez urządzenia klienckie. Parametry głównego strumienia danych są ustalane w sposób pozwalający na uzyskanie obrazu o możliwie najwyższej jakości osiągalnej dla danego modelu kamery. Kamery generują strumień danych mieszczący się w granicach od 1do 4 Mb/s. Główny strumień danych jest wykorzystywany do wyświetlania oraz zapisu obrazu w sieci LAN o dużej przepustowości (np. 100 Mb/s). Parametry strumienia pomocniczego są ustalane tak, aby ograniczyć przepływność do 32–512 kb/s kosztem rozdzielczości obrazu, umożliwiając jego płynną transmisję z poklatkowością dochodzącą do 25 kl./s. Strumień pomocniczy pozwala na poprawną transmisję obrazów w sieci Internet.

Oprogramowanie systemu IP

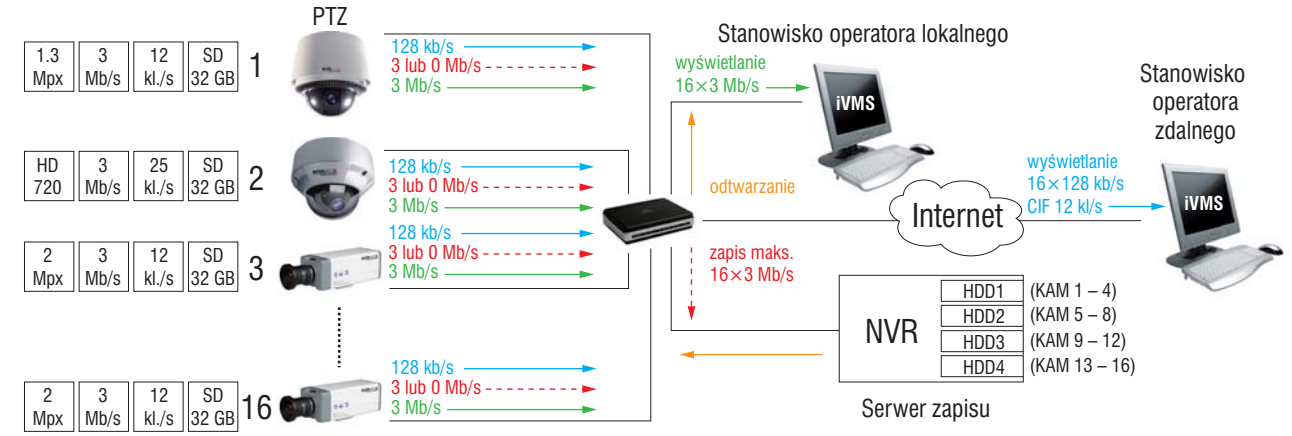
Wszystkie urządzenia IP Internec są obsługiwane przez nieodpłatny pakiet oprogramowania. Najważniejszymi aplikacjami są Internec iVMS, tworząca stanowisko operatora systemu z obsługą do 50 urządzeń IP, oraz aplikacja serwera zapisu NVR. Funkcje iVMS pozwalają na pełne zarządzanie systemem dzięki możliwości zdalnej konfiguracji wszystkich zawartych w nim urządzeń sieciowych. Ponadto system zapewnia podgląd obrazów z kamer w czasie rzeczywistym, pozwala na wizualizację swojego działania na e-mapie, a także umożliwia dostęp do nagrań i stwarza możliwość ich archiwizacji. Aplikacja NVR umożliwia zbudowanie stabilnego rejestratora obrazów pobieranych z maksymalnie 60 urządzeń IP Internec. Oprogramowanie NVR jest wyposażone w funkcję *watchdog*, a także w funkcję automatycznego restartu z naprawą bazy danych. Zestaw iVMS oraz NVR umożliwia zbudowanie profesjonalnego systemu IP o stopniu złożoności spełniającym wymagania projektowe dotyczące liczby stanowisk służących do podglądu oraz do zapisu obrazów.

Użyteczne funkcje

Szereg funkcji, które w systemach analogowych były realizowane przez rejestratory, zostało zaimplementowanych bezpośrednio w kamerach IP Internec. Zaliczyć do nich można detekcję ruchu z możliwością dostosowania stref dozoru oraz czułości, detekcję prób sabotowania systemu, objawiających się degradacją parametrów obrazu, zastosowanie wejść alarmowych oraz możliwość reagowania na awarie systemowe. W przypadku wykrycia wydarzenia wymagającego ingerencji ludzkiej informacja z kamery IP Internec zostaje przesłana do stanowiska obserwacyjnego. Wydarzenie może być sygnalizowane dźwiękiem, aktywnością na mapie synoptycznej oraz pojawieniem się tak zwanego wyskakującego obrazu, wyświetlającego scenę obserwowaną przez kamerę w chwili powstania alarmu. Prawidłowo zaprogramowany system IP Internec pozwala na poprawę komfortu pracy operatora, umożliwiając mu skupienie uwagi na istotnych faktach.

Rozproszona inteligencja

Z punktu widzenia budowy i działania systemu monitoringu bazującego na urządzeniach IP Internec bardzo istotny jest fakt, że detekcja ruchu odbywa się w kamerach. Rozproszenie inteligencji odciąża system w dwóch aspektach. Serwer zapisu



Rys. 1. Ruch w sieci TCP/IP dla systemu 16 kamer megapikselowych IP Internec z oprogramowaniem iVMS oraz NVR

NVR, pracujący w trybie zapisu aktywowanego detekcją ruchu, nie wykorzystuje żadnych mocy obliczeniowych w celu analizy obrazu. Ponadto ruch sieciowy jest zmniejszony, ponieważ transmisja obrazów z kamer IP do serwera zapisu NVR odbywa się wyłącznie na skutek wykrycia ruchu w tych kamerach. W przypadku niewielkiego systemu można sobie pozwolić na centralne przetwarzanie obrazów, jednak wraz ze wzrostem liczby megapikselowych kamer IP rosną korzyści wynikające z rozproszonej inteligencji, przekładając się bezpośrednio na oszczędności związane z zastosowaniem prostszych i tańszych jednostek obliczeniowych w roli serwerów zapisu.

Zapis wewnętrzny

Kamery IP Internec dają możliwość zainstalowania kart SDHC o pojemności do 32 GB. Na takich kartach może odbywać się zapis w trybie ciągłym lub alarmowym, z nadpisywaniem lub prowadzony do momentu zapełnienia karty. Uzyskiwane czasy zapisu, w zależności od rozdzielczości i poklatkowości obrazów, wahają się od kilkunastu do kilkuset godzin. Dodatkowa, wewnętrzna archiwizacja dokonywana przez kamery IP Internec otwiera drogę do poprawienia bezpieczeństwa systemu poprzez zapewnienie ciągłości nagrań nawet w przypadku uszkodzenia łączy między kamerami IP a serwerem zapisu NVR. Kamery IP Internec mogą być również wykorzystane w sposób nietypowy, jako system typu „wszystko w jednym", charakteryzujący się mobilnością, niewielkim poborem prądu oraz małą wrażliwością na drgania mechaniczne.

Możliwość integracji z istniejącymi systemami CCTV

Urządzenia Internec IP są obsługiwane przez platformę Alnet Net Professional, co oznacza możliwość integracji kamer IP Internec z istniejącymi systemami wykorzystującymi urządzenia IP różnych producentów, a także rozbudowy systemów analogowych wynikającej z zastosowania kamer IP Internec.

Koszt systemu

Oczywiście cena megapikselowej kamery IP kilkakrotnie przewyższa cenę kamery analogowej. Jeśli uwzględni się fakt, że poprawnie zainstalowana kamera o rozdzielczości 1,3 Mpx lub 2 Mpx może zastąpić kilka analogowych punktów kamerowych, zapisujących obrazy w rozdzielczości D1, koszt systemu jest porównywalny. W tym miejscu należy wyraźnie podkreślić, iż na tle innych, dostępnych rynku urządzeń sprzęt Internec IP wyróżnia się korzystnym stosunkiem możliwości technicznych do ceny.

System Internec IP w praktyce

Przyjrzymy się przepływowi danych w sieci TCP/IP w systemie kamer IP Internec. Rysunek przedstawia system monitoringu złożony z 16 kamer megapikselowych ze stanowiskiem obserwacyjnym iVMS oraz wydzielonym serwerem zapisu NVR. Sytuacja, w której obsługa nie ma bezpośredniego, fizycznego dostępu do serwera zapisu, wydatnie poprawia bezpieczeństwo systemu.

Kolejną zaletą systemu Internec jest oferowana przez serwer zapisu NVR ciekawa możliwość rozdzielenia obciążenia dysków w przypadku zapisu obrazów z wielu kamer. Do danego dysku przypisywany jest zapis grupy wybranych kamer, a nie wszystkich kamer jednocześnie. Przy założeniu, że ruch aktywujący zapis będzie występował przez 40% czasu pracy całego systemu, przy zastosowaniu czterech dysków o pojemności 1,5 TB każdy uzyskamy akceptowalny wynik 30 dni okresu archiwizacji. W przedstawianym systemie IP Internec przewidziany został zdalny podgląd obrazów przez Internet z wykorzystaniem pomocniczego strumienia danych, transmitującego obrazy o ograniczonych parametrach. Każda z kamer IP Internec została dodatkowo wyposażona w kartę SDHC o pojemności 32 GB, która umożliwia tworzenie lokalnego, co najmniej 24-godzinnego archiwum.

Na schemacie umieszczone zostały opisy rozdzielczości poszczególnych kamer oraz dane dotyczące poklatkowości obrazu. Dla przyjętych parametrów należy ustawić przepływność głównego strumienia danych na poziomie 3 Mb/s. Kolorowe strzałki obrazują ruch w sieci TCP/IP. Do stanowiska iVMS, przy włączonym podglądzie ze wszystkich 16 kamer, dociera strumień danych o stałej wartości 16 x 3 Mb/s = 48 Mb/s. Natomiast maksymalny strumień danych na wejściu serwera NVR, tj. 48 Mb/s., wystąpi tylko w chwili, gdy każda z kamer jednocześnie przejdzie w tryb rejestracji związany z wykryciem ruchu. W trakcie odtwarzania lub archiwizacji nagrań na stanowisku iVMS następuje transmisja danych na drodze od NVR do iVMS. Proszę zwrócić uwagę na fakt, że do poprawnego działania opisywanego systemu IP Internec wystarczy najszerzej obecnie stosowana sieć 100 Mb/s.

Mariusz Jastrząbek
Bezpośredni kontakt z autorem: m.jastrzabek@internec.pl
Więcej o systemie IP Internec na www.internec.pl

Nowa jakość dźwięku!

UNISPEAKER

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

Głośniki UNIspeaker posiadają odpowiednie Certyfikaty i Świadectwa Dopuszczenia CNBOP.

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

Rejestratory czasu rzeczywistego

DV-IP RT Dedicated Micros

Karol Fietkiewicz

Prędkość życia nieustannie rośnie. Liczba i szybkość samochodów na drogach wzrasta, robimy coraz więcej zakupów w coraz większych sklepach, organizowane są imprezy masowe – koncerty, zawody sportowe, wiece. Systemy bezpieczeństwa muszą być coraz doskonalsze, coraz szybsze, muszą oferować coraz lepszą jakość nadzoru wizyjnego, jednocześnie dając operatowi możliwość błyskawicznej reakcji i dokładnego rozpoznania sytuacji celem ustalenia przebiegu zdarzenia. Krytycznym parametrem jest często jakość i wydajność transmisji sieciowej oraz oprogramowania. Bardzo ważna jest też możliwość szybkiego reagowania na różnego rodzaju alarmy. Tak samo istotne są funkcje wyszukiwania zdarzeń w już nagranym materiale. Aby maksymalnie wspomóc operatora w centrum monitoringu, konieczny jest wysokiej jakości obraz wyjściowy

Ostatnio firma Dedicated Micros opracowała kilka modeli rejestratorów, których parametry są zgodne z najwyższymi standardami. Takimi urządzeniami są rejestratory serii DV-IP RT, DV-IP HD czy DV-IP Express.

Czym jest najwyższej jakości nadzór wizyjny? Najczęściej kojarzy się on z rejestracją i transmisją obrazów o wysokiej rozdzielczości (PAL, 4CIF), a także ze standardową prędkością 25 kl./s. W wielu systemach CCTV rejestracji dokonuje się z prędkością 6 kl./s lub nawet mniejszą. Czy wobec tego tak wysokie wymagania co do prędkości zapisu nie są zbyt wygórowane?

Wyobraźmy sobie nadzór ruchu drogowego. W każdej sekundzie przez dany fragment dwupasmowej drogi może przejeżdżać kilkanaście samochodów. Przy prędkości ruchu pojazdów równej 100 km/godz. oraz przy prędkości zapisu równej 25 kl./s długość odcinka przejeżdżanego przez pojazdy w okresie pomiędzy dwoma kolejnymi klatkami telewizyjnymi waha się w granicach metra. Dla wolniejszej rejestracji – np. 6 kl./s – jest to prawie siedem metrów, co przekracza już długość pojazdu. W przypadku kolizji lub innego incydentu drogowego trudno jest ustalić właściwy przebieg zdarzenia. Z jaką prędkością poruszały się pojazdy? Jakie było ich ustawienie względem siebie? W którym momencie nastąpiła zmiana świateł?

Z analogiczną sytuacją mamy do czynienia w przypadku nadzoru obiektów sportowych, kasyn, sklepów lub banków. Zbyt wolna rejestracja i mała rozdzielczość obrazu często nie pozwalają jednoznacznie wskazać sprawcy. Nagrywanie obrazu z prędkością sześciu lub czasem tylko trzech klatek na sekundę to zbyt mało – wprawnemu napastnikowi daje dużo czasu na wymierzenie ciosu, wyjęcie lub schowanie jakiegoś przedmiotu (np. żetonów czy pliku pieniędzy). Niska jakość obrazu nie pozwoli dokładnie rozpoznać sprawców. W takiej sytuacji operator systemu ma utrudnione zadanie i musi opierać się na poszlakach.

Kompleksowym a jednocześnie elastycznym rozwiązaniem, które sprawia, że parametry zapisu są doskonałe, jest zastosowanie rejestratorów Dedicated Micros z serii RT (RT – *Real Time* – „czas rzeczywisty"), które umożliwiają rejestrację z pełną prędkością przy maksymalnej rozdzielczości.

Urządzenia z serii RT mają 8 lub 16 przelotowych wejść wizyjnych. Zapis w każdym z kanałów odbywa się z maksymalną prędkością do 25 kl./s. Dla systemów o niższych wymaganiach funkcjonalnych istnieje również wersja NRT z 16 lub 32 wejściami wizyjnymi, gdzie zapis odbywa się z prędkością 12 kl./s. Obrazy ze wszystkich kamer analogowych są rejestrowane z maksymalną rozdzielczością 4CIF, z użyciem kodowania MPEG-4 lub MJPEG. Możliwy jest też zapis obrazów z kamer sieciowych (IP), w tym kamer megapikselowych. Dla każdej z kamer indywidualnie definiujemy ilość zapisywanych informacji – w przypadku kodowania MPEG-4 przez podanie wielkości strumienia w kb/s (*bit-rate*), a w przypadku kodowania MJPEG przez podanie wielkości pojedynczej klatki. Podobnie jak w innych rejestratorach Dedicated Micros, w DV-IP RT użytkownik może elastycznie konfigurować parametry zapisu dzięki technologii **MultiMode**. Technologia ta daje możliwość ustawienia parametrów zapisu dla trybu alarmowego, trybu dzień/noc lub trybu rejestracji w dni świąteczne osobno, niezależnie dla każdej kamery. **MultiMode** pozwala na wybór pomiędzy rodzajem kodeka, stopniem kompresji obrazu, prędkością nagrywania lokalnego i parametrami transmisji do użytkownika zewnętrznego. W zależności od harmonogramu, trybu alarmowego lub gdy zachodzi potrzeba rejestracji obrazu ze szczególnie ważnych kamer w wysokiej jakości, urządzenie jest w stanie samo wybrać odpowiedni, wcześniej zdefiniowany, rodzaj pracy.

