CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 1(59)/2008

ZABEZPIECZENIA

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

W NUMERZE:

Międzynarodowe Targi Poznańskie

securex 2008 POLAND

Targi z rekomendacją Polskiej Izby Przemysłu Targowego

Największa Międzynarodowa Wystawa Zabezpieczeń

22-25.04.2008 Poznań

SECUREX
bo nie wszyscy są Fair…

Zapraszamy na największe targi branży zabezpieczeń w Polsce!

BEZPIECZEŃSTWO — OCHRONA — MONITORING

Już teraz zarejestruj się on-line **www.securex.mtp.pl**

Międzynarodowe Targi Poznańskie sp. z o.o.
ul. Głogowska 14, 60-734 Poznań, e-mail: securex@mtp.pl
Tel. 061 869 25 75, 061 869 22 02, Fax 061 869 29 99

CZASOPISMO ZABEZPIECZENIA 1/2008

24 Wprowadzenie do zagadnienia bezpieczeństwa oprogramowania i monitorowania IT

28 Polskie antyterrorystyczne roboty mobilne

34 *iProtect* – sieciowy system zabezpieczenia obiektów

46 Nowości w ofercie JVC Professional

Prezes Polalarmu w składzie Rady Normalizacyjnej

Na podstawie uzyskanych z PKN (**Polskiego Komitetu Normalizacyjnego**) informacji zawiadamiamy Państwa, że w składzie Rady Normalizacyjnej II Kadencji (**2007–2011**), w grupie Przedstawicieli Ogólnopolskich Organizacji Zawodowych i Naukowo-Technicznych, znalazł się m.in. **Bogdan Tatarowski**, prezes Ogólnopolskiego Stowarzyszenia Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „**Polalarm**", który będzie reprezentował przede wszystkim interesy całej branży technicznej ochrony osób i mienia.

Teresa Karczmarzyk
Źródło: PKN

securex 2008 POLAND

Pierwsze starcie instalatorów systemów alarmowych

Międzynarodowe Targi Poznańskie (*MTP*) i Polska Izba Systemów Alarmowych (*PISA*) przygotowują ciekawie zapowiadające się przedsięwzięcie konkursowe, sprawdzające wiedzę i umiejętności instalatorów systemów alarmowych.

MTP i PISA podpisały niedawno **porozumienie** w sprawie wspólnej organizacji, w trakcie najbliższej edycji Międzynarodowej Wystawy Zabezpieczeń „Securex 2008", **I Mistrzostw Polski Instalatorów Systemów Alarmowych**.

Strony porozumienia uznały zgodnie, że mistrzostwa będą ważnym elementem promocji wystawy Securex i branży zabezpieczeń technicznych, popularyzacji sposobów, technik i urządzeń służących podnoszeniu poziomu bezpieczeństwa osób i mienia oraz doskonałą okazją do prezentacji doświadczeń i umiejętności w zakresie technik instalatorskich.

Trwają obecnie prace i dokonywane są uzgodnienia w sprawie określenia jak najbogatszej merytorycznie i jak najatrakcyjniejszej pod względem medialnym formuły rywalizacji.

Znane są już pierwsze efekty pracy Zespołu Organizacyjnego Mistrzostw, działającego w składzie: Georgis Bogdanis – komisarz Mistrzostw, Włodzimierz Cieślak – przewodniczący Komisji Konkursowej, Henryk Dąbrowski – przewodniczący Zespołu, Maksymilian Majerski, Jakub Mamla, Włodzimierz Matlak – członek Komisji Konkursowej, Janusz Olesiewicz, Stefan J. Siudalski – członek Komisji Konkursowej, Andrzej Tomczak, Bartosz Zeidler – dyrektor Projektu MTP.

Projekt Regulaminu Mistrzostw zakłada, że będą to mistrzostwa drużynowe. Zespoły instalatorów, w składach dwuosobowych, będą reprezentować przedsiębiorców, przy czym każdy przedsiębiorca lub podmiot gospodarczy będzie miał prawo zgłoszenia dowolnej liczby zespołów. Uczestnicy muszą legitymować się licencją pracownika zabezpieczenia technicznego.

Mistrzostwa przeprowadzone zostaną **najprawdopodobniej w dniu 23 kwietnia 2008 r**., w drugim dniu trwania wystawy Securex.

Eliminacje będą miały formę testów pisemnych, sprawdzających wiedzę wymaganą przy wykonywaniu usług instalowania, konserwacji i serwisowania urządzeń systemów alarmowych.

Jedynym kryterium oceny będzie liczba punktów uzyskanych za udzielenie poprawnych odpowiedzi w przewidzianym czasie. Każdy zestaw testowy ma zawierać pytania o różnym stopniu trudności i różnej liczby punktów do uzyskania.

W **finale mistrzostw** uczestniczyć będzie maksymalnie **sześć zespołów**, które uzyskały w eliminacjach najlepsze wyniki.

Finaliści będą wykonywać, wykorzystując urządzenia systemów alarmowych i oprzyrządowanie techniczne, zadania i czynności występujące w praktyce instalatorskiej.

Kryteriami oceny będą:
- czas wykonania zadania konkursowego,
- prawidłowość wykonania zadania,
- osiągnięcie efektu zadaniowego,
- estetyka wykonania zadania – jako kryterium pomocnicze.

Organizatorzy zakładają wstępnie, że uczestnicy eliminacji otrzymają, na dwa tygodnie przed mistrzostwami, informację o zakresie tematycznym zadań testowych oraz rodzajach i nazwach urządzeń systemów alarmowych przewidzianych do pracy podczas konkurencji finałowych.

Mistrzostwa Polski Instalatorów Systemów Alarmowych, jako przedsięwzięcie dedykowane całej branży zabezpieczeń technicznych, mają szansę stać się kolejnym istotnym elementem integracji środowisk ją reprezentujących.

MTP i PISA zwrócą się do wszystkich organizacji branżowych, czasopism branżowych i portali internetowych, a także bezpośrednio do dystrybutorów urządzeń systemów alarmowych i firm świadczących usługi projektowania i instalowania systemów alarmowych, z ofertą współpracy i jak najszerszego udziału w tym pionierskim dla historii Securexu przedsięwzięciu.

Bezpośr. inf. PISA

Na początku 2008 roku mija dziesięć lat obecności czasopisma ***Zabezpieczenia*** na rynku wydawniczym branży *security*.

W postaci drukowanej nasz magazyn dociera do tysięcy odbiorców w całym kraju. Objętość czasopisma wzrosła od 12 stron w numerze 1/1998 i 32 stron w numerze następnym do około 100 stron i więcej obecnie (rekordowy numer 6/2004 miał 136 stron). Od roku zasięg naszego oddziaływania jest w istotny sposób większy – praktycznie globalny – dzięki możliwości bezpłatnego uzyskania kompletnych numerów *Zabezpieczeń* przez każdego zainteresowanego, także spoza branży ochrony osób i mienia, wprost z witryny internetowej. W Internecie oprócz tekstów publikujemy również m.in. galerie zdjęć z konferencji, seminariów, targów, wystaw i innych imprez, w których braliśmy udział, np. jako zaproszeni goście albo w charakterze patrona medialnego. Wśród cyklicznych imprez branżowych niewątpliwie największymi, w których regularnie uczestniczymy, są międzynarodowa wystawa zabezpieczeń Securex w Poznaniu oraz Targi Alarm w Kielcach.

Z wieloma firmami współpracujemy od pierwszych miesięcy obecności *Zabezpieczeń* na rynku wydawnictw specjalistycznych (np. Polon-Alfa, Kabe, Schrack-Seconet). Niektóre firmy uległy zmianom organizacyjnym lub połączyły się z innymi, ale nadal, choć pod innym szyldem, utrzymują kontakt z naszym czasopismem. Są i takie, które rozpoczęły swoją działalność później niż *Zabezpieczenia* i nadal ją prowadzą, równolegle ze współpracą z nami, co obu stronom przynosi wyłącznie korzyści.

Współpraca z naszymi partnerami jest wielopłaszczyznowa. To nie tylko dostarczanie przez nich materiałów reklamowych i tekstów artykułów, ale także bieżące kontakty osobiste oraz udział w wydarzeniach dla nich ważnych, a i dla nas nieobojętnych. Wszystkim współpracującym z nami autorom oraz firmom chcielibyśmy, przy okazji jubileuszu, gorąco podziękować, licząc na owocną kontynuację wspólnych przedsięwzięć.

Pisząc o autorach nie sposób pominąć tych, którzy są członkami zespołu redakcyjnego nieprzerwanie od dziesięciu lat i systematycznie zamieszczają swoje artykuły, a także służą radą i pomocą podczas prac nad innymi tekstami. To koledzy: Ryszard Sobierski, Norbert Góra i Daniel Kamiński. Jeszcze tylko dwie osoby działają w *Zabezpieczeniach* równie długo: pierwszy redaktor naczelny, z czasów, gdy *Zabezpieczenia* były kwartalnikiem, czyli Adam Wojcinowicz (obecnie w zespole redakcyjnym), oraz Teresa Karczmarzyk – przez pierwsze pięć lat członek zespołu redakcyjnego, a od kolejnych pięciu lat redaktor naczelny. Jest to czwarta osoba na tym stanowisku w historii *Zabezpieczeń* i najdłużej je piastująca. W wersji drukowanej *Zabezpieczeń* i na naszej witrynie internetowej można łatwo znaleźć teksty redakcyjne oraz zdjęcia jej autorstwa.

Zakres tematyczny materiałów publikowanych w poszczególnych działach stale się powiększa, zgodnie z postępem dokonującym się w dziedzinie technologii i pojawiającymi się nowymi potrzebami oraz możliwościami. Telewizja dozorowa, nazywana telewizją przemysłową w czasach, gdy rozpoczynaliśmy naszą aktywność, to dziś już nie tylko tradycyjnie rozumiane systemy CCTV, działające w zamkniętych obwodach, ale coraz częściej rozległe systemy wykorzystujące sieciową transmisję IP. Ochrona przeciwpożarowa to obecnie także dźwiękowe systemy ostrzegawcze, dziś powszechne, a jeszcze kilka lat temu dopiero raczkujące w naszym kraju. Dział, który zajmował się początkowo wyłącznie tematyką monitorowania alarmów pochodzących z obiektów stałych, obejmuje ostatnio także monitoring środowiskowy i przemysłowy oraz zagadnienia związane z monitorowaniem obiektów ruchomych, między innymi za pomocą satelitarnych systemów wykorzystujących technologię GPS do określania lokalizacji pojazdów. W stosunkowo młodym dziale poświęconym ochronie informacji czytelnik znajdzie nie tylko rozważania teoretyczne i opisy norm lub standardów, ale również źródło praktycznej wiedzy na temat sposobów zabezpieczania informacji podczas jej transmisji czy przechowywania w postaci elektronicznej. To w tym dziale czytelnicy mieli okazję zapoznać się także z mało rozpowszechnioną, a ciekawą i mogącą dotyczyć pośrednio każdego, kto podróżuje drogą powietrzną, tematyką bezpieczeństwa w kontroli ruchu lotniczego.

W ciągu ostatniej dekady zmieniali się pracownicy, współpracownicy i zespół redakcyjny, reklamodawcy, nazwy działów, zawartość czasopisma, a także adres redakcji. Od połowy 2002 roku format *Zabezpieczeń* jest nieco mniejszy (a przez to bardziej poręczny), uległa też zmianom szata graficzna (większość czytelników z nostalgią wspomina okładki z lat 1998–2001, ożywiane w tym czasie standardowo wizerunkami pań). Nie zmieniło się to, że *Zabezpieczenia* są nadal bezpłatne, a jedynym źródłem finansowania są wpływy z reklam. Pod tym względem stanowimy wyjątek wśród wydawnictw naszej branży.

Jesteśmy przeświadczeni, że Czytelnicy *Zabezpieczeń* doceniają starania zmierzające do zapewnienia im możliwie wysokiego poziomu zadowolenia z czasopisma i będą nam towarzyszyć w ciągu następnej dekady w coraz to szerszym gronie.

Adam Bułaciński
Redakcja

Ośrodek Szkoleniowy PISA zaprasza na kursy i seminaria

Kursy:

– kurs pracownika zabezpieczenia technicznego pierwszego stopnia *Instalowanie i konserwacja systemów zabezpieczeń technicznych Klas SA1 – SA4*,
– kurs pracownika zabezpieczenia technicznego drugiego stopnia *Projektowanie systemów zabezpieczeń technicznych klas SA1– SA4*,
– kurs inwestorów systemów zabezpieczeń technicznych,
– kurs ekspertów i doradców w zakresie bezpieczeństwa,
– kurs montażu, eksploatacji, konserwacji i napraw urządzeń i środków mechanicznego zabezpieczenia,
– kurs kosztorysowania systemów zabezpieczeń technicznych.

Seminaria:

– 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. OSPISA

Zapraszamy do Budapesztu na targi Securex 2008

Centrum Promocji Eksportu „Proexpo”, partner organizatora na terenie Polski, zaprasza do zaprezentowania oferty firmy podczas IX edycji Międzynarodowych Targów BHP, Ochrony i Zabezpieczeń „**Securex 2008**”, które odbędą się w dniach **27–30 maja 2008 r**. **w Budapeszcie na Węgrzech**.

Targi Securex odbywają się **co dwa lata**, równolegle z innymi targami z cyklu Industria, Electrosalon i Chemexpo.

W ostatniej edycji targów, w roku 2006, zaprezentowało się łącznie 734 wystawców, z czego 103 firmy z dziesięciu krajów przypadły na Securex. Ekspozycje zajęły ok. 1700 m^2 powierzchni. Według oficjalnych statystyk liczba odwiedzających, łącznie z targami Industria, wynosiła ponad 18600 osób.

Podstawowy zakres tematyczny obejmuje następujące działy:

– bezpieczna praca: ochrona techniczna, środki i urządzenia ochrony osobistej, instrumenty i urządzenia pomiarowe, ochrona zdrowia w miejscu pracy, oznakowania, ochrona przeciwpożarowa,
– ochrona i zabezpieczenia: środki i urządzenia ochrony mienia, systemy alarmowe, specjalne środki transportu, ochrona i zabezpieczanie danych.

Jednocześnie informujemy, że Centrum Promocji Eksportu „Proexpo” oferuje obsługę logistyczną uczestników targów.

O przydziale powierzchni wystawienniczej decyduje kolejność zgłoszeń.

Proexpo oferuje również: **rezerwacje hotelowe**, **vouchery**, **bilety lotnicze**, **transport miejscowy**.

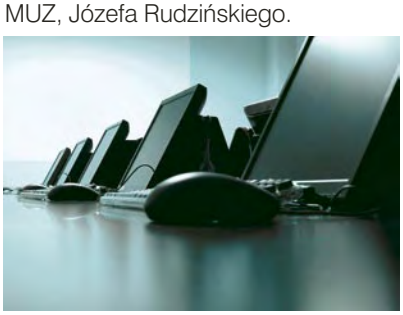
Centrum Promocji Eksportu „Proexpo”
ul. Hetmańska 28, pok. 311, 85-039 Bydgoszcz
tel./faks: (052) 345 46 00, 345 43 01
e-mail: proexpo@proexpo.com.pl
Kontakt: Małgorzata Zasada

Zapraszamy na szkolenie doskonalenia zawodowego

Sekcja Mechanicznych Urządzeń Zabezpieczających /MUZ/, skupiająca mechaników zamknięć skarbcowych NBP, rzeczoznawców SIMP i wykładowców z wieloletnim stażem, prowadzi szkolenia doskonalenia zawodowego poświęcone zabezpieczeniom mechanicznym, w tym sterowanym elektronicznie.

Szkolenia te są prowadzone od 25 lat przez działacza SIMP, obecnie prezesa Sekcji MUZ, Józefa Rudzińskiego.

Szkolenia prowadzone są corocznie w październiku (20 godzin lekcyjnych – przez trzy dni – dla grup dwudziestoosobowych).



Organizacją szkoleń zajmuje się Ośrodek Doskonalenia Kadr /ODK/ SIMP w Warszawie – tel. (022) 839 01 51, (022) 839 08 76 – posiadający wszystkie wymagane uprawnienia MEN.

Osoby rozpoczynające pracę w branży powinny brać udział w szkoleniach, przez pierwsze trzy lata corocznie, potem – co kilka lat.

Józef Rudziński
prezes Sekcji MUZ SIMP

Nadajniki wizyjne z serii VideoJet X rozszerzają obszary zastosowań sieciowych systemów CCTV

Nadajniki wizyjne we wzmocnionej obudowie pracują w trudnych warunkach środowiskowych. Oto ich najważniejsze właściwości:

– odporność na ekstremalne temperatury, wilgoć oraz wibracje,
– możliwość nadzorowania rozległych obszarów oraz infrastruktury transportowej,
– zaawansowana analiza obrazu w urządzeniu końcowym.

Nowa rodzina nadajników wizyjnych VideoJet X firmy Bosch łączy wysoką jakość obrazu, inteligencję oraz wzmocnioną obudowę, umożliwiając zastosowanie sieciowych systemów CCTV w najbardziej wymagających warunkach środowiskowych.

Nadajniki wizyjne VideoJet X10 (1-kanałowy), X20 (2-kanałowy) i X40 (4-kanałowy) pracują w temperaturze od -30 do +60°C i przy wilgotności względnej maks. 95%. Urządzenia te są także wyjątkowo odporne na wibracje, dzięki czemu są idealnym rozwiązaniem dla przemysłu ciężkiego, do monitoringu ruchu oraz centrów miast, a także do zastosowań mobilnych. Szeroki zakres napięć zasilających, od 10 do 30 V_{DC}, oznacza też, że nadają się one do dozoru wizyjnego odległych obszarów – wykorzystują zasilanie dostarczane za pomocą akumulatorów lub baterii słonecznych. Uzupełnieniem wzmocnionej obudowy jest kilka rodzajów połączeń sieciowych zapewnionych przez trzy porty: dwa standardowe porty Ethernet 10/100 Mb oraz 1-gigabitowe złącze SFP optycznego nadajnika – odbiornika. Złącze to umożliwia dołączenie nadajników bezpośrednio do modułu interfejsu światłowodowego zapewniającego proste połączenie z lokalizacjami zdalnymi za pomocą światłowodu (maks. 550 m dla światłowodu wielomodowego i nawet 100 km w przypadku światłowodu jednomodowego).

Urządzenia oferują także kilka opcji zapisu, poczynając od zapisu lokalnego w pamięci RAM, na karcie pamięci Compact Flash lub zintegrowanym dysku twardym, aż do zapisu na dołączonej za pomocą interfejsu iSCSI przez sieć macierzy dyskowej RAID5 lub w centralnym, sieciowym rejestratorze wizyjnym (NVR). Opcja iSCSI RAID5 oferuje znaczące korzyści, np. pełną elastyczność w lokalizacji urządzeń iSCSI w sieci, łatwość skalowania sieci, prostszy i w związku z tym bardziej niezawodny niż w przypadku standardowego sieciowego rejestratora wizyjnego zapis, a także możliwość skonfigurowania zapisu tych samych danych na innych macierzach iSCSI w celu zwiększenia integralności danych.

Nadajniki VideoJet X10 i X20 przesyłają przez sieć IP obraz w standardzie MPEG-4 z pełną częstotliwością odświeżania 25 obrazów (PAL) lub 30 obrazów (NTSC) na sekundę w rozdzielczości 4CIF w każdym kanale wizyjnym. Model VideoJet X40 może transmitować obraz w rozdzielczości 4CIF przy częstotliwości odświeżania 12,5/15 obrazów na sekundę lub w pełnej częstotliwości odświeżania 25 lub 30 obrazów na sekundę w rozdzielczości 2CIF lub 2/3 D1 w każdym kanale wizyjnym.

Podobnie jak w przypadku najnowszych wersji sieciowych produktów firmy Bosch, nowa seria nadajników VideoJet X zawiera licencjonowaną opcję inteligentnej wizyjnej detekcji ruchu (IVMD). Inteligentna wizyjna detekcja ruchu oferuje niezwykle zaawansowaną analizę zawartości obrazu (VCA), która obejmuje identyfikację obiektu na podstawie współczynnika proporcji, wykrywanie nieruchomego oraz usuniętego obiektu oraz mapowanie trajektorii do wykrywania podejrzanego zachowania, takiego jak długie przebywanie w jednym miejscu.

Wbudowana w nadajniki inteligentna wizyjna detekcja ruchu zapewnia „inteligencję w urządzeniu końcowym", która znacząco redukuje obciążenie sieci przez wykonywanie analizy zawartości obrazu w samym nadajniku. Ponadto, wraz ze stabilizacją obrazu stosowaną dla kamer instalowanych na maszcie lub narażonych na wibracje, inteligentna wizyjna detekcja ruchu wspomaga dodatkowo zastosowania zewnętrzne oraz mobilne. Urządzenia zapewniają także najwyższy poziom zabezpieczeń za pomocą szyfrowania przy wykorzystywaniu do podglądu przeglądarki sieciowej oraz obsługę autoryzacji standardu 802.1x.

Nowe nadajniki obsługują protokół DHCP, dynamicznie przydzielający adresy IP, oraz protokół SNTP, zapewniający podczas synchronizacji czasu z serwerem dokładność na poziomie 0,25 mikrosekund. Dolnoprzepustowy filtr wizyjny, dostępny w najnowszym oprogramowaniu układowym, jest przeznaczony dla kamer CCTV, które generują zaszumione sygnały powodujące niepożądany wzrost obciążenia kodowania.

Seria nadajników VideoJet X jest kompatybilna z nowym oprogramowaniem do zarządzania zapisem obrazu (VRM) firmy Bosch. Zapewnia ono pełne zarządzanie macierzami iSCSI RAID5, włączając w to automatyczne przekazywanie sygnału wizyjnego do alternatywnych urządzeń iSCSI w przypadku awarii. Nowe oprogramowanie VRM oferuje także inteligentną funkcję wyszukiwania metadanych (ciągów tekstowych zawierających słowa kluczowe opisujące określone scenariusze), które są przesyłane razem z obrazem na nośnik zapisu.

Przeszukiwanie plików metadanych jest znacznie szybsze od przeszukiwania wielu godzin materiału wizyjnego i jest jedną z kluczowych zalet idei przenoszenia inteligencji do urządzeń końcowych.

Bezpośr. inf.
Bosch Security Systems

XII edycja konkursu Polski Mistrz Techniki Alarmowej 2008

Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „Polalarm" zaprasza polskich oraz zagranicznych producentów i dystrybutorów elektronicznych i elektromechanicznych urządzeń oraz systemów przeznaczonych do ochrony osób i mienia do udziału w XII edycji konkursu „**Polski Mistrz Techniki Alarmowej 2008**".

Konkurs będzie przeprowadzony w następujących kategoriach przedmiotowych:

I Urządzenia i systemy sygnalizacji włamania i napadu
II Urządzenia i systemy sygnalizacji pożaru
III Urządzenia i systemy nadzoru telewizyjnego i rejestracji obrazów
IV Urządzenia i systemy kontroli dostępu
V Zintegrowane systemy sygnalizacji zagrożeń
VI Urządzenia i systemy transmisji alarmu oraz monitoringu
VII Systemy zabezpieczenia przeciwkradzieżowego pojazdów
VIII Systemy zarządzania i bezpieczeństwa transportu
IX Systemy zarządzania i bezpieczeństwa ładunków
X Inne urządzenia i systemy technicznej ochrony oraz wspomagające ochronę fizyczną

Zgłoszenia do udziału w konkursie będą przyjmowane **do dnia 27 lutego 2008 roku**, na drukach „Wniosku o udział w konkursie", które prosimy przesłać na adres biura zarządu stowarzyszenia Polalarm: ul. Nowogrodzka 18/8, 00-511 Warszawa, e-mail: polalarm@polalarm.com.pl lub polalarm@alter.pl.

Ogłoszenie wyników konkursu i uroczystość wręczenia nagród laureatom odbędzie się w pierwszym dniu Międzynarodowej Wystawy Zabezpieczeń „Securex 2008" **w Poznaniu**, **tj. 22 kwietnia 2008 r**.

Regulamin konkursu i wniosek o udział w konkursie dostępne są w na stronie www.polalarm.com.pl oraz w biurze zarządu stowarzyszenia Polalarm w Warszawie, przy ul. Nowogrodzkiej 18/8, tel./faks **(0-22) 625-57-43**, **626-90-31**.

Serdecznie zapraszamy do udziału w konkursie i życzymy sukcesów!

Bezpośr. inf. Polalarm

IP3701 – nowa kamera IP z Pelco

Pelco z dumą przedstawia nową kamerę IP w obudowie typu „box" – model IP3701. Produkt spotkał się z bardzo dobrym przyjęciem podczas imprez targowych. „Wysoka jakość za przystępną cenę" – takie były najczęstsze oceny klientów. Kamera ma wbudowany webserwer, strumień MJPEG może być odbierany przez przeglądarkę internetową Internet Explorer lub Mozilla Firefox.

Podstawowe cechy nowego produktu:
- zasilanie w standardzie PoE (IEEE802.3af) lub 24 V~,
- otwarta architektura,
- trzy jednoczesne strumienie wideo:
  - dwa strumienie MPEG-4 (25 obr/s przy QCIF, CIF, 2CIF, 4CIF),
  - skalowalny strumień MJPEG do przeglądarki internetowej,
- wielopoziomowa hierarchia dostępu,
- rozszerzony zakres dynamiki (EDR),
- możliwość mocowania obiektywów C/CS,
- rozdzielczość 480 TVL.

Firma Pelco ogłosiła wzmocnienie współpracy z firmą On-Net Surveillance Systems, Inc. (OnSSI), liderem rynku oprogramowania do rejestracji wideo w systemach dozorowych IP. Owocem współpracy z Pelco jest przystosowanie oprogramowania OnSSI do rejestracji strumieni wideo MPEG-4 wysyłanych przez kamery IP3701 i Camclosure IP. Obecni i przyszli użytkownicy oprogramowania OnSSI będą mogli używać kamer IP Pelco w swoich systemach telewizji dozorowej.

Współpraca Pelco z firmą Milestone Systems jest kontynuowana. Kamera IP3701, podobnie jak seria Camclosure IP, może pracować z oprogramowaniem Milestone XProtect.

Więcej informacji można uzyskać u dystrybutorów Pelco w Polsce. Karta katalogowa jest dostępna na witrynie internetowej Pelco **http://www.pelco.com/ipcam**.

Bezpośr. inf. Pelco

Nowy czytnik odcisków palców

Firma **Trijay Technologies International Corporation** (TTI) zapowiedziała 11 stycznia wprowadzenie na rynek nowego przenośnego optycznego biometrycznego czytnika odcisków palców **BCR200 BT**. Jest to zaprojektowany w unikatowy sposób czytnik kart chipowych z wbudowanym optycznym skanerem odcisków palców. Produkt opracowano w celu zapewnienia wygodnego użytkowania zarówno z komputerami przenośnymi, jak i stacjonarnymi. Wykorzystujące nowoczesne rozwiązanie biometrii optycznej urządzenie zapewnia najwyższy poziom funkcjonalności w zakresie odczytu i porównywania odcisków palców.

Czytnik BCR200 BT może zdalnie przesyłać odczytane odciski palców do dowolnego urządzenia obsługującego Bluetooth, takiego jak palmtop, laptop czy telefon komórkowy. Możliwa jest integracja BCR200 BT z istniejącymi rozwiązaniami służącymi do identyfikacji oraz zdalne uwierzytelnianie i weryfikacja odcisków. Wbudowany akumulator litowo-polimerowy może być ładowany przez port USB, co ułatwia mobilne zastosowania urządzenia.

– *Nowe urządzenie BCR200 BT do odczytu odcisków palców jest naturalnym dodatkiem do naszych innych urządzeń służących do mobilnej weryfikacji tożsamości* – powiedział Chuck Weiglin, szef ds. operacyjnych w firmie TTI.

Adam Bułaciński
Źródło: TTI

Zapraszamy na Międzynarodowe Targi Narzędziowe/Practical World

Międzynarodowe Targi Narzędziowe/Practical World, które odbędą się **w Kolonii** w dniach **9–12 marca 2008 roku**, będą nie tylko prezentować wystawców, pokazujących swoje nowe produkty **na terenie kolońskiego centrum wystawienniczego**, ale także zapewnią gościom z Niemiec i zza granicy ekscytującą dawkę imprez związanych z interesującymi tematami i osiągnięciami rynkowymi.

Program informacyjno-rozrywkowy skupi się na specjalnych obszarach wiodących, takich jak środowisko, zdrowie fizyczne i dobra kondycja, projekty mebli i wnętrz, energia oraz narzędzia i technologia. Imprezy będą się odbywać w różnych miejscach, między innymi na scenach „forum nowego wymiaru – ukształtuj swoją przyszłość!" (w wersji angielskiej: „forum new DIYmension – shape your own future!" zastosowano grę słów ze skrótem DIY, czyli Do-It-Yourself, po polsku Zrób-To-Sam, a „Meet NEW DIYmension", czyli „Spotkaj się z nowym wymiarem", jest sloganem targów). Forum to zgromadzi razem użytkowników dóbr oraz przedstawicieli handlu i przemysłu, pozwalając im na wspólne doświadczanie hitów i przygotowanych sztuczek. Na miejscu będą też dziennikarze z prasy handlowej, gazet codziennych i mediów zajmujących się sprawami ogólnymi.

W ciągu niecałego miesięca, który pozostał do rozpoczęcia Międzynarodowych Targów Sprzętowych/Practical World 2008, swój udział potwierdzą jeszcze niektórzy wielcy gracze. Wystawcy, którzy już wpisali się na listę, to między innymi BauMarkt, OBI – lider sektora DIY, silna sieć regionalna BayWa oraz słynni dostawcy przemysłowi, tacy jak ABUS, Burg-Wächter, GAH Alberts, Hettich, HSI Schwerter, Meffert i Westag & Getalit.

Targi kolońskie wspierają członków każdej ze stron łańcucha dystrybucji przez organizowanie imprez, które zaspokajają ich specyficzne potrzeby. Należą do nich np. prezentacje nowej koncepcji Akademii Zrób-To-Sam, ekscytujące imprezy dla konsumentów, wymagające od nich praktycznych umiejętności, konkursy „Miss Zrób-To-Sam" i inne, przeznaczone dla entuzjastów „Zrób-To-Sam".

Podobnie jak asortyment produktów Międzynarodowych Targów Narzędziowe/Practical World zróżnicowane są także typy restauracji, które Kolonia ma do zaoferowania gościom pragnącym spędzić relaksujący wieczór po całym dniu w centrum wystawienniczym. Chlubiąca się ponad trzema tysiącami pubów i restauracji Kolonia rozpuści gości bogatym wyborem. Typowym kolońskim napojem jest piwo, znane jako „Kölsch", które smakuje najlepiej serwowane w jednej z historycznych piwiarni, w wąskich szklankach o pojemności 0,2 litra. Ale Kolonia ma wiele do zaoferowania także podczas dnia, kiedy goście mogą sami odkrywać historię miasta, która liczy dwa tysiące lat. Na uwagę zasługuje słynna w świecie katedra ze 150-metrowymi iglicami. Miasto ma też wiele zróżnicowanych muzeów, takich jak np. Kolońskie Muzeum Karnawału i Muzeum Czekolady nad Renem, co zapewnia zaspokojenie każdych gustów, także w zakresie kultury.

Wybierzesz się do Kolonii? Szybki, wygodny i niedrogi sposób dotarcia tam to lot do lotniska Kolonia Bonn (*Köln-Bonn Airport*), które stało się ostatnio punktem centralnym wielu tanich linii lotniczych. Tanie loty do i z Kolonii oferują różne linie lotnicze, a w ostatnim letnim rozkładzie było ich ok. 100. Dzięki temu goście targowi mogą w tani sposób połączyć wycieczkę do Kolonii z dodatkowymi spotkaniami biznesowymi w innych krajach europejskich, a im wcześniej zarezerwują swój lot, tym bardziej korzystne ceny zostaną im najprawdopodobniej zaproponowane. System rezerwacji targów kolońskich, oferujący takie tanie loty, jest dostępny w sekcji „Flights and packages" witryny internetowej Międzynarodowych Targów Narzędziowe/Practical World (**http://www.hardwarefair.com**).

Opracował
Adam Bułaciński
Redakcja

Serwisowanie mechanicznych urządzeń zamykających

W dniu 11 stycznia 2008 roku odbyła się pierwsza konferencja z cyklu poświęconego zagadnieniom serwisowania mechanicznych urządzeń zamykających na przykładzie firmy Systemy Zabezpieczeń – Józef Matyjas.

W spotkaniu udział wzięli członkowie **Sekcji MUZ** i zaproszeni goście.

Józef Matyjas zademonstrował działanie narzędzi, przyrządów i urządzeń umożliwiających awaryjne otwieranie zamków bezpośredniego ryglowania, wkładek kluczowych, kłódek oraz zamków współpracujących z mechanizmami zamykającymi.

Pokaz wzbudził wielkie zainteresowanie wśród uczestników spotkania.

Prezes Sekcji, Józef Rudziński, zwrócił uwagę na konieczność podnoszenia kwalifikacji zawodowych w zakresie technik awaryjnego otwierania zamknięć mechanicznych.

Uhonorował szczególnie wyróżniających się aktywnością członków Sekcji Srebrnymi Honorowymi Odznakami SIMP oraz wręczył legitymację nowemu członkowi – Bogusławowi Zjawińskiemu.

Przypomniał członkom Sekcji o potrzebie zgłaszania uwag do raportu o stanie branży MUZ w kraju oraz o szkoleniu doskonalenia zawodowego dla rozpoczynających pracę w branży (szkolenie odbywa się corocznie w październiku – pod warunkiem zgłoszenia się na nie co najmniej 20 chętnych).