W przypadku pracy w trybie alarmowym definiować można również zależności między wejściami alarmowymi (lub alarmami wywołanymi na skutek wykrycia ruchu), czas prealarmu i czas zapisu alarmowego. Jeśli nastąpiło zdarzenie alarmowe, urządzenie jest w stanie uaktywnić odpowiednie wyjście, wysłać wiadomość e-mail (wraz ze zmniejszoną kopią klatki obrazu) lub przekazać informację o zdarzeniu do Punktu Dystrybucji Zdarzeń (wykorzystującego oprogramowanie EDP). Funkcja ochrony alarmów zabezpiecza przed nadpisaniem ważnego zdarzenia przez najnowszy materiał wizyjny. Przybliżony czas archiwizacji jest obliczany automatycznie dla ustawionych parametrów nagrywania. Jeśli użytkownik chciałby go skrócić, ma możliwość ręcznego wprowadzenia nowych parametrów (tak zwany okres zapisu cyklicznego).

Zapis obrazów odbywa się na montowanych fabrycznie wysokiej jakości wewnętrznych dyskach twardych o pojemności maksymalnej do 2 TB. Rejestrator DV-IP RT posiada również interfejsy eSATA, do których można podłączyć dyski lub macierze dyskowe JBOD o pojemności ponad 10 TB w celu wydłużenia okresu rejestracji. Fabrycznym wyposażeniem jest napęd DVD-R, pozwalający na archiwizację danych, wmontowany w przedni panel, oraz złącze USB, służące do podłączenia myszy, klawiatury lub pamięci flash (służącej także do archiwizacji danych). Sterowanie urządzeniem jest realizowane zdalnie, z wykorzystaniem ręcznego nadajnika zdalnego sterowania, poprzez sterownik na podczerwień, stronę WWW lub oprogramowanie systemu monitoringu NetVu Observer, natomiast dostęp do ustawień można uzyskać poprzez czytelne graficzne menu z hierarchicznie ułożonymi grupami funkcji.

Rejestrator RT posiada dwa interfejsy sieciowe o przepustowości 1 Gb i 100 Mb. Jest to szczególnie ważne przy pracy z kamerami IP, zwłaszcza megapikselowymi – dzięki temu unika się problemów z przepustowością sieci w przypadku dostępu zdalnego.

Tym, co polepsza komfort pracy operatora, jest wyposażenie rejestratora w wyjście HDMi, przydatne zwłaszcza podczas podglądu obrazów z wielu kamer na wspólnym, podzielonym ekranie – wówczas obrazy z każdej z kamer mogą być wyświetlane z pełną rozdzielczością PAL lub megapikselową. Wyjście HDMi służy do sterowania monitora głównego. Oprócz tego urządzenie jest wyposażone w standardowe gniazda BNC, realizujące funkcję wyjść na monitor główny oraz na monitor pomocniczy.

Wyjątkowo funkcjonalnym rejestratorem jest model DV-IP HD. Podobnie jak DV-IP RT, zapisuje on z pełną prędkością i w maksymalnej rozdzielczości, wykorzystuje technologię **MultiMode**, obsługuje kamery IP, w tym kamery megapikselowe. Występuje w wersji ośmiokanałowej. Urządzenie posiada dwa wyjścia HDMi. Jedno z nich może pracować jako wyjście główne, drugie – jako wyjście pomocnicze. W tej sytuacji wyświetlenie kilkunastu obrazów z różnych kamer w pełnej rozdzielczości na jednym monitorze nie stanowi problemu.

Fot. 1. Różnice w położeniu obiektów w przypadku rejestracji z prędkością 6 kl./s

Fot. 2. Różnice w położeniu obiektów w przypadku rejestracji z prędkością 25 kl./s

Dla prostszych systemów zaprojektowano rejestrator DV-IP Express. W odróżnieniu od wyżej opisanych, DV-IP Express umożliwia nagrywanie materiału z pełną prędkością 25 kl./s w rozdzielczości CIF, 12 kl./s w rozdzielczości 2CIF i 6 kl./s w rozdzielczości 4CIF. Posiada on osiem, 12 lub 16 przelotowych wejść wizyjnych.

Jak wszystkie urządzenia z serii DV-IP, wyżej opisane rejestratory cechują się dużą wydajnością i elastycznością w pracy sieciowej. W warunkach zdalnego dostępu za pośrednictwem oprogramowania zarządzającego **NetVu Observer** technologia **TransCoding** pozwala na dopasowanie jakości strumienia danych wysyłanego przez rejestrator w zależności od jakości dostępnego łącza sieciowego. Operator może zdefiniować (do podglądu na żywo lub przy zdalnym odtwarzaniu) trzy tryby jakości obrazu i liczby klatek na sekundę, jak również rodzaj kodeka użytego podczas transmisji danych (MJPEG lub MPEG-4). Dzięki temu w przypadku wystąpienia zdarzenia alarmowego do podglądu można wybrać strumień danych o lepszej jakości (np. kodowany w MJPEG). W typowych przypadkach do transmisji stosuje się kodek MPEG-4, aby nie obciążać łącza.

Oprogramowanie zarządzające **NetVu Observer** umożliwia dostęp do systemu rejestratorów i zarządzanie nim poprzez strukturę typu „drzewo". Dla dowolnej kamery należącej do systemu, do której użytkownik ma przyznane odpowiednie prawa dostępu, możliwe jest uzyskanie podglądu na żywo lub odtworzenie nagranego materiału. Program pozwala wyszukać zdarzenie alarmowe lub informację systemową według daty, nazwy kamery, nazwy zdarzenia systemowego, wykrycia ruchu. Szczególnie przydatna dla systemów monitoringu jest funkcja wtórnej detekcji w już nagranym materiale. Na dowolnym rejestratorze operator może przeprowadzić powtórną detekcję ruchu, rozpoczęcia lub zakończenia aktywności, zgodnie z nowo dobranymi kryteriami detekcji.

Oprogramowanie NetVu Observer umożliwia uzyskanie obrazu z 36 kamer z różnych rejestratorów w trybie podziału ekranu. Dostępne są również mieszane tryby podziału oraz tak zwany „obraz w obrazie" (ang. *Picture in Picture* – PiP). Technologia DuoVu, wykorzystująca PiP, pozwala na jednoczesne odtwarzanie nagrań i podgląd obrazów na żywo. Dla ułatwienia zarządzania systemem kamer program obsługuje mapy synoptyczne (**e-mapy**) – wystarczy kliknąć symbol odpowiedniej kamery na obrazie przedstawiającym wnętrze budynku lub innego obiektu, aby automatycznie uzyskać podgląd z tej kamery. Wykorzystując omawiane oprogramowanie, użytkownik jest w stanie sterować kamerami obrotowymi, ustawiać je w zaprogramowanych pozycjach (presety), a także uaktywniać odpowiednie wyjścia alarmowe. Do obsługi alarmów przychodzących z większej liczby urządzeń służy Centralny Punkt Dystrybucji Zdarzeń. Wybrane fragmenty materiału można zapisać do pliku AVI lub wygenerować z nich raporty w postaci pliku PDF.

Urządzenia wykorzystują technologię **NetVuConsole**, dzięki której za pośrednictwem dowolnego z rejestratorów połączonych siecią TCP/IP mamy możliwość sterowania kamerami podłączonymi do innych urządzeń oraz wyświetlania obrazów generowanych przez te kamery (funkcja rozproszonej cyfrowej krosownicy wizyjnej). Dostępna w rejestratorze funkcja obsługi map synoptycznych pozwala na swobodne poruszanie się po rozległym systemie, bez konieczności instalowania oprogramowania zarządzającego na dodatkowych komputerach.

W systemach monitoringu, w których bezpieczeństwo zależy od przetwarzania i rejestracji znacznych ilości informacji, wymagana jest najwyższa jakość urządzeń i wygoda pracy operatora. Możliwość łączenia urządzeń w większe systemy, zwłaszcza w przypadku wykorzystania technologii IP, jest nieoceniona. Rejestratory serii DV-IP znajdują zastosowanie w zaawansowanych systemach CCTV, spełniając najwyższe wymagania bezpieczeństwa.

Karol Fietkiewicz
SPS Trading

kompleksowe zabezpieczanie obiektów

firma ATLine®

Zapraszamy na targi **SECUREX**
MTP Poznań, 26-29.04.2010

ALFA

Czujka mikrofalowa
z efektem Doppler'a

MURENA

Cyfrowa czujka mikrofalowa
z efektem Doppler'a

PIRAMID

Zewnętrzne czujki dualne
(PIR+MW)

www.atline.pl

ZSJZ

AQAP 2110:2006

SYSTEM ZARZĄDZANIA PCBC Certyfikowany na zgodność z: PN - EN ISO 9001 : 2001

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

17 LAT DOŚWIADCZENIA

Udoskonalenie monitoringu obiektów handlowych

Kamera hemisferyczna

Witold Faber

Absolutnie prawdziwe wydaje się stwierdzenie, że systemy telewizji dozorowej są standardowym wyposażeniem większości obiektów handlowych. Głównym celem ich stosowania jest zapewnienie jak najwyższego bezpieczeństwa prowadzonej działalności handlowej poprzez wykrywanie intruzów, aktów wandalizmu i przemocy, jak również (co jest prawdopodobnie największym problemem) ograniczenie kradzieży. Ponadto kamery pełnią funkcję prewencyjną, co także nie jest bez znaczenia

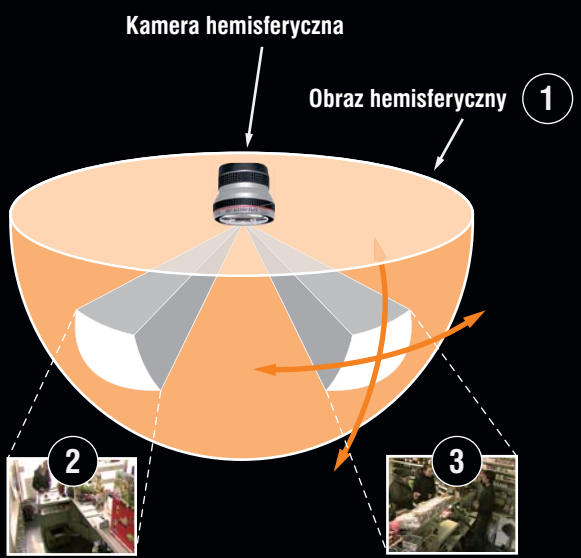
Głównym zadaniem stawianym przed kamerami CCTV jest zapewnienie wyraźnego obrazu o wysokiej rozdzielczości, który zagwarantuje identyfikację osób uczestniczących w zdarzeniu, a także umożliwi rozróżnienie jak największej liczby szczegółów. Jednocześnie w polu widzenia kamer powinien znajdować się jak największy obszar. Z drugiej strony kamery te powinny być dyskretne, czy wręcz niezauważalne, tak aby klienci nie odczuwali żadnego dyskomfortu.

Znakomitym przykładem takiego właśnie rozwiązania jest kamera wykorzystująca technologię obserwacji hemisferycznej, czyli półsferycznej, zapewniającej pełną, dookolną (360°) obserwację określonego obszaru (np. całego niedużego sklepu, określonego stoiska, kasy). Oznacza to możliwość jednoczesnego rejestrowania obrazu całego pomieszczenia lub określonego obszaru oraz szczegółowego obserwowania wybranego fragmentu sceny. Obecnie do osiągnięcia tego celu wystarczy zastosowanie tylko jednej kamery z pojedynczym obiektywem i nie ma konieczności używania np. dedykowanego komputera PC ze specjalizowanym oprogramowaniem.

Jak pracuje kamera hemisferyczna?

Kamera hemisferyczna składa się z obiektywu typu rybie oko i przetwornika obrazu o wysokiej rozdzielczości (3,1 Mpx), jednak najważniejszym elementem składowym kamery jest wbudowane oprogramowanie, które zapewnia korekcję zniekształceń geometrycznych obrazu prezentowanego na żywo i inteligentną rejestrację całej sceny.

Obszar obserwacji kamery hemisferycznej zamontowanej pod sufitem obejmuje całe nieduże pomieszczenie lub wybrane stoisko w promieniu kilku metrów w każdym kierunku. Obraz tworzony bezpośrednio z takiej perspektywy wykazuje największe zniekształcenia w obszarach obwodowych. Dzięki zaimplementowanym w oprogramowaniu kamery algorytmom te obszary obrazu są w sposób płynny, czyli bez widocznych krawędzi ani sztucznych przejść, korygowane z uwzględnieniem właściwego kąta i perspektywy. Dzięki obróbce w kamerze możliwie najbardziej naturalny obraz jest dostępny w dowolnej przeglądarce internetowej (nie jest przekształcany dopiero na komputerze). Co więcej, za pomocą wirtualnej funkcji PTZ możliwe jest płynne



Taka inteligentna kamera ma wbudowane kompletne oprogramowanie zapewniające zarówno przetwarzanie obrazu (w tym m.in. korekcję zniekształceń geometrycznych), jak i wszystkie inne, typowe dla kamer funkcje, takie jak analiza obrazu na potrzeby alarmów i zarządzanie długookresową rejestracją lokalną (wbudowaną w kamerę) lub zdalną (np. z wykorzystaniem popularnych i tanich NAS-ów). Ponadto oprogramowanie to daje możliwość kompleksowego zarządzania zdarzeniami alarmowymi (również sygnałami zewnętrznymi, np. z czujników) z wykorzystaniem programowanej logiki i automatyki oraz pełny, dwukierunkowy tor audio z wbudowanym mikrofonem i głośnikiem.

Zastosowanie takiego unikatowego rozwiązania sprawia, że tylko jedna kamera stanowi cały wizyjny system alarmowy w instalacji samodzielnej (jedna kamera w małym sklepie) albo element systemu rozbudowanego (kilka, kilkadziesiąt kamer w większym obiekcie handlowym).

przeglądanie całego monitorowanego obszaru – analogiczne do przeglądania za pomocą kamery PTZ. Najważniejsze, że cały czas rejestrowany jest cały obszar sklepu czy stoiska. Tym sposobem skupienie się na jednym zdarzeniu podczas podglądu na żywo nie spowoduje pominięcia tego, co dzieje się w innych, nie obserwowanych w danym momencie obszarach – nie można np. odwrócić uwagi w jednym miejscu, aby dokonać kradzieży w innym.

Zamontowawszy kamerę hemisferyczną na ścianie, można monitorować cały widziany obszar – od ściany do ściany. Uzyskuje się wówczas efekt pełnej panoramy 180°. Dzięki temu za pomocą tylko jednej kamery można monitorować np. całą ladę w sklepie lub recepcji. Ponadto można stale obserwować dwa niezależne, newralgiczne miejsca będące w zasięgu kamery (niekoniecznie w zakresie panoramy), np. wejście i stanowisko kasowe.

Dzięki tym cechom kamery hemisferycznej obserwator może w sposób płynny śledzić wybrany obszar lub obiekt, nie tracąc nic z wydarzeń rozgrywających się w innych miejscach dozorowanego obszaru. Dotychczas zapewnienie analogicznej skuteczności wymagało użycia kilku kamer, a obserwacja przemieszczającego się obiektu wiązała się z koniecznością przechodzenia z kamery na kamerę.

Łatwo, tanio i wygodnie – zintegrowane rozwiązanie

Przeniesienie całego oprogramowania realizującego wszystkie funkcje do kamery pozwala na budowanie rozwiązań bez centralnego systemu zarządzającego. Daje to nową jakość i nowe możliwości przy projektowaniu systemów telewizji dozorowej, w szczególności wówczas, gdy są to systemy rozproszone, znajdujące się w nawet kilku odległych lokalizacjach. Używając tych samych kamer, można stworzyć sieci dozorowe różnej wielkości, a także dowolnie rozbudować je w przyszłości. Zarówno systemy nieduże, wykorzystujące jedną lub kilka kamer, odpowiednie np. dla mniejszych sklepów, recepcji, placówek, punktów obsługi klientów itp., jak również większe i bardziej rozbudowane, np. złożone z kilkudziesięciu kamer znajdujących się w różnych miejscach, komunikujących się ze sobą w sytuacjach alarmowych, zawsze gwarantują rejestrację wydarzeń z całego obserwowanego obszaru (bez żadnych martwych stref) i dostarczają użytkownikowi obraz najwyższej jakości.

Bardzo istotne są również cechy eksploatacyjne kamer, do których należą m.in.:

- współpraca ze standardowymi urządzeniami informatycznymi podczas transmisji danych, zasilania (również awaryjnego), jak i archiwizacji obrazów;
- łatwość instalacji kamer – kamery są podłączane zawsze jednym przewodem (wspólne zasilanie i dane), tak jak sieci komputerowe, i bez znaczenia jest to, czy kamera pracuje wewnątrz budynku, czy na zewnątrz – zawsze wystarczy tylko jeden przewód;
- możliwość wykorzystania dwukierunkowego toru audio oraz mikrofonu i głośnika, wbudowanych w kamerę, zarówno do automatycznego odtwarzania przez kamerę własnych komunikatów użytkownika, jak również do transmisji audio na żywo; automatyczne usuwanie efektu echa dodatkowo poprawia jakość dźwięku;
- wygodna i elastyczna eksploatacja systemu telewizji dozorowej w dowolnym miejscu, za pomocą wydajnego, wygodnego w obsłudze i bezpłatnego oprogramowania;
- elastyczność i nieograniczoność archiwum danych (wideo i audio) zarówno pod względem miejsca rejestracji (w standardowych lub dodatkowych zasobach pamięciowych kamery lub w zdalnych zasobach sieciowych), jak i zakresu czasowego oraz ilości przechowywanych danych.

Podsumowanie

Nowoczesne kamery do monitoringu wizyjnego są autonomicznymi i inteligentnymi urządzeniami. Nie wymagają stosowania specjalnych komputerów czy rejestratorów w celu uruchomienia systemu monitoringu, np. jedno- lub kilkukamerowego. Specjalna konstrukcja i ekonomiczne zarządzanie energią pozwalają na całoroczną eksploatację kamer również na zewnątrz, przy standardowym zasilaniu po sieci komputerowej, przez co nie ma potrzeby budowania oddzielonych instalacji zasilających kamery. Ponadto ze względu na to, że kamery dysponują w pełni zintegrowanym oprogramowaniem zarządzającym (rejestracja, transmisja, archiwizacja, alarmy, obsługa), możliwe jest zaoferowanie rozwiązania prostego, szybkiego w instalacji i łatwego w obsłudze, a w konsekwencji także ekonomicznego, które doskonale nadaje się do wykorzystania zarówno w małym sklepie, jak i w centrum handlowym.

Witold Faber
Linc

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

ŻYWIOŁY
POD KONTROLĄ

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

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

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

Zakłócenia elektromagnetyczne

w elektronicznych systemach alarmowych

Waldemar Szulc
Adam Rosiński
Jacek Paś

Wstęp

Dążenie do uzyskiwania coraz korzystniejszych parametrów konstrukcyjnych (niewielki ciężar, małe rozmiary) i użytkowych (niezawodność, określone parametry elektryczne, łatwość eksploatacji) elementów układów i urządzeń, w tym elektronicznych systemów alarmowych, pociąga za sobą konieczność obniżania średniej mocy sygnałów użytecznych i zwiększenia sprawności energetycznej tych obiektów. Konsekwencją jest coraz mniejsza różnica między średnią mocą sygnałów użytecznych oraz zawsze towarzyszącymi im sygnałami niepożądanymi, zwanymi zakłóceniami. Zewnętrzne i wewnętrzne źródła sygnałów niepożądanych nie powinny wpływać zakłócająco na współczesne urządzenia elektroniczne, a więc także elektroniczne systemy alarmowe, ale te urządzenia same nie powinny być źródłami zakłóceń. Ta cecha zgodnego współistnienia obiektów w danym środowisku elektromagnetycznym nazywa się kompatybilnością elektromagnetyczną (ang. *electromagnetic compatibility* – EMC). Zagadnienia kompatybilności elektromagnetycznej dotyczą zarówno emisji elektromagnetycznej urządzeń (ang. *electromagnetic emission*), jak i podatności lub odporności urządzeń na zakłócenia (ang. *electromagnetic susceptibility, electromagnetic immunity*). Z praktycznego punktu widzenia kompatybilne urządzenie elektromagnetyczne to obiekt, który jest zdolny do pracy w określonym środowisku elektromagnetycznym (na ogół bardzo zróżnicowanym i scharakteryzowanym w normach szczegółowych) i nie wprowadza do tego środowiska niedopuszczalnych zakłóceń (o poziomie przekraczającym przyjęte normy). Z powyższych stwierdzeń wynika, że zagadnienie zmniejszenia wpływu sygnałów niepożądanych (zakłóceń) powinno być uwzględnione w procesie projektowania, konstruowania i realizacji elektronicznych systemów alarmowych (każdego typu). Późniejsze zmiany mogą okazać się bardzo trudne, a czasami wręcz niemożliwe.

Należy pamiętać, że źródła zakłóceń są wszechobecne. Występują we wszystkich bez wyjątku środowiskach i obiektach. W sposób najbardziej ogólny, ze względu na źródła powstawania, zakłócenia można podzielić na:

- naturalne (pochodzenia pozaziemskiego i ziemskie),
- spowodowane przez działalność człowieka.

Występuje również głębszy podział – te zjawiska fizyczne, które są pierwotną przyczyną zakłóceń, można podzielić na:

- mechaniczne (np. wibracje, udary, wstrząsy),
- biologiczne, związane z przyrodą,
- elektryczne (szumy własne elementów i układów elektronicznych, sygnały nadajników, sygnały z linii energetycznych, nieodkłócone systemy energetyczne, sygnały z urządzeń oświetleniowych itp.).

Te ostatnie spotykane są najczęściej i mają znaczący wpływ na prawidłową pracę elektronicznych systemów alarmowych. Zakłócenia mogą przenikać do urządzeń i systemów (odbiorników zakłóceń) poprzez:

- sprzężenia konduktancyjne, pojemnościowe i indukcyjne,
- propagacje fal w liniach (w liniach dozorowych, magistralach transmisyjnych),
- promieniowania.

Podstawowe sposoby przeciwdziałania zakłóceniom elektromagnetycznym to:

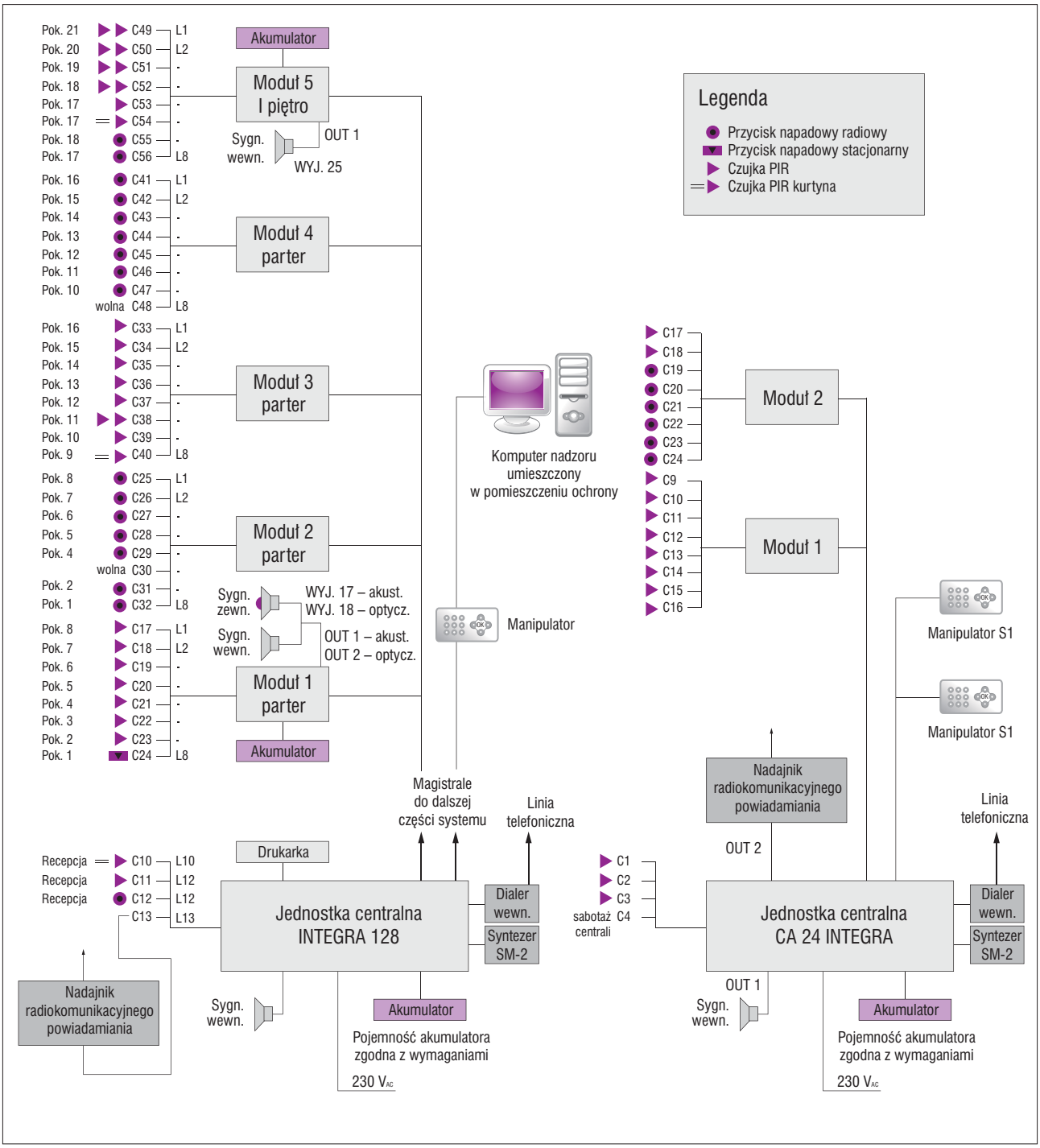
- określenie źródła (lub źródeł) zakłóceń elektromagnetycznych,
- wskazanie elementów, układów, podzespołów podatnych na zakłócenia elektromagnetyczne,
- określenie mechanizmu przenikania zakłóceń elektromagnetycznych (a więc sposobu sprzęgania się źródła zakłóceń z obiektem wrażliwym na zakłócenia).

Można stwierdzić, że istnieją trzy podstawowe metody zmniejszania wpływu zakłóceń, do których zalicza się:

- tłumienie zakłóceń w miejscu ich powstawania (sfera projektowania elektronicznych systemów alarmowych),
- projektowanie i wykonywanie układów elektrycznych i elektronicznych (dotyczy to elektronicznych systemów alarmowych o podwyższonej odporności na zakłócenia elektromagnetyczne),
- utrudnianie przenikania zakłóceń elektromagnetycznych przez kanały sprzężeń (ekranowanie urządzeń elektronicznych i linii dozorowych, prawidłowe łączenie żył masowych kabli, stosowanie pierścieni ferrytowych).

Przykładowy elektroniczny system alarmowy będący przedmiotem analizy zakłóceń elektromagnetycznych

Przedstawiony na rys. 1 schemat blokowy elektronicznego systemu alarmowego jest schematem obiektu rzeczywistego, zaprojektowanego przez autorów w obiekcie specjalnego przeznaczenia; obiekt ten był już przedmiotem analizy niezawodnościowo-eksploatacyjnej, opisywanej na łamach *Zabezpieczeń*. Składa się z ok. 250 punktów charakterystycznych, w tym 152 linii dozorowych. Wcześniejsza analiza dotyczyła jednak problematyki związanej ze wskaźnikiem gotowości K_g, a nie wpływu zakłóceń elektromagnetycznych na pracę systemu alarmowego. Analizowany obecnie system alarmowy składa się z dwóch niezależnych podsystemów połączonych łączem radiokomunikacyjnym (433,92 MHz) na odcinku ok. 300 m. W trakcie analizy wpływu zakłóceń elektromagnetycznych istotna stała się bardzo mała odległość obiektu chronionego elektronicznym systemem alarmowym od stacji kolejowej, a więc trakcji elektrycznej (3 kV) oraz urządzeń SRK (sterowanie ruchem kolejowym). Odległość ta jest ważna z punktu widzenia bezpieczeństwa ruchu pociągów. W bezpośrednim sąsiedztwie chronionego obiektu zlokalizowana jest duża stacja bazowa telefonii komórkowej oraz kilka łączy mikrofalowych. W samym obiekcie znajduje się kilka punktów klimatyzacyjnych, każdy o mocy ponad 25 kW. Podczas analizy zbierano dane dotyczące zakłóceń elektromagnetycznych emitowanych przez kolejowe urządzenia trakcyjne, SRK i radiokomunikacyjne oraz pochodzących bezpośrednio od transportu kolejowego. Również punkty klimatyzacyjne już wcześniej były źródłem dużych zakłóceń (przepięć), które spowodowały uszkodzenie rejestratora cyfrowego wchodzącego w skład monitoringu wizyjnego. Chroniony obiekt jest wyposażony w system ochrony przeciwpożarowej; znajduje się w nim również informatyczna sieć dostępowa, zarówno przewodowa, jak i bezprzewodowa (WLAN). Wszystkie wymienione systemy