Józef Rudziński
prezes Sekcji MUZ SIMP

II Konferencja Security Management Audit Forum (Semafor) – relacja

W dniach 22 i 23 stycznia 2008 roku w hotelu Marriott w Warszawie odbyła się konferencja **Security Management Audit Forum**, określana też w skrócie jako **Semafor 2008**.

Tematyka konferencji dotyczyła następujących zagadnień:
– outsourcingu usług bezpieczeństwa,
– ładu informatycznego (ang. *IT Governance*),
– incydentów naruszenia bezpieczeństwa,
– zarządzania bezpieczeństwem informacji,
– audytowania bezpieczeństwa informacji.

Konferencja została zorganizowana przez ISACA – stowarzyszenie do spraw audytu i kontroli systemów informatycznych, ISSA Polska – stowarzyszenie ds. bezpieczeństwa systemów informacyjnych oraz tygodnik informatyków i kadry kierowniczej *Computerworld*, we współpracy merytorycznej z NASK i Oracle.

Podczas konferencji zaprezentowano 23 referaty (w tym jeden o charakterze warsztatowym, dotyczący bezpieczeństwa systemów biznesowych).

Pierwszego dnia konferencji miała także miejsce dyskusja panelowa pod hasłem „Prawo, bezpieczeństwo i biznes", która cieszyła się bardzo dużym zainteresowaniem.

Gośćmi specjalnymi konferencji byli Daniel Barriuso z Credit Suisse, odpowiedzialny za zarządzanie ryzykiem IT i bezpieczeństwem informatycznym, oraz Mary Ann Davidson z Oracle, zajmująca się bezpieczeństwem produktów, jego testowaniem i oceną oraz zarządzaniem incydentami naruszania bezpieczeństwa w tej korporacji.

W konferencji wzięło udział stu kilkudziesięciu uczestników, reprezentujących m.in. operatorów telekomunikacyjnych, banki i duże organizacje rządowe. W kuluarach zorganizowano stoiska, na których można było np. sprawdzić bezpieczeństwo swojego komputera przenośnego (Evercom), zapoznać się ze sposobami mechanicznego zabezpieczania notebooków przed kradzieżą (Kensington), a także z ofertą firmy świadczącej usługi informatyki śledczej (ang. *computer forensics*) w Polsce (Mediarecovery).

Następna konferencja Semafor jest przewidziana za rok.

Adam Bułaciński

ADT obniża koszty wdrożenia systemu RFID w handlu detalicznym

Firma **ADT** radykalnie poprawia opłacalność wdrożeń wewnątrz sklepowych systemów kontroli przepływu towarów opartych na technologii identyfikacji radiowej (**RFID**) poprzez ograniczenie wymogów dotyczących czytników o 90% i kosztów inwestycji o 60%. Dzięki nowatorskiemu wykorzystaniu standardu EPCglobal Gen 2 nowa platforma Sensormatic iREAD pozwala ograniczyć złożoność i koszty wdrożenia technologii RFID i uczynić wielki krok w kierunku zasadniczej poprawy zwrotu z inwestycji firm handlowych.

Platforma Sensormatic iREAD umożliwia wyeliminowanie oddzielnych infrastruktur zasilania, nadzoru i dystrybucji danych, które dotychczas były nieodzowne w przypadku wewnątrzsklepowych systemów kontroli przepływu towarów RFID. Połączenie ich w jedną sieć zapewnia znaczące oszczędności finansowe i ułatwia instalację w środowisku sklepowym, co z kolei zwiększa atrakcyjność rozwiązania RFID dla handlowców rozważających zastosowanie tej technologii w celu poprawy wyników prowadzonej działalności.

iREAD to elastyczna i skalowalna platforma dla detalistów, która umożliwia im wykorzystanie zalet technologii RFID. Pozwala także ograniczyć stosunkowo dużą liczbę czytników, kabli i anten, niezbędnych w tradycyjnych systemach RFID. Właściwa dla tego rozwiązania modułowość i prostota oznacza możliwość dostosowania jego możliwości do praktycznie każdej konfiguracji infrastruktury sklepowej – półek, stelaży, stołów oraz innych systemów ekspozycji towarów.

Wdrożenie systemu RFID na poziomie pojedynczych artykułów w typowym, średniej wielkości sklepie detalicznym wymaga zainstalowania około 100 czytników i wstępnej inwestycji w sprzęt na poziomie 300000 EUR. Dzięki platformie iREAD porównywalny system wymaga instalacji tylko około dziesięciu czytników, co oznacza ograniczenie liczby tych urządzeń o 90%. Wstępny koszt inwestycji spada do około 100000 EUR (redukcja o ponad 60%), zaś dalsze oszczędności uzyskuje się w trakcie eksploatacji systemu. Korzyści i oszczędności mogą znacznie wzrosnąć wraz ze wzrostem wielkości i skali wdrożenia.

Firma ADT i jej wiodąca w branży marka **Sensormatic**, obejmująca elektroniczne systemy przeciwkradzieżowe (**EAS**), może poszczycić się długą tradycją stosowanych na szeroką skalę rozwiązań przeznaczonych do znakowania towarów w celu ich zabezpieczenia. Firma Karstadt Warenhaus GmbH – jedno z wiodących przedsiębiorstw handlu detalicznego w Niemczech, korzystające z rozwiązań EAS Sensormatic w celu zabezpieczenia towarów i ograniczenia strat – wdrożyła ostatnio platformę iREAD w ramach dużego działu odzieżowego w jednym ze swoich flagowych sklepów.

– *Dzięki zastosowaniu platformy Sensormatic iREAD firma Karstadt może uzyskać znaczące oszczędności związane z wdrożeniem systemu RFID na poziomie pojedynczych artykułów. Oszczędności te pomogą nam w uzyskaniu szybszego zwrotu z inwestycji w związku z lepszym zarządzaniem zapasami i polityką cenową, udoskonaleniem łańcucha dostaw oraz ograniczeniem ubytku masy towarów. Co więcej, wgląd na poziomie pojedynczych artykułów pomoże nam zwiększyć ich dostępność na półkach, a w efekcie również satysfakcję klientów oraz sprzedaż* – twierdzi Rainer Jilke, kierownik ds. systemów RFID w firmie Karstadt.

– *Detaliści z pewnością docenią, że nie wprowadziliśmy nowego protokołu, lecz w nowatorski sposób wykorzystaliśmy przemysłowy standard EPCglobal Gen 2* – mówi John Smith, wiceprezes ds. sprzedaży detalicznej w ADT Europe, Middle East and Africa. – *Innymi słowy, bazując na istniejącym standardzie stworzyliśmy unikatową aplikację, aby ograniczyć złożoność i koszty związane z wdrażaniem systemów RFID. Łącząc w sobie nasze pionierskie doświadczenia w dziedzinie systemów EAS i RFID, rozwiązanie to pozwala w znacznym stopniu usprawnić działalność detaliczną i zwiększyć zadowolenie klientów. Przewidujemy, że platforma Sensormatic iREAD przyczyni się do znaczącego wzrostu zainteresowania technologią RFID w branży handlu detalicznego*.

Bezpośr. inf. ADT Poland

Inteligentny zawór bezpieczeństwa
do instalacji gazowych, wodnych i cieplnych

LJ Elektronik proponuje nowy produkt – inteligentny zawór zabezpieczający do instalacji wodnych, cieplnych i gazowych. Konstrukcja urządzenia bazuje na zaworze elektrycznym i sterującym nim układzie elektronicznym. Programowalna elektroniczna centrala za pomocą zaworu elektrycznego steruje dopływem wody, ciepła lub gazu wg wcześniej zaprogramowanego toku działania. Użytkownik za pomocą klawiatury urządzenia programuje czas, w jakim zawór zamyka i otwiera dopływ medium. Przykładowo: użytkownik programuje godzinę, o której ma zamknąć się dopływ wody (np. godzina, o której opuszcza mieszkanie). Zawór zamyka się, a w momencie powrotu użytkownika do mieszkania może otworzyć się automatycznie (o określonej wcześniej godzinie) lub użytkownik może otworzyć go ręcznie, wciskając jeden przycisk na klawiaturze urządzenia.

Zalety urządzenia
- prosta instalacja i obsługa;
- zastosowanie do różnych typów medium: woda, gaz, ciepło;
- umożliwienie (po zastosowaniu urządzenia) redukcji kosztów eksploatacji mieszkania (mniejsze rachunki za zużycie energii cieplnej, gazu i wody);
- zabezpieczenie przed wyciekiem wody z instalacji wodociągowej;
- redukcja zużycia energii cieplnej w mieszkaniu;
- zabezpieczenie przed wyciekiem gazu podczas nieobecności lokatora.

Bezpośr. inf. LJ Elektronik

15-lecie Polalarmu – relacja z uroczystości

W dniu 23 listopada w Warszawskim Domu Technika NOT odbyło się spotkanie koleżeńskie z okazji **jubileuszu 15-lecia** Ogólnopolskiego Stowarzyszenia Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „**Polalarm**".

W uroczystości wzięło udział ponad 100 osób: członkowie zwyczajni, honorowi i wspierający Stowarzyszenie wraz z osobami towarzyszącymi, goście z Federacji Stowarzyszeń Naukowo-Technicznych NOT, Krajowej Izby Gospodarczej, Ministerstwa Obrony Narodowej, Komendy Głównej Policji, Polskiego Komitetu Normalizacyjnego, organizacji branżowych, Międzynarodowych Targów Poznańskich i redaktorzy naczelni prasy branżowej (*Systemy Alarmowe, Ochrona Mienia i Informacji, Zabezpieczenia*).

Po przywitaniu uczestników uroczystości referat wygłosił prezes zarządu Polalarm, Bogdan Tatarowski (referat jest zamieszczony na stronie www.zabezpieczenia.com.pl).

Wiceprezes FSNT NOT wręczył panu Bogdanowi Tatarowskiemu Dyplom Uznania za jego działalność na rzecz rozwoju technicznej ochrony osób i mienia w Polsce.

Prezes Krajowej Izby Gospodarczej wręczył Złote Honorowe Odznaki KIG członkom założycielom Stowarzyszenia:

- Włodzimierzowi Paupie – wieloletniemu przewodniczącemu Sądu Koleżeńskiego Stowarzyszenia,
- Andrzejowi Jurkowi – członkowi zarządu,
- Jackowi Szewczykowi – członkowi zarządu.

Przedstawiciele Komendy Głównej Policji wyróżnili Dyplomami Uznania rzeczoznawców systemów technicznego zabezpieczenia osób i mienia Stowarzyszenia za ich społeczną pracę w komisjach egzaminacyjnych podczas egzaminów na licencje pracowników ochrony fizycznej oraz za inną działalność wspierającą pracę policji na rzecz poprawy bezpieczeństwa w naszym kraju.

Polski Komitet Normalizacyjny wyróżnił Dyplomami Uznania członków Komitetu Technicznego Nr 52 ds. Systemów Alarmowych Włamania i Napadu.

Rada Stowarzyszenia Polalarm nadała Złote Honorowe Odznaki Stowarzyszenia członkom zwyczajnym oraz godność członka honorowego pracownicy Biura Zarządu.

Wszyscy członkowie Stowarzyszenia otrzymali Dyplomy Uznania z okazji jubileuszu 15-lecia działalności Polalarmu, a działacze pełniący funkcje w organach statutowych oraz założyciele wyróżnieni zostali Złotymi Dyplomami Uznania.

Spotkanie zakończyło się bankietem. Z okazji jubileuszu Zakład Elektroniki „Compas" przygotował płytę „Wspomnienia", na której znalazły się zdjęcia i filmy z wybranych imprez Stowarzyszenia organizowanych w minionych 15 latach.

Płytę oraz zdjęcia z uroczystości można oglądać na stronie Stowarzyszenia Polalarm www.polalarm.com.pl.

Redakcja

Opracowano na podstawie materiałów firmowych Stowarzyszenia Polalarm.
Więcej informacji na stronie **www.zabezpieczeniacom.pl**.

Targi Alarm i Sport-Obiekt w Kielcach – podsumowanie

W dniach 7–8 listopada 2007 roku w kieleckim ośrodku wystawienniczym odbyła się **VIII Ogólnopolska Konferencja „Bezpieczne Miasto – Monitoring Wizyjny Miast”** i **wystawa Alarm 2007**, a także **VII Międzynarodowa Konferencja „Bezpieczny stadion”** oraz **VII Wystawa Wyposażenia i Budowy Obiektów Sportowych „Sport-Obiekt”**.

Pierwszego dnia odbyła się konferencja **„Bezpieczny stadion”**. Przybyłych gości, wśród których znaleźli się między innymi Przemysław Gosiewski, przedstawiciele parlamentu – Maria Zuba, Henryk Milcarz, Adam Masalski, wiceprezydent Kielc – Andrzej Sykut, wiceprezes Federacji Futbolu Ukrainy – Borys Voskresensky, a także Jerzy Engel, Stanisław Bobkiewicz, Grzegorz Lato, Wiesław Wieczorek oraz przedstawiciele miast, powiatów i policji, powitał prezes zarządu Targów Kielce – dr Andrzej Machoń, a uroczystego otwarcia dokonał wiceprezes PZPN – Eugeniusz Kolator.

Przyznanie Polsce i Ukrainie praw do zorganizowania w 2012 roku Mistrzostw Europy w Piłce Nożnej, trzeciej co do wielkości imprezy sportowej na świecie, spowodowało, że wszyscy przeżyliśmy ogromny wybuch radości. Oczami wyobraźni widzieliśmy już nowe autostrady i trasy ekspresowe, zmodernizowane koleje i rozbudowaną infrastrukturę lotniczą z nowymi portami regionalnymi, rozwiniętą bazę turystyczną oraz rzesze odwiedzających nasz kraj turystów.

Do 2015 roku Polska ma do wykorzystania na rozwój infrastruktury drogowej, kolejowej oraz lotniczej ponad 19 mld 75 mln euro z UE (informację podał minister transportu Jerzy Polaczek). Z kolei, jak zapowiadał minister sportu Tomasz Lipiec, na budowę i modernizację stadionów mamy do dyspozycji ponad 2 mld zł z budżetów samorządowych oraz z Funduszu Rozwoju Kultury Fizycznej.

Sprawdziliśmy, jak poradzili sobie Portugalczycy w 2004 roku, kiedy to oni byli gospodarzami ME. Jak podają różne źródła, ME obejrzało 1 mln 156 tys. widzów na stadionach i ok. 4,8 mld przed telewizorami. Portugalię odwiedziło ponad 2 mln turystów, którzy zostawili prawie miliard euro. Mecz finałowy pokazało na żywo 239 kanałów telewizyjnych z 200 krajów.

Przewiduje się, że w Polsce i na Ukrainie będzie jeszcze lepiej. Szacuje się, że wpływy z tytułu opłat za prawa telewizyjne przekroczą miliard euro (transmisję prawdopodobnie będziemy mogli obejrzeć przez Internet oraz w telefonach komórkowych).

Brzmi pięknie, ale czy sprostamy zadaniu? Optymiści uważają, że damy radę – przecież nie możemy być pierwszym w historii organizacji turnieju krajem, któremu odbierze się prawo do zorganizowania Euro.

Budowa nowych stadionów i dróg oraz rozbudowa bazy hotelowej to główne punkty planów rozwoju infrastruktury, niezbędnej do organizacji mistrzostw. Organizacja tak dużych imprez jest związana z koniecznością zapewnienia bezpieczeństwa i porządku, nie tylko na stadionach i wokół nich. Wszelkiego rodzaju konferencje, chociażby takie, jak ta w Kielcach, cieszą się dużą popularnością i wysoką frekwencją, gdyż dotyczą spraw ważnych dla nas wszystkich.

W tym roku na kieleckiej konferencji „Bezpieczny stadion" dyskutowano głównie na temat bezpieczeństwa imprez masowych. Uczestnicy konferencji, w tym przedstawiciele MSWiA, PZPN, Ekstraklasy i policji, byli zgodni co do konieczności zmian w ustawie „Bezpieczeństwo imprez masowych". Zwrócono uwagę na konieczność opracowania standardów dotyczących wyposażania obiektów sportowych w systemy monitoringu wizyjnego, za przykład podano rozwiązania stosowane w Wielkiej Brytanii.

Na zakończenie pierwszego dnia – tradycyjnie już – odbyła się **Gala Fair Play**, podczas której PZPN w szczególny sposób wyróżnił Targi Kielce. Jak podkreślał obecny na gali wiceprezes PZPN Eugeniusz Kolator, organizacja konferencji „Bezpieczny stadion" i targów Sport-Obiekt nie mogła pozostać bez echa w świecie polskiego sportu. **Puchar** wręczono **Andrzejowi Mochoniowi** – prezesowi Targów Kielce, **Dariuszowi Michalakowi** – dyrektorowi ds. targów w Targach Kielce i **Grzegorzowi Figarskiemu** – menedżerowi targów Sport-Obiekt.

Podczas Gali Fair Play wręczono **medale i wyróżnienia Targów Kielce** w kategoriach „Bezpieczny stadion" oraz „Sport-Obiekt 2007".

Miło nam poinformować, że wśród nagrodzonych znalazły się między innymi agencje ochrony, które otrzymały wyróżnienia za działania podejmowane na rzecz poprawy bezpieczeństwa na obiektach piłkarskich. Wyróżniono:

– Agencję Ochrony „**Bokser**" z Poznania,
– Agencję Ochrony „**Ekotrade**" – przedstawicielstwo z Gdyni,
– Agencję Ochrony „**Skorpion**" z Katowic.

Drugiego dnia odbyła się konferencja **„Bezpieczne Miasto"**, podczas której wymieniono doświadczenia związane z monitoringiem wizyjnym i przedstawiono wnioski użytkowników związane z eksploatacją systemów. Szczególnie interesujące były wnioski z eksploatacji monitoringu miejskiego w Warszawie, przekazane przez Tadeusza Grzybowskiego – zastępcę dyrektora Biura Bezpieczeństwa i Zarządzania Kryzysowego Urzędu Miasta w Warszawie oraz Jacka Gniadka – dyrektora Zakładu Obsługi Systemu Monitoringu. Zakład jest operatorem systemu monitoringu miejskiego i został to tego celu specjalnie powołany. Uznano to za lepsze rozwiązanie niż angażowanie do tego celu policji czy straży miejskiej.

Aby przybliżyć Państwu tematykę konferencji, poniżej przedstawiamy listę wygłoszonych referatów:

– *System Monitoringu Wizyjnego Miasta Stołecznego Warszawy jako narzędzie w służbie bezpieczeństwa mieszkańców* – Tadeusz Grzybowski, Biuro Bezpieczeństwa i Zarządzania Kryzysowego Urzędu Miasta w Warszawie, Jacek Gniadek, Zakład Obsługi Systemu Monitoringu,
– *Zintegrowany system bezpieczeństwa w mieście* – Dominik Tokarski, Fortuna Communication, Jacek Zajkowski, Robert Bosch,
– *Profesjonalne przygotowanie inwestycji monitoringu miejskiego* – Maciej Włodarczyk, Dipol,

– *Zdalne zarządzanie systemami wideo* – Andrzej Jarzyna, S.P.S. Trading,
– *Wideomonitoring Miasta Bydgoszczy* – Adam Ferek, Wydział Zarządzania Kryzysowego Urzędu Miasta w Bydgoszczy,
– *System automatycznego rozpoznawania tablic rejestracyjnych pojazdów – przykładowe zastosowania na przykładzie monitoringu ulic w Warszawie* – Maciej Mroszczak, Sprint,
– *Historia budowy systemów w Zielonej Górze, konfrontacja praktyki z teorią* – Zbigniew Legieta, Sekcja Łączności i Informatyki KMP w Zielonej Górze,
– *Monitoring wizyjny w szkołach – spojrzenie alternatywne* – Piotr Ichniowski, Straż Miejska w Oświęcimiu,
– *Najnowsze trendy w cyfrowym zapisie obrazu na podstawie rejestratora DVR RH 5016* – Janusz Pawłowski, GV Polska,
– *Ujęcie osób posiadających narkotyki dzięki monitoringowi miejskiemu w Płocku* – Jacek Olejnik, Komenda Miejska Policji w Płocku,
– *Skuteczne działania policji w reakcji na przestępstwa na terenie woj. małopolskiego i miasta Krakowa – przykłady zastosowania monitoringu podczas operacji policyjnej w czasie wizyty Papieża Benedykta XVI oraz pożaru kamienicy na rynku głównym w Krakowie* – Andrzej Skotnicki, Małopolska Komenda Wojewódzka, KWP w Kielcach,
– *Możliwości systemu monitoringu wizyjnego miasta Szczecina zaimplementowanego systemem wspomagania dowodzenia KMP w Szczecinie* – KMP w Szczecinie.

Tradycyjnie konferencjom towarzyszyła wystawa. W tym roku wzięło w niej udział 60 wystawców. Była ona doskonałą okazją do zaprezentowania nowości w budownictwie sportowym i wyposażeniu obiektów sportowych, sprzętu sportowo-rekreacyjnego i odzieży sportowej, a także najnowszych urządzeń z bogatej oferty systemów monitoringu wizyjnego.

Nagrody i wyróżnienia przyznane w czasie targów w kategorii „Alarm” Medale Targów Kielce:

– za ARTR – system automatycznego rozpoznawania tablic rejestracyjnych, Sprint z Gdańska,
– za rejestrator cyfrowy RH5000DVR, **GV Polska** z Nadarzyna,
– za kamerę 5-megapikselową, **Dipol Szydłowski i Wspólnicy** z Krakowa.

Wyróżnienia Targów Kielce:

– za system bezpiecznego stadionu Pentasexta, **Pentacomp Systemy Informatyczne** z Warszawy,
– za rejestrator Digital Sprite2 Dedicated Micros, **S.P.S. Trading** z Warszawy.

W kategorii „Bezpieczny stadion” Medal Targów Kielce:

– za kamerę szybkoobrotową VCC-9800 Sanyo 36x zoom, **S.P.S. Trading** z Warszawy.

Opracowała
Teresa Karczmarzyk

Fotoreportaż na stronie www.zabezpieczenia.com.pl.

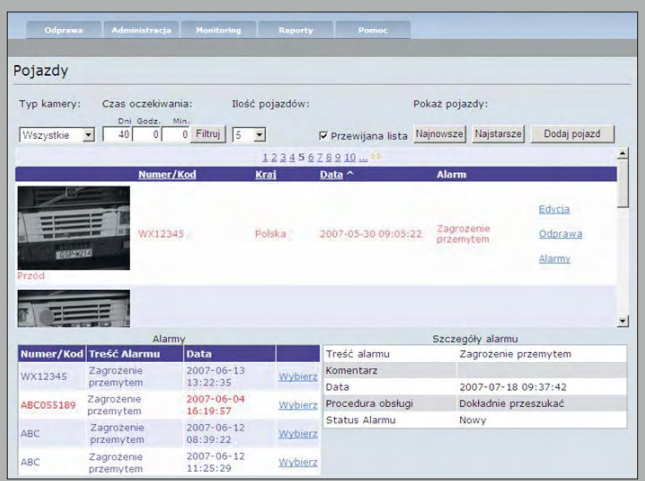
Polskie granice gotowe na Schengen

W nocy z 20 na 21 grudnia ubiegłego roku zniknęły kontrole na granicach Polski z innymi państwami członkowskimi Unii Europejskiej. To efekt przystąpienia naszego kraju do układu z Schengen. Obecnie cała uwaga służb celnych i granicznych skupi się na uszczelnieniu granic z pozostałymi sąsiadami.

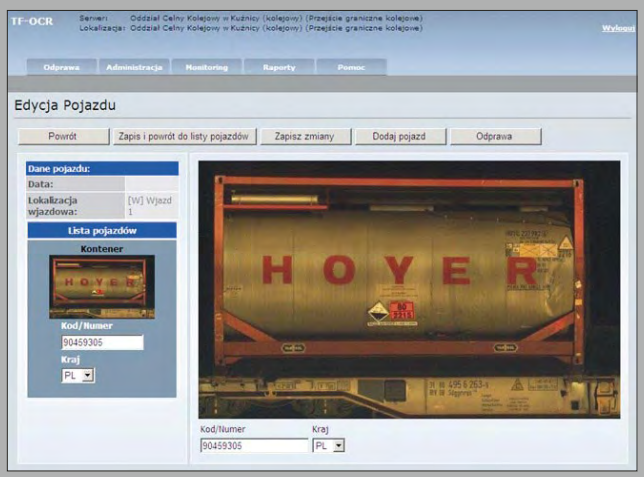
Zniesienie granic z Niemcami, Litwą, Słowacją i Czechami, a jednocześnie wzmocnienie kontroli na przejściach z Ukrainą, Białorusią i Rosją kosztowało wspólnotowy budżet kilkaset milionów euro. Pieniądze przeznaczono na wyposażenie pograniczników w najnowocześniejszy sprzęt, za pomocą którego mają skuteczniej walczyć z przemytem czy nielegalną emigracją ludności. W ich posiadaniu znalazły się między innymi urządzenia termo- i noktowizyjne, specjalistyczne samoloty i łodzie patrolowe oraz tzw. schengen-busy, zaopatrzone w komputery podłączone do bazy danych i rozbudowane laboratoria chemiczne. Na samych przejściach zainstalowano systemy TF-OCR, których zadaniem jest rejestracja wszystkich pojazdów przekraczających drogowe i kolejowe granice Polski.

– *Nieustanny monitoring ma uchronić Unię Europejską przed wjazdem na jej terytorium pojazdów, które wcześniej zamieszane były w działalność przestępczą* – mówi Andrzej Oliński z firmy **T4B**, która jest twórcą i wykonawcą **systemu TF-OCR**. – *System wyposażony jest w kamery, które potrafią automatycznie sczytywać numery rejestracyjne pojazdów lub kody kontenerów kolejowych. Następnie dane trafiają bezpośrednio do bazy, gdzie podlegają szczegółowej weryfikacji. Co istotne, system TF-OCR współpracuje nie tylko z polskimi programami kontrolującymi politykę celną, ale również z systemami zainstalowanymi w innych krajach Wspólnoty. Dzięki temu jeśli przykładowo dany samochód był zatrzymany na przejściu fińsko-rosyjskim, natychmiast otrzymamy na ten temat informację* – dodaje A. Oliński.

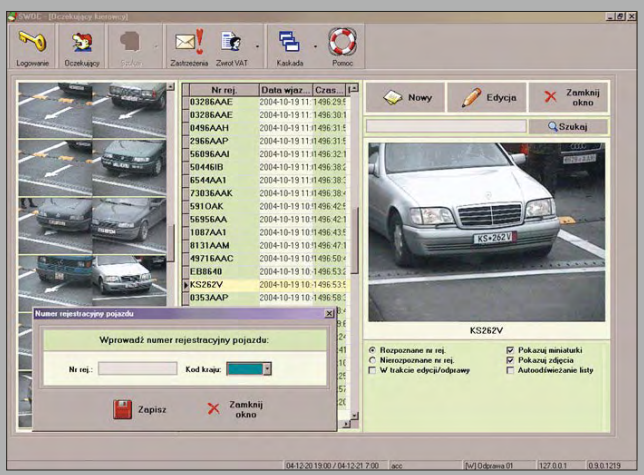
Pierwsze pilotażowe testy potwierdziły wysoką skuteczność sczytywania numerów rejestracyjnych aut, kodów kontenerów pojazdów ciężarowych i kodów kontenerów kolejowych, która wedle zaleceń Unii Europejskiej ma wynosić nie mniej niż 95 procent.



Rys. 1. Automatyczne sczytywanie przez kamerę numeru rejestracyjnego pojazdu i zapisanie go w bazie



Rys 2. Rejestracja kodu kontenera na przejściu granicznym



Rys 3. Skuteczność sczytywania tablic rejestracyjnych na przejściach granicznych ma wynosić nie mniej niż 95 procent

– *Oddziały celne zostały wyposażone w dobre narzędzie, które pozwala im w jeszcze lepszy niż dotychczas sposób realizować przypisane zadania. Wdrożenie systemu TF-OCR pozwoliło w dużym stopniu ujednolicić zasady postępowania w obsłudze ruchu granicznego, a w dłuższej perspektywie pozwoli ograniczyć liczbę narzędzi wykorzystywanych w codziennej pracy przez funkcjonariusza celnego* – ocenia Grzegorz Smogorzewski, zastępca dyrektora w Departamencie Służby Celnej Ministerstwa Finansów.

System TF-OCR został zainstalowany na 13 przejściach granicznych z Ukrainą, Białorusią i Rosją, w tym na dziesięciu przejściach drogowych i osobowych (Bezledy, Bobrowniki, Kuźnica Białostocka, Dorohusk, Hrebenne, Sławatycze, Koroszyn, Korczowa, Medyka, Krościenko) oraz trzech kolejowych (Kuźnica Białostocka, Medyka, Dorohusk).

Z nowego sprzętu na polskich przejściach korzystać będzie potężna grupa pograniczników, która w momencie wejścia w życie układu z Schengen miała wynosić ponad 10 tysięcy. Wkrótce przed nimi kolejne wyzwanie, którym będzie zniesienie kontroli celnej na lotniskach. Jest ono planowane na marzec 2008 roku.

Bezpośr. inf. T4B

Standaryzacja bezpieczeństwa granic i inne projekty – relacja z seminarium PIAP

„Monitorowanie i wspomaganie bezpieczeństwa”

8 stycznia 2008 roku w Przemysłowym Instytucie Automatyki i Pomiarów (**PIAP**) w Warszawie odbyło się seminarium pt. **„Monitorowanie i wspomaganie bezpieczeństwa”**, poświęcone rozwiązaniom systemów monitorowania i wspomagania bezpieczeństwa w ruchu granicznym oraz międzynarodowym transporcie drogowym i kolejowym. Podstawą tych rozwiązań są prace realizowane przez PIAP w następujących projektach międzynarodowych:

- **STABORSEC** (*Standards for Border Security Enhancement*),
- **TRIPS** (Transport Infrastructure Protection System),
- **RIPCORD-ISEREST** (*Road Infrastructure Safety Protection – Core Research and Development for Road Safety in Europe*).

W prezentacjach, których autorami byli pracownicy PIAP: Artur Wieczyński, Arkadiusz Perski, Piotr Szynkarczyk i Marzena Baczyńska oraz Piotr Pęksa z samodzielnego Pododdziału Antyterrorystycznego Policji w Poznaniu, omówiono, na przykładach realizowanych projektów, podstawowe zagrożenia bezpieczeństwa i sposoby ich detekcji oraz neutralizacji. Seminarium prowadził Stanisław Kaczanowski – Zastępca Dyrektora ds. Badawczo-Rozwojowych instytutu. Pierwsze dwa projekty omówił Artur Wieczyński, a ostatni – Arkadiusz Perski.

Projekt **STABORSEC**, który ma zakończyć się w lipcu br., jest poświęcony standardom dotyczącym zwiększenia bezpieczeństwa granic. Prowadzony jest przy współudziale różnych instytucji europejskich, w tym służb granicznych Wielkiej Brytanii i Malty, które wnoszą swoje cenne doświadczenia dotyczące bezpieczeństwa granic morskich. Celem projektu jest ocena stanu standaryzacji działań służb granicznych Unii Europejskiej, zarówno pod względem urządzeń, jak i procedur. Przewidywane rezultaty prowadzonego projektu obejmują m.in. stworzenie listy istniejących standardów dotyczących ochrony granic, dokonanie oceny zakresu niezbędnych zmian i uzupełnień tych standardów oraz określenie technologii służących do zapewnienia bezpieczeństwa granic, do

czego przewiduje się wykorzystanie rezultatów innych projektów europejskich.

Kluczowe technologie, którymi zajmują się uczestnicy projektu, są związane z:

- detektorami (w dwóch kategoriach: materiałów wybuchowych, narkotyków i broni oraz ludzi, pojazdów i przedmiotów),
- biometrią – na potrzeby zwalczania nielegalnej imigracji oraz do kontroli przemieszczania się osób,
- bezpieczną łącznością pomiędzy służbami,
- bazami danych (w zakresie integralności i kontroli dostępu do danych),
- bezpiecznym i szybkim dostępem do danych.

Polsce, która posiada najdłuższe granice z krajami nie należącymi do Unii Europejskiej, w tym trudne do zabezpieczenia granice górskie oraz morskie, przypadła szczególna rola. Przez nasz kraj przechodzą także trzy główne korytarze transportowe (Via Baltica do Estonii i Finlandii, trasa do Moskwy oraz do Kazachstanu i Chin), co nie jest bez znaczenia dla zapewnienia harmonijnego ruchu granicznego. W tym celu, zgodnie z opracowanymi zasadami monitorowania przekraczania granicy (ang. *Crossborder Monitoring*), należy wyposażyć zarówno pojazdy przewożące ładunki i przekraczające granicę, jak i służby graniczne, w odpowiednie urządzenia.

Przykładem takich urządzeń pojazdowych mogą być moduły elektroniczne, dostarczające informacji o kontenerach, w tym danych dotyczących lokalizacji, uzyskiwanych dzięki systemowi GPS i przekazywanych na bieżąco, z wykorzystaniem systemów GSM oraz łączności satelitarnej, do Centrum Kontroli. Takie dane, w celu wspomagania obsługi granicznej, powinny być automatycznie przekazywane do raportów kontroli granicznej, co obecnie nie jest jeszcze uwzględnione w standardach. Istnieją natomiast standardy dotyczące elektronicznych plomb kontenerowych (ang. *Fright Containers Electronic Seals*), w tym dwa standardy komunikacyjne, opisujące zasady łączności urządzeń RFID działających na często-

tliwościach 2,45 GHz oraz w paśmie GSM 860-960 MHz, odpowiednio:

– ISO/IEC 18000-4:2004 (Information technology - radio frequency identification for item management - Part 4: Parameters for air interface communications at 2,45 GHz)

i

– ISO/IEC 18000-6:2004 (Information technology - radio frequency identification for item management - Part 6: Parameters for air interface communications at 860 to 960 MHz).

Projekt **TRIPS** dotyczył systemu zabezpieczenia kolejowych sieci transportowych na trasach europejskich Wschód-Zachód, w tym aspektów związanych z terrorystycznymi zagrożeniami bezpieczeństwa. Wykorzystywał zaawansowane technologie, takie jak monitoring satelitarny przy użyciu satelitów INMARSAT D+ i systemów GSM, technologię GIS (System Informacji Geograficznej, ang. *Geographic Information System*) oraz autonomiczne systemy decyzyjne. W ramach projektu TRIPS, podczas pokazu na poligonie pod Paryżem, zaprezentowano unikatowe rozwiązanie PIAP – mobilnego robota neutralizująco-wspomagającego Expert, który może służyć do wyszukiwania niebezpiecznych materiałów i uzyskał tam bardzo dobre oceny. Urządzenie to, jako pierwsze na świecie, wykonuje swoje zadania we wszystkich środkach transportu, a także w małych i ciasnych pomieszczeniach. Ochronie przed atakami terrorystycznymi służy także urządzenie brytyjskiej firmy Smith Detection do rozpoznawania substancji chemicznych, również uwzględnione w projekcie.

Celem trzeciego z zaprezentowanych projektów – **RIPCORD-ISEREST** – było także, podobnie jak w przypadku TRIPS, podniesienie bezpieczeństwa na trasach Wschód-Zachód – tym razem w odniesieniu do infrastruktury drogowej. W prezentacji największy nacisk położono na omówienie polskiej części tego projektu – badań PIAP nad możliwościami prognozowania (z wykorzystaniem modeli matematycznych) wpływu zastosowania środków związanych z konstrukcją tras drogowych (modyfikacji dróg) na poprawę bezpieczeństwa. Wskaźnikami była tu liczba ofiar śmiertelnych oraz hospitalizowanych w wyniku wypadków drogowych na określonym odcinku reprezentatywnej drogi II kategorii (drogi wojewódzkiej nr 719) o dużym natężeniu ruchu. W ramach badań zebrano dane na temat zdarzeń drogowych z czterech lat, a następnie wykorzystano je w badaniach symulacyjnych, prowadzonych z wykorzystaniem narzędzi programistycznych DST (precyzyjne narzędzie do wspierania decyzji, ang. *Decision Support Tool*) i SEROES Expert System, przygotowanych przez zagranicznych partnerów PIAP. Podano wyniki analiz DST, pokazujące m.in. na ile może zmniejszyć się śmiertelność wśród ofiar wypadków drogowych dzięki zastosowaniu takich środków zaradczych, jak np. budowa chodnika dla pieszych, obniżenie nachylenia drogi czy wybudowanie barier ochronnych. Jednym z wniosków jest budujące stwierdzenie, że „istnieją już bardzo nowoczesne narzędzia, dzięki którym jeszcze na poziomie projektu można analizować warianty poprawy bezpieczeństwa drogowego".

Adam Bułaciński, Redakcja

Partnerstwo kluczem do bezpieczeństwa europejskiego sektora finansowo-bankowego

Przedstawiciele czołowych europejskich instytucji finansowych spotkali się niedawno w Londynie na sympozjum „Bezpieczeństwo Finansowe 2007" (2007 *Financial Security Symposium*), na którym dyskutowano na temat bezpieczeństwa sektora. Zdaniem zebranych odpowiedzią na coraz większe wyrafinowanie i międzynarodowy charakter działalności przestępczej powinno być zacieśnienie współpracy między firmami, organami regulacyjnymi i organami ochrony porządku publicznego.Konferencji przewodniczył Sir Chris Fox, były prezes brytyjskiego Stowarzyszenia Komendantów Policji (*Association of Chief Police Officers*). – *Zagrożenia dla bezpieczeństwa szybko zmieniają swoje oblicze wraz ze zmianą oferty instytucji finansowych* – stwierdził. – *Nadal mamy do czynienia z konwencjonalnymi zagrożeniami w postaci kradzieży z bronią w ręku, porwań i napadów na konwoje z pieniędzmi, jednak obecnie w większym stopniu skupiamy uwagę na wzroście zagrożeń o charakterze niematerialnym, takich jak kradzież tożsamości czy oszustwa*.

– *Internet sprawił, że świat stał się mniejszy. Znajdując się w Rosji lub Nigerii, można popełnić przestępstwo w miejscu oddalonym o tysiące kilometrów. Zagrożenie ma wyrafinowany charakter i dotyczy w równym stopniu instytucji i osób fizycznych. Konferencja umożliwiła spotkanie decydentów z europejskich instytucji finansowych w celu wymiany doświadczeń i pomocy w przeciwdziałaniu zmieniającym się zagrożeniom* – powiedział Chris Fox.

Ankieta przeprowadzona wśród delegatów wykazała, że prawie trzy czwarte z nich (74%) za największe zagrożenie dla bezpieczeństwa sektora uznaje kradzież tożsamości i oszustwa. Są oni także przekonani, że w ostatnich latach najważniejszym osiągnięciem technologii w dziedzinie poprawy bezpieczeństwa był rozwój elektronicznych systemów zabezpieczających przed kradzieżą tożsamości i oszustwami, a także coraz szersze zastosowanie telewizji dozorowej.

Dwie trzecie delegatów (66%) stwierdziło, że głównym czynnikiem wpływającym na kształtowanie strategii bezpieczeństwa były coraz bardziej wyrafinowane typy zachowań przestępczych. Opinie co do najlepszych sposobów zapewnienia bezpieczeństwa w przyszłości były jednak podzielone. Najczęściej wskazywano na konieczność wprowadzenia w niektórych krajach dowodów tożsamości, dalszy rozwój zabezpieczeń w bankowości w trybie online, a także surowsze karanie osób popełniających przestępstwa. Podkreślano także potrzebę lepszej wymiany informacji między instytucjami.

Martin Gill, profesor kryminologii z University of Leicester w Wielkiej Brytanii, wskazał na potrzebę poznawania motywów, które skłaniają ludzi do popełniania przestępstw. – *Bardzo ważne w zrozumieniu powodów popełniania przestępstw są rozmowy z ich sprawcami. Poznając sposób ich myślenia, możemy opracować najlepsze metody działania* – stwierdził Martin Gill.

– *Często, kiedy porównuję to, co mówią sprawcy przestępstw, z tym, co robią firmy, dostrzegam istotne luki* – kontynuował profesor Gill. – *Instytucje często opracowują swoje strategie bezpieczeństwa, posiadając niewielką wiedzę na temat rzeczywistych zagrożeń. Konieczne jest natomiast, aby dysponowały przemyślanymi i dojrzałymi strategiami, które zostały przetestowane w realnych warunkach pod kątem skuteczności działania*.

– *Zagrożenia dla bezpieczeństwa mają rzeczywisty wpływ na sektor finansowo-bankowy* – powiedział Ron Krisanda, prezes firmy ADT na Europę, Bliski Wschód i Afrykę. – *Na przykład straty poniesione na skutek użycia w bankomatach nielegalnie skopiowanych kart płatniczych przekroczyły w 2006, w całej Europie, kwotę 306 milionów euro. Mimo że opracowaliśmy nowe rozwiązania, które mają pomóc w opanowaniu tego typu problemów, wymiana doświadczeń w ramach sympozjum dowodzi, że żadna osoba, firma lub instytucja sama nie znajdzie odpowiedzi na wszystkie zagrożenia. Aby zapewnić sobie skuteczniejszą ochronę, instytucje finansowe powinny tworzyć struktury służące szybkiej wymianie informacji i bliżej ze sobą współpracować*.

Więcej informacji na temat sympozjum „Bezpieczeństwo Finansowe 2007" zorganizowanego pod patronatem firmy ADT – w tym wywiady dźwiękowe z najważniejszymi prelegentami – można znaleźć na stronie www.adt.co.uk/financial.

Bezpośr. inf. ADT Poland

Esprit TI – wejdź z Pelco w świat termowizji!

Wszystkim poszukującym skutecznych, nowoczesnych rozwiązań w dziedzinie telewizji dozorowej **Pelco** chce przedstawić swój nowy produkt – **termowizyjny system kamerowy Esprit TI** (**ES30TI**). Obserwując dowolne przedmioty, struktury i konstrukcje, takie jak mosty, rurociągi, zapory wodne, elektrownie, stacje energetyczne, baseny portowe lub pasy graniczne, Esprit TI jest w stanie wychwycić nawet niewielkie zmiany temperatury. Dzięki temu w sposób natychmiastowy można wykryć ludzi, zwierzęta, punktowe wycieki lub np. obszary przegrzania materiału. Termowizja pozwala wykryć intruza znacznie wcześniej, niż uczyni to standardowa kamera lub oko ludzkie. System kamerowy Esprit TI wykonuje obserwacje w całkowitej ciemności, we mgle, w zadymieniu, poprzez przesłony z folii, wewnątrz i na zewnątrz.

Produkty serii ES30TI to połączenie nowoczesnej kamery termowizyjnej z systemem pozycjonowania Esprit. W rezultacie klient otrzymuje całkowicie zintegrowany termowizyjny system PTZ. Wewnątrz ES30TI znajduje się kamera pracująca w zakresie fal długich podczerwieni (ang. *Long Wave Infrared* – LWIR), zbudowana z wykorzystaniem mikrobolometru (przyrządu do pomiaru energii promieniowania) z tlenkiem wanadu jako materiałem aktywnym detektora. Warto podkreślić, że, w odróżnieniu od znacznie droższych matryc HgCdTe, wymagających znacznego chłodzenia, mikrobolometry pracują bez chłodzenia, w temperaturze otoczenia.

Kamera dostarcza obraz o rozdzielczości 320 x 240 z rozmiarem piksela 38 μm. Dostępne jest dwukrotne powiększenie cyfrowe.

Inne właściwości:

- czułość poniżej 40 mK przy F1,0;
- ustawienia kamery definiowane przez użytkownika;
- wyświetlanie na obrazie parametrów obrotu, pochylenia i powiększenia zoom;
- zintegrowany wieloprotokołowy odbiornik;
- 3 obiektywy do wyboru: 14,25 mm, f/1,3; 35 mm, f/1,4; 50 mm, f/2,0.

Więcej informacji można uzyskać u dystrybutorów Pelco w Polsce. Karta katalogowa jest dostępna na stronie internetowej Pelco http://www.pelco.com.

Bezpośr. inf. Pelco

Spotkanie członków ESBOC

W dniach 30 listopada – 1 grudnia 2007 r. w Ośrodku Wypoczynkowym „Majak" w Senec k/Bratysławy (Słowacja) odbyło się robocze spotkanie członków Klubu Europejskich Organizacji Branży Ochrony /**ESBOC**/.

W spotkaniu udział wzięli przedstawiciele Czech, Polski, Słowacji i Węgier.

Polską Izbę Ochrony Osób i Mienia reprezentowali: prezes zarządu Sławomir Wagner, wiceprezes zarządu Marcin Pyclik, dyrektor biura zarządu Zenon Parchimowicz oraz radca prawny Izby mecenas Jan Rybczyński.

Spotkaniu przewodziła delegacja czeska, która pełni obecnie rolę lidera Klubu.

Podczas spotkania dokonano następujących ustaleń:

1. Przedstawicielstwo czeskie do końca 2007 r. zamieści w Internecie stronę WWW Klubu w języku angielskim, a państwa członkowskie utworzą strony w rodzimym języku.
2. Przyjęto postanowienie o rozszerzeniu szeregów Klubu. Węgry podejmą działania w celu pozyskania Austrii, Włoch, Rumunii i Słowenii, natomiast Polska – Estonii, Litwy, Łotwy oraz Niemiec.
3. Powołano komisję ds. standaryzacji, której koordynatorem będzie dyrektor biura zarządu Polskiej Izby Ochrony Osób i Mienia – Zenon Parchimowicz.
4. Powołano komisję ds. zorganizowania Centrum Informacyjnego ESBOC na wniosek przedstawicielstwa czeskiego. Projekt nadzoruje dr Frantiszek Brabec.
5. Powołano komisję do rozmów z Unią Europejską, której przewodzić będzie przedstawicielstwo węgierskie.
6. Upoważniono przedstawicielstwo czeskie i słowackie do uzyskania informacji w zakresie dotacji z funduszy Klubu Wyszehradzkiego.
7. Ustalono, że do końca stycznia 2008 r. członkowie ESBOC prześlą do lidera Klubu informację o zamierzonych działaniach na najbliższy okres.

Spotkanie zakończono wyborem nowego lidera Klubu.

Od 1 stycznia 2008 r. liderem klubu ESBOC będzie Polska Izba Ochrony Osób i Mienia.

Opracował
Zenon Parchimowicz
dyrektor biura zarządu PIOOiM

Nowy system szybkiego pozycjonowania firmy Bosch: od 0 do 100 stopni w 1 sekundę!

Nowy system szybkiego pozycjonowania firmy Bosch, charakteryzujący się zaawansowanymi właściwościami użytkowymi oraz wysoką jakością, przeznaczony jest do wymagających zastosowań w instalacjach dozorowych. System bazujący na głowicy uchylno-obrotowej o wysokiej prędkości umożliwia montaż modułu kamery z automatycznym ogniskowaniem oraz różnych zestawów kamer o wysokiej rozdzielczości i obiektywów zoom. Wszystkie elementy są umieszczone w trwałej obudowie wykonanej z poliwęglanu oraz aluminium.W trybie ręcznym ciągły obrót w zakresie 360° z prędkością maks. 100°/s jest uzupełniany możliwością pochylania z prędkością do 40°/s. Zakres pochylenia od –90° do +40° umożliwia obserwację ponad horyzontem. Szybki ruch sterowany ręcznie odznacza się płynnością, ponieważ prędkości obrotu i pochylenia są automatycznie dostosowywane do krotności zoomu. Funkcje automatycznego obrotu oraz patrolowania są wyjątkowo precyzyjne i umożliwiają przywołanie położeń zaprogramowanych z dokładnością do 0,02°. Do sekwencji patrolowania oraz automatycznego obrotu można przypisać różne prędkości (maks. 40°/s dla obrotu, 30°/s dla pochylenia). Istnieje także możliwość skonfigurowania obszarów maskowania.

Rozwiązanie jest bardzo elastyczne i umożliwia dostosowanie systemu do różnych zastosowań. Firma Bosch oferuje kompletną gamę modeli kamer oraz obiektywów zoom, m.in. zoptymalizowane zestawy kamery Dinion i obiektywów. Kamera Dinion, generująca ostry i wyraźny obraz o najwyższej jakości, jest doskonałym uzupełnieniem systemu szybkiego pozycjonowania.

Obsługa wielu protokołów, łącznie z protokołami Bilinx i Bi-phase opracowanymi przez firmę Bosch, sprawia, że nowy system szybkiego pozycjonowania jest łatwy w obsłudze oraz integracji z istniejącymi systemami. Instalacja i konserwacja jest bardzo prosta ze względu na trwałą, aerodynamiczną obudowę, która całkowicie ukrywa system w swoim wnętrzu. Osłona przeciwsłoneczna stanowi dodatkową ochronę przed niesprzyjającymi warunkami pogodowymi i promieniami słonecznymi. Dodatkowo dostępne są wersje z wycieraczką oraz opcjonalnym spryskiwaczem.

System szybkiego pozycjonowania firmy Bosch, odporny na trudne warunki środowiskowe, jest wszechstronnym rozwiązaniem dozorowym, odznaczającym się wysoką jakością, szybkością działania oraz zaawansowanymi właściwościami użytkowymi.

Bezpośr. inf. Bosch Security Systems

Kalendarz targów 2008
(02-12-2008)

LUTY

12.02-15.02
SECURITY 2008
15-th International Specialised Exhibition
and Seminar for Security, Safety, Protection
Sofia, Bułgaria
www.bcci.bg/fairs/security
e-mail: fairs@bcci.bg

26.02 –29.02
SICUR
International Security, Safety and Fire Exhibition
Madryt, Hiszpania
e-mail: sicur@ifema.es
www.sicur.ifema.es

MARZEC

04.03-07.03
SECURITY SHOW 2008 (16th edition)
International Exhibition Center Tokyo Big Sight
Tokio, Japonia
e-mail: info@securityshow.jp
www.securityshow.jp

09.03-12.03
INTERNATIONAL HARDWARE FAIR/PRACTICAL WORLD
Kolonia, Niemcy
e-mail: info@koelnmesse.pl
www.hardwarefair.com

11.03-12.03
FIREX SOUTH 2008
Sandown Park, Wielka Brytania
e-mail: ppoole@cmpi.biz
www.firexroadshows.co.uk

14.03-16.03
PREWENCJA
IV Targi Zabezpieczeń i Ochrony Mienia
Szczecin
e-mail: piotrowska@mts.pl
www.mts.pl

KWIECIEŃ

02.04-04.04
ISC WEST 2008
Las Vegas, USA
e-mail: inquiry@isc.reedexpo.com
www.iscwest.com

03.04-06.04
ISAF FAIR 2008
Ankara, Turcja
e-mail: marmara@marmarafuar.com.tr
www.ankara.isaffuari.com

8.04-10.04
INTERTELECOM
XIX Międzynarodowe Targi Komunikacji Elektronicznej
Łódź
e-mail: intertelecom@mtl.lodz.pl
www.mtl.lodz.pl

14.04-17.04
MIPS
14th Moscow International Exhibition
Protection, Security & Fire safety
Moskwa, Rosja
e-mail: security@ite-expo.ru
www.mips.ru

16.04-18.04
SECUTECH EXPO 2008
11th Asian Security Week
Taipei World Trade Centre, Taiwan
e-mail: int'l@asmag.com
www.secutech.com

21.04-24.04
EXPOSECURITY 2008
Bukareszt, Rumunia
e-mail: m.dicianu@romexpo.org
www.exposecurity.ro

22.04-25.04
SECUREX 2008
Międzynarodowa Wystawa Zabezpieczeń
Poznań
e-mail: securex@mtp.pl
www.securex.mtp.pl

22.04-25.04
SAWO
XIX Międzynarodowe Targi Ochrony Pracy,
Pożarnictwa i Ratownictwa
Poznań
e-mail: sawo@mtp.pl
www.sawo.mtp.pl

MAJ

12.05-15.05
IFSEC 2008
NEC Birmingham, Wielka Brytania
e-mail: kjohnstone@cmpi.biz
www.ifsec.co.uk

27.05-30.05
SECUREX 2008
International Trade Exhibition of Labour Safety,
Fire Protection and Security
Budapeszt, Węgry
e-mail: info@hungexpo.hu
www.securex.hu

Kalendarz targów 2008

(02-12-2008)

CZERWIEC

04.06-06.06
SECURITEX 2008
10th Asian International Security, Safety and Fire Protection Show & Conference
Hong Kong, Chiny
e-mail: exhibit@hkesallworld.com
www.asiansecuritex.com

11.06-13.06
INFOSYSTEM
Informatyka dla budownictwa i nieruchomości
Poznań
e-mail: infosystem@mtp.pl
www.infosystem.pl

25.06-27.06
BALT-MILITARY-EXPO
Bałtyckie Targi Militarne
Gdańsk
e-mail: military@mtgsa.com.pl
www.baltmilitary.pl

WRZESIEŃ

08.09-11.09
MSPO
XVI Międzynarodowy Salon Przemysłu Obronnego
Kielce
e-mail: mspo@targikielce.pl
www.targikielce.pl

8.09-11.09
LOGISTYKA
XIV Międzynarodowe Targi Logistyczne
Kielce
e-mail: logistyka@targikielce.pl
www.targikielce.pl

30.09 – 03.10
SKYDD 2008
Security, Fire&Rescue Expo
Sztokholm, Szwecja
e-mail: magnus.eriksson@stofair.se
www.skydd.stofair.se

PAŹDZIERNIK

03.10-04.10
CŁO I GRANICA 2008
XIII Międzynarodowa Wystawa Wyposażenia dla Kontroli Celnej i Granicznej
Warszawa
e-mail: ztw@ztw.pl
www.brsa.pl

07.10–10.10
SECURITY ESSEN 2008
The World Forum for Security and Fire Prevention
Essen, Niemcy
e-mail: info@messe-essen.de
www.security-messe.de

LISTOPAD

04.11-07.11
EXPOPROTECTION
International Exhibition of Risks Management
Paryż, Francja
e-mail: patricia.jacquot@reedexpo.fr
www.expoprotection.com

05.11-06.11
ALARM
IX Konferencja i Wystawa Monitoringu Wizyjnego
Kielce
e-mail: alarm@targikielce.pl
www.targikielce.pl

05.11-06.11
SPORT OBIEKT
VIII Wystawa Wyposażenia i Budowy Obiektów Sportowych
Kielce
e-mail: figrski.g@targikielce.pl
www.targikielce.pl

19.11-20.11
SECTECH
Expo & Seminars
Kopenhaga, Dania
e-mail: info@armedia.se
www.sectech.dk

25.11-28.11
SICUREZZA
Mediolan, Włochy
e-mail: Daniela.pitton@fieramilanotech.it
www.sicurezza.it

GRUDZIEŃ

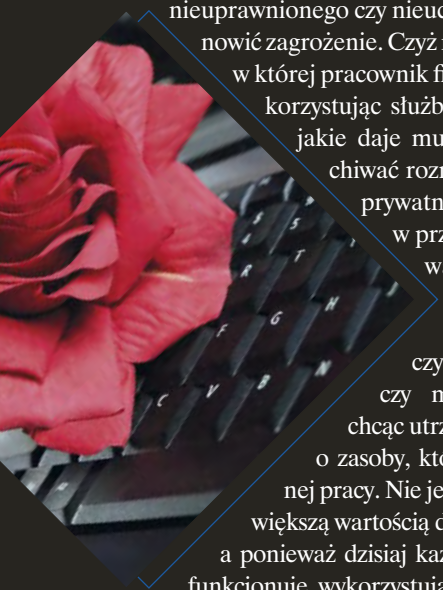
05.12-06.12
KARTA 2008
Międzynarodowa Wystawa Producentów i Użytkowników Kart i Systemów Kartowych
Warszawa
e-mail: milewska@ztw.pl
www.karta.info.pl

Uwaga! Redakcja nie ponosi odpowiedzialności za zmianę terminów targów

Wprowadzenie do zagadnienia bezpieczeństwa oprogramowania i monitorowania IT

W ostatnim czasie bardzo głośny medialnie stał się temat monitorowania informatycznego. W publikacjach prasowych z codziennych gazet oraz w reportażach telewizyjnych tematyka monitorowania została przedstawiona powierzchownie, a największy nacisk położono jedynie na możliwość poznania przez pracodawcę treści korespondencji pracowników prowadzonej przy wykorzystaniu poczty elektronicznej. Monitorowanie zostało przedstawione jako inwigilacja oraz naruszanie prywatności pracowników przedsiębiorstw. Przeglądanie przez pracodawcę poczty elektronicznej, analiza stron WWW odwiedzanych przez pracowników w godzinach pracy, przeglądanie bilingów rozmów telefonicznych przeprowadzonych z telefonów służbowych potraktowano jako naruszanie prywatności zatrudnionego

Tak słowo „monitorowanie" kojarzy się wielu z nas, co jest jednak błędnym rozumieniem przedmiotu. Oczywiście istnieją narzędzia umożliwiające stosowanie tego rodzaju praktyk, jednak należy pamiętać o tym, iż każde narzędzie w rękach nieuprawnionego czy nieuczciwego człowieka może stanowić zagrożenie. Czyż nie ma tu analogii do sytuacji, w której pracownik firmy telekomunikacyjnej, wykorzystując służbowy sprzęt oraz możliwości, jakie daje mu pracodawca, może podsłuchiwać rozmowy prowadzone z naszego prywatnego telefonu? Podobnie jest w przypadku systemów monitorowania teleinformatycznego.



Właściciel każdego podmiotu, niezależnie od tego, czy jest to jednoosobowa firma, czy międzynarodowa korporacja, chcąc utrzymać się na rynku, musi dbać o zasoby, które wykorzystuje do codziennej pracy. Nie jest tajemnicą, że aktualnie największą wartością dla organizacji jest informacja, a ponieważ dzisiaj każda, nawet najmniejsza firma funkcjonuje wykorzystując nowoczesne techniki teleinformatyczne, naturalną konsekwencją jest konieczność ochrony tych zasobów. Zjawisko wywiadu gospodarczego nie jest już tworem rodem z powieści kryminalnych, lecz faktem, o którym co jakiś czas mamy okazję usłyszeć lub przeczytać w mediach. Każdy dba zarówno o sprzęt informatyczny będący na wyposażeniu firmy, jak i o informację przetwarzaną na tym sprzęcie, która w niepowołanych rękach mogłaby być przyczyną ogromnych strat. Strat tych nierzadko nie jesteśmy w stanie przeliczyć na pieniądze, dopóki chroniona informacja nie ujrzy światła dziennego.

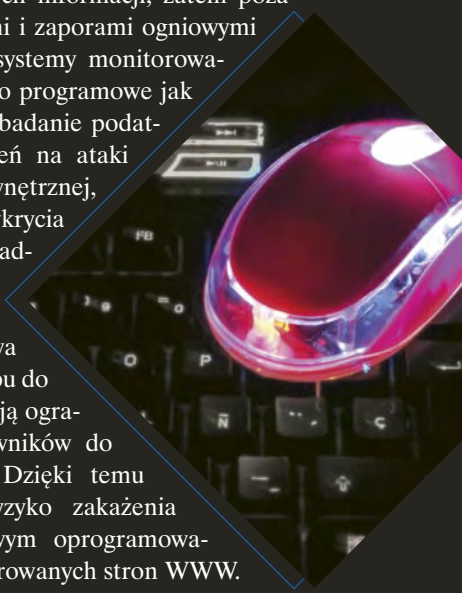
W zależności od wielkości organizacji oraz specyfiki przetwarzanych informacji stosowane są różne rozwiązania w zakresie bezpieczeństwa informatycznego, mające na celu ochronę danych przed niepożądanym dostępem do nich z zewnątrz oraz wyciekiem z wewnątrz organizacji. Muszą być one jednak stosowane zgodnie ze sformalizowanymi zasadami bezpieczeństwa funkcjonującymi w danej organizacji, często nazywanymi „polityką bezpieczeństwa". Dokument dotyczący polityki bezpieczeństwa, będący zbiorem praw i obowiązków każdego użytkownika systemu informatycznego w zakresie bezpieczeństwa, powinien funkcjonować w każdym szanującym się podmiocie. Musi on między innymi jasno opisywać reguły, do których stosowania zobligowani są wszyscy użytkownicy systemu informatycznego, a konsekwencją tego jest konieczność zapoznania każdego pracownika z zapisami polityki bezpieczeństwa. Zasady te powinny zawierać również informacje o możliwości stosowania przez pracodawcę mechanizmów monitorowania – jednego z elementów polityki bezpieczeństwa – jako profilaktyki zwiększającej poziom bezpieczeństwa chronionych zasobów.

Skąd się wziął pomysł na monitorowanie? Główną ideą, która przyświecała i przyświeca twórcom systemów monitorowania,

jest dążenie do stałego podnoszenia poziomu bezpieczeństwa organizacji, w której systemy monitorowania są stosowane, a także do ograniczenia kosztów zarządzania obszarem objętym monitorowaniem. W bezpieczeństwie stosowana jest zawsze zasada ograniczonego zaufania, która odnosi się nie tylko do współpracowników zewnętrznych, ale również do własnej kadry pracowniczej. Stąd monitorowaniu informatycznemu podlega zewnętrzny styk organizacji ze światem, a w sieci wewnętrznej prowadzone są badania stanu bezpieczeństwa. W zależności od wielkości i specyfiki funkcjonowania danej organizacji wykorzystywane są różne narzędzia i metody monitorowania, jednak wspólną ich cechą zawsze powinno być ograniczenie możliwości przedostania się chronionej informacji w niepowołane ręce oraz – w przypadku wystąpienia tego typu zdarzenia – możliwość wskazania odpowiedzialnego za zaistniałą sytuację.

W niewielkich firmach jako minimum stosuje się przede wszystkim oprogramowanie antywirusowe oraz firewalle programowe lub sprzętowe, mające za zadanie ochronę zasobów przed włamaniami z zewnątrz. Dla tych rozwiązań najważniejszym parametrem umożliwiającym pełne wykorzystanie ich funkcjonalności jest ich bieżąca aktualizacja, a monitorowanie wiąże się jedynie z dbałością o jej systematyczne przeprowadzanie. Dotyczy to również systemów operacyjnych zainstalowanych na wszystkich komputerach funkcjonujących w danej sieci. Odkąd komputery zaczęły się ze sobą komunikować pracując w środowisku sieciowym, rozpoczął się nieustanny wyścig twórców systemów operacyjnych i oprogramowania zabezpieczającego komputery oraz hakerów, którzy działają pojedynczo jako „wolni strzelcy" lub coraz częściej organizują się w grupy, wyszukując luki w systemach. Cel tych działań bywa różny. Niektórzy informują o ujawnieniu luki, nazywanej również „podatnością", autorów oprogramowania, inni publikują ujawnione podatności w Internecie, a jeszcze inni zatrzymują wiedzę wyłącznie dla siebie w celu jej późniejszego wykorzystania. Kiedyś „złośliwe" oprogramowanie miało za zadanie jedynie unieruchomienie komputera lub zniszczenie znajdujących się na dyskach danych. Współczesne złośliwe oprogramowanie to skomplikowane i bardzo zaawansowane programy, mające na celu przejęcie kontroli nad zaatakowanym komputerem oraz pełną inwigilację przetwarzanych na komputerze zasobów i informacji. Wyścig ten jest na tyle szybki, że aktualności systemów nie bada się już jak niegdyś w tygodniach, lecz dniach. W przypadku aktualizacji krytycznych mówi się natomiast już o godzinach. Należy tutaj również dodać, iż konieczne jest stosowanie jedynie legalnego oprogramowania, pochodzącego z zaufanego źródła – nie tylko dlatego, że grożą nam przykre konsekwencje prawne w przypadku wykrycia wykorzystywania nielegalnego oprogramowania, ale również dlatego, że tylko takie narzędzia mogą korzystać z możliwości pełnej aktualizacji. Zasadne jest również ostrożne stosowanie różnego rodzaju oprogramowania w wersji freeware oraz shareware (szczególnie pochodzącego z wątpliwych źródeł), które kusi tym, iż jest darmowe, lecz niejednokrotnie ma dodatkowe – niewidoczne dla przeciętnego użytkownika – funkcje, umożliwiające nieautoryzowany dostęp do sieci lub niekontrolowany wypływ informacji na zewnątrz.

Im większa organizacja, tym więcej użytkowników, urządzeń sieciowych oraz przetwarzanych danych, a tym samym większe nakłady, jakie należy ponieść na zapewnienie bezpieczeństwa. W takich miejscach „ręczne" prowadzenie aktualizacji systemów antywirusowych byłoby nieefektywne, dlatego stosowane są rozwiązania automatyzujące tę czynność. Przy dużych wdrożeniach wykorzystywane są różnego rodzaju rozwiązania umożliwiające aktualizację systemów operacyjnych oraz oprogramowania antywirusowego przy wykorzystaniu zadanych harmonogramów pracy. Wykorzystuje się je po to, by z jednej strony jak najczęściej przeszukiwać strony producenta oprogramowania w poszukiwaniu nowych aktualizacji, a jednocześnie zminimalizować ryzyko nadmiernego obciążenia sieci w przypadku pojawienia się nowej „paczki" z definicjami wirusów czy nowej „łaty" dla systemu operacyjnego lub innego oprogramowania stosowanego w firmie. W dużych organizacjach kładziony jest większy nacisk na bezpieczeństwo przetwarzanych informacji, zatem poza systemami antywirusowymi i zaporami ogniowymi wykorzystywane są inne systemy monitorowania. Jedne z nich (zarówno programowe jak i sprzętowe) umożliwiają badanie podatności systemów i urządzeń na ataki prowadzone z sieci wewnętrznej, a w przypadku ich wykrycia wskazują, jakie kroki zaradcze należy podjąć, by zminimalizować ryzyko wystąpienia niebezpieczeństwa nieautoryzowanego dostępu do systemów. Inne umożliwiają ograniczenie dostępu użytkowników do zasobów internetowych. Dzięki temu zminimalizowane jest ryzyko zakażenia sieci wewnętrznej złośliwym oprogramowaniem pobranym ze spreparowanych stron WWW. Najczęściej tego typu programy umieszczane są na stronach, których przeglądanie ma niewiele wspólnego z zakresem zadań służbowych danego pracownika. Jeszcze inne wykrywają uruchomienie na danej stacji roboczej oprogramowania niezgodnego z wykazem zaakceptowanych w organizacji aplikacji (o ile taki jest opracowany). Powoduje to ograniczenie możliwości zarażenia zasobów różnego rodzaju wirusami. Użytkownicy często nieświadomie wprowadzają do sieci firmowej złośliwe oprogramowanie, uruchamiając na służbowym sprzęcie aplikacje zapisane na własnych nośnikach zewnętrznych. Takie aplikacje niejednokrotnie w szybki sposób rozprzestrzeniają się w obrębie sieci „zarażając" inne komputery lub mają ukryte dodatkowe właściwości, powodujące wysyłanie informacji znajdujących się w danej stacji roboczej na zewnątrz.



W jednym artykule nie sposób opisać wszystkich rozwiązań i możliwości, jakie dają systemy monitorowania bezpieczeństwa informatycznego. Można jedynie zasygnalizować złożoność tego zagadnienia. Należy jednak pamiętać, iż niezależnie od ilości i jakości stosowanych systemów monitorowania każdy z nich powinien być wykorzystywany zgodnie ze swoim przeznaczeniem oraz ogólnie przyjętą polityką bezpieczeństwa, gdyż w przeciwnym razie osoba z niego korzystająca może narazić się na przykre i dotkliwe konsekwencje wynikające z przepisów prawa.