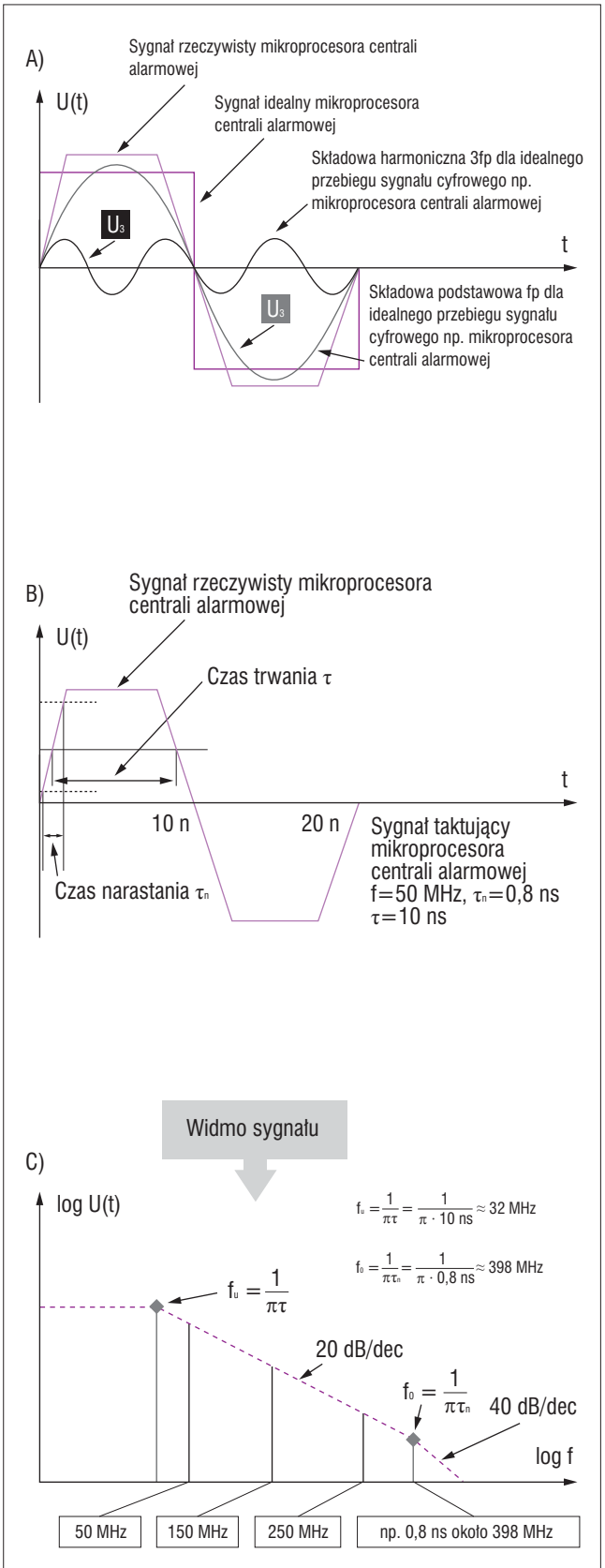
Rys. 1. Schemat blokowy elektronicznego systemu alarmowego zbudowanego na dwóch centralach alarmowych typu INTEGRA 24 i INTEGRA 128

(zarówno wewnętrzne, jak i zewnętrzne) są źródłami emisji zakłóceń elektromagnetycznych, które mogą mieć wpływ na pracę elektronicznych systemów alarmowych.

Do badań widma zakłóceń użyto mierników natężenia pola elektromagnetycznego oraz analizatorów widma. Zebrano dane oraz dokonano obliczeń i analizy, co pozwoliło na określenie poziomu zakłóceń elektromagnetycznych oraz ich wpływu na elektroniczny system alarmowy obiektu.

Kompatybilność elektromagnetyczna w systemach bezpieczeństwa

Każdy sygnał elektryczny (prąd, napięcie, natężenie pola magnetycznego lub elektrycznego) zawiera składową użyteczną i składową pasożytniczą. Składowa użyteczna jest niezbędna do pracy urządzenia (np. kamery, rejestratora, centrali alarmowej, czujki) lub systemu (CCTV, kontroli dostępu, sygnalizacji pożarowej). Sygnały zakłócające towarzyszą pracy ww. urządzeń i systemów. Wynikają one m.in. z przetwarzania sygnałów użytecznych w urządzeniach systemu bezpieczeństwa. Zjawiska, które występują podczas pracy systemu bezpieczeństwa – niepotrzebne do działania danego urządzenia/systemu, lecz jednocześnie nieuniknione przy przetwarzaniu sygnałów – zobrazowano na rys. 2. W wielu przypadkach sygnały, które są użyteczne dla jednych urządzeń czy systemów, dla innych stają się sygnałami zakłócającymi.



Rys. 2. Przetwarzanie sygnałów w mikroprocesorowej centrali alarmowej systemu bezpieczeństwa
a) idealny i rzeczywisty sygnał mikroprocesorowego systemu obróbki sygnału;
b) rzeczywisty sygnał taktujący mikroprocesora centrali alarmowej o parametrach $f = 50$ MHz, $\tau_n = 0{,}8$ ns; $t = 10$ ns;
c) widmo sygnału taktującego o parametrach $f = 50$ MHz, $\tau_n = 0{,}8$ ns; $t = 10$ ns

Wyższa Szkoła Menedżerska w Warszawie
WSM 1995 WYŻSZA SZKOŁA MENEDŻERSKA WARSZAWA
Rekrutacja tel.: (22) 59 00 730

WYDZIAŁ INFORMATYKI STOSOWANEJ
STUDIA PODYPLOMOWE
na kierunku:
Bezpieczeństwo obiektów i informacji

Studia przeznaczone są dla absolwentów szkół wyższych, zainteresowanych nabyciem lub podwyższeniem kwalifikacji w zakresie szeroko rozumianego bezpieczeństwa obiektów i informacji.

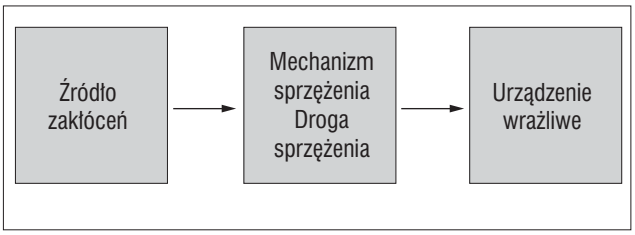
Program studiów obejmuje 240 godzin (dwa semestry) wykładów, ćwiczeń i laboratoriów.

Kontakt:
(22) 59 00 765

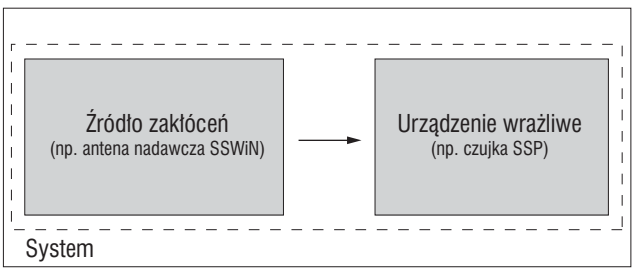
Informacje dodatkowe
- Kampus powierzchni ponad 30 tys. m²
- Ponad 100 sal dydaktycznych
- Kompleks sportowy
- Dom Studenta
- Podziemny parking
- 12.000 studentów
- 22.000 absolwentów

WIARYGODNA SZKOŁA

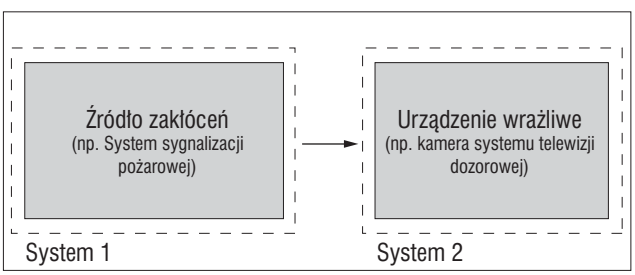
www.wsm.warszawa.pl



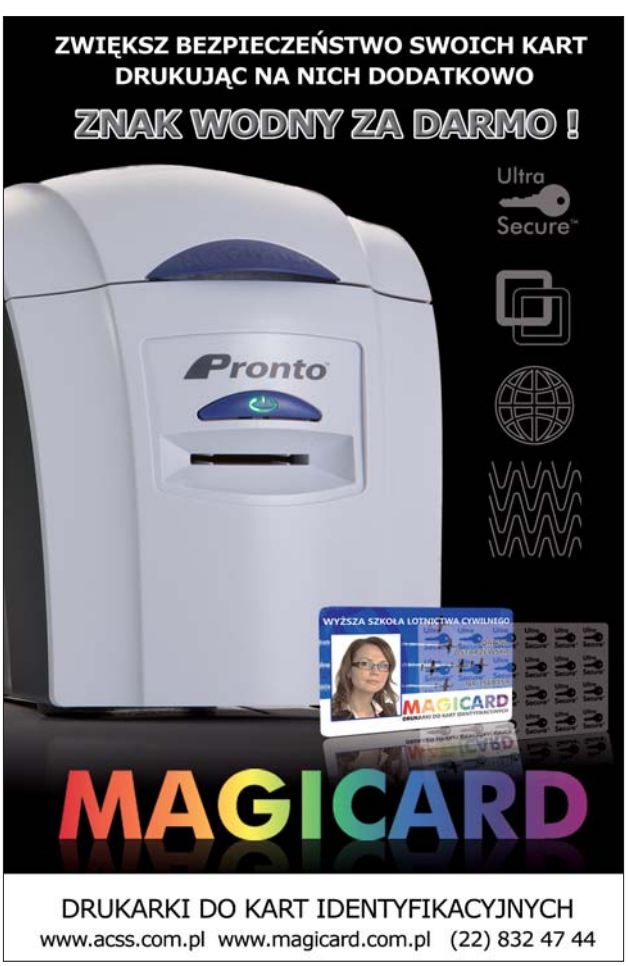
Rys. 3. Mechanizm zakłóceń kompatybilności elektromagnetycznej

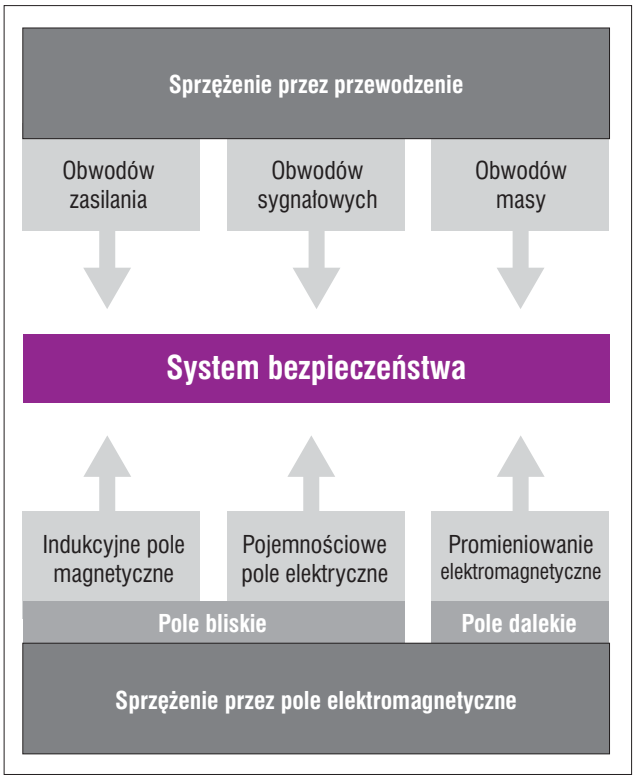


Rys. 4. Oddziaływanie zakłóceń wewnątrz systemu bezpieczeństwa



Rys. 5. Oddziaływanie zakłóceń między systemami bezpieczeństwa





Rys. 6. Mechanizm oddziaływania zaburzeń pola elektromagnetycznego na system bezpieczeństwa

Sygnały zakłócające (zaburzające) mogą spowodować wadliwe działanie urządzenia (obniżenie jakości) lub jego zniszczenie, jeżeli między źródłem zakłoceń a urządzeniem wrażliwym istnieje sprzężenie elektromagnetyczne (rys. 3, 4, 5).

Elektromagnetyczna kompatybilność to:

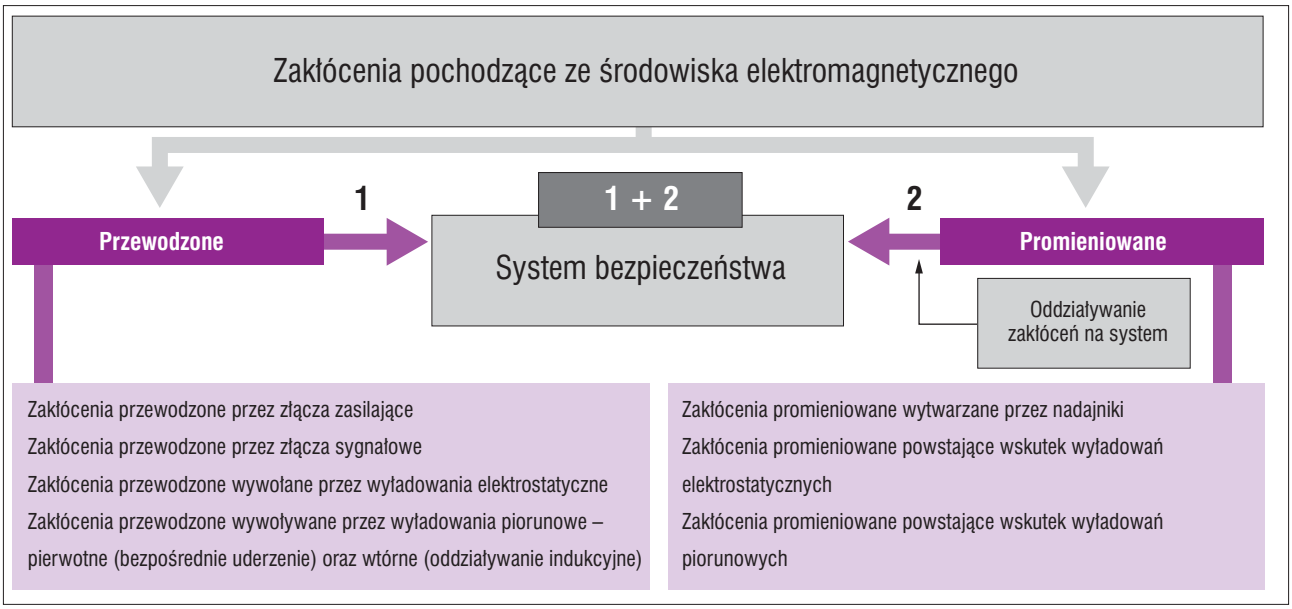
– działanie zgodnie z przeznaczeniem w danym środowisku elektromagnetycznym,
– działanie w sposób nie wywierający niedopuszczalnego wpływu na dane środowisko elektromagnetyczne.

Ze względu na złożoną strukturę pola elektromagnetycznego i różnice jego własności w zależności od odległości od jego źródła – w pobliżu źródła (pole bliskie) i w pewnym oddaleniu od źródła (pole dalekie – odległość zależy od częstotliwości) – sprzężenie przez pole elektromagnetyczne dzielimy na sprzężenie indukcyjnościowe lub pojemnościowe w polu bliskim oraz promieniowanie elektromagnetyczne w polu dalekim (rys. 6, 7).

Według normy międzynarodowej IEC 50(161) dla urządzeń systemu bezpieczeństwa definicja kompatybilności elektromagnetycznej (EMC) jest następująca:

„EMC jest zdolnością urządzenia do jego zadawalającej pracy w środowisku elektromagnetycznym, bez jednoczesnego powodowania zaburzeń elektromagnetycznych, które byłyby niedopuszczalne dla innych urządzeń występujących w tym środowisku". [1]

Dla systemu bezpieczeństwa można wyprowadzić następującą definicję EMC – „Kompatybilność elektromagnetyczna jest to zdolność danego urządzenia (np. kamery) lub systemu (KD) do działania w środowisku elektromagnetycznym w sposób zadawalający i bez wytwarzania zakłóceń nietolerowanych przez wszystko, co się w tym środowisku znajduje – inne systemy (urządzenia) bezpieczeństwa".