Krzysztof Białek

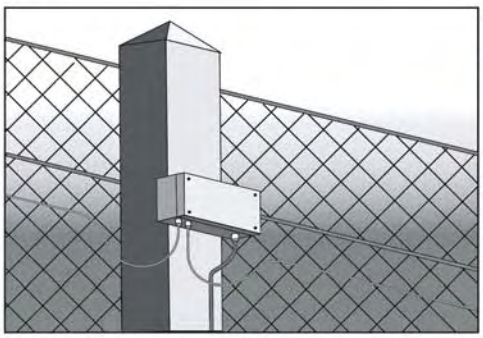
firma ATLine®

Firma ATLine spółka jawna
91-845 Łódź, ul. Franciszkańska 125
tel. +48 042 657 30 80, fax +48 042 655 20 99
e-mail: info@atline.pl
www.atline.pl

Liniowy czujnik wibracyjny na ogrodzenie
– konfiguracja na 600m:

klasa

AN 303 – sterownik czujnika wibracyjnego • 2 strefy po 300m, • 2 terminatory do zakończenia stref	1 szt. x 4 150,- zł = 4 150,- zł netto
AS 257 – kabel sensoryczny do systemu AN	600 m x 8,30 zł = 4 980,- zł netto



PIRAMID XL2
zewnętrzna, dualna czujka procesowa, z możliwością regulacji czułości PIR i MW oraz położenia.

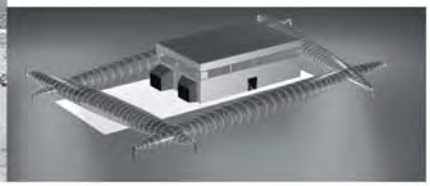
• **szeroki kąt:** SDI-76 XL2 (kąt 15m x 15m) SDI-77 XL2-A (kąt 27m x 15m) • **średni kąt:** SDI-77 XL2-B (kąt 30m x 10,5m) • **wąski kąt:** SDI-77 XL2-C (kąt 37,5m x 6m) SDI-77 XL2-D (kąt 30m x 3m)	2 830,- zł netto

ERMO 482
bariera mikrofalowa do zewnętrznej ochrony obwodowej konfiguracja na 4 strefy po 50 m:

klasa

ERMO 482/50 – zewn. bariera mikrofalowa do 50 m (nadajnik i odbiornik)	4 kpl. x 2 386,- zł = 9 544,- zł netto
PALO VERDE – słupek do bariery Ermo, ze stali nierdzewnej, malowany proszkowo • fi 60mm, h=1,9m	8 szt. x 195,- zł = 1 560,- zł netto

• ERMO 482 - bariera analogowa,
• ERMO 482X PRO - bariera cyfrowa z analią przebiegu sygnału.
Dostępne zasięgi:
50, 80, 120 lub 200 metrów.



GPS
niewidoczny, zakopywany system ochrony obwodowej

Zestaw na 1 strefę 100 m (w tym dwa kable ciśnieniowe)	22 800,- zł netto

Niewidoczny, zakopywany system GPS Plus wykrywa zmiany nacisku na grunt jakie powoduje wtargnięcie intruza w chroniony obszar. System ignoruje małe zwierzęta, ptaki i zakłócenia pogodowe, ponadto jest całkowicie nieczuły na działanie pola elektromagnetycznego. Temperatura pracy: od -40°C do +70°C.

Satel - nowe urządzenia bezprzewodowe

Wszechstronne bezpieczeństwo

Rozbudowując system ABAX o nowe urządzenia udało się nam stworzyć bezkonkurencyjny system bezprzewodowy – stanowiący idealne połączenie najwyższej klasy bezpieczeństwa, łatwej instalacji i obsługi oraz wszechstronności zastosowań.

Gamę bezprzewodowych produktów ABAX poszerzyliśmy o:

dualną czujkę ruchu **APMD-150** (na zdjęciu)
czujkę stłuczenia szyby **AGD-100**
czujkę wibracyjną **AVD-100**
czujkę zalania **AFD-100**
czujkę dymu i ciepła **ASD-100**

Jednym z owoców pracy kadry inżynierskiej firmy SATEL jest dualna czujka ruchu PIR + MW, łącząca wysoką odporność na niekorzystne warunki środowiskowe z niskim zapotrzebowaniem na energię charakterystycznym dla innych urządzeń ABAX.

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

Polskie antyterrorystyczne ROBOTY MOBILNE

Rosnące zagrożenie ze strony terrorystów oraz rozwój stosowanych przez nich technik i metod powodują wzrost wymagań i oczekiwań służb zajmujących się zapobieganiem i zwalczaniem terroryzmu wobec użytkowanych przez nich urządzeń. W odpowiedzi na taki stan rzeczy konstruktorzy z Przemysłowego Instytutu Automatyki i Pomiarów PIAP opracowali roboty mobilne o przeznaczeniu antyterrorystycznym, które zwiększają zakres wykonywanych zadań i możliwości wsparcia pracy służb zajmujących się rozminowywaniem

Roboty antyterrorystyczne przeznaczone są do wykorzystania przede wszystkim przez służby ochrony porządku i bezpieczeństwa publicznego, takie jak:
- policję (oddziały prewencji i antyterrorystyczne),
- wojsko (służby inżynieryjno-saperskie i pirotechniczne),
- służby graniczne i celne, ratownictwa i ochrony środowiska,
- oddziały obrony cywilnej,
- służby ochrony obiektów,

oraz w miejscach wymagających stałego nadzoru w celu zapewnienia bezpieczeństwa, np.:
- w portach lotniczych i samolotach,
- w portach, na przystaniach pasażerskich, na statkach i promach,
- na dworcach kolejowych i w pociągach,
- na dworcach autobusowych i w autobusach.

Typowe zastosowania robotów to:
- inspekcja, przenoszenie i neutralizacja ładunków niebezpiecznych,
- wspomaganie operacji antyterrorystycznych,
- praca w warunkach szkodliwych lub niebezpiecznych dla człowieka,
- ochrona i inspekcja obiektów.

Historia ta rozpoczęła się w roku 1999, kiedy specjaliści z Zespołu Inteligentnych Systemów Mobilnych (ZSM) Przemysłowego Instytutu Automatyki i Pomiarów w Warszawie stworzyli prototyp robota **Inspector**. Warto wspomnieć, że od początku w pracach nad projektem brali udział, w charakterze konsultantów, przyszli użytkownicy urządzenia – policyjni specjaliści pirotechnicy, którzy na każdym etapie testowali i opiniowali zastosowane rozwiązania.

Fot. 1. Robot interwencyjno-inspekcyjny Inspector

Od roku 2000 oddziały pirotechniczne polskiej policji były sukcesywnie wyposażane w roboty Inspector. Pozytywna opinia użytkowników oraz zgłaszane z ich strony uwagi, zwłaszcza dotyczące coraz to nowych potrzeb w zakresie zadań, które powinien wykonywać robot, zachęciły konstruktorów z PIAP do podjęcia prac nad budową i wdrożeniem nowej konstrukcji. W ten sposób w 2003 roku powstał prototyp robota **Expert**.

Roboty Inspector oraz Expert

Roboty Inspector oraz Expert składają się z gąsienicowej platformy mobilnej, zamontowanego na niej manipulatora z chwytakiem oraz stanowiska operatora. Są napędzane dwoma silnikami prądu stałego, zasilanymi z akumulatorów umieszczonych wewnątrz platformy mobilnej lub przez kabel z sieci 220V, i zdalnie sterowane przez operatora z użyciem komunikacji radiowej lub kablowej. W zasilanie akumulatorowe wyposażone są również stanowiska operatora i przenośne konsole sterownicze. Podobieństwa konstrukcji i rozwiązań wynikają z faktu, że oba urządzenia powstały w tym samym podstawowym celu: zastąpić człowieka w wykonywaniu niebezpiecznych zadań, związanych z rozpoznaniem i neutralizacją niebezpiecznych przedmiotów, przede wszystkim materiałów wybuchowych. Zastosowanie robota pozwala zminimalizować czas przebywania pirotechnika w strefie niebezpiecznej, a tym samym zmniejszyć ryzyko zagrożenia jego życia i zdrowia.

Oba roboty są także przystosowane do współpracy z różnymi narzędziami i urządzeniami, podnoszącymi skuteczność pracy pirotechników. Są to przede wszystkim: urządzenie rentgenowskie, wyrzutnik pirotechniczny, urządzenie do wybijania szyb, rejestratory dźwięku i obrazu. Z pomocą każdego z tych robotów wraz z wyposażeniem można dokonać m.in.: zdalnej inspekcji obiektu zagrożonego, rozpoznania niebezpiecznego ładunku, przeniesienia niebezpiecznego ładunku w wyznaczone miejsce, neutralizacji niebezpiecznego ładunku.

Robot interwencyjno-inspekcyjny Inspector jest robotem dużym (waży ponad pół tony), przeznaczonym głównie do pracy w terenie. Dzięki konstrukcji gąsienic jest w stanie pokonywać nierówności terenu oraz schody. Szerokość platformy mobilnej pozwala na przejechanie przez standardowe drzwi, co daje możliwość działania w budynkach po dostaniu się do nich robota z zewnątrz. Operator obserwuje otoczenie robota

Fot. 2. Robot neutralizująco-wspomagający Expert

za pośrednictwem czterech kamer, z których obraz wyświetlany jest na ekranie stanowiska operatorskiego. Ma także możliwość odsłuchania dźwięków przekazywanych przez mikrofon dookolny, zamontowany na robocie. Na pulpicie operatorskim pokazywana jest graficzna wizualizacja położenia ramion manipulatora, co jest szczególnie istotne, gdy robot znajduje się poza zasięgiem wzroku operatora.

Dzięki swojej dużej masie Inspector przenosi ładunki do 60 kg. Może także przeciągnąć lub przepchnąć ważący 1500 kg samochód pozostawiony na biegu lub ręcznym hamulcu.

Antyterrorystyczny robot neutralizująco-wspomagający Expert został zaprojektowany w ramach projektu celowego dawnego KBN, a obecnie MNiSW. W czasie prac projektowych konstruktorzy konsultowali się ze specjalistami z policji, BOR, Pionu Bezpieczeństwa Portu Lotniczego Okęcie i Straży Granicznej.

Expert, jako pierwszy tego typu robot na świecie, został opracowany specjalnie do działań prowadzonych we wszystkich środkach transportu, np. w samolotach, autobusach, wagonach kolejowych, na okrętach, a także w małych i ciasnych pomieszczeniach.

Robot Expert, wysłany w rejon zagrożony wybuchem bomby (lub np. w rejon skażony chemicznie) zamiast człowieka, może dokonać m.in.: zdalnej inspekcji obiektu zagrożonego, rozpoznania niebezpiecznego ładunku, przeniesienia niebezpiecznego ładunku w wyznaczone miejsce, neutralizacji niebezpiecznego ładunku, negocjacji z terrorystami.

Wymiary bazy mobilnej zostały dobrane w taki sposób, aby umożliwić poruszanie się między rzędami foteli w samolocie lub autobusie oraz w przedziale wagonu kolejowego, zaś manipulatora i chwytaka tak, by ich prawie trzymetrowy zasięg obejmował zarówno powierzchnię podłogi pod fotelami, jak i górne półki i schowki na bagaże. Pociągnęło to za sobą konieczność zastosowania stabilizatorów poprzecznych w postaci rozkładanych skrzydełek, które bądź blokują bazę mobilną robota, rozpierając się pod siedziskami foteli, bądź podpierają się o podłoże, zapobiegając przewróceniu robota podczas manipulowania wyciągniętym ramieniem.

Unikatowość robota Expert polega na tym, że nie tylko jest w stanie samodzielnie wjechać do wnętrza samolotu czy pociągu, ale także, podobnie jak Inspector, pokonuje schody i nierówności terenu, może podjechać po pochylni lub pasie do transportu bagażu i dokonać jego szczegółowej inspekcji przy pomocy swoich sześciu kamer i mikrofonu, daje operatorowi możliwość otwarcia zamkniętych schowków bagażowych i drzwi, a przede wszystkim wyniesienia podejrzanego przedmiotu na zewnątrz. Ważący ok. 200 kg Expert podnosi ładunki o masie 5–15 kg, jednak mniejszą niż Inspector „siłę" rekompensuje znacznie większymi możliwościami operacyjnymi.

Urządzenie Explorer

Kolejnym produktem opracowanym w PIAP jest urządzenie inspekcyjne Explorer, pozwalające uzyskać ocenę wizyjną miejsc trudnodostępnych lub niebezpiecznych. Urządzenie składa się z wysięgnika teleskopowego o regulowanej długości od 0,7 do 1,7 metra oraz dodatkowego wysięgnika teleskopowego o długości 4,2 m. Na wysięgnikach tych umieszczana jest kamera kolorowa wraz ze zdalnie sterowaną głowicą, umożliwiającą ruch o 180 stopni. Dodatkowo oświetlacze diodowe kamery umożliwiają pracę urządzenia w warunkach ograniczonej widoczności. Moduł wizualizacji znajduje się w specjalnej kamizelce operacyjnej, którą nosi operator. Obraz, prezentowany na ciekłokrystalicznym monitorze modułu wizualizacji, może być nagrywany na zewnętrznym rejestratorze lub przesyłany do odbiorników zdalnych. Urządzenie cechuje się dużą uniwersalnością, jest lekkie i łatwe w obsłudze.

Fot. 3. Urządzenie inspekcyjne Explorer

Zastosowania urządzenia Explorer są szerokie. Urządzenia te są wykorzystywane, co jest szczególnie ważne, przez polską policję i Biuro Ochrony Rządu. Ważne jest również zakupienie Explorera przez jednostki bezpieczeństwa Litwy, gdyż buduje zaufanie nie tylko polskich odbiorców do tego urządzenia. Z kolei służby bezpieczeństwa portów stosują urządzenie do inspekcji portów, statków i pojazdów transportowych. Zastosowanie urządzenia Explorer do pracy w przemyśle

stwarza duże szanse obniżenia kosztów obsługi maszyn i usuwania ewentualnych szkód powstałych w wyniku awarii maszyny.

Wymierne i niewymierne efekty użytkowania urządzenia Explorer są oczywiste. Policja uzyskała narzędzie, które może zostać użyte nie tylko do zadań prewencyjnych, ale i do bezpośrednich działań szturmowych – rozpoznawczych jak i antyterrorystycznych. Dzięki temu znacznie wzrosło bezpieczeństwo pracy osób, które wszystkie czynności inspekcyjne wykonywały narażając zdrowie lub życie. Służby nadzoru i dozoru uzyskały znacznie większe bezpieczeństwo pracy i inspekcji obiektów, wykonywanej nierzadko z narażeniem życia. W przemyśle zwiększa się szybkość diagnozowania groźnych uszkodzeń urządzeń produkcyjnych oraz szybkość inspekcji urządzeń i liczników. W pewnym znanym nam przypadku czas inspekcji skrócił się z 40 min do zaledwie 5 min, a więc aż ośmiokrotnie.

W 2004 roku PIAP rozpoczął prace nad nowym robotem, przeznaczonym do wspierania akcji antyterrorystycznych. Robot miał umożliwić zdalną inspekcję rejonów zagrożenia, w szczególności w małych przestrzeniach, takich jak np. podwozia pojazdów lub miejsca pod fotelami w autobusach. Drugim ważnym czynnikiem, który miał wpływ na konstrukcję robota, była chęć uzyskania niskiej ceny urządzenia. W efekcie dotychczasowych prac nad projektem powstał prototyp robota przeznaczony do badań i analizy wykorzystania małych robotów mobilnych w akcjach antyterrorystycznych. Robot będzie stanowił konkurencję dla innych robotów w swojej klasie o podobnych gabarytach. Tak powstał prototyp robota **Scout**.

Robot Scout

Robot Scout charakteryzuje się małymi rozmiarami, umożliwiającymi poruszanie się w ciasnych pomieszczeniach. Z przodu robota została umieszczona kamera posiadająca możliwość obrotu w płaszczyźnie pionowej. Podstawowy zespół jezdny stanowią gąsienice, lecz w razie potrzeby istnieje możliwość zamocowania zwykłych kół jezdnych. Solidna konstrukcja wraz z dynamicznym systemem napędowym zapewnia wysoką zwrotność robota i dużą prędkość.

Scout jest sterowany drogą radiową lub poprzez kabel z pulpitu sterowniczego wyposażonego w mały monitor. Zasięg robota przy sterowaniu radiowym wynosi około 300 m, natomiast przy sterowaniu poprzez kabel może wynosić w razie potrzeby nawet 200 m.

Robot ma możliwość podłączenia niewielkich urządzeń zewnętrznych, takich jak mały chwytak, kamera na wysięgniku czy wyrzutnik pirotechniczny. Jest to szczególnie ważna cecha, ponieważ dzięki temu Scout może wspierać działania większych robotów Inspector lub Expert. Obecnie robot Scout jest dostępny w wersji komercyjnej.

Fot. 4. Robot zwiadowczy Scout

Fot. 5. Robot bojowy Ibis

Kolejny innowacyjny projekt realizowany w pracowniach PIAP miał na celu opracowanie dużego robota bojowego. W wyniku tych prac powstał prototyp robota **Ibis**.

Robot Ibis

Ibis jest robotem do zastosowań pirotechnicznych i bojowych. Robot został wyposażony w platformę mobilną o napędzie sześciokołowym. Każde z kół jest napędzane niezależnie. Koła przednie połączone są wspólną osią, która ma możliwość ograniczonego obrotu wokół osi wzdłużnej robota. Pozostałe koła są połączone wahaczem parami, po każdej ze stron robota. Wahacze mają możliwość ograniczonego obrotu względem osi poprzecznej robota. Taka konstrukcja zawieszenia zapewnia w większości przypadków kontakt wszystkich kół z podłożem, a co za tym idzie sprawne pokonywanie nierówności terenu, dużą stabilność podczas jazdy oraz optymalne rozłożenie mocy na wszystkie koła.

Sterowanie robotem może być realizowane drogą radiową lub przez światłowód z walizkowego stanowiska operatora lub bardzo lekkiego pilota. Na stanowisku operatora możliwe jest oglądanie nie tylko tradycyjnego widoku obrazu z jednej z kamer (tryb Standard), ale również obrazu z wielu kamer jednocześnie (tryb QUAD lub PIP). Na monitorze LCD prezentowane są również w postaci cyfrowej i graficznej dane pochodzące z czujników robota. Ze stanowiskiem operatora zintegrowany został system negocjacyjny.

Robot został przystosowany do współpracy z bronią używaną w policji i wojsku.

Więcej szczegółów dotyczących danych technicznych, zdjęć robotów lub targów, na których można obejrzeć roboty produkcji PIAP, znajdą Państwo na stronie internetowej *www.antyterroryzm.com*.

Anna Łacic
Przemysłowy Instytut Automatyki i Pomiarów
Zespół Inteligentnych Systemów Mobilnych

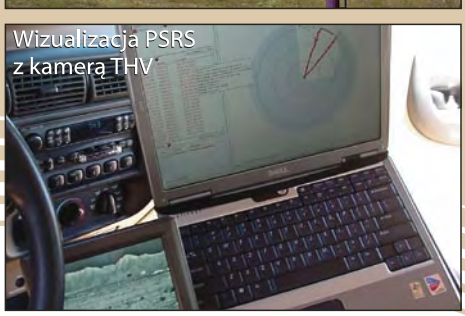
KABE

Najnowsza
technologia ochrony
rozległych terenów zewnętrznych

RADARY

Idealne zabezpieczenie
dla lotnisk i baz wojskowych


Radar RDTS
na granicy USA


Wizualizacja PSRS
z kamerą THV


Radar PSRS
z kamerą THV

Systemy radarowe wykrywają każde wtargnięcie na chroniony obszar i stale monitorując aktualną pozycję intruza mogą sterować zintegrowanym systemem nadzoru wizyjnego

KABE

43-190 MIKOŁÓW
ul. Waryńskiego 63

www.kabe.pl
e-mail: handel@kabe.pl

tel.: (+48 32) 32 48 900
faks: (+48 32) 32 48 901

Dziesięć lat minęło...

W sierpniu 2007 roku minęła dziesiąta rocznica uchwalenia przez Sejm i podpisania przez prezydenta RP ustawy o ochronie osób i mienia. Pomimo tego, że była to „okrągła" rocznica, nie dało się zauważyć specjalnego entuzjazmu z tego powodu ani w prasie branżowej, ani wśród firm branży. Może wynika to z faktu, że rocznica ta wypada zawsze w okresie urlopowym. Oczywiście specyfika działalności naszych firm nie powoduje „wyhamowania" działalności z tego powodu. Chronić trzeba, z jednakowym zaangażowaniem, przez cały rok. Są pewnie jakieś inne powody takiego podejścia do rocznicy uchwalenia ustawy. Zapraszam wszystkich do podzielenia się swoimi spostrzeżeniami związanymi z tym tematem. Chciałbym przy tej okazji przypomnieć, że były propozycje, aby dzień 22 sierpnia uczynić „Świętem Pracownika Ochrony".

Wykorzystując okazję, chciałbym podzielić się z Państwem swoimi refleksjami odnośnie niewątpliwych zalet naszej ustawy w kontekście jej dziesięcioletniego obowiązywania.

Prace nad projektem ustawy rozpoczęły się w lutym 1997 roku. Od początku postępowały one w szybkim tempie, przy dużym zaangażowaniu środowiska branży ochrony. Pomimo sprzeciwu środowiska wskazującego na wady przedstawionego projektu, ówcześni przedstawiciele projektodawców ustawy nawoływali do szybkich prac nad projektem, twierdząc, że po uchwaleniu ustawy przez Sejm ewentualne wady zostaną szybko usunięte. Oceniam, że był to pośpiech spowodowany zbliżającymi się wyborami do Sejmu i chęcią wykazania się sprawnością legislacyjną. Wszystko pewnie byłoby dobrze, gdyby nie to, że w wyniku wyborów nastąpiła zmiana rządzących. Przedstawiciele nowej administracji, w związku z niewydaniem wszystkich rozporządzeń, w tym rozporządzenia dotyczącego badań lekarskich osób ubiegających się o licencje, zmuszeni zostali do przesunięcia terminu wejścia w życie ustawy z marca 1998 roku na jego koniec. Czteroletni okres rządów doprowadził wprawdzie do wypracowania projektu nowelizacji ustawy, lecz projekt ten tylko w części uwzględniał uwagi środowiska branży. Niemniej kolejne wybory na jesieni 2001 roku znowu doprowadziły do zmiany opcji politycznej. Wypracowany projekt nowelizacji, mówiąc kolokwialnie, poszedł do kosza. Kolejna rządząca ekipa przystąpiła z powrotem do prac nad nowelizacją ustawy. Tak jak poprzednio, w pracach tych brali udział przedstawiciele środowiska ochrony. Wypracowany został projekt nowelizacji, który w szerszym zakresie uwzględniał opinie środowiska i doświadczenia wynikłe ze stosowania ustawy. Gdyby wypracowany projekt trafił do Sejmu, a ponadto został uchwalony, można by uznać to za sukces. Mijało bowiem właśnie osiem lat od jej pierwotnego uchwalenia. Ale życie sprawiło nam kolejnego psikusa. Jest jesień 2005 roku. Zbliżają się kolejne wybory. I znowu zmiana opcji politycznej. Nasz projekt nowelizacji ustawy, widzę to oczyma wyobraźni, przewiązany sznurkiem zostaje złożony ad acta. Nowa, wyłoniona w wyniku wyborów opcja polityczna dość szybko wzięła na tapetę naszą ustawę. Na jesieni 2007 roku przedstawiono środowisku branży ochrony już nie projekt nowelizacji, a projekt nowej ustawy o ochronie osób i mienia. Projekt ten w sposób zdecydowany odbiegał od projektów wcześniej wypracowanych. Podczas komisji uzgodnieniowej, która odbyła się pod koniec września tego roku, przedstawiciele naszej branży w sposób zdecydowany zaprotestowali przeciwko próbom wprowadzenia do ustawy zapisów jeszcze bardziej reglamentujących możliwość prowadzenia swobodnej działalności gospodarczej w tym obszarze. No i przyszedł październik 2007 roku. W wyniku przyśpieszonych wyborów w Sejmie nastąpiła kolejna zmiana rządzących. Można przypuszczać, że i ten projekt nowej ustawy, nad którym prace starano się zakończyć przed wyborami, trafi w to samo miejsce, do którego trafiły poprzednie. Na dzień dzisiejszy trudno powiedzieć, kiedy ustawa o ochronie osób i mienia znajdzie się w obszarze zainteresowań nowego rządu.

Z całą pewnością można powiedzieć, że ustawa ta, oprócz kilku kosmetycznych zmian, dokonanych z powodu naszej akcesji do UE, przez dekadę skutecznie opiera się próbom jej nowelizacji, czego efekt został wyżej przedstawiony.

Pewnie zwróciliście Państwo uwagę na to, że nie używam nazw kolejnych opcji i ekip politycznych. Robię to celowo. Nie chcę też wyciągać wniosków o korelacji ustawy i prac nad jej kolejnymi nowelizacjami z kolejnymi wyborami. Pozostawiam to Państwu do przemyślenia i zachęcam do dyskusji.

Pisząc powyższe uwagi przed utworzeniem nowego rządu, usłyszałem deklaracje zniesienia biurokracji i zbędnej reglamentacji w postaci koncesji. Czy będzie taki etap żywota naszej ustawy?

Sławomir Wagner

przyspieszamy...

druga edycja systemu *iP-pro*

System ***iP-pro*** należy do rodziny systemów IP video i jest idealnym rozwiązaniem dla takich obiektów jak: szkoły, dworce, szpitale, hotele, obiekty przemysłowe i biurowe. Druga edycja ***iP-pro*** posiada rozszerzoną ofertę kamer IP oraz wysoką jakość obrazu.

Do systemu dedykowane są dwie platformy zarządzania, dające możliwość łatwego tworzenia systemów hybrydowych. Podnoszą również funkcjonalność oraz poziom bezpieczeństwa, są to:

- √ **NVR-PRO** – aplikacja rejestrująca obraz i dźwięk z maks. 64 kanałów, przeznaczona do zarządzania wszystkimi urządzeniami systemu ***iP-pro*** oraz rejestratorami cyfrowymi **MY-DVR**.
- √ **NETSTATION** – profesjonalna platforma, dla rozwiązań zaawansowanych.

Rejestratory wykorzystujące platformę Netstation, przeznaczone są do pracy z kamerami IP, transmiterami 1-kanałowymi systemu ***iP-pro*** oraz dedykowanymi kamerami megapikselowymi .

MIWI-URMET Sp. z o. o.
91-341 Łódź, ul. Pojezierska 90 A, tel (042) 616 21 00, fax (042) 616 21 13
www.miwiurmet.com.pl, e-mail: miwi@miwiurmet.com.pl

urmet MIWI

iProtect
– sieciowy system zabezpieczenia obiektów

iProtect jest idealnym rozwiązaniem do zarządzania bezpieczeństwem dzięki integracji wielu różnych systemów zabezpieczeń oraz sprawnemu zarządzaniu nimi. Dzięki zastosowaniu go można zredukować całkowite koszty eksploatacji chronionego obiektu, uzyskać większe możliwości niż w przypadku zastosowania systemów działających odrębnie oraz osiągnąć skoordynowaną strategię kontroli i współpracy między systemami.

Obecnie system iProtect oferuje następujące moduły:
- kontroli dostępu (SKD) wraz z rejestracją gości,
- systemu sygnalizacji włamania i napadu (SSWiN),
- telewizji dozorowej IP,
- rejestracji czasu pracy (RCP),
- ochrony osób,
- zarządzania parkingiem.

Jednolita platforma systemowa i integracja systemów pozwalają na redukcję kosztów instalacji i obsługi systemu, a także na sprawne zarządzanie. Poszczególne moduły wymieniają pomiędzy sobą informacje, dzięki czemu możliwe jest bardziej efektywne i skuteczne zabezpieczenie obiektu.

W nawiązaniu do artykułu opublikowanego w nr 6/2007 *Zabezpieczeń*, który dotyczył ogólnych właściwości systemu *iProtect*, chcemy przybliżyć Państwu moduły kontroli dostępu oraz telewizji dozorowej IP (Video IP) stanowiące integralną część omawianego systemu.

Moduł kontroli dostępu

Moduł kontroli dostępu w systemie *iProtect* może obsługiwać 100000 osób. Liczba czytników w systemie jest w zasadzie nieograniczona.

Udzielanie i blokowanie dostępu jest naturalnie podstawowym zadaniem systemów kontroli dostępu. Poza tym platforma *iProtect* oferuje szereg funkcji, które powodują, że system kontroli dostępu jest jeszcze bardziej szczelny. Jedną z takich funkcji jest anti-passback (APB), czyli kontrola przejścia wstecz, która zapobiega używaniu tej samej karty przez wiele osób. Dostępny jest także czasowy APB, który blokuje ponowne użycie karty na tym samym czytniku przez określony czas, oraz czasowy, odwrócony APB, dzięki któremu system kontroluje, czy użytkownik opuścił strefę przed upływem ustalonego czasu.

Dodatkowo możliwe jest konfigurowanie stref kwarantanny, w których użytkownik karty musi pozostać przez określony czas, oraz przejść śluzowych, gdzie jednocześnie mogą być otwarte tylko jedne drzwi w śluzie.

Rejestracja obecności

Dzięki kontroli dostępu *iProtect* możliwe jest bezproblemowe kontrolowanie, jakie osoby znajdują się na danym obszarze w określonym czasie. System może dostarczyć taką informację jako drukowany raport lub jako podgląd w czasie rzeczywistym na ekranie komputera. W przypadku zagrożenia automatycznie drukowany raport obecności osób w budynku może nawet ocalić ludzkie życie.

Rejestracja gości

System *iProtect* oferuje zaawansowane funkcje, które umożliwiają zarejestrowanie gości „na bieżąco” lub z wyprzedzeniem, a także ustalenie, kto miał spotkanie z gościem oraz kto był za niego odpowiedzialny. Osoby odwiedzające są uwzględniane w raportach obecności, co jest kluczowe

w przypadku zaistnienia niebezpieczeństwa. Odpowiednie filtry i raporty umożliwiają łatwą i przejrzystą kontrolę wizyt.

Inne funkcje

System *iProtect* oferuje w standardzie wiele zaawansowanych funkcji i opcji. Interaktywne mapy umożliwiają ciągłą obserwację stanu stref oraz znajdujących się w nich elementów kontroli dostępu (np. stanu czytników, wejść, wyjść, czujek, osób w pomieszczeniach itd.) w trybie online. Klikając na odpowiednie elementy na mapie, można zmienić status stref i innych elementów systemu, a także podejrzeć ostatnie transakcje dotyczące wybranego elementu (np. czytnika). W systemie działa zintegrowany moduł zarządzania alarmami, który inicjuje odpowiednie postępowanie (wraz z opisem dla operatora) w przypadku zdefiniowanych zdarzeń alarmowych.

Design systemu

Podczas projektowania systemu *iProtect* położono duży nacisk na jego skalowalność i niezawodność. Oprócz serwera podstawowymi elementami systemu są inteligentny kontroler sieciowy iPU-8 oraz zaawansowany interfejs czytników Orbit. Kontroler sieciowy iPU-8 pracuje ciągle, nawet jeżeli komunikacja z serwerem zostanie przerwana. Gwarantuje to optymalne bezpieczeństwo i ciągłość pracy w przypadku problemów z komunikacją. Oprócz czytników SmartID jednostki Orbit obsługują również wiele innych typów czytników cyfrowych. Każda taka jednostka posiada także wejścia i wyjścia do obsługi czujników i sterowania urządzeniami zewnętrznymi.

Połączenie między serwerem a kontrolerami sieciowymi iPU-8 wykorzystuje sieć Ethernet (TCP/IP), natomiast połączenie między kontrolerem sieciowym iPU-8 a jednostką Orbit realizowane jest za pomocą przewodu UTP zakończonego wtyczką RJ45. Dzięki temu system może wykorzystywać okablowanie strukturalne budynku, co zmniejsza koszty okablowania systemu. Dodatkową zaletą takiego rozwiązania jest jego prostota, która przyczynia się do zmniejszenia ryzyka pomyłek w okablowaniu (z tym z kolei związany jest czas wykonywania instalacji, a tym samym możliwość redukcji kosztów).

Moduł video IP

System zarządzania bezpieczeństwem *iProtect* może być wyposażony w moduł oprogramowania integrujący system z telewizją dozorową. Podnosi to znacznie wartość użytkową całego systemu bezpieczeństwa dzięki połączeniu funkcji systemu telewizji dozorowej z innymi systemami, takimi jak SSWiN, SKD, RCP, Parking Zaawansowany czy Moduł Ochrony Osób i Dóbr Materialnych.

Dlaczego Video IP?

Wzrost jakości dostępnych na rynku kamer sieciowych spowodował zwiększenie ich potencjalnych zastosowań. Kamery IP oferują podstawowe funkcje i wysoką jakość obrazu przy coraz mniejszych kosztach, jednocześnie umożliwiając obsługę systemu szerokiej grupie użytkowników. Odległości w systemie przestają mieć jakiekolwiek znaczenie. Elastyczność oraz uproszczone okablowanie czynią system Video IP najbardziej odpowiednim dla nowoczesnych, zintegrowanych systemów zabezpieczenia obiektów.

Moduł Video IP może być oddzielnym systemem lub zostać zintegrowany z innymi modułami systemu *iProtect*. Pełna integracja z nowoczesnym systemem Video IP daje użytkownikowi możliwość korzystania z wielu zaawansowanych funkcji, takich jak zapisywanie obrazów i powiązanie ich z transakcjami, śledzenie ruchu, a także obserwacja i rejestracja prowadzona w programie *iProtect*.

Istniejące kamery

Istniejące kamery analogowe mogą być z powodzeniem używane w systemie *iProtect*. Aby było to możliwe, należy w budowanym systemie Video IP zastosować konwertery IP.

Rozwiązania

System *iProtect* oferuje kompleksowe rozwiązania, które ułatwiają nadzór nad systemem Video IP w obrębie aplikacji. Rozwiązania Video IP pozwalają na znaczne oszczędności oraz oferują dużą poprawę jakości obrazu. Użytkownik może z każdego miejsca zarządzać obrazami z kamer, wyszukiwać zdarzenia, wyświetlać zapisane dla nich obrazy i, jeżeli to konieczne, przesłać je. Transmisja danych przez sieć IP umożliwia przeprowadzenie nadzoru w efektywny sposób. Fizyczna obecność na miejscu osoby zarządzającej nie jest wymagana. Zarządzanie może być realizowane z każdego miejsca z dostępem do sieci. Zarejestrowane obrazy powiązane ze zdarzeniem mogą być w prosty i szybki sposób przywołane, co pozwala oszczędzić czas. W dodatku sprawność całego systemu wzrasta, ponieważ nie jest konieczne przeglądanie obrazów, które nie są powiązane ze zdarzeniem. Weryfikacja wideo przy udzielaniu dostępu może być realizowana z każdego miejsca, co dodatkowo obniża koszty stacji monitorowania. Można łatwo zmienić lokalizację centrum monitorowania po zakończeniu pracy (np. po godzinie 17) i kontynuować monitorowanie w dowolnym miejscu z dostępem do sieci internetowej.

Opisywane funkcje bazują na istniejących i sprawdzonych rozwiązaniach sieciowych. Wobec powyższego kilka sygnałów wideo może być transmitowanych tym samym kanałem, a dodatkowo przy użyciu mniejszego nakładu sprzętowego może być monitorowany większy obszar (technologia megapikselowa ogranicza liczbę stosowanych kamer). Technologia PoE (*Power over Ethernet* – zasilanie wprost z kabla UTP) wychodzi naprzeciw potrzebom szybkiej instalacji, a także deinstalacji sprzętu. Nie jest wymagane okablowanie zasilające, więc nie są ponoszone dodatkowe koszty instalacyjne, co czyni system bardziej elastycznym.

Niezawodność i bezpieczeństwo

Obecnie sieć może być skonfigurowana tak, by przesyłane dane trafiały bezpiecznie tylko tam, gdzie powinny. Właściwa

konfiguracja oraz autoryzacja (zarządzanie) może skutecznie zapobiegać „wypływaniu" danych. Przechowywane dane są zabezpieczone znakiem wodnym i mogą być przesyłane w formacie zakodowanym. Dziś, bazując na systemie sieciowym Video IP i używając PoE oraz konfiguracji RAID, można zbudować redundantny, kompletny system telewizji dozorowej wyposażony w zasilanie awaryjne.

Integracja omawianych modułów

Integracja systemu Video IP z innymi modułami *iProtect* powoduje znaczne zwiększenie funkcjonalności całego systemu.

Obraz wideo dla transakcji

Dla każdego modułu w systemie *iProtect* wszystkie zdarzenia są zapamiętywane w postaci transakcji. Dzięki modułowi *iProtect* Video IP dla każdej transakcji może być zapamiętany obraz z odpowiedniej kamery. Podczas przeglądania transakcji wystarczy kliknąć na symbol wybranej kamery, aby automatycznie odtworzyć zapamiętaną dla niej sekwencję wideo. Dzięki temu nie trzeba przeszukiwać zapisu wideo z kilku systemów, z wielu kamer, aby odnaleźć odpowiedni obraz z odpowiedniej kamery i z odpowiedniego czasu. Funkcja ta jest ogromnym ułatwieniem, szczególnie w rozbudowanych systemach.

Weryfikacja wideo

Jedną z kluczowych funkcji systemu *iProtect* jest weryfikacja wideo. Najczęściej wykorzystywana jest w strefach czasowych poza normalnymi godzinami pracy/otwarcia biur oraz na przejściach oddalonych lub o podwyższonym stopniu kontroli. Przejścia z włączoną funkcją weryfikacji wideo nie otwierają się od razu po odczytaniu karty przystawionej do czytnika. Zamiast tego na komputerze operatora wyświetla się okno żądania dostępu z kartą użytkownika i jego zdjęciem. Jednocześnie pojawia się okno z obrazem „na żywo" z kamery przypisanej do czytnika. Operator na podstawie porównania zdjęcia użytkownika z obrazem z kamery udziela dostępu lub dostęp ten blokuje.

Rozpoznawanie tablic rejestracyjnych

System rozpoznawania tablic rejestracyjnych jest opcją w module *iProtect* Video IP. System ten może być używany na przykład do udzielania dostępu do parkingu firmowego dla samochodów, których numer rejestracyjny zostanie rozpoznany. W tej sytuacji nie jest konieczne przykładanie karty do czytnika przez kierowcę pojazdu.

W kolejnych artykułach postaramy się przedstawić Państwu pozostałe moduły wchodzące w skład Zintegrowanego Systemu Zarządzania Bezpieczeństwem *iProtect*, aby w pełni przedstawić jego rozbudowane możliwości. Dodatkowo zachęcamy do kontaktu z firmą Miwi-Urmet w celu zaczerpnięcia dodatkowych informacji dotyczących systemu *iProtect* oraz innych produktów z naszego asortymentu.

Łukasz Szafoni
Miwi-Urmet

AVerMedia

www.avermedia.com

AVerDiGi EB1504 NET | 4CH Real Time MPEG4 DVR

Nowe oblicze monitoringu...

- ☑ **wysoka prędkość zapisu:**
  50 FPS dla PAL D1 (720x576)
  100 FPS dla CIF (360x288)

- ☑ **kompleksowe oprogramowanie:**
  Zarządzanie przez www
  Zarządzanie przez urządzenia mobilne
  Obróbka zarejestrowanego obrazu

- ☑ **charakterystyka:**
  2 dyski twarde (1 w kieszeni) o max pojem. 750GB
  4 wejścia audio
  1 Port RS485 (PTZ)

- ☑ **bezawaryjność:**
  Inteligente pomijanie błędnych sektorów na dysku
  Autodiagnostyka rejestratora
  Bezgłośna praca

- ☑ **zaawansowane funkcje sieciowe:**
  Zaawansowana transmisja danych
  Kompresja MPEG4

AVerDiGi EB1504 NET

ALPOL Sp. z o.o. wyłączny dystrybutor urządzeń AVerMedia na terenie całego kraju.

ALPOL HURTOWNIA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ

tel: 0 801 77 77 90

Bielsko-Biała	Gliwice	Katowice	Kraków	Lublin	Łódź
0 32 7907621	0 32 7907623	0 32 7907656	0 32 7907646	0 32 7907650	0 32 7907625
Poznań	Sopot	Szczecin	Warszawa Mokotów	Warszawa Praga	Wrocław
0 32 7907637	0 32 7907643	0 32 7907630	0 32 7907634	0 32 7907633	0 32 7907627

alpol@e-alpol.com.pl www.e-alpol.eu www.e-alpol.com.pl

Metody zabezpieczania transmisji skompresowanych danych multimedialnych

Część 2. Wybrane narzędzia zapewniające poufność, uwierzytelnianie oraz kontrolę dostępu

Artykuł przedstawia wybrane metody ochrony transmisji mediów strumieniowych. Jest to technika polegająca na przesyłaniu skompresowanych danych multimedialnych przez sieć w postaci strumienia pakietów przetwarzanych na bieżąco w odbiorniku, tzn. nie występuje potrzeba pobrania całego pliku przed rozpoczęciem odtwarzania. Znajduje ona zastosowanie w realizacji szeregu usług – wideo na życzenie, telewizja internetowa, wideokonferencja, telefonia VoIP, przeglądanie baz danych z obrazami medycznymi. W pierwszej części artykułu dokonano przeglądu algorytmów kryptograficznych powiązanych z kompresją danych, poświęcając najwięcej miejsca selektywnemu szyfrowaniu. W niniejszej części zostaną przedstawione opisy narzędzi dostarczających usług poufności, uwierzytelniania i integralności oraz kontroli dostępu obrazów i materiału wideo, a także implementacja standardów JPEG 2000, MPEG-4 oraz niektórych algorytmów szyfrowania wideo. Tematyka artykułu jest poruszana w źródłach poświęconych bezpiecznej transmisji multimedialnej

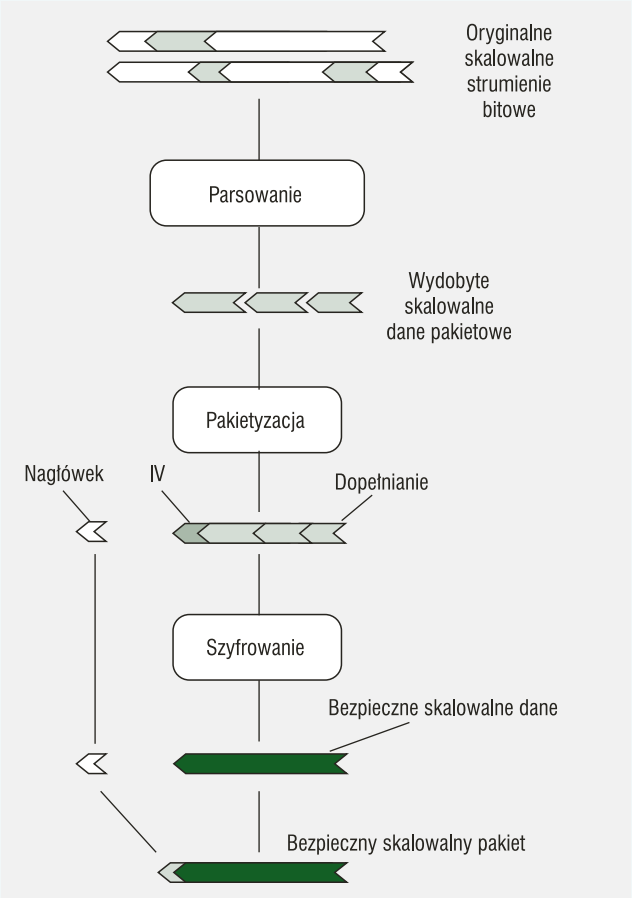
1. Rozwiązania dostarczające poufności

1.1. Bezpieczna skalowalna transmisja strumieniowa i transkodowanie

W części ósmej specyfikacji JPEG2000 o nazwie Secure JPEG 2000 (JPSEC) zdefiniowano kilka rozwiązań oferujących usługę poufności. Jednym z nich jest bezpieczna skalowalna transmisja strumieniowa i transkodowanie (bezpieczny skalowalny streaming i transcoding – BSSiT) [WeAp03, WeAp04]. Zabezpieczony w nim strumień bitowy JPSEC jest adaptowany do dynamicznie zmieniających się warunków sieciowych lub pojemności odbiorników/klientów, bez wymogu deszyfrowania w węzłach pośredniczących. BSSiT jest realizowany poprzez obcinanie lub porzucanie zaszyfrowanych pakietów JPEG2000 (różnych od pakietów sieciowych) w węzłach pośredniczących, na podstawie wcześniejszej analizy ich nagłówków. Skutkuje to zmianami parametrów strumienia bitowego – redukcją przepływności bitowej/szerokości pasma lub rozdzielczości.

Proces tworzenia zaszyfrowanych pakietów JPEG2000 został przedstawiony na rys. 1. Obejmuje on: analizę składni skalowalnych strumieni bitowych, pobranie wybranych segmentów danych, formowanie pól danych pakietów (łączenie segmentów, dodawanie losowego wektora inicjującego, dopełnianie długości), szyfrowanie pakietów, dołączanie nagłówków do pakietów. Analizowane są między innymi dane nagłówkowe w celu uzyskania informacji o użytych parametrach kodowania strumienia. Losowy wektor początkowy (Initial Vector, IV) jest stosowany do zróżnicowania wyników szyfrowania poszczególnych pakietów, natomiast dopełnianie – w celu osiągnięcia rozmiaru danych wejściowych wymaganego przez dany algorytm szyfrowania, przykładowo AES. Nagłówki pakietów nie są szyfrowane; zawierają informacje o punktach odcięcia oraz priorytetach pakietów.

W BSSiT nie stosuje się deszyfrowania strumienia JPSEC w węźle pośredniczącym, ponieważ jest to nieodpowiednie do systemu wymagającego gwarancji bezpieczeństwa w ujęciu od końca do końca. Z kolei tworzenie szyfrogramu w węzłach startowych może być uzyskane różnymi sposobami, a optymalna metoda stanowi wypośrodkowanie pomiędzy zakresem danych poddawanych szyfrowaniu a swobodą późniejszego transkodowania.



Rys. 1. Tworzenie bezpiecznego skalowalnego pakietu [WeAp03]

Może ona polegać na szyfrowaniu segmentów JPEG2000, obejmujących nagłówki i ciała pakietów, oraz umieszczeniu markera SEC w głównym nagłówku strumienia kodowego, który to marker określa rodzaj zaszyfrowanych danych. Metadane mogą zawierać parametry związane zarówno z obrazem jak i strumieniem bitowym określonej Strefy Wpływów (Zone of Influence, ZOI), odzwierciedlające odpowiedniość między zaszyfrowanymi segmentami danych a właściwościami obrazu oraz wykorzystywane podczas bezpiecznego transkodowania strumienia kodowego JPSEC.

Łączne przetwarzanie nagłówków i ciał pakietów oraz wielu segmentów JPEG2000 wiąże się z mniej dokładną analizą składniową strumienia kodowego, posługiwaniem się ZOI, ukrywaniem granic pomiędzy indywidualnymi pakietami. Zmniejsza to złożoność szyfrowania/deszyfrowania, a także skomplikowanie oraz elastyczność transkodera w porównaniu z szyfrowaniem ograniczonym tylko do ciała pakietu.

Z kolei zastosowanie szyfrowania ograniczonego tylko do pól danych pakietów JPEG2000 wiąże się z większą swobodą adaptacji i ma bardzo niewielki wpływ na wydajność kompresji.

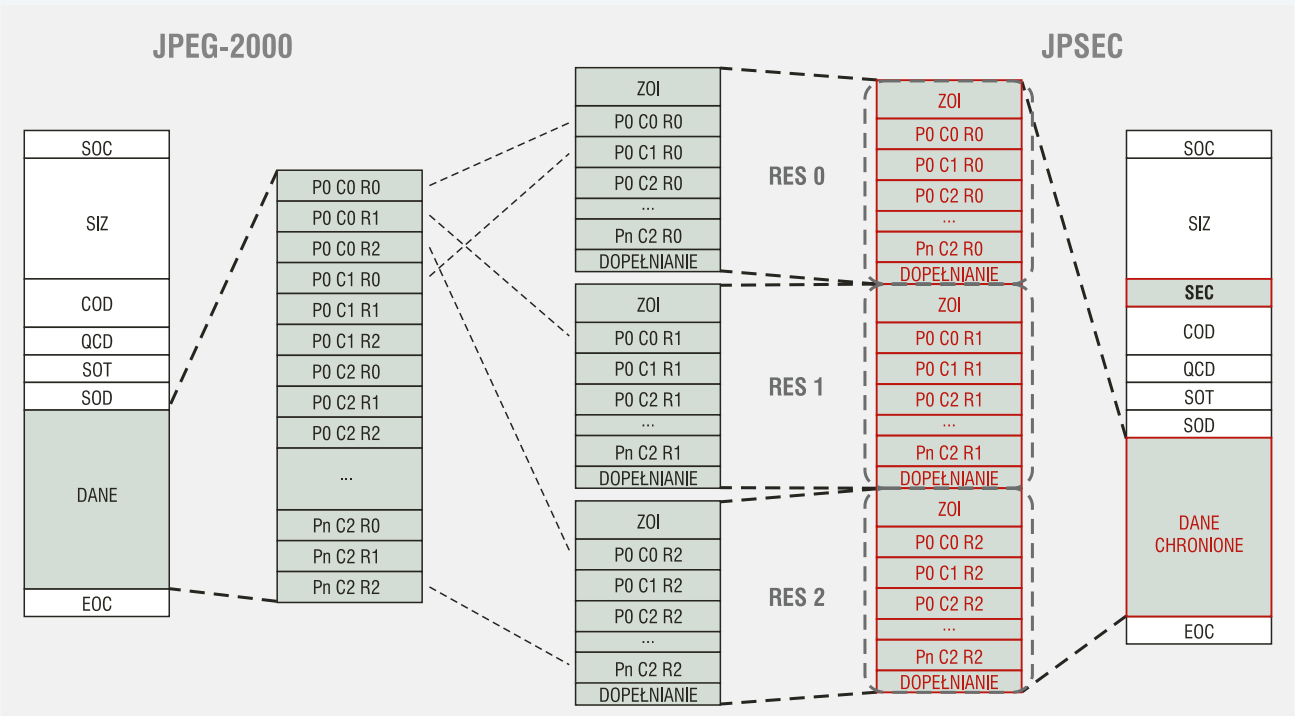
Szyfrowanie i bezpieczne transkodowanie można zastosować do zabezpieczenia strumienia kodowego JPEG2000, zawierającego segmenty danych uszeregowane w porządku RLCP (wiodące rozdzielczości i warstwy jakości).

Szyfrowane są kolejne segmenty danych, odpowiadające trzem rozdzielczościom. Nagłówek JPSEC definiuje trzy ZOI, które precyzują: rozdzielczość, segment strumienia bitowego i szablon szyfrowania (zbiór wartości parametrów procesu szyfrowania).

Transkoder analizuje nagłówek SEC, identyfikuje położenie segmentów danych odpowiadających określonym rozdzielczościom, które są porzucane lub zachowywane.

Jeżeli adaptacja ma być przeprowadzana według rozdzielczości takiej, jak powyżej, a segmenty danych są rozmieszczone w strumieniu kodowym JPEG2000 w innej kolejności, przykładowo PCRL, to w celu przeprowadzenia szyfrowania należy dodatkowo zmienić kolejność segmentów tak, aby były one ciągłe ze względu na rozdzielczość. Wymaga to wprowadzenia ZOI także w polu danych strumienia kodowego, zawierających parametry związane ze strumieniem bitowym oraz pakietami, które odzwierciedlają proces zmiany kolejności segmentów danych poprzez wskazanie granic między pakietami w obrębie segmentów. ZOI w polu danych JPSEC służy do odwrócenia zmian kolejności oraz prowadzenia bardziej dokładnego transkodowania. Z kolei znaczniki SEC mają ZOI z parametrami dotyczącymi obrazu oraz strumienia bitowego i są stosowane przy zgrubnej adaptacji.

BSSiT może być również użyty do zabezpieczania drobnoziarnistej skalowalności (Fine Granularity Scalability, FGS) [WeAp01, ZhYu05], funkcjonującej w ramach standardu MPEG-4, która zapewnia elastyczną adaptację do zmiennych warunków sieciowych lub różnych potrzeb aplikacji. Skompresowana sekwencja wideo tworzy strumień bitowy złożony z warstwy bazowej oraz wzbogacającej. Nieskalowalna część bazowa przenosi dane dotyczące niskich jakości i przepływności binarnych, natomiast składnik udoskonalający to dodatkowe dopełniające bity, prowadzące do otrzymania zbioru różnych, większych szybkości transmisji oraz wyższej jakości wideo. Fragment wzmacniającego strumienia bitowego jest



Rys. 2. Formowanie strumienia JPSEC przy rozmieszczeniu segmentów JPEG2000 w kolejności PCRL [WeAp04]

uzyskiwany z różnicy pomiędzy zakodowaną warstwą bazową ramki a oryginalną ramką i zalicza się do niego rezydua ramek zakodowane w sposób gwarantujący skalowalność. Przy tworzeniu warstwy bazowej stosowane jest kodowanie predykcyjne z użyciem ramek typu I, P, B, a przy tworzeniu warstwy wzbogacającej – kodowanie bitplanów.

BSSiT w tym przypadku koduje i szyfruje obie warstwy do postaci pakietów reprezentujących różne priorytety, których nagłówki nie są szyfrowane oraz przechowują dane wpływające na kolejność porzucania. Jeśli dane warstwy wzmacniającej są transmitowane w obrębie pojedynczego pakietu, to implementuje się progresywne szyfrowanie, aby dane mogły być obcięte w dowolnym punkcie w celu osiągnięcia dokładnej redukcji szybkości bitowej przez transkoder. W przeciwnym wypadku używane są różne opcje pakietyzacji.

Ramka wzmacniająca może być kodowana w jeden strumień bitowy, który jest następnie segmentowany w pakiety. Wcześniejsze fragmenty strumienia posiadają wyższy priorytet. Redukcja przepływności jest osiągana poprzez porzucanie pakietów związanych z niższą jakością. Dokładniejsze dopasowanie szybkości bitowej jest osiągane poprzez obcięcie pakietu.

Innym sposobem jest podział danych uwydatniających na przestrzenne regiony. Każdy z nich jest skalowalnie kodowany do oddzielnych pakietów z użyciem technik progresywnego szyfrowania. Każdy pakiet odpowiada wtedy regionowi w ramce wideo i może być transkodowany przez obcięcie, stąd transkoder węzła sieciowego dokonuje dostrajania szybkości bitowej przez obcięcie przechodzącego przez niego zaszyfrowanego pakietu FGS.

Bezpieczny skalowalny streaming i transkodowanie znajdują potencjalne zastosowanie również w trójwymiarowym podpasmowym kodowaniu – procesie prowadzącym do uzyskania na bazie sekwencji wideo niezależnie dekodowalnych pakietów o równym priorytecie. Koder BSSiT szyfruje progresywnie każdy pakiet, z wyjątkiem nagłówków, które przechowują informacje o punktach odcięcia wykorzystywanych do realizacji transkodowania.

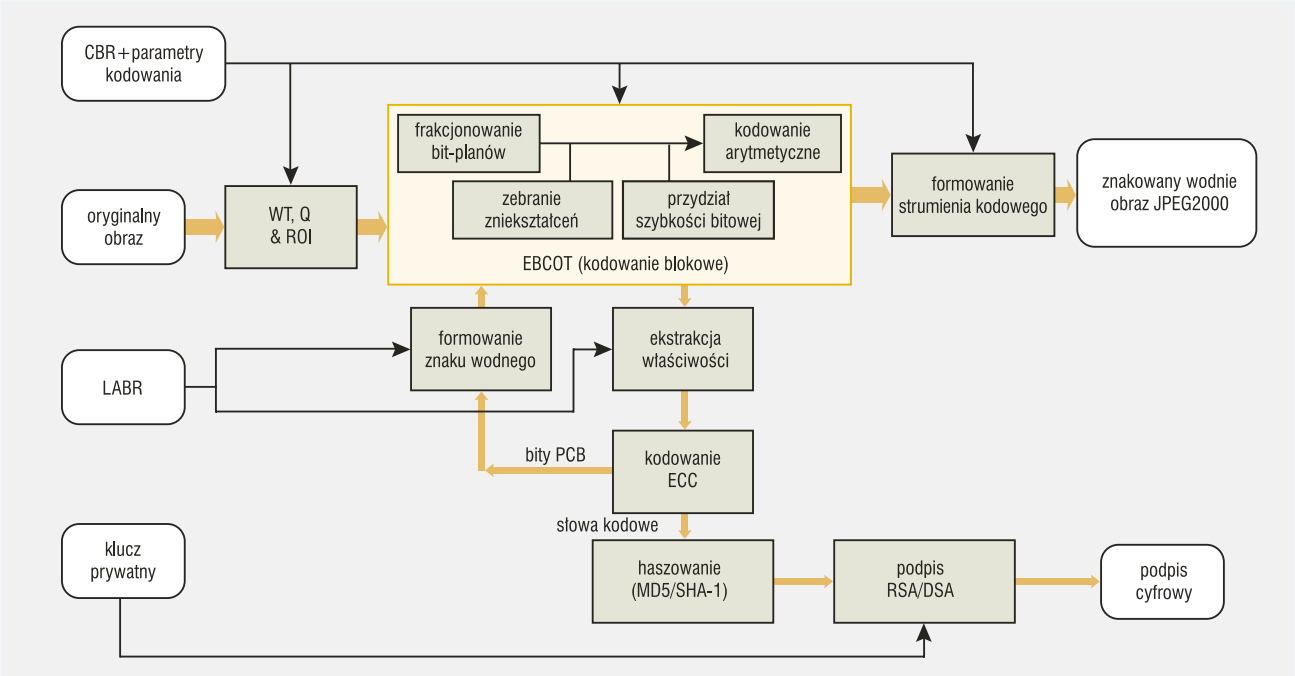
1.1.1. Wpływ warunków transmisji

W BSSiT ma miejsce adaptacja do warunków transmisji oraz pojemności odbiorników końcowych. Polega ona na zoptymalizowanym pod kątem wielkości wprowadzanych zniekształceń, wyrażonym za pośrednictwem błędu średniokwadratowego, transkodowaniu wielu pakietów, przeprowadzanym z zastosowaniem punktów obcięcia pakietów.

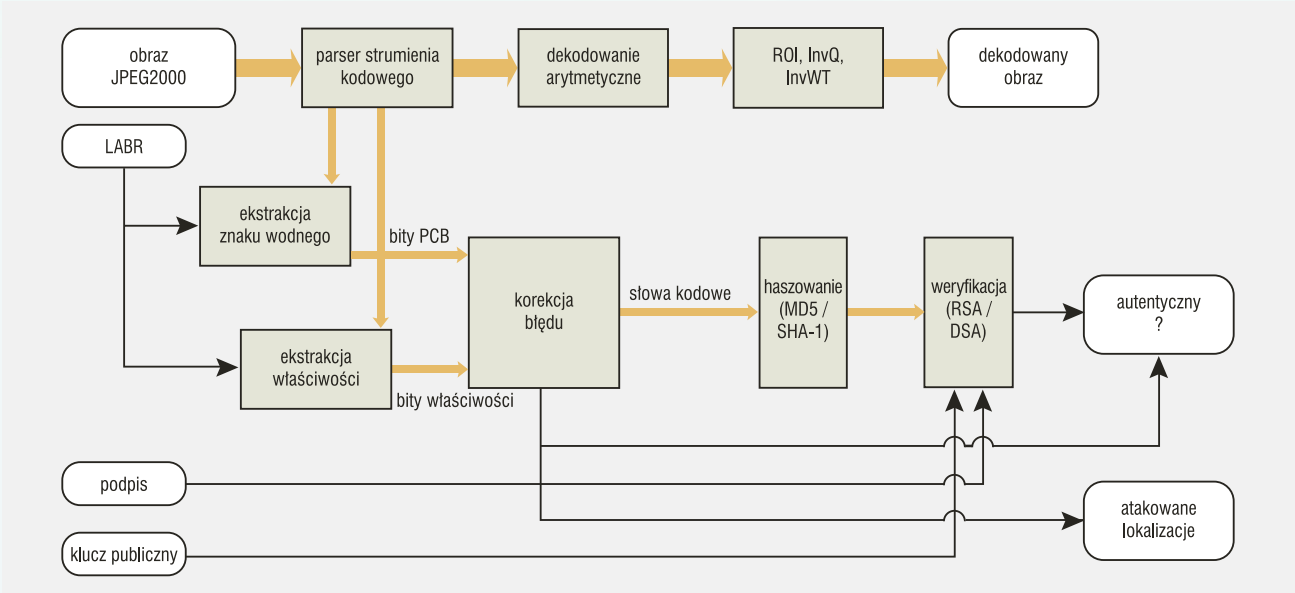
Jeżeli koder JPEG2000 używa trzech poziomów rozdzielczości i trzech warstw jakości na daną rozdzielczość, to przy wzroście odbieranej szybkości bitowej, wyrażonej poprzez liczbę bitów na piksel, wielkość MSE spada skokowo. Przy większych szybkościach bitowych osiąga się lepsze aproksymacje obrazów.

BSSiT charakteryzuje również narzut na tle oryginalnej szybkości kodowania, związany z nagłówkami oraz offsetami segmentów JPEG2000, który przy zastosowaniu szyfru AES maleje z 14 do 4% przy liczbie dekodowanych segmentów wynoszącej od 1 do 9, co wiąże się ze stałym rozmiarem nagłówków pakietów.

Podobne wyniki w zakresie MSE oraz narzutu występują, gdy zachodzi kodowanie ramek wideo w trzy rozdzielczości i dziewięć warstw jakości – MSE jest mniejszy o 100 jednostek.



Rys. 3. Tworzenie podpisu w trybie uwierzytelnienia stratnego [ZhQi04]; znaczenie skrótów: WT – transformacja falkowa (wavelet transform), Q – kwantyzacja (quantization), ROI – obszar zainteresowania (region of interest), ECC – kod korekcji błędów (error correction code), PCB –bity kontroli parzystości (parity check bits)



Rys. 4. Sprawdzenie podpisu wygenerowanego w trybie uwierzytelniania stratnego [ZhQi04]; znaczenie wcześniej nie wyjaśnionych s

Wpływ warunków transmisji jest zależny od wymienionych powyżej właściwości metod szyfrowania stosowanych przy tworzeniu pakietów BSSiT.

1.2. Szyfrowanie drobnoziarnistej skalowalności standardu MPEG-4

Szyfrowanie FGS nie powinno zaburzać zdolności adaptacyjnych i powinno umożliwiać ich realizację bez potrzeby zamiany szyfrogramu na tekst jawny. Dwa przykładowe algorytmy ochrony skalowalności zostały przedstawione w pracy pt. Scalable Protection for MPEG-4 Fine Granularity Scalability [ZhYu05].

Jeden z nich szyfruje strumień FGS w pojedynczą warstwę dostępową, zachowując jednak oryginalne właściwości skalowania oraz odporność na błędy w zaszyfrowanym strumieniu. Jest to osiągnięte poprzez szyfrowanie bezpośrednie lub selektywne warstwy bazowej i selektywne części wzmacniającej. Selektywne przetwarzanie warstwy podstawowej obejmuje wartości DC oraz bity znaków współczynników DCT, bity znaków i rezydua wektorów ruchu każdej płaszczyzny obiektu wideo (Video Object Plane, VOP). Z kolei bezpośrednie szyfrowanie nie dotyczy nagłówków VOP. W selektywnym szyfrowaniu warstwy wzbogacającej przetwarzane są wymienione elementy składni MPEG. Procesy te są wdrażane po działaniu kodera entropijnego , dlatego nie obniżają wydajności kodowania, natomiast zmniejszenie stopnia kompresji nie występuje lub jest pomijalnie małe. Propagacja błędów jest taka sama jak w nieprzetwarzanym FGS ze względu na zastosowanie szyfru strumieniowego. Mimo zaszyfrowania warstwy wzbogacającej wszelakie operacje skalowania są możliwe, ponieważ zachodzi pełna zgodność z formatem FGS MPEG-4.

Drugi algorytm szyfruje strumień FGS na wiele warstw jakości, rozróżnianych według wartości szczytowej stosunku sygnału do szumu (peak signal-to-noise ratio, PSNR) lub szybkości bitowej, przy czym płaszczyzny wyższe mają dostęp do swych niższych odpowiedników tego samego typu. Inaczej rzecz ujmując, jeżeli użytkownik chce uzyskać dostęp do danej warstwy jakości, to są do niego przesyłane klucze służące do odszyfrowania wspomnianej warstwy i jej niskojakościowych odpowiedników. W aplikacjach strumieniowych szczególnie przydatne są warstwy szybkości bitowej. Jeśli serwer strumieniowy posiada informacje o punktach granicznych pomiędzy poszczególnymi warstwami, to nie dochodzi do utraty pasma na przesyłanie dodatkowych danych, z których użytkownik i tak nie korzysta. Podstawowa część strumienia bitowego jest często nieszyfrowana i stanowi podgląd materiału wideo. Warstwę PSNR definiuje się jako grupę sąsiadujących płaszczyzn bitowych w każdym VOP wzbogacającym, natomiast warstwę szybkości bitowej tworzy zbiór przyległych pakietów wideo. Punkty rozróżnienia między obydwoma rodzajami warstw są określane na podstawie charakterystyki wideo lub potrzeb biznesowych. Specjalnymi, dodatkowymi markerami, umieszczonymi w nagłówku VOP, oznaczane są porcje danych podlegające jednoczesnemu szyfrowaniu, którymi są pakiety danych wideo. Podobnie jak w poprzednim algorytmie wydajność kompresji pozostaje zachowana, a narzut związany z dodatkowymi nagłówkami jest niewielki. Algorytm jest odporny na błędy i straty pakietów. Występuje jednak niewielki negatywny wpływ na szybkość przetwarzania. Poza tym możliwa jest skalowalność na poziomie pakietów bezpośrednio na zaszyfrowanym strumieniu bez potrzeby deszyfrowania i ponownego szyfrowania.

2. Rozwiązania prowadzące do osiągnięcia integralności i uwierzytelnienia

2.1. Bezpieczna skalowalna transmisja strumieniowa i transkodowanie (BSSiT)

BSSiT jest również narzędziem uwierzytelniania [WeAp04]. Algorytm uwierzytelnienia w standardzie JPEG2000, przykładowo HMAC, może być obliczony na segmentach danych

odpowiadających trzem określonym rozdzielczościom obrazu, przed lub po wykonaniu szyfrowania. Rezultat działania kodu uwierzytelniającego jest obcinany w celu zmniejszenia narzutu związanego z użyciem tejże funkcji i zapisywany w znaczniku SEC.

2.2. Jednolita struktura uwierzytelniania dla obrazów JPEG2000

W pracy pt. A unified authentication framework for JPEG 2000 [ZhQi04] zaproponowano system, który charakteryzuje się możliwością doboru stopnia odporności uwierzytelnienia. Jest to osiągane za pomocą trybów uwierzytelnienia (kruche, bezstratne, stratne) oraz parametru LABR.

Najniższą przepływnością uwierzytelnienia (Lowest Authentication Bit Rate, LABR) jest przepływność, powyżej której wszystkie dane obrazu są chronione. Inaczej rzecz ujmując, obraz uważa się za autentyczny, jeżeli jest transkodowany do przepływności większej od LABR.