Rys. 7. Oddziaływanie zakłóceń przewodzonych i promieniowanych na system bezpieczeństwa

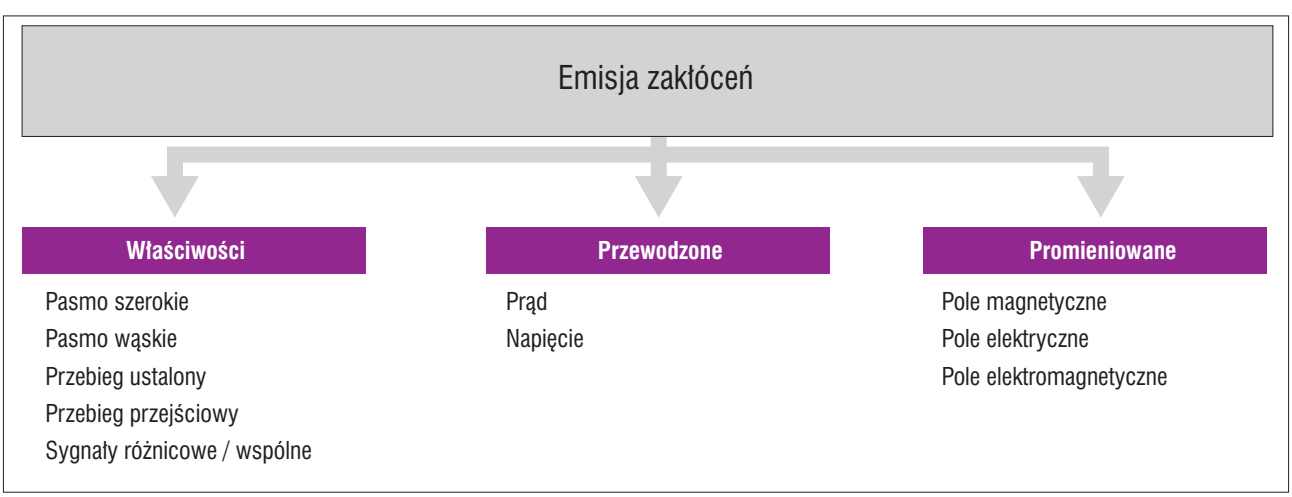
Występujące w definicji pojęcia instalacji, podzespołu lub systemu można zdefiniować następująco:

– **instalacje** – składają się z przestrzennie rozmieszczonych systemów, urządzeń, jednego lub kilku wsporczych elementów konstrukcyjnych oraz przestrzennie usytuowanych połączeń z systemami i urządzeniami traktowanymi jako urządzenia końcowe, eksploatowane we wzajemnym powiązaniu funkcjonalnym;
– **podzespół** – każdy element, który jest przewidziany do wbudowania w urządzenie, nie posiadający jednak samodzielności funkcjonalnej oraz nie przeznaczony do bezpośredniego zastosowania przez użytkownika;
– **system** – według dyrektywy EMC jest to „kilka połączonych wzajemnie, w określonym celu urządzeń, które są wprowadzone do obrotu wyłącznie jako jedna jednostka funkcjonalna”;
– **system** tworzą funkcjonalnie powiązane ze sobą urządzenia, które są eksploatowane z wykorzystaniem konstrukcji wsporczej (otwartej lub zamkniętej) oraz przestrzennie rozłożonych połączeń (przewody elektryczne, pola elektromagnetyczne, połączenia optyczne i mechaniczne). [1]

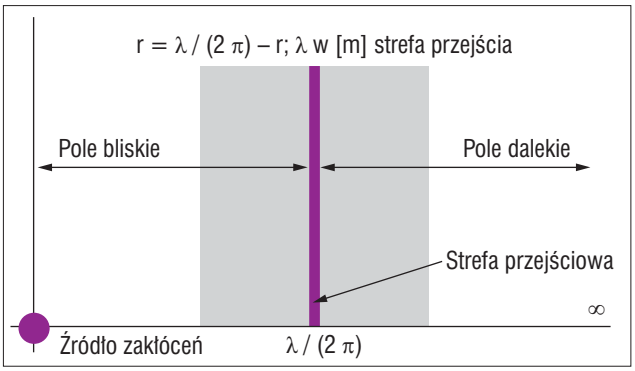
Wewnętrzna kompatybilność systemu jest zachowana wtedy, gdy wszystkie urządzenia i pozostałe elementy składowe systemu – przy uwzględnieniu pewnych zapasów wrażliwości i odporności na zakłócenia – pracują bezbłędnie, mimo pozostawania pod wpływem wytworzonej w systemie energii zakłócającej.

Zewnętrzna kompatybilność systemu występuje wówczas, gdy system jako całość pracuje bezbłędnie pod wpływem wielkości zakłócających go z zewnątrz. Również w tym przypadku mogą być uwzględnione zapasy wrażliwości i odporności na zakłócenia. Ponadto należy uwzględnić wymaganie, aby emisje zaburzające systemu nie oddziaływały w sposób niedopuszczalny na środowisko elektromagnetyczne, tzn. na inne pracujące w tym środowisku systemy. [2, 3]

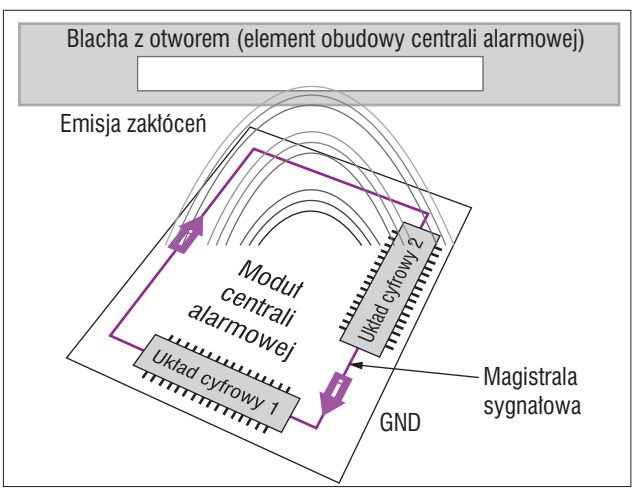
Jeżeli odległość między źródłem pola elektromagnetycznego i urządzeniem (systemem bezpieczeństwa czy też jego obwodem wrażliwym) staje się duża, posługujemy się parametrami pola. Jeżeli odległość pomiędzy przewodami jest większa niż 0,1 λ (długość fali), pole elektromagnetyczne jest emitowane na zewnątrz. Zjawisko to jest wykorzystywane w bezprzewodowej transmisji informacji.



Rys. 8. Właściwości i emisja zakłóceń przewodzonych i promieniowanych



Rys. 9. Pola bliskie i dalekie



Rys. 10. Emisja zakłóceń przez moduł centrali alarmowej systemu bezpieczeństwa

Warunki propagacji pola zależą od:
– zakresu częstotliwości,
– charakterystyki promieniowania anteny nadawczej,
– tłumienia przez przeszkody (przewodzące, nieprzewodzące, struktury geometryczne).

Pole bliskie

Jeżeli pole magnetyczne nie zależy bezpośrednio od pola elektrycznego, to mówimy o polu bliskim. Zjawisko to występuje zawsze w pobliżu przewodów elektrycznych. W polu bliskim bierze się pod uwagę albo pole elektryczne, albo magnetyczne, w zależności od tego, który składnik jest ważniejszy. Warunek pola bliskiego dotyczy obszaru od powierzchni przewodu aż do odległości równej $\lambda/(2\pi)$.

Dla częstotliwości f = 50 Hz to pole bliskie wystepuje do odległości D = 955,4 km.

Pole dalekie

W dużej odległości od układu przewodów (linii lub anteny) wielkość i faza pola elektrycznego zależą od odpowiednich wielkości pola magnetycznego. Oba składniki są związane zależnością:

$$\frac{\overline{E}}{\overline{H}} = Z_f \qquad (1)$$

gdzie:
E – wektor pola elektrycznego,
H – wektor pola magnetycznego,
Z_f – impedancja falowa środowiska.

Wartość Z_f zależy tylko od właściwości elektrycznych i magnetycznych środowiska, w którym rozchodzi się pole elektromagnetyczne. W ogólnym przypadku

$$Z_f = \sqrt{\frac{\mu_0}{\varepsilon_0}} \cdot \sqrt{\frac{\mu_r}{\varepsilon_r}} \qquad (2)$$

gdzie:
ε_0, μ_0 – stałe fizyczne równe, odpowiednio, przenikalności dielektrycznej i magnetycznej próżni,
ε_r, μ_r – stałe fizyczne równe, odpowiednio, względnej przenikalności dielektrycznej i magnetycznej środowiska.

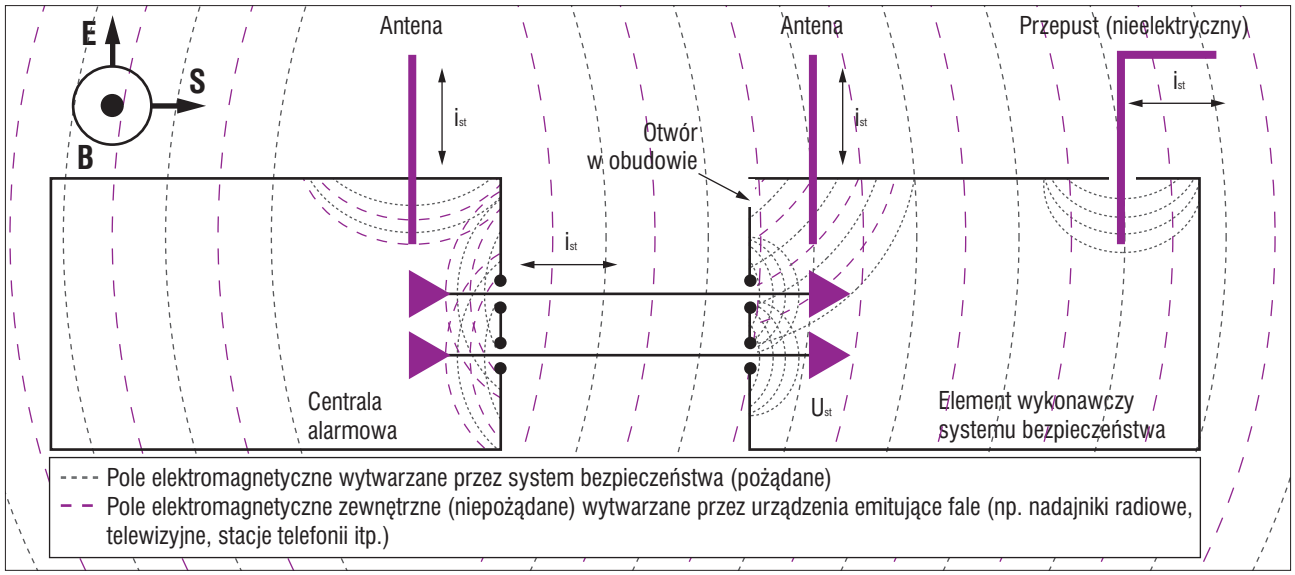
$$Z_f = \sqrt{\frac{\mu_0}{\varepsilon_0}} = 377\ [\Omega] \qquad (3)$$

określa się mianem impedancji falowej próżni.

Ponieważ względna przenikalność dielektryczna ε_r i względna przenikalność magnetyczna μ_r powietrza są w przybliżeniu równe 1, impedancja falowa powietrza jest równa 377[Ω].

Jeżeli fala elektromagnetyczna napotyka strukturę przewodzącą, wówczas indukuje w niej napięcia i prądy. Niepożądanymi antenami są np. przewody łączące (elektryczne), ekrany linii, konstrukcje metalowe , przewody gazowe lub wodociągowe, części obudowy (rys. 11).

Istotny związek z rozprzestrzenianiem się zaburzeń elektromagnetycznych ma otoczenie systemów bezpieczeństwa – izolacyjne lub przewodzące (rys. 12). Otoczenie systemu jest elementem ekranującym sygnały zakłóceń rozchodzące się w wolnej przestrzeni.



Rys. 11. Pożądane i niepożądane pole elektromagnetyczne wytwarzane przez system bezpieczeństwa

Sprzężenie pojemnościowe występujące w systemach bezpieczeństwa

Na drodze indukcji elektrycznej pole elektryczne przewodu zakłócającego wywołuje napięcie na przewodach obwodu zakłócanego. Współczynnik sprzężenia pojemnościowego można przedstawić za pomocą pojemności sprzęgającej (rys. 13):

$$C = \frac{\pi \cdot \varepsilon \cdot l}{2} \cdot \frac{\ln\left[\frac{d_{14} \cdot d_{23}}{d_{13} \cdot d_{24}}\right]}{\ln\frac{d_{12}}{r} \cdot \ln\frac{d_{34}}{r}} \qquad (4)$$

gdzie:

r – promień przewodu,

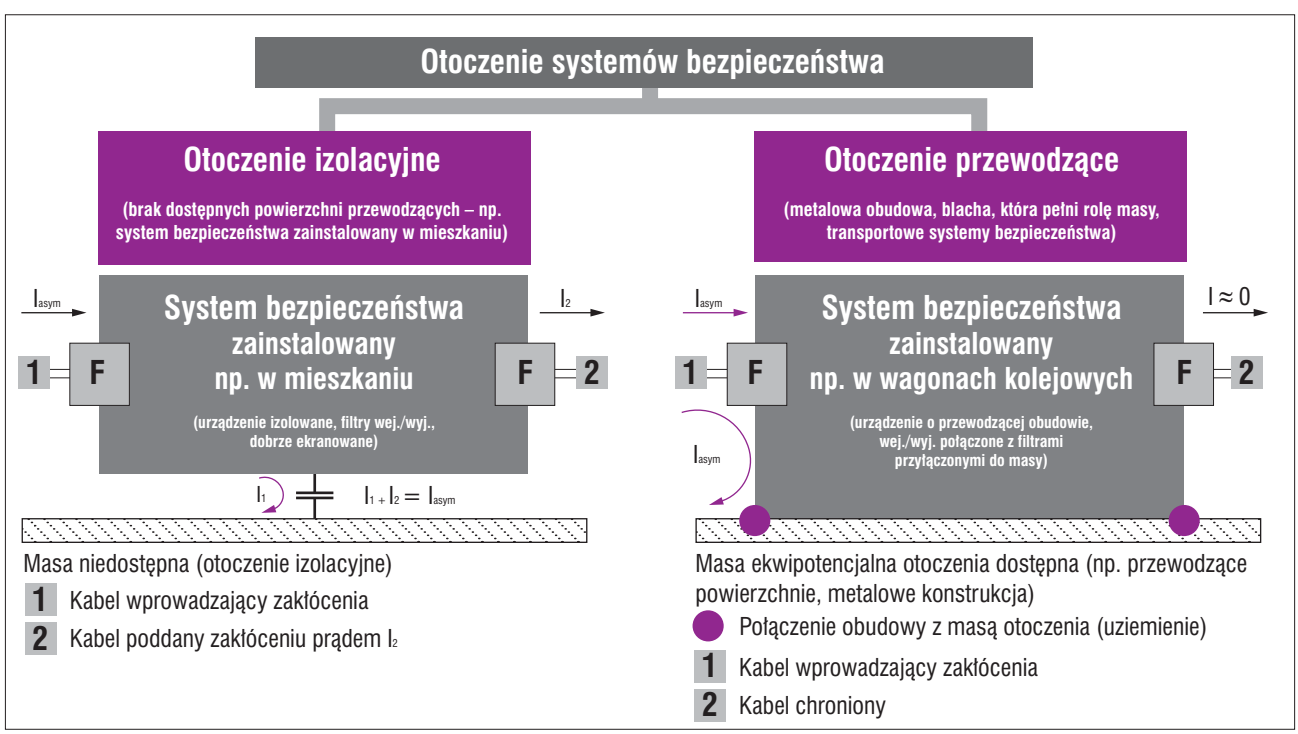
ε – przenikalność dielektryczna (przenikalność dielektryczna próżni ε_0 pomnożona przez odpowiednią dla zastosowanego materiału izolacyjnego przenikalność względną). Wykorzystując symetrię pracy obwodu, można uzyskać schemat zastępczy jak na rys 13.