W trakcie kruchego uwierzytelniania, na podstawie wartości LABR i innych parametrów, ze strumienia kodowego JPEG 2000 wyodrębniane są części podlegające zabezpieczeniu. Następnie są one poddawane działaniu funkcji skrótu oraz podpisywane. Obraz jest uważany za sfałszowany, jeżeli w jego chronionej części zmianie uległ choćby pojedynczy bit.

Stratne i bezstratne uwierzytelnianie posiada wyższy próg odporności na modyfikacje obrazu wprowadzane przez jego transkodowanie lub zmianę formatu w porównaniu z kruchym uwierzytelnianiem.

W stratnym uwierzytelnianiu proces kodowania blokowego (Embedded Block Coding with Optimal Truncation, EBCOT) znajduje dla każdego zakodowanego bloku te bitplany, których wartość jest wyższa niż LABR. Podejmowana jest decyzja, który poziom rozdzielczości jest odpowiedni do wydobycia właściwości obrazu, a który do umieszczenia znaku wodnego. Cecha obrazu jest kodowana, a bity kontroli parzystości otrzymanego słowa kodowego są stosowane jako ziarno do uzyskania znaku wodnego. Znak wodny jest następnie umieszczany w odpowiednim bloku zawartym w podpaśmie LH lub HH stosownego poziomu rozdzielczości. Dodatkowo właściwości ze wszystkich bloków są łączone i wynikowa sekwencja bitów jest haszowana, a następnie podpisywana. Parametrami wejściowymi przy operacji weryfikacji są: obraz JPEG2000, LABR, podpis i klucz publiczny. W strumieniu kodowym dla każdego bloku wyszukiwane są bitplany powyżej LABR, na bazie których podejmowana jest decyzja o przyporządkowaniu danego poziomu rozdzielczości do ekstrakcji właściwości lub znaku wodnego. Ekstrakcja cechy ma taką samą postać jak w procedurze podpisywania. Natomiast znak wodny jest uzyskiwany z każdego bloku w danym poziomie rozdzielczości. Właściwości i znaki wodne formułują słowa kodowe, na których jest obliczana funkcja skrótu. Potem podpis jest sprawdzany przy użyciu klucza publicznego.

Bezstratne uwierzytelnianie jest stosowane w aplikacjach wymagających odtworzenia oryginalnego obrazu, przykładowo w medycynie. Etapy są podobne do tych występujących w trybie stratnym, niewielkie różnice występują w module znakowania wodnego.

Opisane narzędzie znajduje zastosowanie także w dystrybucji i strumieniowaniu obrazu, obrazowaniu medycznym oraz militarnym, egzekwowaniu prawa, handlu przez Internet (e-commerce), elektronicznej Administracji Publicznej (e-government).

2.3. Metoda skalowalnego uwierzytelniania

Metoda skalowalnego uwierzytelniania [DeWu03] pozwala poszczególnym użytkownikom weryfikować autentyczność i integralność transkodowanych podobrazów otrzymywanych ze strumienia kodowego JPEG2000 zabezpieczonego pojedynczym podpisem. Zabiegi uwierzytelniania są wykonywane w celu potwierdzenia pochodzenia obrazu oraz wykrycia ewentualnych modyfikacji powstałych podczas transmisji. Główną zaletą metody jest uniknięcie potrzeby oddzielnego podpisywania poszczególnych części strumienia kodowego.

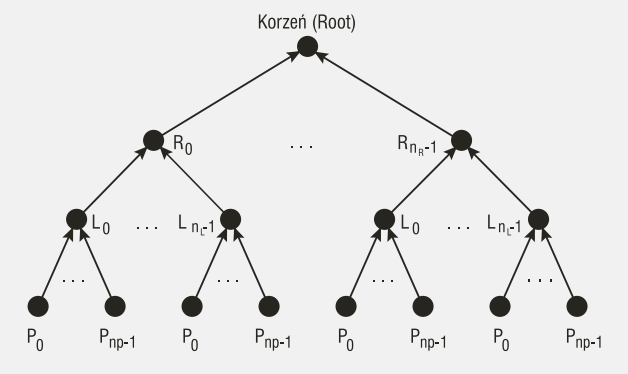
W procesie uwierzytelniania stosowane są drzewa Merklego (Rys. 5). Podpisywany jest korzeń drzewa. Parametry narzędzia są umieszczone w markerze SEC. Aby sprawdzić autentyczność otrzymanej części obrazu n_i, użytkownik musi posiadać wartości funkcji skrótu siostrzanych węzłów, leżących na ścieżce od wspomnianej części obrazu do korzenia drzewa włącznie. Fragment strumienia kodowego obrazu jest uznawany za autentyczny, jeżeli obliczona wartość funkcji skrótu korzenia jest identyczna z przechowywaną przez użytkownika.

Algorytm uwierzytelnienia prowadzi do uzyskania podobrazów o różnych rozmiarach, co wywołuje różną zajętość pasma.

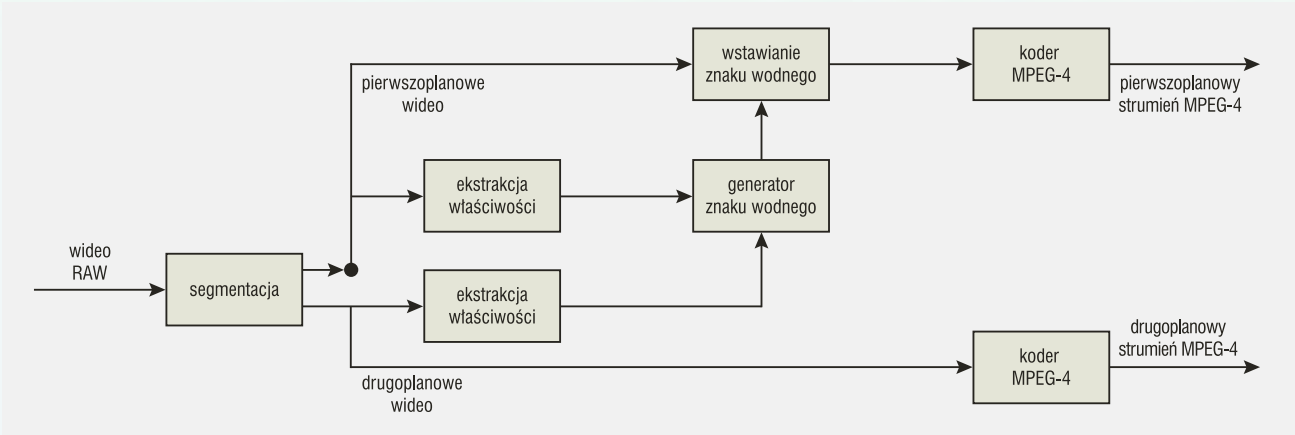
Podobrazy są wyodrębniane na podstawie określonych: rozdzielczości, warstw, komponentów, obrębów.

2.4. Uwierzytelnianie wideo MPEG-4

Uwierzytelnianie wideo może być realizowane poprzez zastosowanie znaku wodnego umieszczanego w obiektach [DaQi03], uzyskiwanego zarówno z pierwszoplanowych obiektów jak i tła. Po stronie odbiornika integralność pomiędzy obiektem i tłem jest weryfikowana poprzez porównanie wydobytego znaku wodnego z ponownie otrzymanym znakiem wodnym. Materiał jest autentyczny, jeśli obydwa znaki są identyczne. Metoda uwierzytelniania oraz znak wodny powinny być odporne na operacje



Rys. 5. Drzewo Merklego – wierzchołki odpowiadają składnikom strumienia bitowego [DeWu03]



Rys. 6. System znakowania wodnego stosowany przy uwierzytelnianiu wideo [DaQi03]

przetwarzania wideo – translację, skalowanie, rotację, segmentację. Uzyskuje się to poprzez odpowiednie zaprojektowanie algorytmu znakowania wodnego oraz tolerowanie zmian wywołanych wymienionymi operacjami przez cechę obrazu. Algorytm znakowania wodnego jest oparty na wyborze i przekształcaniu współczynników DFT (dyskretnej transformaty Fouriera). Do ukrywania znaku wodnego używane są zależności pomiędzy podgrupami współczynników.

3. Rozwiązania zapewniające kontrolę dostępu

3.1. Schemat elastycznej kontroli dostępu

Idea schematu elastycznej kontroli dostępu [DeWu03] jest podobna do rozwiązania przedstawionego w metodzie skalowalnego uwierzytelniania. W tym przypadku użytkownicy mają zróżnicowany dostęp do fragmentów zaszyfrowanego jednolicie strumienia kodowego.

W schemacie stosowana jest koncepcja drzewa Sandhu. Korzeń drzewa wyposażony jest w główny klucz, służący do szyfrowania całego strumienia kodowego. W kolejnym etapie algorytmu generowane są iteracyjnie klucze dla węzłów rozdzielczości, poczynając od największej, z wykorzystaniem funkcji skrótu operujących na kluczu głównym oraz odpowiedniej stałej. Następnie dochodzi do tworzenia kluczy dla węzłów jakości na podstawie znajomości wartości kluczy rozdzielczości i stałej. Dla danej rozdzielczości oraz warstwy jakości generowane są klucze poszczególnych obrębów obrazu, które służą do zaszyfrowania pakietów JPEG 2000.

Żądanie użytkownika dotyczy podobrazu o określonych rozdzielczościach, warstwach lub zbiorach obrębów. Przykładowo, jeżeli użytkownik chce uzyskać obraz o zadanej rozdzielczości, to musi posiadać odpowiadający jej klucz oraz na jego podstawie obliczyć wartości kluczy mniejszych rozdzielczości, warstw jakości odpowiadających wszystkim posiadanym rozdzielczościom i w końcu dostępnych obrębów, a następnie deszyfrować odpowiednie pakiety JPEG 2000.

3.2. Skramblowanie w dziedzinie falkowej i strumienia bitowego

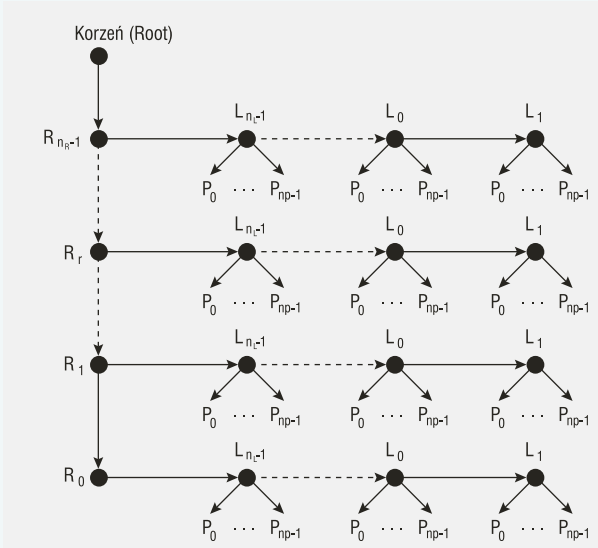
System składa się z trzech podstawowych komponentów: skramblowania, generatora liczb pseudolosowych i algorytmu szyfrowania [DuWe04]. Skramblowanie jest stosowane selektywnie w odniesieniu do skwantowanych współczynników transformaty falkowej lub strumienia kodowego. Poziom zniekształceń wprowadzanych w poszczególne części obrazu jest sterowany, co pozwala zrealizować kontrolę dostępu według rozdzielczości, jakości lub regionów zainteresowania. Dodatkowe zróżnicowanie jest osiągane poprzez użycie różnych kluczy szyfrujących.

Skramblowanie polega na pseudolosowym zmienianiu znaków współczynników falkowych należących do najbardziej znaczących bitplanów.

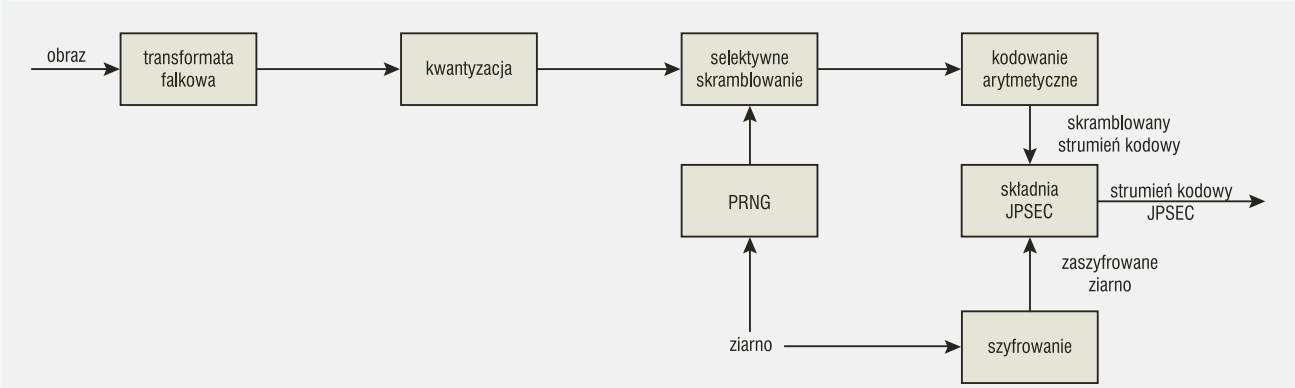
W drugim podejściu skramblowanie może przykładowo dotyczyć części strumienia kodowego przenoszących informacje o wysokich rozdzielczościach, co jest stosowane przy realizacji kontroli dostępu według rozdzielczości. Zmiany nie mogą obejmować znaczników strumienia. 64-bitowe ziarna generatorów PRNG są szyfrowane algorytmem RSA.

4. Przykładowe implementacje

Implementacje niektórych algorytmów szyfrowania wideo [UhPo05] występujących w literaturze zostały zintegrowane



Rys. 7. Drzewo Sandhu stosowane w narzędziu kontroli dostępu [DeWu03]



Rys. 8. Skramblowanie w dziedzinie transformaty falkowej [DuWe04]

w koderze MPEG typu open-source o nazwie mpeg2enc, zawartym w pakiecie mjpgTools dostępnym na stronie *http://sourceforge.net/projects/mjpgtools/*. Wyniki działania wybranych algorytmów mogą być porównywane na stronie *http://www.ganesh.org/book* poprzez zadawanie rozmaitych parametrów wejściowych, w tym docelowych przepływności i obrazów testowych.

Rekomendowane oprogramowanie dla JPEG2000 znajduje się w piątej części tegoż standardu o nazwie Reference Software. Obejmuje ono: JasPer w języku C (*http://www.ece.uvic.ca/~mdadams/jasper/*) oraz JJ2000 w Javie (*http://jpeg2000.epfl.ch/*). Obydwie implementacje zawierają kod źródłowy pierwszej części standardu i posiadają licencję typu freely available standards. Natomiast Kakadu (*http://www.kakadusoftware.com/*) jest komercyjna i wyposażona, oprócz pierwszej części standardu, w kilka użytecznych właściwości pochodzących z drugiej części, przykładowe aplikacje, w tym klient-serwer, obejmujące dziewiątą część standardu (protokół JPIP). Komercyjne oprogramowanie jest oferowane np. przez firmę Aware Inc. (http://www.aware.com/imaging/jpeg2000.htm).

Czwarta część standardu JPEG2000 – Conformance testing – zawiera oprogramowanie służące do testowania zgodności strumienia kodowego z tym formatem.

W MPEG-4 jej odpowiednikiem jest czwarta część standardu, natomiast piąta to Reference Software. W implementacjach MPEG-4 występują ścisłe restrykcje w zakresie standaryzacji formatu strumienia bitowego oraz operacji dekodera, natomiast poszczególni producenci stosują dowolne rozwiązania koderów i dekoderów. Znanymi przykładami kodeków są: DivX, XviD, 3ivx D4, X.264, Windows Media Video 9, Nero Digital.

5. Podsumowanie

W drugiej części artykułu zawarto opisy narzędzi dostarczających usług poufności, uwierzytelniania i integralności oraz kontroli dostępu obrazów oraz materiału wideo. Niektóre z rozwiązań zostały tak zaprojektowane, że istnieje możliwość adaptacji zabezpieczeń do warunków transmisyjnych i pojemności terminali użytkowników. Dokonano analizy rozwiązań operujących na obrazie oraz wideo skompresowanych przy użyciu nowszych standardów, takich jak JPEG2000 czy MPEG-4/H.264.

Na końcu wspomniano o implementacjach standardów JPEG 2000, MPEG-4 oraz niektórych algorytmów szyfrowania wideo.

Piotr Piotrowski
Instytut Telekomunikacji, Wydział Elektroniki i Technik Informacyjnych,
Politechnika Warszawska
P.T.Piotrowski@elka.pw.edu.pl

Literatura

[DaQi03] Dajun H., Qibin S., „A semi-fragile object based video authentication system.” ISCAS2003.
[DeWu03] Deng R., H., Wu Y., „Securing JPEG2000 Code-Streams.” Int. Workshop on Advanced Developments in Software and Systems Security (WADIS’03), December 2003.
[DuWe04] Dufaux F., We S., „JPSEC for Secure Imaging in JPEG 2000.” Procedings of SPIE – Volume 5558, November 2004.
[UhPo05] Uhl A., Pommer A., Image and Video Encryption. From Digital Rights Management to Secured Personal Communication, Springer, 2005.
[WeAp01] Wee S., Apostolopoulos J., „Secure scalable streaming enabling transcoding without decryption” IEEE International Conference on Image Processing, Thessaloniki, Greece, October 2001.
[WeAp03] Wee S., Apostolopoulos J., „Secure scalable streaming and secure transcoding with JPEG-2000.” IEEE International Conference on Image Processing, September 2003.
[WeAp04] Wee S., Apostolopoulos J., „Secure transcoding with JPSEC confidentiality and authentication.” Invited paper in Media Security Issues in Streaming and Mobile Applications, IEEE, ICIP 2004.
[ZhQi04] Zhang Z., Qiu G., „A unified authentication framework for JPEG 2000” in IEEE International Conference on Multimedia and Expo (ICME), 2004.
[ZhYu05] Zhu B., Yuan C., „Scalable Protection for MPEG-4 Fine Granularity Scalability”, IEEE Transactions on Multimedia, vol. 7, no. 2, April 2005.

C & C

TH GROUP

idealna łączność ...

COMMEND

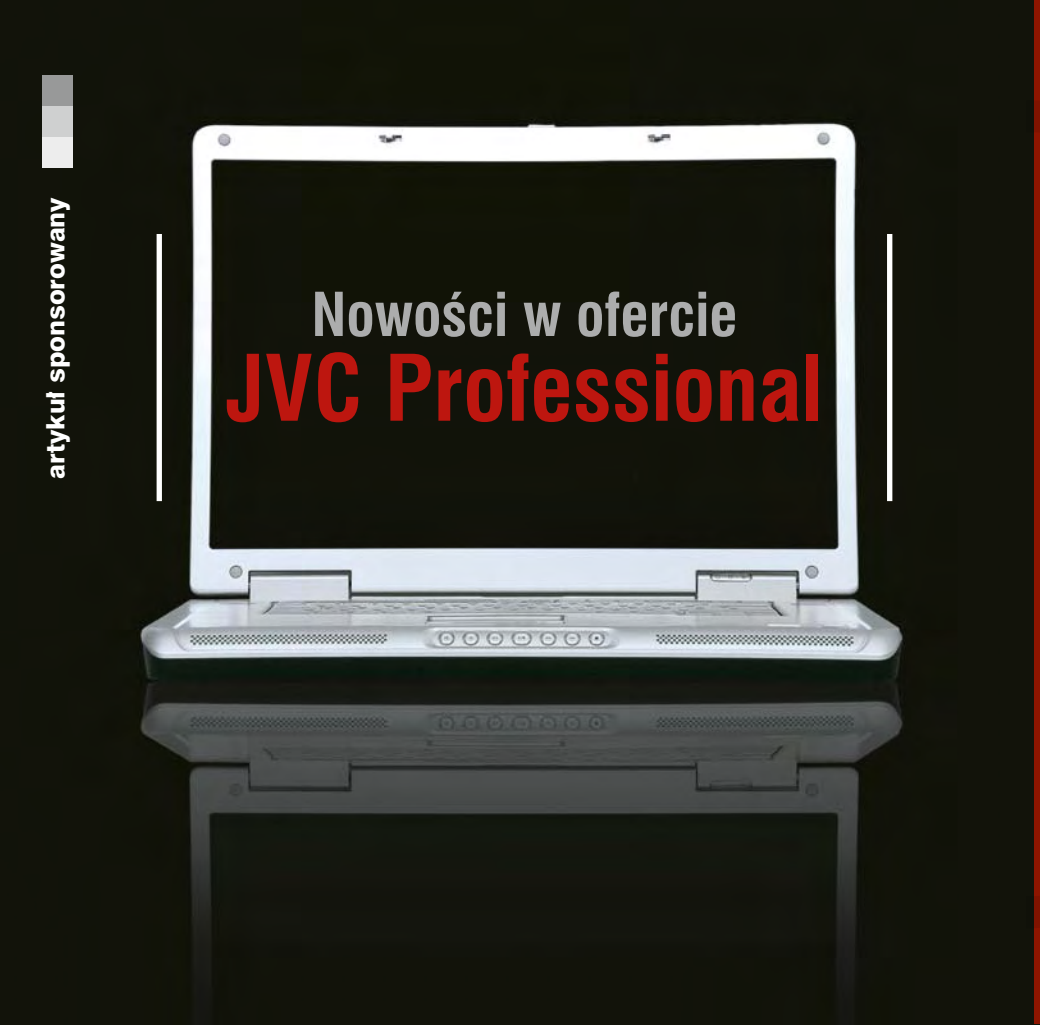
Zintegrowane systemy komunikacji i nadzoru COMMEND

- Cyfrowa jakość głosu
- Globalny zasięg sieci interkomów poprzez internet (Intecom Over IP)
- Integracja z innymi systemami zewnętrznymi (np.: CCTV, PA, systemy alarmowe, kontrola dostępu)
- Szeroka funkcjonalność w wyselekcjonowanych sektorach

C&C Partners Telecom Sp. z o.o., 64-100 Leszno, ul. 17 Stycznia 119/121
tel. 065 525 55 55, fax 065 525 56 66, e-mail: zabezpieczenia@ccpartners.pl

www.commend.ccpartners.pl

artykuł sponsorowany



Nowości w ofercie JVC Professional

Przełom roku 2007/2008 to czas wprowadzenia do oferty firmy JVC Professional kilku nowych urządzeń telewizji dozorowej. Nowości odzwierciedlają wyraźnie zauważalny trend, jakim jest większy udział rozwiązań sieciowych w CCTV

Wraz z wprowadzeniem stacjonarnej kamery sieciowej VN-V25U firma JVC Professional zainaugurowała nową serię urządzeń IP VN-Vxx.

Kamera JVC VN-V25U została wyposażona w przetwornik CCD 1/4" z progresywnym skanowaniem. W rezultacie otrzymujemy bardzo dobrej jakości obraz bez efektu smużenia szybko poruszających się obiektów, z wyraźnymi szczegółami i bardzo dobrą ostrością.

W zależności od potrzeb można wykorzystać dwa rodzaje kompresji: MPEG-4 lub Motion JPEG. Kamera wysyła do 30 klatek na sekundę w rozdzielczości VGA. Klient ma pełną możliwość ustawienia wielkości pojedynczej klatki w celu dobrania optymalnej wielkości strumienia. Kamera została wyposażona w funkcję *Easy Day/Night*, dzięki której może automatycznie przechodzić w czarno-biały tryb pracy w trudnych warunkach oświetleniowych. Minimalne oświetlenie to 0,5 lx w kolorze oraz 0,4 lx w trybie czarno-białym (wideo 50%, F1.2, AGC włączone). Ponadto VN-V25U posiada funkcję *Sense Up*, dzięki której przy słabym oświetleniu wydłużony jest czas migawki (x2, 4, 8, 16, 32, 64) w celu uzyskania prawidłowo naświetlonej sceny. W przypadku sytuacji odwrotnej, czyli dużych kontrastów, z pomocą przychodzi funkcja *Easy Wide-D*. Po jej włączeniu zarówno bardzo jasne jak i ciemne partie obrazu są oddawane prawidłowo, co pozwala na dostrzeżenie wszystkich szczegółów obserwowanej sceny.

Inne przydatne funkcje, które należy wymienić, to:
- maski prywatności,
- detekcja ruchu,
- wybór typu monitora (LCD1/ LCD2/ CRT/ custom),
- wyjście wideo RCA,
- serwer WWW, FTP,
- powiadamianie e-mailem o zdarzeniach,
- POE.

Istotny jest również fakt, że kamera może pracować w zakresie temperatur od -10 do +50°C bez obudowy zewnętrznej.

Kolejny model kamery wprowadzony do sprzedaży przez firmę JVC to sieciowa kamera stacjonarna o symbolu VN-V26U. Posiada ona wszystkie funkcje kamery VN-V25U oraz dodatkowo:
- mechanicznie usuwany filtr IR i w związku z tym lepszą czułość (minimalne oświetlenie 0,3 lx w kolorze, 0,03 lx w trybie czarno-białym, wideo 25%, F1.2, AGC włączone),
- wbudowany mikrofon.

Następny nowy produkt sieciowy to kamera szybkoobrotowa o symbolach VN-V686U (wersja wewnętrzna) oraz VN-V686WPU (w obudowie zewnętrznej IP66).

Wyróżniającą cechą kamer VN-V686U i VN-V686WPU jest zoom optyczny x36 (zakres ogniskowych 3,4–122 mm). W związku z tak dużym zoomem konieczne było zastosowanie stabilizatora obrazu. Ponadto zaimplementowano funkcję śledzenia obiektów, detekcji ruchu i maski prywatności. Mechanicznie usuwany filtr IR pozwala na uzyskanie bardzo dobrej jakości obrazu w trudnych warunkach oświetleniowych: minimalne oświetlenie to 0,04 lx w trybie czarno-białym (wideo 50%, F1.6, AGC włączone).

W kamerach zastosowano nowy mechanizm obrotu głowicy Direct Drive Motor. Dzięki temu zwiększono dokładność obrotu i uchyłu do 0,01 stopnia, uzyskano zakres zmian prędkości uchyłu i obrotu od 0,04 stopnia na sekundę

do 400 stopni na sekundę, a głowica pracuje bardzo cicho. Tym samym, w porównaniu z poprzednimi modelami, w znaczący sposób poprawiono jej funkcjonalność – można nią sterować szybciej, a jednocześnie bardziej precyzyjnie.

Listę użytecznych funkcji uzupełniają: *Easy Wide-D*, czyli rozszerzenie zakresu dynamiki kamery, automatyczny balans bieli, *Sense Up* wydłużająca czas migawki (x2, 4, 8, 16, 32, 64), kompensacja oświetlenia tylnego z możliwością zdefiniowania czterech stref, *One-Touch Lock* umożliwiająca szybki i bezpieczny montaż kamery.

Kamery VN-V686U i VN-V686WPU charakteryzują się podobnymi funkcjami sieciowymi, jak model VN-V25U – wysyłają do 30 klatek na sekundę w kompresji MPEG-4 lub Motion JPEG o rozdzielczości VGA, pozwalają definiować wielkość strumienia wideo, obsługują do 20 zdalnych klientów jednocześnie. Zarówno VN-V686U jak i VN-V686WPU są zasilane napięciem $24V_{AC}$.

Fot. 1. Kamera JVC VN-V686WPU w obudowie zewnętrznej IP66

Uzupełnieniem oferty produktów sieciowych jest rejestrator VR-N1600U. Wyprodukowano go wykorzystując doświadczenia dwóch znaczących w branży firm: JVC Professional i Milestone. JVC dostarczyło części sprzętowej, natomiast Milestone jednego ze swoich sztandarowych produktów programistycznych – *Xprotect Enterprise*. W rezultacie uzyskano urządzenie o wyglądzie i sposobie obsługi rejestratora cyfrowego, co znacznie ułatwia pracę operatorom, oraz nowej funkcji – możliwości podglądu, rejestracji i odtwarzania archiwum z 16 kamer sieciowych.

Ponieważ liczba funkcji dostępnych w rejestratorze jest duża, a ramy niniejszego artykułu wąskie, wymienione zostaną tylko najistotniejsze spośród nich:

– automatyczna rejestracja kamer bez konieczności zakupu dodatkowych licencji,
– do 5 TB powierzchni dyskowej,
– obsługa funkcji PTZ w sieciowych kamerach obrotowych JVC z poziomu rejestratora,
– łatwe dodawanie kamer do systemu,
– nagrywanie do 160 klatek na sekundę.

VR-N1600U jest już drugim urządzeniem serii. Od ponad roku dostępny jest 9-kanałowy rejestrator hybrydowy VR-N900U.

Fot. 2. Kamera obrotowa JVC TK-C686E

Wśród analogowych urządzeń JVC na uwagę niewątpliwie zasługuje kamera obrotowa TK-C686E (wersja wewnętrzna) oraz TK-C686WPE (wersja zewnętrzna w obudowie IP66) – jest to moduł kamery obrotowej opisany powyżej, przy opisie VN-V686U. Podstawową cechą kamery jest bardzo duży zoom optyczny (x36). Tym samym JVC po raz kolejny wprowadza do sprzedaży urządzenie wyprzedzające produkty konkurencji. Kamera TK-C676E, obecna na rynku już od kilku lat, była również przez długi okres jedynym produktem o tak wysokim parametrze zoomu optycznego (x27).

Napęd głowicy PTZ stanowi nowy mechanizm *Direct Drive Motor*, zwiększający równocześnie szybkość oraz precyzję obrotu i przechyłu kamery. Ponadto kamera wyposażona jest w bardzo użyteczne funkcje rozszerzonego zakresu dynamiki ExDR, Auto Tracking, stabilizację obrazu, maski prywatności oraz 100 presetów.

Wraz z kamerą dostępne są różnego rodzaju uchwyty ścienne i sufitowe.

Opisane produkty nie są jedynymi nowościami, które pojawiły się lub pojawią w najbliższym czasie na rynku telewizji dozorowej. Duża konkurencja w tej branży wymaga ciągłego doskonalenia produktów i wprowadzania nowych, dlatego firma JVC Professional właśnie takie założenia realizuje.

Fot. 3. Rejestrator sieciowy JVC VR-N1600U

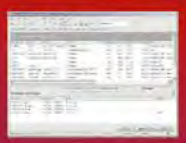
Więcej informacji na temat opisywanych kamer i rejestratorów JVC znajduje się na stronie *www.jvcpro.pl*.

Sławomir Janiso
Radioton

PROTECTOR

Centrum Zarządzania Ruchem Osobowym

Rozliczanie Czasu Pracy



Kontrola Dostępu "SOYAL"

System zarządzania kuczami oraz skrytkami

Widzimy Twoją przyszłość z nami!

Centralny System Monitoringu "CMS 24"

Tripody, Bramki, Śluzy

Kontrola Wartowników

DVR + System POS

System zarządzania depozytami "PILLAR"

System przesyłania obrazu po skrętce

System przesyłania obrazu po sieci LAN

Zapraszamy na nasze stoisko podczas zbliżających się targów SECUREX 2008

www.protector-polska.pl

tel: +48 (091) 431 83 10
fax: +48 (091) 431 83 11

biuro@protector-polska.pl

Nowe systemy kamerowe Pelco (cz. 1)

artykuł sponsorowany

Na przełomie roku firma Pelco, światowy lider w dziedzinie systemów CCTV, wprowadziła do swojej oferty nowe modele kamer dzienno-nocnych: system Spectra IV SE Horizon oraz serię kamer kompaktowych C10DN. Celem artykułu jest dostarczenie podstawowych informacji o tych produktach

Systemy kamerowe Spectra IV SE Horizon z 35-krotnym zoomem to najnowsze produkty w rodzinie Spectra. Jest to linia prestiżowych dla Pelco, wysokiej jakości produktów zawierających wiele innowacji technologicznych. Ważnym, choć często niedostrzeganym czynnikiem wpływającym na jakość obrazu z kamery szybkoobrotowej jest zależność między kształtem klosza kamery a ułożeniem obiektywu modułu kamerowego. Podczas projektowania systemu kamerowego Spectra Horizon zwrócono na to szczególną uwagę. Celem projektantów było zapewnienie krystalicznie czystego obrazu przy dużych powiększeniach optycznych i poszerzonym kącie widzenia w pionie.

Unikatowy, zintegrowany zestaw optyczny (ang. *Integrated Optics Package*, *IOP*) głowicy obrotowej systemu Spectra IV SE Horizon pozwala na uzyskanie wysokiej jakości obrazu wideo w najtrudniejszych warunkach otoczenia. Głowica kamery systemu Spectra IV SE Horizon może wychylić się w pionie o 18 stopni ponad horyzont, dając tym samym możliwość uzyskania czystego obrazu przestrzeni znajdującej się powyżej miejsca instalacji kamery. Technologia LowLight zapewnia uzyskanie dobrej jakości obrazu podczas obserwacji obszarów z minimalną ilością oświetlenia. Kamera charakteryzuje się 128-krotnym zakresem dynamiki, co pozwala wykonywać kompensację obrazu, jeśli w obserwowanej scenie występują bardzo duże różnice oświetlenia. Funkcja elektronicznej stabilizacji obrazu zmniejsza poprzez obróbkę cyfrową rozmazywanie obrazu spowodowane wibracjami, których źródłem jest np. wiatr lub przemieszczające się ciężkie pojazdy.

Obudowa systemu Spectra IV SE Horizon jest dostępna w trzech wersjach: standardowej do montażu na uchwycie, do pracy w trudnych warunkach temperaturowych montowana w suficie oraz do pracy w trudnych warunkach temperaturowych do montażu na uchwycie.

Każda obudowa zawiera wbudowaną pamięć, która przechowuje informacje o ustawieniach modułu kamery, takich jak nazwy zdefiniowane przez użytkownika, zaprogramowane ujęcia (presety), trasy obserwacji i obszary zabronione. Do transmisji wideo przez skrętkę przeznaczony jest pasywny moduł UTP, który znajduje się na klapce zamykającej dostęp do wnętrza obudowy. Moduł Pelco do transmisji przez jedno- lub wielomodowy światłowód może być także zainstalowany jako podzespół wewnątrz obudowy.