Sprzężenie przez przewodzenie występujące w systemach bezpieczeństwa

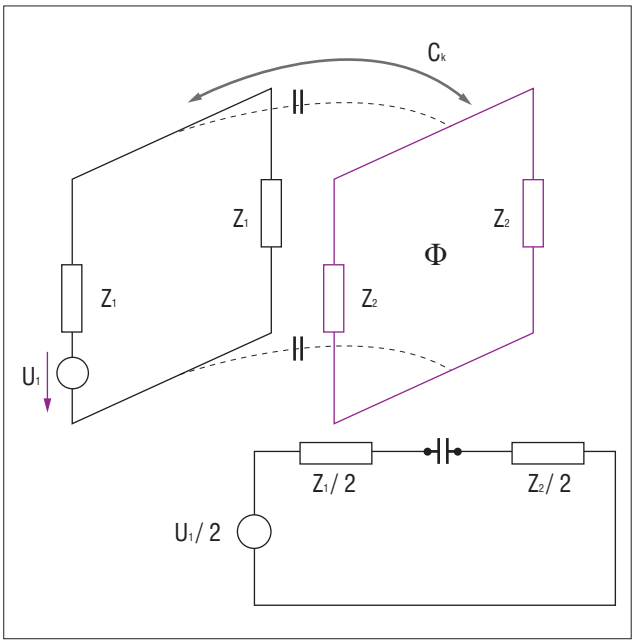
W przypadku, w którym dwa lub więcej obwodów elektrycznych wykorzystuje ten sam przewód powrotny, należy liczyć się z wystąpieniem sprzężenia przez przewodzenie.

Przewód powrotny ma określoną impedancję Z_k nazywaną impedancją sprzeżenia zwrotnego. Prąd I_1 płynący w obwodzie 1 (zakłócającym) wywołuje w przewodzie powrotnym spadek napięcia (rys. 14).

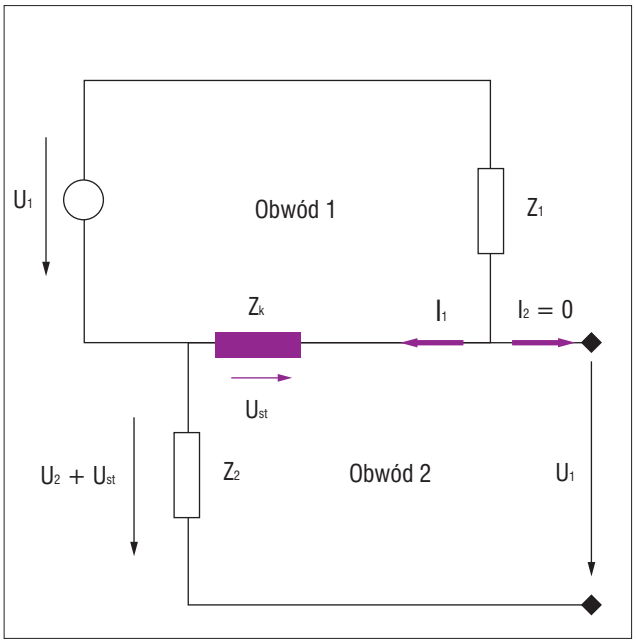
Spadek napięcia U_{st} nakłada się na napięcie sieci (np. sygnał przenoszony w obwodzie 2). W przypadku, w którym obwód 2 (np. tor transmisji danych) jest otwarty (lub obciążony rezystorem o dużej wartości), a do obwodu dołączono źródło U_2, napięcie wyjściowe będzie równe $U_{st}+U_2$.



Rys. 12. Otoczenie systemów bezpieczeństwa



Rys. 13. Sprzężenie pojemnościowe występujące w systemach bezpieczeństwa



Rys. 14. Sprzężenie przez przewodzenie występujące w systemach bezpieczeństwa

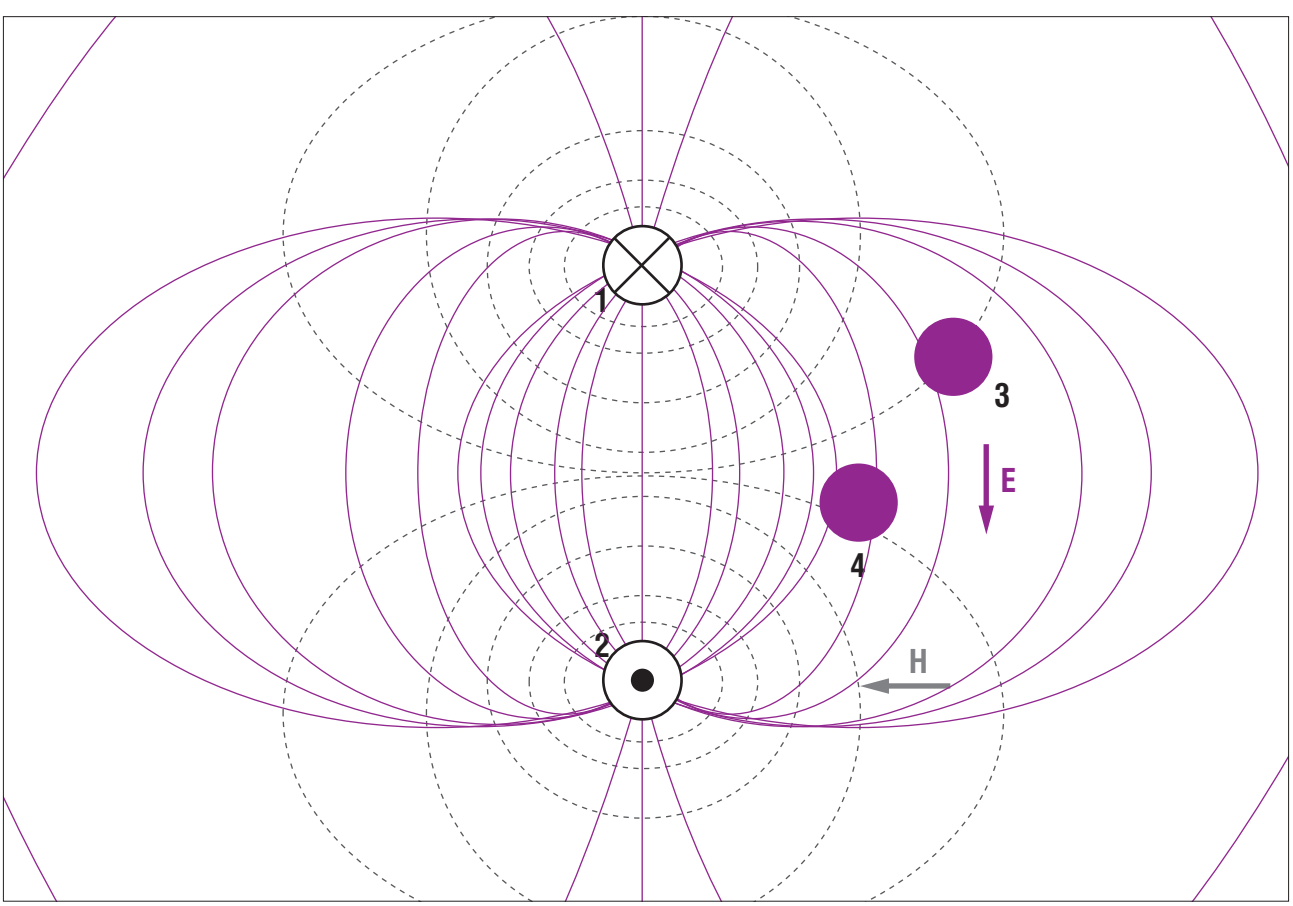
Opis zakłócenia jako stosunek sygnał/szum – U_2/ U_{st}:

$$\frac{S}{N}\ [\mathrm{dB}] = 20\log \frac{U_2}{U_{st}} \qquad (5)$$

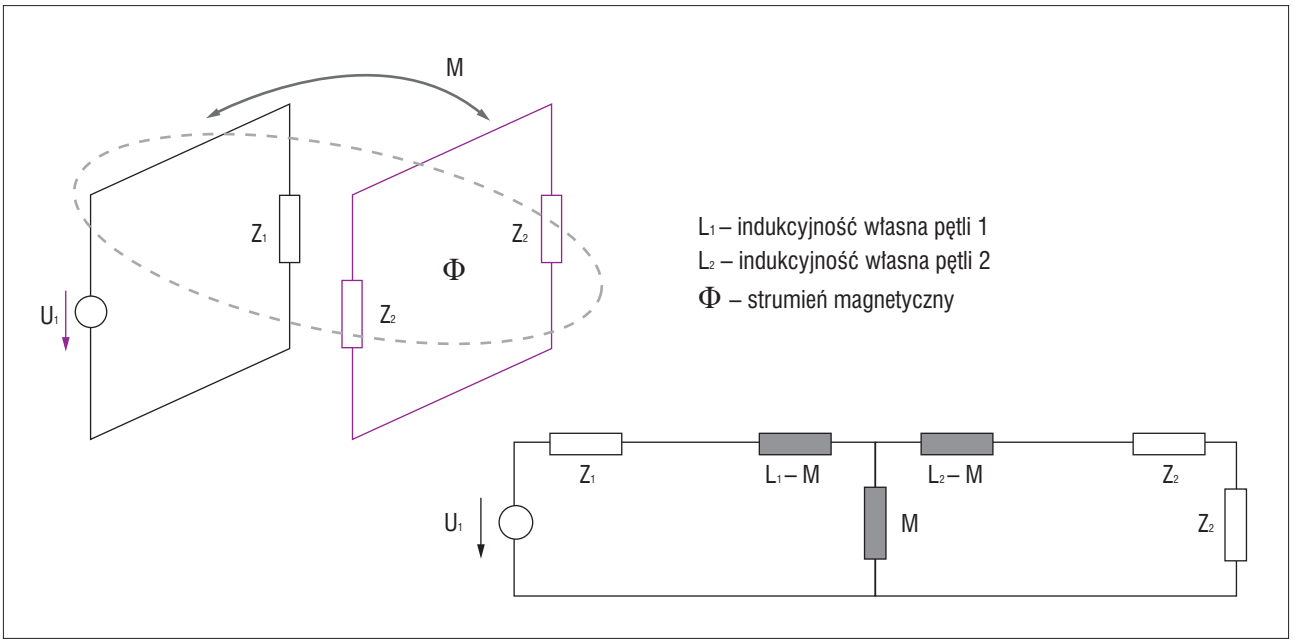
Środki zaradcze:

1) Odcinek przewodu mający wpływ na Z_k powinien być tak krótki, jak to tylko jest możliwe.
2) Wzrost przekroju przewodu obniża rezystancję dla prądu stałego. Przy wyższych częstotliwościach – przewód płaski, mała indukcyjność, duża w porównaniu z polem przekroju, korzystniejsza ze względu na zjawisko naskórkowości powierzchnia przewodu.

Przy niskich częstotliwościach pełna separacja potencjałów (sprzężenie transformatorowe, optoelektroniczne) redukuje do minimum sprzężenie przez przewodzenie, jednak przy wyższych częstotliwościach sprzężenia tego nie można pominąć.



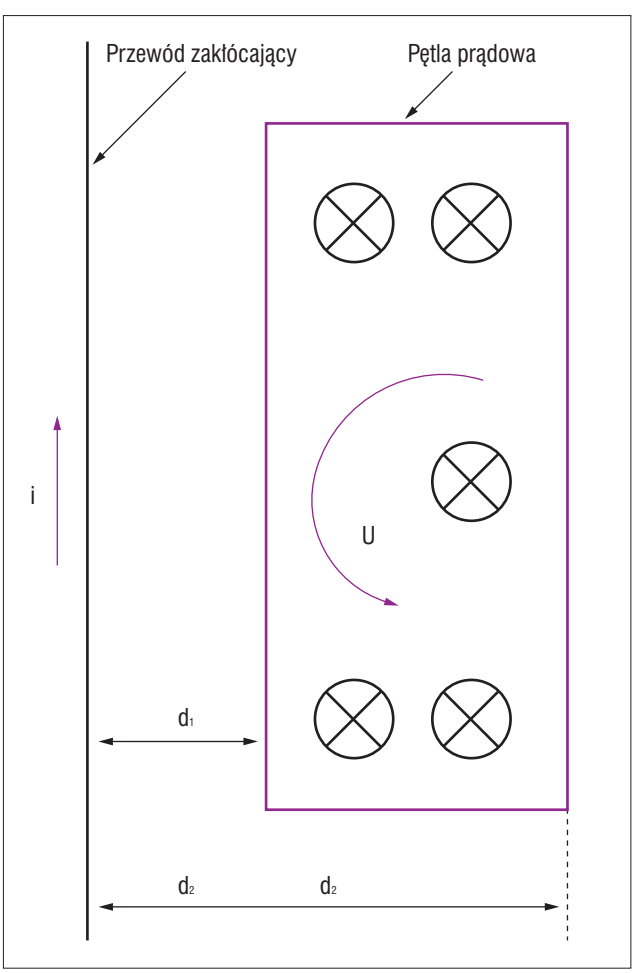
Rys. 15. Pole elektromagnetyczne linii dwuprzewodowej (przewody 1 i 2) i jego wpływ na sąsiednią, nieobciążoną linię (przewody 3 i 4)



Rys. 16. Sprzężenie indukcyjne – wytworzony przez linię zakłócającą (przewody 1 i 2) strumień magnetyczny przenika częściowo przez pętlę składającą się z przewodów 3 i 4

Sprzężenie indukcyjne występujące w systemach bezpieczeństwa

Ten rodzaj sprzężenia występuje szczególnie pomiędzy sąsiadującymi przewodami (rys.15).



Rys. 17. Przewód linii sygnałowej systemu bezpieczeństwa umieszczony w pobliżu toru zakłócanego

Wytworzony przez linię zakłócającą (przewody 1 i 2) strumień magnetyczny przenika częściowo przez pętlę składającą się z przewodów 3 i 4. Zmiana części strumienia magnetycznego przenikającego linię zakłócającą w czasie powoduje indukowanie się napięcia zakłócającego. Napięcie to jest tym większe, im większa jest zmiana strumienia magnetycznego w czasie (czyli częstotliwość sygnałów).

Wielkość tego napięcia zależy również od wzajemnej odległości przewodów linii sygnałowej (3 i 4) i zakłócającej (1 i 2).

Dla stacjonarnych, sinusoidalnie zmiennych (o częstotliwości f) przebiegów można obliczyć napięcie U_i indukowane w zakłócanej pętli:

$$U_i = 2\pi \cdot f \cdot M \cdot I_1 \qquad (6)$$

Dla przykładu z rys. 16 można obliczyć indukcyjność wzajemną:

$$M = \frac{\mu_0 \cdot l}{2\pi} \cdot \ln\left[\frac{d_{14} \cdot d_{23}}{d_{13} \cdot d_{24}}\right] \qquad (7)$$

gdzie:

d_{14}, d_{23}, d_{13}, d_{24} – odległości przewodów,

l – długość przewodu.