Usprawnienia w programie Spectry IV SE Horizon sprawiają, że urządzenie jest wydajniejsze, a programowanie i obsługa łatwiejsze. Wewnętrzny zegar steruje harmonogramami związanymi z zaprogramowanymi presetami i trasami obserwacji. Użytkownik może zaprogramować osiem czworobocznych obszarów prywatnych. Dostęp do menu opcji programowania jest chroniony hasłem, co zabezpiecza przed dostępem osób nieupoważnionych. Informacje o pozycji i nachyleniu mogą być wyświetlane na ekranie, jeśli jest taka potrzeba. Menu programowania kamery jest dostępne w wielu językach: angielskim, polskim, hiszpańskim, portugalskim, włoskim, francuskim, niemieckim, rosyjskim, tureckim i czeskim.

Szybkość ruchu modułu kamery Spectra Horizon może się zmieniać w szerokim zakresie od płynnego, szybkiego ruchu 400 stopni/s do powolnego 0,1 stopnia/s. System ma możliwość ciągłego obrotu o 360 stopni. Ciekawa jest funkcja „auto-przerzutu", która umożliwia obrót o 180 stopni i samoczynną zmianę pozycji kamery podczas obserwacji obiektu poruszającego się bezpośrednio pod kamerą.

Typ obudowy	Kolor obudowy	Klosz	Model (PAL)
Montaż sufitowy, trudne warunki pracy*	Czarna	Przyciemniony	SD4H35-F-E0-X
Montaż sufitowy, trudne warunki pracy*	Czarna	Przeźroczysty	SD4H35-F-E1-X
Montaż na uchwycie, standardowa	Jasnoszara	Przyciemniony	SD4H35-PG-0-X
Montaż na uchwycie, standardowa	Jasnoszara	Przeźroczysty	SD4H35-PG-1-X
Montaż na uchwycie, trudne warunki pracy **	Jasnoszara	Przyciemniony	SD4H35-PG-E0-X
Montaż na uchwycie, trudne warunki pracy**	Jasnoszara	Przeźroczysty	SD4H35-PG-E1-X

Tab. 1. Dostępne modele systemu kamerowego Spectra Horizon
**Zawiera podgrzewacz i wentylator; **Zawiera podgrzewacz, wentylator i osłonę przeciwsłoneczną*

C10DN-6X	C10DN-7X
CCD 1/3 cala, dzienno-nocna, 540 TVL, PAL	CCD 1/3 cala, dzienno-nocna, 540 TVL, PAL
24V~/12V=	230V~
	

Tab. 2. Dostępne modele kamery C10DN

Opcjonalne urządzenia instalacyjne i diagnostyczne, takie jak IPS-RMK i IPS-CABLE, pozwalają instalatorowi podglądać obraz na małym ekranie LCD 5,6 cala, a przy pomocy palmtopa sterować PTZ oraz programować system kamerowy w miejscu instalacji.

Główne cechy Spectry IV SE Horizon:

- wysokiej jakości obraz pod każdym kątem;
- nachylenie pionowe do 18° ponad horyzont;
- automatyczne ogniskowanie;
- kamera wysokiej rozdzielczości ze zintegrowaną optyką;
- kamera dzienno-nocna, 540 TVL, 128-krotny zakres dynamiki (WDR);
- detekcja ruchu, elektroniczna stabilizacja obrazu;
- obszary zastrzeżone;
- strefy z nazwami do 20 znaków każda;
- informacje o pozycji, nachyleniu i zoomie na ekranie;
- zabezpieczenie hasłem
- „zamrażanie" obrazu podczas realizacji presetów;
- wbudowane zabezpieczenia przed przepięciami i wyładowaniami atmosferycznymi;
- zintegrowany pasywny obwód UTP;
- wbudowany zegar sterowania harmonogramami;
- wyjście z przeplotem lub progresywnym skanowaniem.

Kamery serii C10DN

Seria C10DN to najmniejsze w ofercie Pelco kamery dzienno-nocne. Technologia dzień/noc z firmy Pelco umożliwia wyjątkową wydajność kamery w szerokim zakresie warunków oświetleniowych. W kamerze znajduje się ruchomy filtr odcinający zakres podczerwieni (IR). Usunięcie filtra następuje podczas przełączania między trybem kolorowym i czarno-białym, np. wówczas, kiedy potrzebna jest większa czułość w warunkach bardzo słabego oświetlenia.

Seria C10DN to kamery wysokiej rozdzielczości (540 TVL), które mogą pracować przy oświetleniu minimum 0,3 luksa w trybie dziennym i minimum 0,07 luksa w trybie nocnym.

Dostępne w kamerze funkcje to: automatyczna detekcja rodzaju zasilania 12V= lub 24V~, automatyczna regulacja wzmocnienia (AGC), elektroniczne sterowanie migawką (ESC), redukcja migotania. Dodatkowo seria C10DN ma wbudowaną funkcję automatycznego balansu bieli (AWB) dla trudnych warunków oświetleniowych i funkcję kompensacji oświetlenia tła, która koryguje obraz tak, aby obiekty nie były widziane jako ciemne, kiedy ich tło jest silnie oświetlone. Funkcje te są ustawiane w prosty sposób, przy użyciu menu ekranowego.

Kamera C10DN jest przystosowana do zamocowania obiektywu typu CS. Zastosowane mogą być obiektywy stałe, ręcznie regulowane oraz z automatyczną przesłoną ze sterowaniem DC lub wideo. Podłączenie sterowania przesłoną jest realizowane poprzez czterostykowy kwadratowy wtyk, który należy do standardowego wyposażenia obiektywów produkowanych przez Pelco.

Wygodne menu ekranowe pozwala wybrać obszary maskowania, nazwy, korekcje pikseli i profile oświetlenia. Nie są to funkcje często spotykane w kompaktowych kamerach. Menu umożliwia także wykonanie ustawień dla kolorowego i czarno-białego trybu pracy.

Instalacja kamer C10DN odbywa się szybko i łatwo. Dla modelu C10DN-6X rekomendowane są obudowy DF5, DF8A, EH100, EH3508 i EH2508. Kamery te mogą być częścią zestawów Pelco DomePak i ImagePak. Opcjonalny uchwyt

C10-UM może być stosowany wszędzie tam, gdzie kamera C10DN-6X lub C10DN-7X będzie montowana bez obudowy – na ścianie, suficie lub do profilu.

Rekomendowane obiektywy

– Seria 13FA, FD – obiektywy o stałej ogniskowej, format 1/3 cala, FA (ręczna przesłona), FD (automatyczna przesłona, DD);
– Seria 13VA, VD, VDIR – obiektywy o zmiennej ogniskowej, format 1/3 cala, VA (ręczna przesłona), VD (automatyczna przesłona, DD), VDIR (automatyczna przesłona, DD, podczerwień);
– Seria 13ZD – obiektywy motor-zoom, format 1/3 cala (automatyczna przesłona, DD). Obiektyw nie należy do wyposażenia kamery.

Główne cechy serii C10DN:

– kompaktowa obudowa, niewielkie rozmiary;
– kamera dzienno-nocna ze sterowaniem ręcznym lub automatycznym;
– przetwornik CCD 1/3 cala;
– cyfrowa obróbka sygnału wizyjnego (DSP);
– rozdzielczość 540 TVL;
– menu kamery na ekranie;
– cztery profile zdefiniowane w fabryce, jeden profil definiowany przez użytkownika;
– automatyczny balans bieli, automatyczna regulacja wzmocnienia;
– kompensacja oświetlenia tła, elektroniczne sterowanie migawką;
– redukcja migotania;
– mocowanie obiektywu typu CS;
– automatyczna detekcja zasilania 12V=/ 24V~.

Więcej informacji na temat opisanych kamer dzienno-nocnych można znaleźć na stronie *http://www.pelco.com* oraz u dystrybutorów Pelco w Polsce. W drugiej części artykułu przedstawione zostaną informacje o nowych kamerach kolorowych wysokiej rozdzielczości z oferty Pelco.

Norbert Góra
Pelco Europe

NOVUS®

Profesjonalne rozwiązanie dla systemów CCTV

NOWA generacja monitorów LCD

monitory LCD serii 300

- zaprojektowane specjalnie dla systemów CCTV
- przekątna ekranu: 17", 19"
- wysoka rozdzielczość: 580 TVL
- menu ekranowe w języku polskim
- złącza sygnału wideo: 2 x BNC, S-Video, VGA
- złącze fonii: RCA, Jack
- wbudowane głośniki
- zasilanie: 12 VDC (zasilacz sieciowy w zestawie)
- kompatybilne ze wszystkimi rejestratorami marki NOVUS®

Wyłączny dystrybutor produktów NOVUS® w Polsce:

AAT Trading Company Sp. z o.o.
02-801 Warszawa, ul. Puławska 431, tel. 022 546 0 546, fax 022 546 0 501
www.aat.pl

Karty wizyjne Novus serii AMPG

Karty wizyjne Novus są obecne na rynku systemów telewizji dozorowej od ponad pięciu lat. Okres ten charakteryzował się bardzo dynamicznym rozwojem technologicznym systemów telewizji. Zmiany dotyczyły również kart wizyjnych. Mówiąc nieco przewrotnie, wiele musiało się zmienić, by wszystko zostało po staremu, tzn. by mogły nadal spełniać ciągle rosnące wymagania klientów oraz sprostać konkurencji

W związku z powyższym w regularnych odstępach czasowych wprowadzano kolejne serie kart wizyjnych Novus: A, B, MPG, które charakteryzowały się nowymi rozwiązaniami sprzętowymi, a główny program do obsługi DVR Main uzupełniany był o nowe funkcje. Na początku roku oferta kart Novus zostanie uzupełniona o serię AMPG – drugą generację kart z kompresją sprzętową.

W porównaniu z kartami serii A i B z kompresją programową karty z kompresją sprzętową posiadają wiele zalet zwiększających możliwości systemu nadzoru i rejestracji, z których główne to:

– sprzętowy układ kodeka MPEG-4 na karcie wizyjnej zapewniający lepszą jakość obrazu przy mniejszym zapotrzebowaniu na zasoby komputera (stabilniejsza praca, obsługa połączeń sieciowych itp.);

– sprzętowe układy detekcji ruchu zapewniające bardziej efektywną analizę obrazu;

– sprzętowy filtr przeplotu umożliwiający, przy rozdzielczości zapisu 720x576, zniwelowanie efektu rozmycia szybko przemieszczających się obiektów;

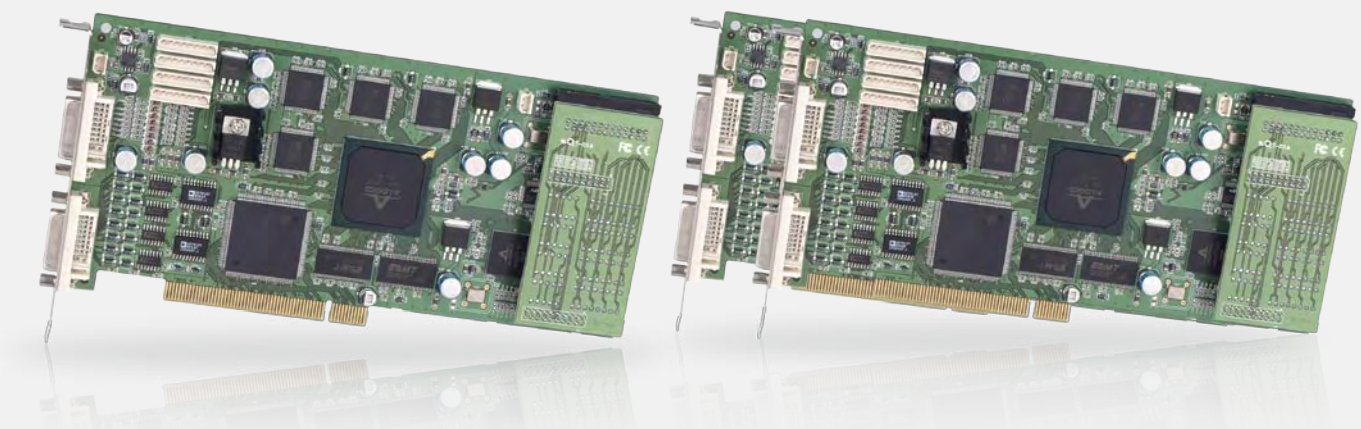
– wyświetlanie „na żywo" i rejestracja w czasie rzeczywistym o szybkości nagrywania 25 obrazów na sekundę (ang. *images per second*, *ips*) dla każdego z kanałów (w rozdzielczości CIF);

– sprzętowe układy do obróbki audio na karcie, które uniezależniają rejestrację audio od zainstalowanych w komputerze kart dźwiękowych oraz zapewniają liczbę wejść audio równą liczbie wejść wideo.

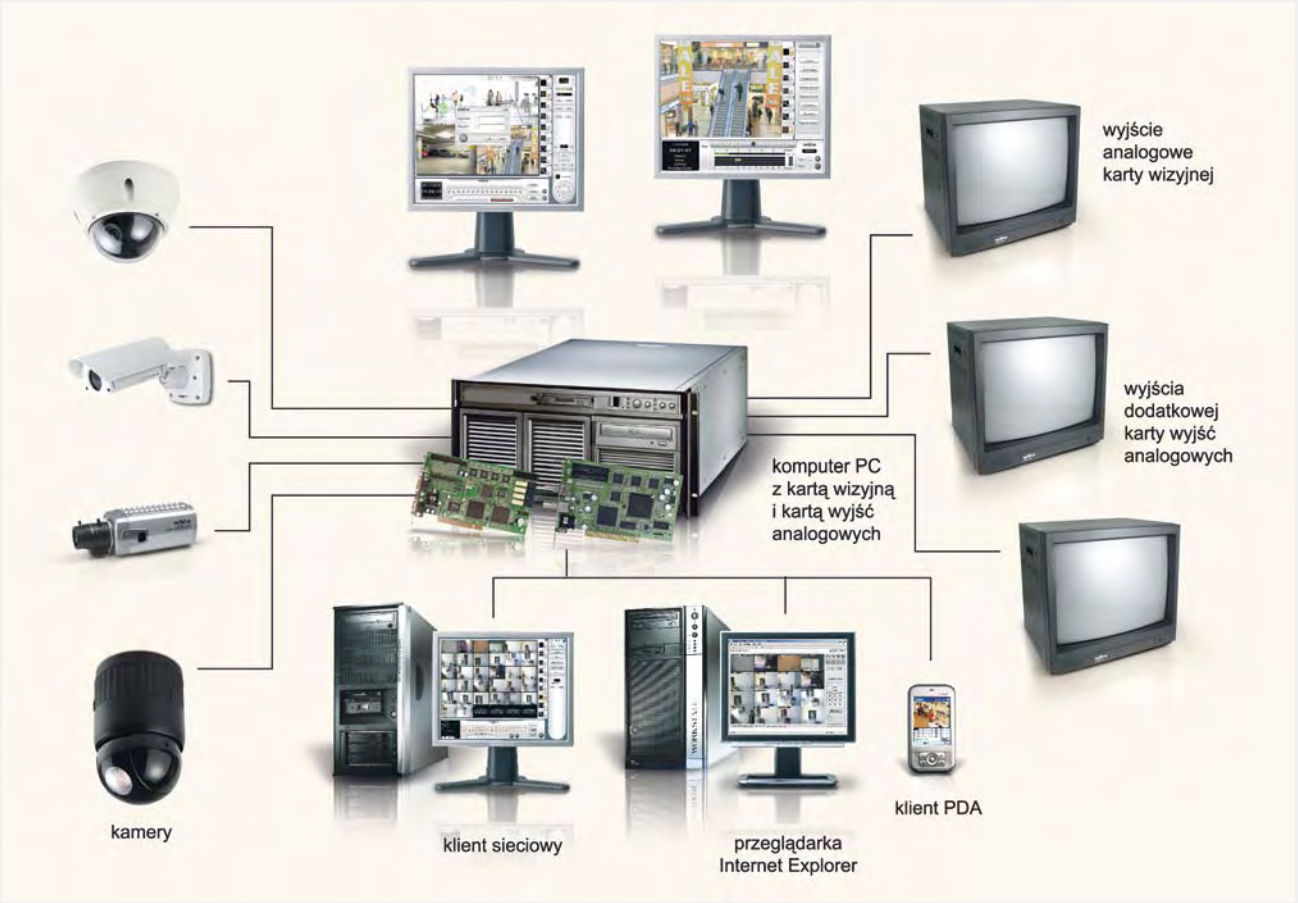
Ogromną zaletą kart wizyjnych, w porównaniu z rejestratorami typu *stand alone*, jest możliwość budowy dużych systemów, składających się nawet z 32 punktów kamerowych. Dostępne na rynku rejestratory są z reguły 16-kanałowe. Rozbudowę kart umożliwił rozwój sprzętu komputerowego, a przede wszystkim wprowadzenie procesorów wielordzeniowych oraz nowszych chipsetów płyt głównych. Karty 32-kanałowe cieszą się dużym uznaniem klientów, a dla wielu obiektów o większej niż 16 liczbie punktów kamerowych są bardzo efektywnym rozwiązaniem.

Wśród kart serii AMPG można wyróżnić dwa modele: NVB-400/16AMPG oraz NVB-800/32AMPG. Zapewniają one efektywną obróbkę 16 lub 32 kanałów wideo z szybkością nagrywania podaną w tabeli 1.

Dodatkowo rejestrują 16 lub 32 kanały audio i pozwalają za pomocą wyjść przekaźnikowych wysterować 4 lub 8 urządzeń



Fot. 1. Karty serii AMPG: NVB-400/16AMPG – jedna karta, NVB-800/32AMPG – dwie karty (Master i Slave)



Rys. 1. Przykładowy schemat systemu zbudowanego z wykorzystaniem kart serii AMPG

zewnętrznych (alarmy, syreny itp.). Oba modele posiadają sprzętowy układ detekcji ruchu oraz sprzętowy filtr przeplotu.

Wszystkie karty serii umożliwiają wyświetlanie „na żywo" obrazów z kamer niezależnie od aktualnej szybkości rejestracji. Funkcja ta ma szczególnie duże znaczenie w systemach z ciągłym nadzorem operatorskim, bowiem przy wyświetlaniu poklatkowym szybciej pojawia się efekt zmęczenia – osłabienie percepcji operatorów. Oprócz głównego wyjścia monitorowego PC (możliwa praca dwumonitorowa dla dwugłowicowych kart graficznych) karty serii AMPG posiadają wyjście analogowe, dublujące podziały wyświetlane na monitorze PC.

W przeciwieństwie do urządzeń z serii MPG nowy model NVB-400/16AMPG jest zbudowany z wykorzystaniem tylko jednej karty PCI. Pozwala to na dowolną alokację zasobów systemu, tzn. każdej kamerze można przypisać dowolną szybkość zapisu, a także dowolną rozdzielczość zapisu. Dla modelu NVB-800/32AMPG alokacja zasobów systemu (szybkość i rozdzielczość) jest realizowana w ramach grupy 16 kamer przyporządkowanych do jednego układu obróbki.

Karty AMPG uzupełniają linię kart Novus z kompresją sprzętową, wprowadzając model 32-kanałowy oraz zamieniając model 16-kanałowy. W tabeli 2. znajduje się zestawienie wszystkich serii i modeli kart Novus.

Rozdzielczość	Prędkość nagrywania (*ips*)	
	NVB-400/16AMPG	NVB-800/32AMPG
CIF (352x288)	400	800
2CIF (704x288)	200	400
4CIF (704x576)	100	200

Tab. 1. Rozdzielczości i prędkości nagrywania kart wizyjnych serii AMPG

Nowe modele kart serii AMPG są obsługiwane, podobnie jak wszystkie poprzednie serie, z poziomu oprogramowania DVR Main. Kompatybilność z nowymi modelami jest zachowana również w przypadku oprogramowania do zdalnej obsługi DVR Net oraz aplikacji dla urządzeń PDA.

Uproszczony schemat systemu zbudowanego z wykorzystaniem kart serii AMPG może wyglądać jak na rys.1.

Wyjście analogowe w kartach serii AMPG dubluje podziały monitora głównego PC. Dostępna jako rozszerzenie serii AMPG karta wyjść analogowych (dwa wyjścia na monitor analogowy z podziałami) rozszerza funkcjonalność systemu o obsługę dodatkowych monitorów pomocniczych (monitorów spot). Karta wyjść może współpracować ze wszystkimi

Fot. 2. Karta wyjść analogowych

Kompresja	Seria	Modele kart (w środkowej kolumnie podano liczbę kanałów)			Seria	Kompresja
programowa	A	NVB-025/4A	4	NVB-100/4MPG	MPG	sprzętowa
		NVB-050/4A				
		NVB-050/8A	8	NVB-200/8MPG		
		NVB-100/8A				
		NVB-050/16A	16	NVB-400/16AMPG	AMPG	
	B	NVB-100/16B				
		NVB-100/16BLV				
		NVB-200/16B				
		NVB-200/16BLV				
		NVB-200/32B	32	NVB-800/32AMPG		
		NVB-400/32B				

Tab. 2. Modele kart wizyjnych Novus

kartami wizyjnymi Novus (oprócz czterokanałowych kart z serii A – NVB-025/4A i NVB-050/4A).

Funkcjonalność karty wyjść analogowych obejmuje:
– wyjście 1 – podziały: pełny ekran, 4, 6, 9, 16,
– wyjście 2 – podziały: pełny ekran, 4,
– ukrywanie kamer,
– definiowane sekwencje kamer,
– pop-up (wymuszenie wyświetlania) obrazów z kamer alarmowych (podział: pełny ekran i 4).

Systemy rejestracji wizji wykorzystujące karty cieszą się uznaniem wielu instalatorów. Według czasopism branżowych rejestratory *stand alone* oraz systemy rejestracji typu *PC based* instalowane są w proporcji 60% do 40% i w najbliższym czasie nie powinniśmy się spodziewać zachwiania tej proporcji. Wydaje się, że powyższe różne sposoby rejestracji zostaną zastąpione przez systemy telewizji dozorowej IP, które w zgodnej opinii analityków mają przed sobą okres dynamicznego rozwoju.

Patryk Gańko
Krzysztof Zych
Novus

Obiektywnie patrząc najlepszy

Computar – szeroka gama
najczęściej na świecie kupowanych obiektywów CCTV.

computar®

CBCGROUP

CBC (Poland) Sp. z o.o., ul. Gustawa Morcinka 5/6, 01-496 Warszawa,
tel.: (0 22) 638 44 40, faks: (0 22) 638 45 41, www.cbcpoland.pl, e-mail: info@cbcpoland.pl

artykuł sponsorowany

Bezpieczna kotłownia gazowa – zgodnie z przepisami

Gaz ziemny i propan-butan to najbardziej wydajne, czyste, łatwo dostępne i ekologiczne paliwa. Dlatego coraz częściej ogrzewają nasze domy, mieszkania i budynki użyteczności publicznej. Wbrew czasami spotykanym opiniom, są także bezpieczne

1. Geneza systemów zabezpieczeń kotłowni gazowych

Nowoczesne gazownictwo opiera się dziś nie tylko na doświadczeniu, nowych materiałach i technologiach, komputeryzacji procesów badawczych i projektowych, ale także na nowych technikach podnoszących bezpieczeństwo eksploatacji paliw gazowych. Nawet przy zastosowaniu najnowszych osiągnięć techniki nie jesteśmy w stanie pominąć wpływu człowieka na proces eksploatacji paliw gazowych, a tam, gdzie ma on decydujący wpływ na właściwości instalacji gazowej, należy spodziewać się możliwości wystąpienia awarii.

W tym momencie możemy oczekiwać wsparcia wszechobecnej elektroniki. Okazało się bowiem, że na bazie zaawansowanych technologicznie elementów elektronicznych (sensorów) można skutecznie wykrywać wycieki gazów wybuchowych w powietrzu. Czułość tych elementów okazała się na tyle wysoka, że możemy dowiedzieć się o rosnącym zagrożeniu znacznie wcześniej niż nastąpi często nieobliczalna w skutkach awaria. Wraz z rozwojem elektroniki koszty systemów zabezpieczających obniżyły się do poziomu, który gwarantuje powszechność stosowania. To właśnie powszechność stosowania systemów zabezpieczających jest gwarantem podniesienia bezpieczeństwa stosowania paliw gazowych. A najczęściej spotykamy się z gazem (ziemnym lub propanem-butanem) w... kotłowni.

2. Nowa era – systemy „aktywne”

Dalszy rozwój myśli technicznej pozwolił na wprowadzenie „aktywnych” elementów do systemów wykrywania gazów. Aktywny element w postaci zaworu odcinającego dopływ gazu do instalacji pozwolił na uniezależnienie skuteczności działania systemu od obecności lub kwalifikacji osób zajmujących się jego obsługą oraz od szybkości i sprawności ich interwencji. W momencie, w którym wprowadzono zawory odcinające, nastąpiła nowa era w dziedzinie bezpieczeństwa użytkowania paliw gazowych.

Tę erę w Polsce zapoczątkował Aktywny System Bezpieczeństwa Instalacji Gazowej typu GX, opracowany i wdrożony do masowej produkcji przez Przedsiębiorstwo Innowacyjno-Wdrożeniowe „Gazex” (producenta detektorów i urządzeń elektronicznych) oraz Polskie Górnictwo Naftowe i Gazownictwo (producenta zaworów odcinających).

Aktywny System Bezpieczeństwa Instalacji Gazowej typu **GX** był pierwszym polskim układem wykrywania i odcinania gazu stosowanym w kotłowniach. Obecnie jest to układ podstawowy i najpopularniejszy, a także najskuteczniejszy. Doświadczenia zdobyte w ciągu przeszło 12 lat produkcji systemu pozwoliły na jego udoskonalenie i dopasowanie go do wymogów nowych przepisów i norm europejskich.

Fot. 1. Zawór MAG-3

Fot. 2. Detektor gazu DEX/FA-B(C)

Nową perspektywę rozwojową otworzyło Rozporządzenie Ministra Infrastruktury RP z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (DzU Nr 75 z 15.06.2002 r.). Rozporządzenie to, będąc wynikiem wielu analiz, między innymi analizy stanu bezpieczeństwa eksploatacji paliw gazowych w budynkach, ustala warunki, jakim powinny odpowiadać instalacje gazowe. Po raz pierwszy ustawodawca **nakłada obowiązek** stosowania systemów sygnalizacyjnych i odcinających dopływ gazu do pomieszczeń o zainstalowanej mocy cieplnej ponad 60 kW. Rozporządzenie określa także umiejscowienie zaworów odcinających (na zewnątrz budynku) i sygnalizacji alarmowej. Było to powodem wdrożenia do produkcji nowych elementów systemu GX.

Podstawową cechą, która zadecydowała o upowszechnieniu się systemu, jest aktywne oddziaływanie na instalację gazową poprzez zawór odcinający. Gwarantuje to pełne bezpieczeństwo eksploatacji instalacji przy braku osób z nadzoru.

Realizowane przez system GX funkcje to:
- wykrywanie podwyższonego stężenia gazu (poziomu ostrzegawczego) i generowanie ostrzegawczego sygnału optycznego oraz sygnału sterującego urządzeniami zewnętrznymi,
- wykrywanie wysokiego stężenia gazu (poziomu alarmowego) i zamykanie zaworu odcinającego dopływ gazu do instalacji oraz generowanie sygnału akustycznego, optycznego i sygnału sterującego urządzeniami zewnętrznymi (np. stycznikiem wyłączającym zasilanie pomieszczeń zagrożonych z sieci energetycznej).

Wszechstronność tego systemu pozwala na zastosowanie go:
- w dużych, miejskich i przemysłowych kotłowniach gazowych (obowiązek stosowania),
- w budynkach użyteczności publicznej (kina, teatry, szkoły),
- w kotłowniach osiedlowych,
- w domowych instalacjach gazowych.

Jest to system, który przez wiele lat o krok wyprzedzał polskie prawodawstwo w zakresie bezpieczeństwa pożarowego i zagrożenia wybuchem w kotłowniach gazowych. Obecnie staje się obowiązującym standardem.

3. Najnowsza era – systemy „aktywne", nadzorowane przez Internet

Cytowane wyżej Rozporządzenie Ministra Infrastruktury ograniczyło możliwość stosowania systemów detekcji gazu w budynkach wielorodzinnych do obiektów ze stałym nadzorem. Nowoczesna elektronika i tym razem udowodniła, że może być wszechobecna. Budynki bez stałej obsługi można przecież nadzorować zdalnie. Niebywały rozwój technik łączności bezprzewodowej i popularyzacja Internetu spowodowały, że nadzór nad rozległymi i skomplikowanymi systemami zabezpieczającymi jest dziś równie prosty jak obsługa komputera PC lub telefonu komórkowego.

Obecny rozwój technologii teleinformatycznych umożliwił dodanie drugiego kierunku „aktywności" w systemie zabezpieczeń kotłowni gazowych. Umożliwił prosty nadzór teleinformatyczny nad systemem detekcji gazu. Wykorzystując technologię GPRS (łączności pakietowej poprzez sieć komórkową GSM), można wiedzieć wszystko nie tylko o stanie bezpieczeństwa kotłowni, ale również o parametrach urządzeń grzewczych, pomiarowych, alarmowych. Nie musimy jedynie oczekiwać sygnałów z nadzorowanego obiektu, możemy także świadomie ingerować w systemy pracujące w obiektach, sterować nimi. Możemy na przykład zdalnie odciąć dopływ gazu, włączyć sygnalizację optyczno-dźwiękową w dozorowanym obiekcie lub włączyć/wyłączyć ogrzewanie.

Dodanie modemu teleinformatycznego GPRS do standardowych elementów systemu detekcji i możliwość autoryzowanego dostępu (przez Internet lub telefon komórkowy) do gromadzonych w „historii" zdarzeń obiektu daje możliwość ekonomicznego nadzoru, kontroli i zarządzania bezpieczeństwem i eksploatacją wielu kotłowni gazowych jednocześnie.

4. Elementy składowe Aktywnego Systemu Bezpieczeństwa Instalacji Gazowej typu GX

Podstawowe elementy systemów GX to:
- pełnoprzelotowy zawór klapowy MAG-3 (fot. 1), posiadający certyfikat ATEX,
- detektor gazu ziemnego lub propanu DEX (fot. 2) o konstrukcji przeciwwybuchowej (certyfikat ATEX),
- moduł alarmowy (fot. 3), którego zadaniem jest sterowanie pracą systemu – MD-n.Z, gdzie n oznacza liczbę możliwych do podłączenia detektorów, a Z – opatentowany sposób sterowania zaworem.

W wersji uproszczonej GX-1 stosowane są domowe detektory gazu typu DK-1.Z... będące jednocześnie sterownikiem

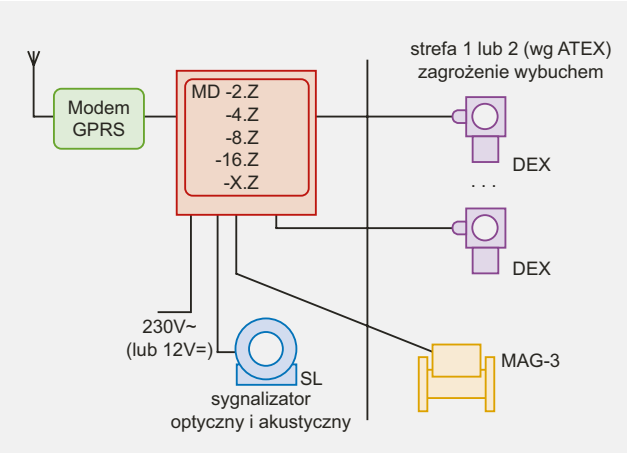
Fot. 3. Moduł alarmowy MD-16.Z i MD-2.Z

zaworu odcinającego. Zawór MAG-3 jest aktywnym elementem systemu GX, realizującym ideę zabezpieczania instalacji. Zawór ten zamykany jest impulsem elektrycznym lub ręcznie. Otwierać zawór można tylko ręcznie, co powoduje wymuszenie świadomej interwencji osób z nadzoru. Brak ciągłego zasilania zaworu (zasilanie jest obecne tylko w chwili jego zamykania) uniezależnia stan zaworu od obecności napięcia zasilającego, przez co zawór jest odporny na zaniki napięcia sieci lub przepięcia. Zawór ten nie reaguje przypadkowo, a wyłącznie w odpowiedzi na świadomą generację sygnału zamykającego. Jest znacznie lżejszy i mniejszy gabarytowo od zaworów kulowych, szczelny (IP44), może pracować na zewnątrz budynków w temperaturze do –30°C. Ten zawór o unikatowej, niebywale prostej, a tym samym taniej i niezawodnej konstrukcji jest zapowiedzią rewolucji w dziedzinie odcinania gazu w instalacjach. Dodatkowo konstrukcja ta jest bardzo bezpieczna i może być stosowana w przestrzeniach zagrożonych wybuchem zgodnie z wymogami Dyrektywy 94/9/WE (ATEX): Ex II 2G c T4.

Detektory gazu typu **DEX** o konstrukcji przeciwwybuchowej zapewniają bezpieczne wykrywanie wszystkich rodzajów gazów wybuchowych. Posiadają wymienny sensor gazu z dwoma fabrycznie ustawianymi progami alarmowymi. Wymienność sensorów powoduje prostotę obsługi i wieloletnią, tanią eksploatację systemu. Detektory zawsze dostarczane są z indywidualnymi zaświadczeniami fabrycznymi oraz atestem kalibracyjnym. Opracowana w 2001 r. wersja detektora DEX/F o budowie rodzaju osłony ognioszczelnej, była pierwszą polską konstrukcją spełniającą wymogi norm europejskich. Po dostosowaniu do wymogów dyrektyw UE w 2004 roku, DEX uzyskał certyfikat ATEX, wydany przez Jednostkę Notyfikowaną nr 1453, GIG KD „Barbara", do stosowania w strefach Ex II 2G. Posiada cechę EEx d IIB lub EEx d IIC.