Jeżeli przewody 1 i 2 linii zakłócającej są zbliżone do siebie, odległości pomiędzy poszczególnymi żyłami linii zakłócającej i sygnałowej stają się sobie równe, przez co indukcyjność wzajemna dąży do zera, tzn. znika sprzężenie indukcyjne.

Jeżeli przewód znajduje się w pobliżu toru zakłócanego (rys. 16), indukcyjność wzajemna M, wyrażana w [μH], jest obliczana następująco:

$$M = 0{,}2 \cdot l \cdot \ln\frac{d_1}{d_2} \qquad (8)$$

W tym przypadku nie ma znaczenia, czy przewód zakłócający leży w tej samej płaszczyźnie co pętla zakłócana, czy nie.

O wartości napięcia indukowanego decyduje zmiana strumienia magnetycznego, który przenika pętlę obwodu, w czasie. Jeżeli linie sił pola magnetycznego przenikają pętlę pod kątem różnym od prostego, to strumień magnetyczny i napięcie indukowane U_s zmniejszają się:

$$U_s = -M\frac{di}{dt} \tag{9}$$

Jeżeli przenikające pętlę prądową pole magnetyczne jest jednorodne (np. przewody zakłócające znajdują się w dużej odległości lub pętla obwodu jest bardzo mała w porównaniu z odległością od źródła zakłóceń), wtedy:

$$U_s = \mu \cdot A \cdot \frac{dH}{dt} \tag{10}$$

A – powierzchnia pętli przenikanej przez pole magnetyczne

Zmniejszenie indukcyjności wzajemnej dwóch obwodów elektrycznych:

– zmniejszenie odległości między przewodem dosyłowym i powrotnym linii (w przypadku linii dwuprzewodowych),
– ułożenie przewodów bezpośrednio nad powierzchnią przewodzącą szczególnie w przypadku niesymetrycznych linii jednoprzewodowych),
– zwiększenie odległości między torem zakłócającym a zakłócanym,
– unikanie równoległego prowadzenia przewodów,
– używanie krótkich, skręconych przewodów (przewody zakłócające muszą mieć inny skok skrętu niż przewody zakłócane),
– zastosowanie ekranu magnetycznego (materiały żelazoniklowe lub ferryty w przypadku wyższych częstotliwości).

Zakończenie i wnioski

Badania autorów dotyczące kompatybilności elektromagnetycznej elektronicznych systemów alarmowych stanowią duże wyzwanie, zważywszy na to, że w wielu przypadkach zakłócenia są zupełnie przypadkowe, a więc ich źródła są bardzo trudne do zlokalizowania. Związane z tymi badaniami pomiary są bardzo żmudne i wymagają sporej wiedzy i doświadczenia. Autorzy zajmowali się problematyką niezawodnościowo-eksploatacyjną już znacznie wcześniej. Wówczas okres badań (zależnie od systemu) wynosił od 12 do 24 miesięcy. Badanie zakłóceń elektromagnetycznych w elektronicznych systemach alarmowych jest bardzo trudne, bo wyniki są zwykle przypadkowe, a w wielu przypadkach zaskakujące. Ze względu na świadome zlokalizowanie badań w pobliżu stacji kolejowej oraz przewodów trakcyjnych pomiary należało wykonywać o różnych porach roku (także w zimie – ze względu na możliwość występowania szadzi, a więc znacznego iskrzenia pomiędzy pantografem jednostki trakcyjnej a jezdnym przewodem trakcyjnym). Pomiary trwały ponad dwa lata. Ponadto potrzebny był czas na analizę zebranych danych oraz wykonanie szeregu wykresów załączonych w niniejszym artykule. Prawie wszystkie dane i wyniki podlegały bardzo wnikliwej analizie. Autorzy świadomie wybrali obiekt z dosyć dużym i rozległym elektronicznym systemem alarmowym, położony w rejonie dużych zakłóceń pochodzących między innymi z zakłóceń trakcyjnych i zakłóceń SRK. Badanie nieco innego elektronicznego systemu alarmowego (również dosyć dużego) wykonywano w okolicach stacji PKP Radom. Podane w części analitycznej niniejszego opracowania wyniki są efektem tylko małej części badań, jakie autorzy od dłuższego czasu prowadzą na terenie Polski. Badania te dotyczą zarówno problematyki niezawodnościowo-eksploatacyjnej, jak i zakłóceń elekromagnetycznych. W wielu przypadkach problematyka badań jest zbieżna i pozwala opracować dosyć skuteczne metody ochrony elektronicznych systemów alarmowych przed skutkami różnych zakłóceń, które najczęściej wywołują fałszywe alarmy, a w przypadkach skrajnych – bardzo poważne awarie systemów alarmowych.

Bibliografia:

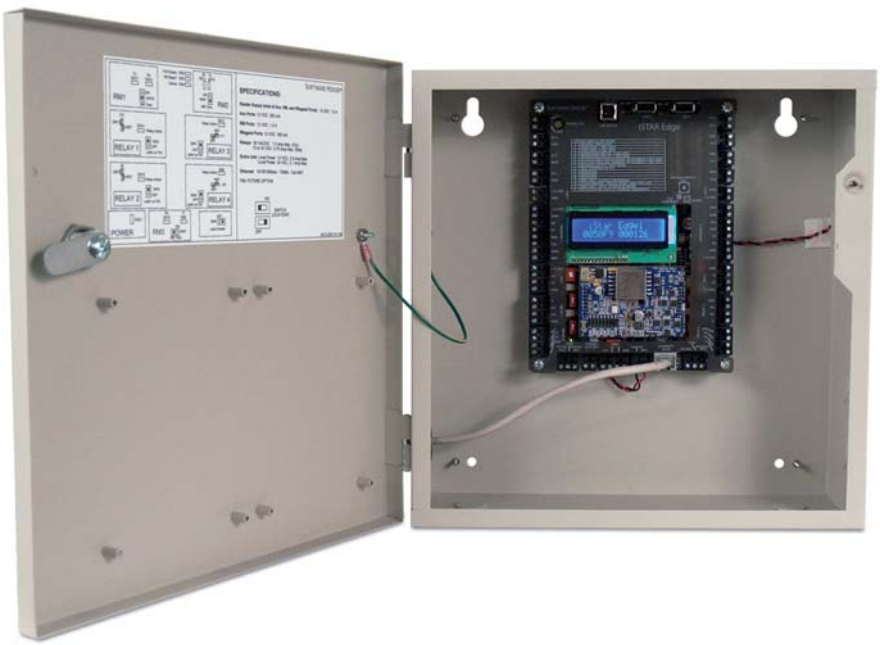
1. Koszmider A., *Praktyczny poradnik. Certyfikat CE w zakresie kompatybilności elektromagnetycznej*, Alfa-Weka, Warszawa 1997.
2. Paś J., *Wpływ rozrzutu właściwości elementów linii dozorowej na niezawodność funkcjonalną systemów bezpieczeństwa*, Biuletyn WAT nr 2 (650), Warszawa 2008.
3. Brejwo W., Paś J., *Charakterystyka wybranych źródeł promieniowania elektromagnetycznego z zakresu wielkich częstotliwości*, XV Międzynarodowa Konferencja Naukowo-Techniczna „Inżynieria środowiska w eksploatacji kompleksów wojskowych" Zakopane 2002.
4. Dyduch J., Paś J., *Zakłócenia elektromagnetyczne oddziaływujące na transportowy system bezpieczeństwa*, w: *PAR* nr 5/2009.
5. Paś J., rozprawa doktorska, Politechnika Radomska, Wydział Transportu i Elektrotechniki, Radom 2009/2010.
6. Z. Karkowski (red.), *Zakłócenia w aparaturze elektronicznej*, Warszawa 1995.

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

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

mgr inż. Jacek Paś
WAT
Wydział Elektroniki

Kontroler IP iSTAR Edge obsługujący 2 czytniki



iSTAR Edge jest niezawodnym urządzeniem IP obsługującym 2 czytniki, dostarczającym jednocześnie zestaw funkcji, w skład których wchodzą zaawansowane opcje łączenia w klastry, komunikacja peer-to-peer, strefy włamań i polecenia z klawiatury, zaawansowane funkcje monitorowania drzwi i globalny anty-passback. Opcjonalny moduł zasilający Power over Ethernet (PoE) jest w stanie zasilić urządzenia kontroli dostępu w obrębie 2 drzwi i pozwala wykorzystać istniejącą infrastrukturę sieciową, aby zredukować całkowity koszt instalacji systemu.

iSTAR Edge zwiększa ogólną niezawodność i funkcjonalność systemu poprzez umiejscowienie podejmowania decyzji w lokalnej bazie danych, znajdującej się w każdym kontrolerze, obsługę rekordów 400 000 użytkowników, buforowanie lokalnych alarmów i zdarzeń w przypadku, gdy nie jest możliwa komunikacja z komputerem - hostem. iSTAR Edge komunikuje się z oprogramowaniem C•CURE 800 v.10.0, C•CURE 9000 i innymi kontrolerami Software House, zapewniając realizację funkcji stawianych i wykorzystanych przez najbardziej wymagających użytkowników. Nie ma różnicy, czy system zainstalowany jest w głównej siedzibie firmy, gdzie zatrudnionych jest tysiące pracowników, czy też w lokalnych biurach z kilkoma pracownikami. iSTAR Edge zapewnia w każdym miejscu realizację tych samych procedur i zasad bezpieczeństwa.

iSTAR Edge dostarcza rozwiązania stosowvane w systemach bezpieczeństwa nie mające sobie równych w tej branży. Ze względu na swoją wszechstronność i bezpieczeństwo kontrolery iSTAR Edge mogą być używane razem z kontrolerami iSTAR Pro i iSTAR eX stanowiąc doskonałe rozwiązanie korporacyjne.

iSTAR Edge został zaprojektowany, aby radykalnie zmniejszyć koszt instalacji i uruchomienia systemu. Wbudowana funkcja zarządzania zasilaniem, eliminuje potrzebę stosowania dodatkowego zasilacza i zabezpieczeń stosowanych w tradycyjnych instalacjach. Podłączenie przy pomocy wymiennych złącz, wbudowanego wyświetlacza i diod LED wskazujących aktualny stan kontrolera iSTAR Edge, w znacznym stopniu ułatwia instalacje w najtrudniejszych warunkach. Ponadto, zdalna diagnostyka systemu poprzez przeglądarkę internetową, umożliwia zidentyfikowanie i rozwiązanie problemów związanych z wydajnością systemu.

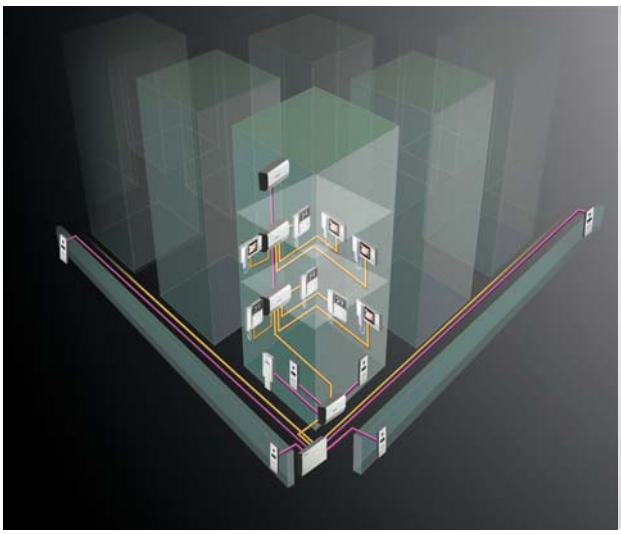
Obudowa iSTAR Edge daje możliwość instalacji dodatkowych modułów I/O i jest zabezpieczona czujnikiem otwarcia w przypadku nieautoryzowanej próby ingerencji w urządzenie. Zagrożenia bezpieczeństwa zostały znacząco zredukowane poprzez szyfrowaną komunikację, zabezpieczenie przed niepożądanym atakiem na system komputerowy czy usługi sieciowe, tworząc kontroler iSTAR Edge urządzeniem o najwyższym poziomie bezpieczeństwa – idealnym rozwiązaniem nawet dla najbardziej sceptycznych managerów IT.

KATON
ACCESS CONTROL & SECURITY SYSTEMS

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

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

System wieloabonentowy serii 2400

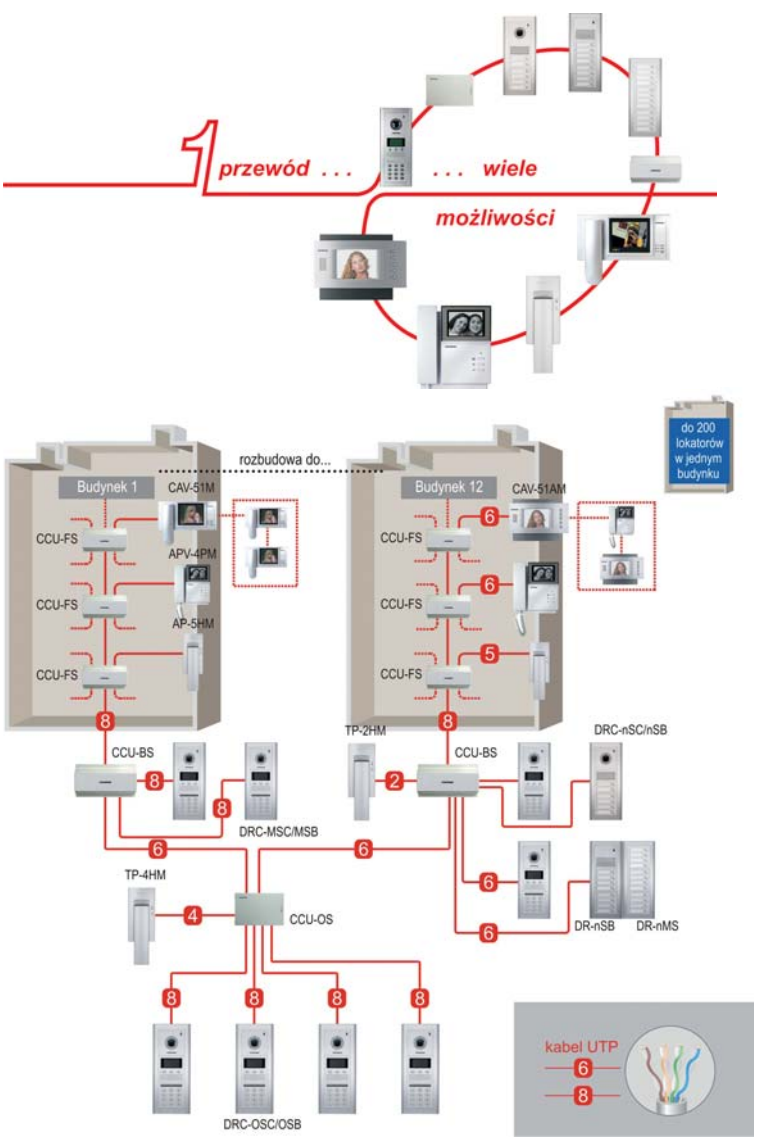


System wieloabonentowy serii 2400 przeznaczony jest do instalacji zarówno w prostych, jak i w bardzo rozbudowanych aplikacjach - maksymalna liczba obsługiwanych przez system abonentów wynosi 2400. U każdego lokatora może być zainstalowane do 3 urządzeń (jedno urządzenie typu Master i dwa urządzenia typu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

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

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

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



GDE POLSKA
Global Distributor of Electronics

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

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

Systemy kolorowe jednoabonentowe

CVD-35H

CVD-50P

CVD-35N

CVD-70AD

Analogowe systemy wideodomofonowe COMMAX znajdują zastosowanie w domach jednorodzinnych, których mieszkańcy cenią sobie wygodę obsługi, jakość komunikacji, indywidualne wzornictwo oraz niezawodność systemu. Klient szukający dla swojej posesji odpowiedniego systemu wideodomofonowego może wybierać pomiędzy kilkunastoma modelami monitorów wewnętrznych oraz paneli zewnętrznych o zróżnicowanym wyglądzie i możliwościach. System wideodomofonowy może być rozbudowywany o dodatkowe panele zewnętrzne (w zależności od zastosowanego modelu monitora), dodatkowe monitory lub unifony (spełniające funkcję domofonu). Ze względu na przyjęte standardy komunikacyjne do systemu wideodomofonowego COMMAX klient ma możliwość podłączenia zewnętrznych kamer CCTV, obserwujących posesję z ukrycia lub z innej perspektywy niż obiektyw kamery w panelu zewnętrznym. Odpowiedni wybór paneli wejściowych pozwala na ukrycie obiektywu w panelu (kamery typu PIN-HOLE) lub regulację kąta obiektywu (w przypadku montażu w warunkach innych niż standardowe).

Dane kolorowych systemów jednoabonentowych

- Monitory LCD o przekątnych 3,5" – 7"
- Zasilanie monitorów 230V lub 17V (w zależności od zastosowanych modeli)
- Kamery typu PIN-HOLE lub z regulacją kąta widzenia
- Montaż paneli zewnętrznych w sposób natynkowy lub podtynkowy
- Sterownie otwieraniem furtki, bramy, załączaniem oświetlenia, itp.
- Prosta instalacja
- Możliwość rozbudowy systemów

DRC-4CG

DRC-4CP

DRC-4CH

DRC-4CAN

GDE POLSKA
Global Distributor of Electronics

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

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

Inteligentny tester akumulatorów GOLD-IBT

GOLD-IBT

inteligentny tester akumulatorów

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

Jak zmierzyć jego pojemność?

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

Automatycznie wyświetla temperaturę otoczenia, napięcie akumulatora i aktualną pojemność.

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

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

alarmnet®

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

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

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

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

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

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

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

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

Cechy

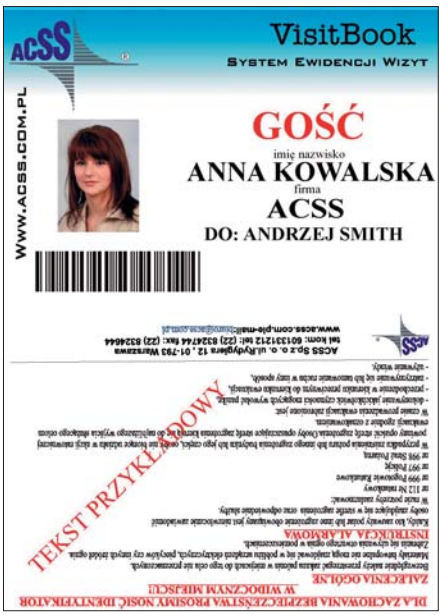
- Podwójny algorytm kompresji:
  - Zapis i odtwarzanie JPEG2000
  - Transmisja przez Internet H.264
- Wysoka jakość zapisanego materiału
- Tryb pracy – Duplex / Triplex
- Złącze USB do archiwizacji danych
- Sterowanie PTZ
- Wygodne wyszukiwanie i przeglądanie materiału
- Łącze USB do aktualizacji oprogramowania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

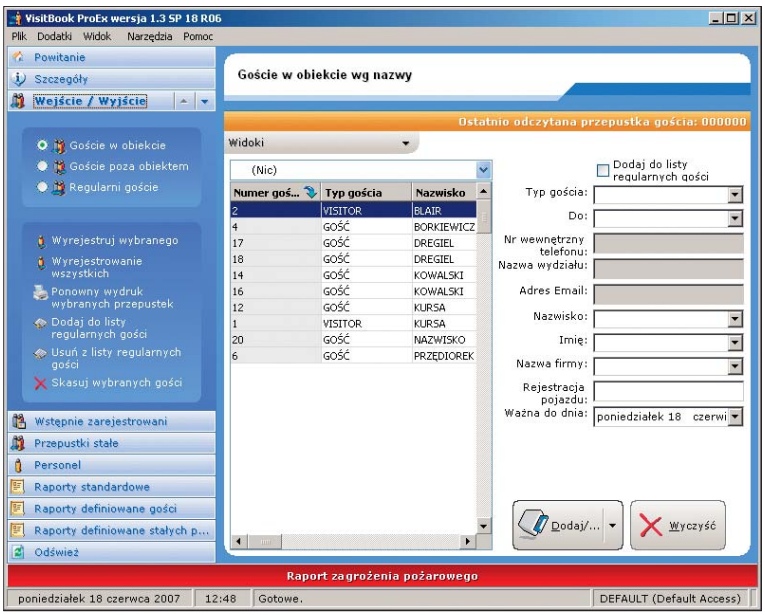
alarmnet®

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

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

System rejestracji gości VisitBook





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

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

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

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

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

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

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

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

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 samodzielnie wykonasz 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ALPOL Sp. z o.o.
ul. Ks. F. Ścigały 10
40-208 Katowice
tel. (32) 790 76 56
Infolinia 0 801 77 77 90
faks (32) 790 76 61
e-mail: alpol@e-alpol.com.pl
www.e-alpol.com.pl

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Biura handlowe:
ul. Mieszczańska 18/1, 30-313 **Kraków**
tel. (12) 260 1 395
faks (12) 260 1 396

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

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

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

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

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

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.com.pl
handel@atline.com.pl
www.atline.com.pl

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

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

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

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

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

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

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

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

Centrum Monitorowania Alarmów
ul. Puławska 359
02-801 Warszawa
tel. (22) 546 0 888
faks (22) 546 0 619
e-mail: warszawa@cma.com.pl
www.cma.com.pl

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

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

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

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

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

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

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

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

DYSKRET Sp. z o.o.
ul. Mazowiecka 131
30-023 Kraków
tel. (12) 423 31 00
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 29
faks (22) 812 62 12
e-mail: office@ebs.pl, m.pioterczak@ebs.pl
www.ebs.pl

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

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

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

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

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

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

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

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

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

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

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

GDE POLSKA
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

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

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

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

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

ICS Polska
ul. Żuławskiego 4/6
02-641 Warszawa
tel. (22) 646 11 38
faks (22) 849 94 83
e-mail: biuro@ics.pl
www.ics.pl

INSAP Sp. z o.o.
ul. Ładna 4-6
31-444 Kraków
tel. (12) 411 49 79, 411 57 47
faks (12) 411 94 74
e-mail: insap@insap.pl
www.insap.pl

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

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

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

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

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

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

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

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

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

MICRONIX Sp. z o.o.
ul. Spółdzielcza 10
58-500 Jelenia Góra
tel. (75) 755 78 78, 642 45 35
faks (75) 642 45 25
e-mail: info@micronix.pl
www.micronix.pl

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

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

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

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

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

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

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

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

POINTEL Sp. z o.o.
ul. Fordońska 199
85-739 Bydgoszcz
tel. (52) 371 81 16
faks (52) 342 35 83
e-mail: biuro@pointel.pl
www.pointel.pl

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

POLON-ALFA
Zakład Urządzeń Dozymetrycznych Sp. z o.o.
ul. Glinki 155
85-861 Bydgoszcz
tel. (52) 363 92 61
faks (52) 363 92 64
e-mail: polonalfa@polon-alfa.com.pl
www.polon-alfa.pl

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

TAP Systemy Alarmowe Sp. z o.o.
Os. Armii Krajowej 125
61-381 Poznań
tel. (61) 876 70 88
faks (61) 875 03 03
e-mail: tap@tap.com.pl
www.tap.com.pl

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

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

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

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

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

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

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

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

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

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

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

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

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
GV Polska	–	–	TAK	–	TAK
HSA	–	–	TAK	–	–
ICS Polska	–	–	TAK	–	TAK
Insap	–	TAK	TAK	TAK	TAK
ISM EuroCenter	–	–	TAK	–	–
Janex International	–	–	TAK	–	–
KABE	–	TAK	TAK	TAK	TAK
KATON	–	–	TAK	–	TAK
Kolektor	–	TAK	–	TAK	–
Kolektor MR	–	TAK	TAK	TAK	–
Laskomex	TAK	TAK	TAK	–	TAK
Legrand Polska	TAK	TAK	TAK	–	TAK
MAXBAT	TAK	TAK	TAK	TAK	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	TAK	TAK	–	–
NAPCO	–	–	TAK	TAK	TAK
Nuuxe – Radioton	–	–	TAK	–	–
OBIS	–	TAK	–	TAK	–
OMC INDUSTRIAL	–	–	TAK	–	–
Petrosin	–	TAK	–	TAK	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	–	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	TAK	–	–
Ramar	TAK	–	TAK	TAK	TAK
ROPAM Elektronik	TAK	–	TAK	–	–
Satel	TAK	–	–	–	–
SATIE	TAK	–	TAK	–	TAK
Sawel	–	TAK	TAK	TAK	TAK
Schrack Seconet Polska	TAK	–	–	–	TAK
Secural	TAK	TAK	TAK	–	TAK
S.M.A.	–	TAK	–	TAK	–
Schneider Electric Buildings Polska	TAK	TAK	TAK	TAK	TAK
Sony	TAK	–	–	–	–
Sprint	–	TAK	TAK	TAK	–
S.P.S. Trading	TAK	–	TAK	–	TAK
STRATUS	–	TAK	TAK	–	TAK
SYSTEM 7	TAK	–	TAK	–	–
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Tayama	–	–	TAK	–	–
Technokabel	TAK	–	–	–	–
TP TELTECH	–	TAK	TAK	TAK	–
W2	TAK	TAK	TAK	–	–
Vision Polska	–	TAK	TAK	–	TAK

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

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
GV Polska	–	TAK	TAK	–	–	–	TAK	–	–
HSA	TAK	TAK	TAK	–	–	–	–	–	–
ICS Polska	TAK	TAK	TAK	–	–	–	–	–	–
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
ISM EuroCenter	–	TAK	TAK	–	–	TAK	TAK	–	–
Janex International	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
KATON	–	TAK	TAK	–	–	TAK	–	–	–
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Laskomex	–	TAK	TAK	–	–	–	–	TAK	–
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MAXBAT	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	TAK	–	–	–	TAK	–
NAPCO	TAK	TAK	TAK	TAK	–	–	–	–	–
Nuuxe – Radioton	–	TAK	–	–	–	TAK	–	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	–	–	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	–	–	–	–	TAK	–
Petrosin	TAK	TAK	TAK	–	–	–	–	–	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	–	–	–	–	–	–	–	TAK	–
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	–	–	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	–	TAK	–	TAK	–	–
ROPAM Elektronik	TAK	–	TAK	TAK	–	–	TAK	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
SATIE	–	–	TAK	–	–	–	–	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.M.A.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Schneider Electric Buildings Polska	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
Sony	–	TAK	–	–	–	–	TAK	–	–
Sprint	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
SYSTEM 7	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	TAK	–	TAK	–	–	–	–	–	–
Tayama	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Technokabel	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
TP TELTECH	TAK	TAK	TAK	TAK	TAK	–	TAK	–	–
W2	TAK	–	–	TAK	–	–	–	–	–
Vision Polska	–	–	–	TAK	–	–	–	–	–

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

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 zagraniczna
Rafał Niedzielski

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

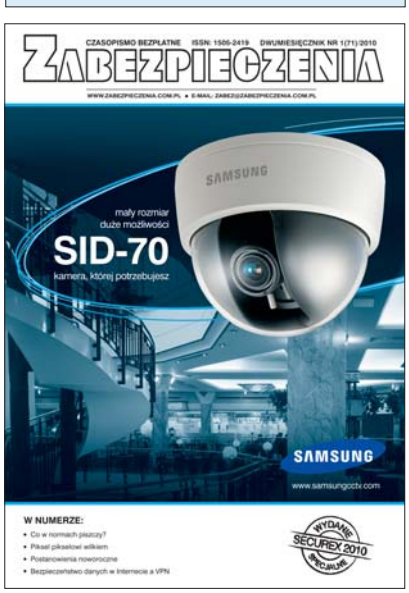
Skład i łamanie
Marek Bladoszewski

Korekta
Paweł Karczmarzyk

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

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

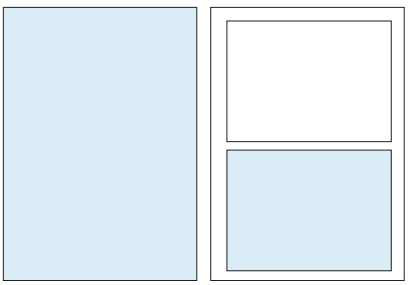
Druk
Regis Sp. z o.o.
ul. Napoleona 4, 05-230 Kobyłka



Cennik reklam

Reklama wewnątrz czasopisma:

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



cała strona (200 x 282 mm + 3mm spad)

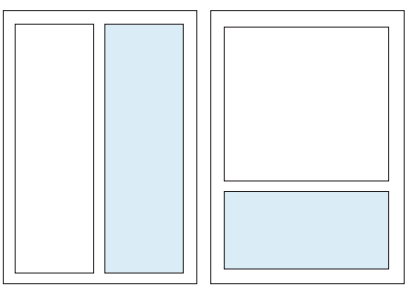
1/2 strony (170 x 125 mm)

Artykuł sponsorowany:

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

Reklama na okładkach:

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

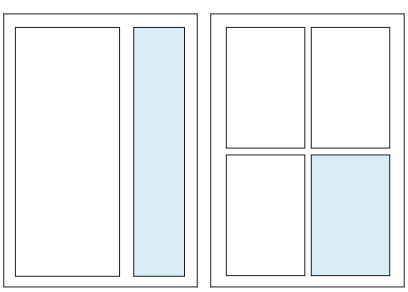


1/2 strony (83 x 260 mm)

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 minimum 6 kolejnych emisji

W przypadku zamówienia na 12 emisji 10% rabat

Podane ceny nie uwzględniają podatku VAT (22%)

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

Spis reklam

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

Międzynarodowe Targi Poznańskie

spotkaj przyszłość

securex
POLAND

Międzynarodowa Wystawa Zabezpieczeń

26 - 29. 04. 2010, Poznań

SECUREX - BĄDŹ O KROK PRZED ZAGROŻENIEM

www.securex.pl

CO WARTO ZOBACZYĆ!

- Mistrzostwa Polski Instalatorów Systemów Alarmowych
- Finał XIII edycji konkursu Polski Mistrz Techniki Alarmowej 2010
- Konferencje:
  - „Bezpieczeństwo w miejscach publicznych i w miejscu zamieszkania - obszar działań Rządowego Programu Razem Bezpieczniej"
  - „Wymagania i wytyczne stosowania nowych polskich norm w praktyce projektowania i budowy systemów alarmowych"
  - „Bezpieczeństwo instytucji finansowych"
  - „I Konferencja Zarządzania Bezpieczeństwem w Obiektach"

ZAPRASZAMY OD PONIEDZIAŁKU DO CZWARTKU!

Tańsze bilety po rejestracji internetowej lub na miejscu.

Nowość! Bilety on-line.

Sprawdź na www.mtp24.pl

Potrzebuję

bezproblemowych rozwiązań dostępu, które oszczędzają pieniądze i zwiększają produktywność.

HID Global dostarcza bezpieczeństwo

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

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

HID

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