Moduł alarmowy **MD...Z** zasila detektory gazu i steruje ich pracą oraz generuje impulsy zamykające zawór MAG. Posiada

Fot. 4. Zawór motylkowy ZM



Rys. 1. Schemat blokowy systemu GX

dwa komplety wyjść (dla każdego progu alarmowego): stykowych, umożliwiających połączenie systemu GX z automatyką lub telemetrią oraz napięciowych 12V, sterujących sygnalizatorami optycznymi i akustycznymi. Możliwe jest sterowanie wieloma zaworami przy znacznych odległościach zaworów od systemu wykrywania gazu. Możliwa jest kaskadowa rozbudowa systemu o kolejne moduły. Moduły można wyposażyć w modem GSM/GPRS do zdalnego, dwukierunkowego nadzoru nad systemem.

Duże zainteresowanie ze strony przemysłowych odbiorców gazu (takich jak np. duże kotłownie przemysłowe) sprawiło, że rozpoczęto dostawy niezawodnych, lekkich i relatywnie niedrogich bezkołnierzowych zaworów motylkowych **ZM** z napędami elektrycznymi (fot. 4), o średnicach **DN 125 – DN 500**.

Umożliwiają one zastosowanie automatycznego odcięcia gazu praktycznie w dowolnie dużych kotłowniach gazowych. Producenci elementów systemu GX posiadają wdrożony i certyfikowany przez TÜV system zapewnienia jakości zgodny z europejską normą **ISO 9001**.

Ze względu na modularność systemu GX, przejrzyste połączenia przewodowe, możliwość stosowania typowych materiałów elektroinstalacyjnych oraz dopuszczalne duże odległości pomiędzy detektorami i modułem projektowanie jest proste i wyjątkowo mało czasochłonne, a instalacja systemów jest szybka i sprawna. Przedstawiony powyżej schemat blokowy typowego systemu odcinającego potwierdza powyższe stwierdzenie.

Dodatkowo modularność i duży wybór elementów składowych umożliwia łatwe konfigurowanie potrzebnych systemów lub rozbudowę systemu o dodatkowe elementy.

Zawory MAG-3, jako najlżejsze zawory odcinające na rynku (2–3 razy lżejsze od podobnych), są bardzo łatwe do zainstalowania i już zdobyły wielce pochlebne opinie instalatorów.

5. Zalety systemu GX:

- modularność, proste projektowanie i instalacja,
- natychmiastowe, automatyczne, pewne odcięcie dopływu gazu w przypadku stwierdzenia wycieku,
- odporność na zakłócenia zasilania systemu,
- jednoznaczność sygnalizacji alarmowej,
- dwa komplety wyjść sterujących (dla każdego poziomu alarmowego),
- dostępność zaworów o różnych średnicach,
- łatwość montażu zaworu odcinającego,

– możliwość stosowania detektorów i zaworów w odległych miejscach (kilkaset metrów),
– możliwość powiadamiania dozoru o emisji gazu z instalacji,
– możliwość zdalnego, dwukierunkowego nadzoru teleinformatycznego (przez GPRS),
– możliwość uruchamiania instalacji wentylacyjnej,
– możliwość wyłączenia zasilania instalacji elektrycznej w kotłowni,
– tania eksploatacja systemu i prosta obsługa (**wymienne** sensory gazu),
– najwyższa, europejska jakość – dzięki ISO 9001,
– system zweryfikowany przez rynek – ponad 30000 systemów pracujących w całej Polsce.

Z takim systemem eksploatacja każdej kotłowni gazowej jest bezpieczna i zgodna z przepisami.

6. Laury dla GX:

– Instalacje ‘2002 – nagroda Medium 2002,
– Instal-Expo ‘2002 – główna nagroda i statuetka Złoty Instalator,
– Pol-Gaz-Expo ‘2003 – I miejsce + nagroda specjalna PZIiTS,
– Gaz-Technika ‘2003 – I miejsce,
– Pol-Gaz-Expo ‘2004 – II miejsce (nadzór przez GPRS),
– Gaz-Technika ‘2004 – wyróżnienie (nadzór przez GPRS),
– Targi Techniki Gazowniczej „Expo-Gas ‘2006” – wyróżnienie ASBIG.

Literatura:

1. Biuletyn informacyjny Info-gazex, nr P13.
2. Katalog produktów 8’2007 oraz www.gazex.pl v 7.10.
3. Zbiór referatów XXXIV Zjazdu Gazowników Polskich, tom 3.
4. I Ogólnopolskie Forum Gazownicze „Forgaz ‘96”, zbiór referatów.
5. Sympozjum „Awarie infrastruktury technicznej w aglomeracjach miejskich”, Jachranka, 14–15 listopada 1996 r., zbiór referatów.
6. II Ogólnopolskie Sympozjum Szkoleniowe „Bezpieczna eksploatacja urządzeń i instalacji gazowych”, Poznań-Kiekrz, marzec 1997 r.
7. II Ogólnopolskie Forum Gazownicze „Forgaz ‘98”, zbiór referatów.
8. Instalacje i urządzenia gazowe, Centrum Szkolenia Gazownictwa PGNiG, 1999 r.
9. III Krajowa Konferencja „Gazterm ‘2000”, Międzyzdroje, 22–24 maja 2000 r.
10. V Forum Ciepłowników Polskich, Międzyzdroje, 17–19 września 2001 r.
11. Ochrona budynków przed zagrożeniem wybuchem gazu, GIG Katowice 2002 r.
12. Konrad Bąkowski, Sieci i instalacje gazowe, WNT 2002/2007 r.
13. Dziennik Ustaw RP Nr 75 z 15.06.2002 r.

Mariusz Karwowski
Gazex

KLAWIATURY DSC SERII POWER

Profilowane klawiatury serii POWER wykonane są z wysokiej jakości plastiku. Ich nowoczesny i estetyczny wygląd idealnie komponuje się z wnętrzem każdego domu. Niewątpliwą zaletą klawiatur jest również prosta instalacja i łatwa obsługa.

Dodatkowy zacisk wejścia/wyjścia na klawiaturze może być opcjonalnie wykorzystany jako dodatkowa linia dozorowa, wyjście programowalne lub czujnik niskiej temperatury. Użytkowanie klawiatury ułatwia również jej podświetlenie oraz dodatkowe przyciski funkcyjne. 64 liniowa klawiatura PK5500/RFK5500 może wyświetlać komunikaty w 8 językach. Została także wyposażona w globalny status podsystemów oraz możliwość definiowania 32 znakowych opisów.

Cechy wspólne wszystkich klawiatur:

- Duże, podświetlane przyciski
- 5 programowalnych przycisków funkcyjnych
- Indywidualne przyciski alarmowe (Pożar, Pomoc i Panika)
- Różne dźwięki gongu dla poszczególnych linii
- Możliwość wykorzystania zacisku wejścia/wyjścia w klawiaturze jako dodatkowej linii dozorowej, wyjścia programowalnego lub czujnika niskiej temperatury
- Regulowane podświetlenie i poziom głośności buzzera
- Zabezpieczenie antysabotażowe przed otwarciem i oderwaniem od ściany
- Elastyczna instalacja

Wyłączny dystrybutor w Polsce:

AAT Trading Company Sp. z o.o.
02-801 Warszawa, ul. Puławska 431, tel. 022 546 0 546, fax 022 546 0 501
www.aat.pl

Prosta obsługa

Klawiatury wyposażone są w pięć programowalnych przycisków funkcyjnych. Fabrycznie zaprogramowane są jako: „włączenie zwykłe", „włączenie domowe", „gong", „reset czujek dymu" oraz „szybkie wyjście". Dzięki funkcji "szybkiego wyjścia" nie trzeba wyłączać i włączać systemu w dozór przy każdym wyjściu z budynku (np. żeby wypuścić psa na zewnątrz).

Zintegrowany czujnik temperatury

Czujnik temperatury zintegrowany w klawiaturze może być zaprogramowany tak, aby aktywować alarm, kiedy temperatura w pomieszczeniu spadnie poniżej 6°C oraz przywrócić system do poprzedniego stanu gdy temperatura otoczenia wzrośnie do 9°C. Wbudowany system logiczny zapobiega cyklicznym wzbudzeniom spowodowanym skokami temperatur, redukując w ten sposób możliwość występowania fałszywych alarmów.

Elastyczność

Klawiatury serii POWER dostępne są również w wersji RFK, z odbiornikiem radiowym. Oprócz posiadania funkcji zwykłych klawiatur, dodatkowo obsługują 32 linie bezprzewodowe oraz 16 bezprzewodowych breloków z przyciskami funkcyjnymi.

Kompatybilność

Klawiatury są kompatybilne ze wszystkimi centralami serii POWER.

Specyfikacja

Wymiary	154 mm x 113 mm x 20,5 mm
Wymiary wyświetlacza LCD	99 mm x 24 mm
Pobór prądu	125mA (Max)
Zasilanie	12 V=
Temperatura pracy	0° do 49° C
Zakres wilgotności	od 5 do 93%

Oblicza RFID
(Część 2)

Identyfikator radiowy – drobinka krzemu z antenką. Na pozór nic wielkiego, ale czy mamy świadomość, jakie możliwości daje technologia radiowej identyfikacji? Czy ktoś jest w stanie przewidzieć wszystkie możliwe dla niej zastosowania? Myślę, że warto zastanowić się już dzisiaj, do czego można zastosować technologię radiowej identyfikacji i jakie korzyści można dzięki temu osiągnąć

Stale malejące koszty implementacji, dostępność, a także coraz większa doskonałość technologii RFID sprawiają, że jej konkurencyjność w stosunku do innych technik automatycznej identyfikacji jest coraz większa. Na podstawie szczegółowej analizy właściwości działających już systemów RFID da się stwierdzić, że liczba nowych potencjalnych zastosowań jest nieograniczona. Trzeba tu jednak zaznaczyć, że decydującym wyznacznikiem będzie prawie zawsze kwestia ekonomiczności adaptacji RFID do danego rozwiązania oraz, co warto podkreślić, szeroko rozumiane bezpieczeństwo jej stosowania. Dlatego na dzień dzisiejszy do znaczących obszarów zastosowań tej technologii należą m.in.:

– logistyka (zarządzanie łańcuchem dostaw),
– kontrola dostępu i rejestracja czasu pracy,
– transport,
– produkcja (szeroko rozumiane nadzorowanie procesów produkcyjnych),
– ewidencja, kontrola i zabezpieczanie towarów, księgozbiorów, archiwów, dokumentów itp.

Logistyka

Producenci, dystrybutorzy oraz sprzedawcy detaliczni jako pierwsi dostrzegli olbrzymie korzyści wynikające ze stosowania identyfikacji radiowej. Szybka ekspansja RFID w sektorze logistycznym jest wynikiem zarówno niedoskonałości powszechnie stosowanych kodów kreskowych, jak również rosnących wymagań wobec producentów co do spełniania wymogów łańcucha dostaw.

W porównaniu z kodami kreskowymi etykiety RFID charakteryzuje szereg nowych zalet. Są to m.in.:

– większa szybkość i odległość odczytu,
– zwiększona ilość informacji o produkcie oraz możliwość jej zmiany,
– możliwość wykorzystywania tych samych metek w całym łańcuchu dostaw,
– większe bezpieczeństwo informacji o produkcie,
– możliwość ukrycia etykiety wewnątrz opakowania.

Opłacalność stosowania RFID w firmach logistycznych zależy głównie od ich wielkości oraz złożoności samych procesów logistycznych (liczby asortymentu, rozproszenia i liczby magazynów, częstości ruchów magazynowych itp.).

Należy wyraźnie zaznaczyć, że systemy RFID wykorzystywane w łańcuchach dostaw są całościowo złożonymi systemami informatycznymi, wykorzystującymi wiele technik, m.in. sieć Internet, hurtownie danych. Tak rozbudowane i umiejętnie zarządzane systemy logistyczne pozwalają m.in. na stałą kontrolę towaru, dokładne śledzenie realizacji zamówień, osiąganie większej wydajności w relacjach z dostawcami oraz efektywniejsze zarządzanie aktywami firmy.

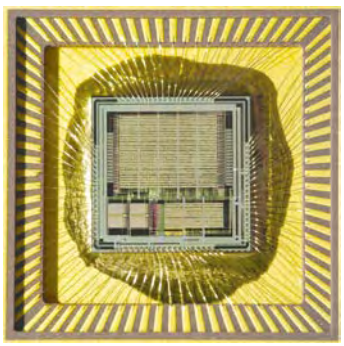
Stosowanie RFID w logistyce to korzyści nie tylko dla producentów, handlowców czy sprzedawców detalicznych. Konsumenci kilku kanadyjskich sklepów testują już pierwsze linie szybkiego skanowania cen. Jak donosi raport TNS Canadian Facts z 2007 roku, blisko połowa z nich oczekuje powszechnego stosowania tej technologii. Myślę, że każdy z nas tracących czas w kilometrowych kolejkach do kas w supermarkecie szybko doceni możliwość szybkiego skanowania zawartości wózka z zakupami, bez potrzeby wykładania kilogramów towaru na taśmę. Taki sposób robienia zakupów bez wątpienia uczyni je jeszcze przyjemniejszymi.

Kontrola dostępu

Technologia RFID doskonale sprawdza się w systemach kontroli dostępu i rejestracji czasu pracy. Plastikowe karty, breloki, opaski z umieszczonym w środku transponderem RFID są stosowane zarówno w firmach, jak też w obiektach użyteczności publicznej (obiekty sportowe, lotniska, parkingi, bramki

metra itp.). Trwałość identyfikatorów RFID (brak elementów ulegających zużyciu – paska magnetycznego, styków metalowych), ich odporność na wstrząsy, wibracje, promienie UV oraz szybkość działania i możliwość wielokrotnego zapisu danych sprawiły, że szybko zyskały one szerokie grono zwolenników.

Podstawową i chyba jedyną poważną wadą systemów kontroli dostępu wykorzystujących identyfikatory RFID jest możliwość nieuprawnionego dostępu osoby, która znalazła bądź ukradła identyfikator. Z tego powodu w systemach, w których szczególny nacisk kładzie się na bezpieczeństwo, stosuje się identyfikatory RFID w połączeniu z kodem PIN. Innym, nowocześniejszym, ale też znacznie droższym rozwiązaniem jest połączenie systemu RFID z systemem identyfikacji biometrycznej. W tym przypadku rolę kodu PIN pełni wzorzec biometryczny zapisany w identyfikatorze RFID. Weryfikacja tożsamości w takim dualnym systemie odbywa się na podstawie porównania wzorca zapisanego w identyfikatorze RFID z wzorcem odczytanym przez czytnik biometryczny.



Komunikacja i transport

Transport i komunikacja to rozległe sektory rynku, w których technologia RFID jest obecna w wielu zastosowaniach. Identyfikowanie przesyłek i pojazdów pozwala na eliminowanie błędów doręczenia, przyspieszenie obiegu informacji, wykonanie większej liczby operacji w tym samym czasie oraz lepsze wykorzystanie zasobów firmy. Dzisiejsze identyfikatory to już nie tylko zdalna identyfikacja. Dzięki zastosowaniu etykiet z czujnikami parametrów otoczenia (temperatura, wilgotność, ciśnienie) możliwy jest monitoring warunków, w jakich przewożony jest towar, co ma ogromne znaczenie np. dla firm farmaceutycznych przy dostarczaniu łatwo psujących się produktów medycznych (krew, szczepionki, organy wewnętrzne). Czujniki wykrywają, rejestrują i alarmują, gdy parametry transportu przekroczą dopuszczalne wartości. Dokumentacja parametrów otoczenia to perspektywa dla wszystkich tych gałęzi przemysłu, które poszukują rozwiązania dla wrażliwych zadań logistycznych, związanych z transportem w warunkach kontrolowanych.

Innym, odmiennym przykładem stosowania identyfikatorów radiowych w transporcie są bilety komunikacji miejskiej, na których zapisywane są informacje dotyczące rodzaju biletu i terminu jego ważności. Korzyści ze stosowania takich biletów dostrzegają pasażerowie (wygoda użytkowania) oraz same przedsiębiorstwa przewozowe (brak możliwości podrabiania kart). Bilet RFID może także dawać uprawnienia do dodatkowych usług miejskich (np. wstęp do kin, muzeów), jak również umożliwiać dokonanie opłat za postój w strefach płatnego parkowania. Zalety stosowania biletów zbliżeniowych doceniło już wiele europejskich miast, w tym także Warszawa, Wałbrzych czy Poznań. Nowością są papierowe bilety RFID, tak samo funkcjonalne i wyposażone w te same układy elektroniczne jak te wykonane z PCV, ale dużo tańsze, przez co mogą być stosowane jako bilety krótkookresowe lub na określoną liczbę przejazdów. Z papierowych biletów RFID korzysta moskiewskie metro, a w Lizbonie czy na Capri są to bilety specjalnie dedykowane turystom.

Produkcja

Zapewnienie jakości wytwarzanego produktu, sprawne zarządzanie zleceniami produkcyjnymi oraz kontrola kosztów produkcji – to trzy podstawowe zadania, których skuteczna realizacja uzależniona jest od odpowiedniego zarządzania całym procesem produkcji. Zarządzanie oparte jest na precyzyjnym śledzeniu i kontroli etapów procesów produkcyjnych, do czego niezbędne są informacje o różnym stopniu szczegółowości dotyczące procesu produkcji. Ręczne zbieranie danych i wprowadzanie ich do systemu niesie ze sobą ryzyko powstania błędów, a ponadto jest kosztowne i czasochłonne, dlatego w celu szybkiego i niezawodnego rejestrowania dużej liczby danych w procesach produkcyjnych stosuje się systemy automatycznej identyfikacji oparte na kodach kreskowych oraz identyfikatorach RFID. W systemach automatycznej identyfikacji każdy element procesu produkcyjnego jest identyfikowany w jednoznaczny (unikatowy) sposób. Każda operacja technologiczna, podzespół oraz pracownik posiada swój kod. Pozwala to na automatyczne odczytanie informacji o historii wytworzenia produktu finalnego, użytych półproduktach, czasie produkcji i osobach odpowiedzialnych za poszczególne etapy produkcyjne.

Nadzór nad procesami produkcyjnymi z wykorzystaniem etykiet RFID znajduje zastosowanie praktycznie w każdej gałęzi przemysłu – od fabryk, poprzez przemysł elektroniczny po spożywczy. Umożliwia on przede wszystkim kontrolę jakości powstającego produktu, zwiększenie wydajności i obniżenie kosztów produkcji.

Kontrola dokumentów

Kontrola obiegu i autoryzacja dokumentów to nowy obszar zastosowań technologii RFID. Automatyczna identyfikacja dokumentów za pomocą identyfikatorów radiowych pozwala m.in. na:

- kontrolę obiegu dokumentów – np. poprzez kojarzenie identyfikatorów dokumentów, książek z osobistymi identyfikatorami RFID pracowników przy wyjściu z firmowego archiwum; umożliwia to sprawowanie nadzoru nad dokumentami oraz ich szybkie odnajdywanie;
- autoryzację dokumentów – przez jednoznaczną identyfikację i potwierdzenie autentyczności dokumentów, co w znaczny sposób podnosi poziom bezpieczeństwa dzięki redukcji możliwości wystąpienia fałszerstw;
- zarządzanie dokumentami – szczególnie w dużych bibliotekach, archiwach, gdzie istnieje potrzeba szybkiej pracy przy sprawdzaniu wypożyczanych i zwracanych książek.

Z zalet technologii RFID korzysta m.in. Biblioteka Watykańska, w której oznaczono blisko 50 tys. pozycji spośród 120 tys. dostępnych dla czytelników. Identyfikatory radiowe zredukowały czas wypożyczenia o ok. 40% w porównaniu z systemami kodów kreskowych, sprawują także lepszą kontrolę nad zbiorami i chronią przed ewentualnymi podmianami cennych pozycji na kopie. Skrócił się także czas potrzebny na pełną inwentaryzację – z miesiąca do zaledwie kilkunastu godzin.

Inne zastosowania

Logistyka, transport czy kontrola dostępu to obszary, w których radiowa identyfikacja istnieje od lat i jej pozycja jak na razie jest niezagrożona. Ostatnio bardzo duże nadzieje wiąże się też z zastosowaniem RFID w medycynie. Osobista identyfikacja pacjenta, któremu dano, naklejono lub wszczepiono identyfikator radiowy, mogłaby zdecydowanie polepszyć jakość usług medycznych oraz je przyspieszyć. Identyfikator zawierający podstawowe dane o pacjencie, historię choroby, informację o uczuleniu na niektóre leki na pewno wpłynąłby pozytywnie na trafność diagnozy lekarskiej, a także mógłby uchronić pacjenta przed podaniem niewłaściwego leku. Innym zastosowaniem RFID w medycynie jest odnajdywanie ciał obcych pozostawionych w ciałach pacjentów. Miniaturowe identyfikatory przykleja się do narzędzi i gazików używanych podczas operacji, a potem wystarczy krótkie skanowanie ręcznym skanerem i już mamy pewność, że pacjent jest „czysty". Skuteczność tej metody została potwierdzona w testach przeprowadzonych w 2006 roku na Uniwersytecie Stanford. Pracują nad nią także firmy RF Surgical Systems oraz ClearCount.

Wiele kontrowersji wzbudza wszczepianie identyfikatorów ludziom, a zwłaszcza dzieciom, których rodzice chcą wiedzieć, gdzie przebywa ich pociecha. Systemy zdalnej lokalizacji łączą ze sobą technologię RFID z siecią telefonów komórkowych oraz systemem GPS i mogą przez 24 godziny na dobę przekazywać informację o położeniu dziecka. Dużą rolę w rozwoju tego typu systemów odegrał brytyjski naukowiec Kevin Warwick, którego zawodowe ambicje skupiają się wokół stworzenia społeczeństwa cyborgów, pół ludzi – pół maszyn. Jak twierdzi, system został stworzony po to, by dać szansę na szybkie odnalezienie zagubionego bądź uprowadzonego dziecka całego i zdrowego. Przeciwnicy tej metody mają wiele wątpliwości, ponieważ nie wiadomo, jak zachowa się porywacz, gdy zorientuje się, że dziecko ma wszczepiony identyfikator. Czy dziecku nie będzie wtedy groziło jeszcze większe niebezpieczeństwo? Opinie na ten temat są różne, często uzależnione od osobistych doświadczeń związanych z kidnapingiem.

Ciekawym zastosowaniem identyfikatorów radiowych jest umieszczenie ich w banknotach. W ten sposób zabezpieczone są już niektóre nominały euro i dolara. Banknoty z RFID są z pewnością trudniejsze do podrobienia, a powszechne ich stosowanie pozwoli na jeszcze szybsze i łatwiejsze liczenie gotówki. Radiowa identyfikacja banknotów umożliwia także śledzenie obiegu brudnych pieniędzy oraz lokalizację osób za pomocą sieci czytników rozmieszczonych w newralgicznych punktach miasta (wejścia do budynków, pojazdów, bramki metra itp.). O tym ostatnim zastosowaniu mówi się w aspekcie walki z rosnącą falą terroryzmu.

Niestety identyfikatory umieszczane w banknotach można zniszczyć, wkładając je do kuchenki mikrofalowej. Te maleńkie układy elektroniczne nie mają żadnych szans i wybuchają wskutek działania na nie promieniowania mikrofalowego. W Internecie można znaleźć fotografie banknotów z wypalonymi dziurami po tagach RFID.

Kolejnym innowacyjnym pomysłem jest wykorzystanie technologii radiowej do walki z piratami drogowymi. Rozmieszczenie czytników RFID na odcinkach drogi (np. przy wjeździe i wyjeździe z miejscowości) pozwoliłoby na kontrolę średniej prędkości pojazdów na danym odcinku, który w zależności od potrzeb mógłby mieć długość od kilku metrów do kilkunastu kilometrów. Oczywiście wiązałoby się to z koniecznością instalacji identyfikatorów RFID w każdym pojeździe, co można byłoby wykorzystać np. do automatycznego pobierania opłat za przejazd autostradą lub lokalizacji skradzionego pojazdu. Jednym z krajów, które już o tym pomyślały, jest Malezja. Tamtejsze Ministerstwo Transportu Drogowego zobowiązało właścicieli pojazdów drogowych do instalowania w swoich samochodach identyfikatorów RFID, co ma ograniczyć zjawisko kradzieży samochodów w tym kraju.

Pomysłem, który może zrewolucjonizować grę w golfa, jest umieszczenie identyfikatorów radiowych w piłeczkach golfowych. Gracze otrzymują osobisty kosz z piłeczkami i udają się na stanowisko, z którego celują do dołków. Oczywiście pole golfowe wygląda nieco inaczej. Wokół chorągiewek są rozmieszczone wyposażone w czytniki RFID sektory, do których wpadają piłeczki, a gracz od razu dostaje informację na ekranie monitora o celności i zdobytych punktach. Przypomina to trochę połączenie gry w golfa z grą w rzutki. Tam też ćwiczymy celność, nie ruszając się z miejsca.

Także telefony komórkowe już niedługo będą wyposażone w technologię RFID. Firma Samsung opracowała czytnik RFID dla telefonów komórkowych, który daje możliwość sczytywania informacji, których ręczne wpisywanie jest często niewygodne i czasochłonne. I tak np. stojąc przed plakatem filmowym wyposażonym w identyfikator RFID będziemy mogli pobrać dane dotyczące godzin seansów, cen biletów, telefonu do rezerwacji lub automatycznie zarezerwować bilety przez przeglądarkę WAP. – Dajemy możliwość zebrania wiadomości wszędzie i w każdej chwili dzięki zwykłej komórce – mówi dr Chilhee Chung, wiceprezes Samsung Electronics System LSI.

Można by jeszcze wiele mówić o koncepcjach i konkretnych zastosowaniach RFID. Jedno jest pewne: zainteresowanie technologią RFID od czasu gdy opuściła ona laboratoria instytutów badawczych stale rośnie. Postępująca miniaturyzacja, a także coraz niższe koszty implementacji oraz ogromne możliwości RFID powodują, że znajduje ona zastosowanie w wielu nowych dziedzinach życia. Niektóre zastosowania budzą wiele kontrowersji, inne wydają się konieczne i przyjmowane są z pełną akceptacją. Rozwój technologii automatycznej identyfikacji jest nieunikniony, ponieważ we współczesnym, opartym na krzemie świecie jest ogromne zapotrzebowanie na tego typu technologie. Czy jednak powszechne stosowanie RFID będzie w pełni bezpieczne? Jakie są zagrożenia i jak możemy się ich ustrzec – to postaram się przedstawić w kolejnym artykule, do którego przeczytania gorąco zachęcam.

Przemysław Mierzwiak
Instytut Inżynierii Systemów Bezpieczeństwa

Literatura:

www.rfidnews.org
www.rfsurg.com
www.bcspolska.pl
www.totnet.com.pl

RACS ROGER ACCESS CONTROL SYSTEM
seria radius

Seria Radius

Seria Radius to całkowicie nowa linia wzornicza czytników i kontrolerów dostępu zaprojektowana w oparciu o wieloletnie doświadczenie firmy Roger w tej dziedzinie.

W skład rodziny wchodzą czytniki i kontrolery różniące się konstrukcją mechaniczną oraz funkcjonalnością, w zależności od modelu obsługują one karty standardu EM 125kHz lub 13.56MHz Mifare. Nową kategorię produktów stanowi wandalo-odporny czytnik zbliżeniowy (PRT64VP) w którym zarówno przednia część obudowy jak i klawisze są wykonane w całości z metalu.
Na szczególną uwagę zasługuje również kontroler PR602LCD, który został specjalnie zaprojektowany dla systemów rejestracji czasu pracy (RCP) co nie wyklucza jednak możliwości stosowania go jako zwykłego kontrolera dostępu. Urządzenia rodziny Radius mogą być instalowane na zewnątrz budynków i są kompatybilne z wcześniej produkowanymi kontrolerami dostępu serii PR oraz czytnikami PRT, mogą one być dołączane do istniejących już systemów kontroli dostępu pracujących autonomicznie lub pod kontrolą programu PR Master (*).

(*) **Informacja**
Począwszy od 1 września 2007 program PR Master jest rozprowadzany z darmową licencją bez ograniczenia liczby kontrolerów w systemie.

CE

profesjonalna
kontrola
dostępu

roger®
www.roger.pl

Bezpieczeństwo pakietowych sieci bezprzewodowych – przegląd

W ostatnich latach technologie bezprzewodowe ze względu na swoje właściwości stają się coraz bardziej popularne i niezbędne zarówno w prowadzeniu biznesu, jak i w codziennym życiu. Obecne osiągnięcia komunikacji bezprzewodowej oferują swoim użytkownikom m.in. mobilność połączenia z siecią, elastyczność rozwiązań, wzrastającą produktywność, przy jednoczesnym zachowaniu niskiego kosztu instalacji

Istotny jest fakt, że technologie te odpowiadają szerokiemu zakresowi potrzeb różnych użytkowników. I tak, sieci typu Ad-hoc, np. Bluetooth, służą do komunikacji między urządzeniami elektronicznymi, takimi jak palmtopy, laptopy, telefony komórkowe itp., w zasięgu około 10 metrów. Radiowe sieci lokalne, o szerszym zasięgu, WLAN (ang. *Wireless Local Area Network*), pozwalają użytkownikom na poruszanie się z miejsca na miejsce bez konieczności rozłączania się z siecią. Sieci komórkowe 3G, o globalnym zasięgu, oferują nowe usługi, większe pasmo i nową jakość telefonii. Mimo nieocenionych korzyści, sieci bezprzewodowe oferują z natury dużo niższy poziom bezpieczeństwa niż sieci przewodowe. Ponieważ bezprzewodowe interfejsy sieciowe wykorzystują powietrze jako medium transmisyjne, są one podatne na nieautoryzowane wykorzystanie lub pasywny podsłuch. Monitorowanie i wykradanie informacji w takich sieciach jest o wiele łatwiejsze aniżeli w przypadku sieci przewodowych. Ponieważ nie istnieje konieczność fizycznego podłączenia w celu uzyskania dostępu do sieci, mogą stać się one łatwym celem dla napastnika.

Celem niniejszego artykułu jest przedstawienie stosowanych zabezpieczeń sieci radiowych oraz ocena odporności tych rozwiązań na różne strategie ataków, począwszy od pasywnych ataków, bazujących na analizie statycznej, poprzez różnorodne ataki aktywne, aż po ataki wykorzystujące długotrwałe monitorowanie sieci.

1. Wprowadzenie – problemy bezpieczeństwa w pakietowych sieciach bezprzewodowych

Oczywistym celem konstrukcji zabezpieczeń w każdej sieci bezprzewodowej jest eliminacja jak największej ilości potencjalnych zagrożeń. Zabezpieczenia tworzą najczęściej zespół mechanizmów, do których zaliczyć można przede wszystkim szyfrowanie danych w łączu radiowym, uwierzytelnianie czy zapewnianie poufności tożsamości i lokalizacji użytkownika. Z upływem czasu okazało się jednak, że stosowanie tego typu mechanizmów w systemach bezprzewodowych nie dostarcza rozwiązań wielu nowo pojawiających się problemów, związanych przede wszystkim z błędami projektowymi, z zaniedbaniami w procedurach potwierdzania autentyczności, z brakiem jawności mechanizmów lub brakiem zaufania do nich.

Do najczęściej wymienianych problemów sieci bezprzewodowych można zaliczyć:

– brak mechanizmów szyfrowania danych użytkownika i danych systemowych;

– brak zabezpieczeń przeciwko podszywaniu się pod element sieciowy (ang. *active attack*);

– brak mechanizmu przechwytywania danych dotyczących aktywności wybranego użytkownika (ang. *lawful interception*);

– brak zabezpieczeń kluczy i danych uwierzytelniających, przesyłanych przez sieć;

– brak kontroli integralności przesyłanych danych;

– brak zaufania dotyczący tożsamości terminala (terminal jest niechronionym środowiskiem);

Atrybut bezpieczeństwa	Słabości technologii Bluetooth
Uwierzytelnianie	Procedura uwierzytelniania jest uproszczoną procedurą wyzwanie – odpowiedź (ang. challenge –response), tzn. uwierzytelnianie odbywa się tylko w jedną stronę, co prowadzi do podatności technologii na tzw. ataki „spotkania w środku" (ang. *man-in-the-middle attacks*). W celu uniknięcia tego typu ataków konieczne jest zastosowanie obustronnego uwierzytelniania.
Uwierzytelnianie	Domyślne ustawienia producenta często nie są wystarczająco bezpieczne (np. uwierzytelnianie jest wyłączone lub użyty PIN ustawiony jest na łatwą do przewidzenia lub taką samą dla wszystkich urządzeń wartość, np. 0000). Ponadto zmiana ustawień często jest niemożliwa albo bardzo trudna do wykonania.
Integralność danych	Niekryptograficzna funkcja CRC (ang. Cyclic Redundancy Check) jako metoda kontroli integralności może być użyta tylko do zidentyfikowania błędów transmisji. Funkcja CRC nie zabezpiecza przed celowo wprowadzanymi zmianami w pakietach.
Poufność	Mechanizm szyfrowania nie jest obligatoryjny. Niezależnie od trybu bezpieczeństwa szyfrowanie pakietów danych podczas transmisji jest tylko opcjonalne. Domyślne ustawienia producenta są mało bezpieczne (np. wyłączone szyfrowanie).
Poufność tożsamości	Możliwe jest określenie położenia użytkownika dzięki użyciu adresu MAC urządzenia.

Tab. 1. Słabości technologii Bluetooth

– brak wskaźnika informującego użytkownika o stosowanym algorytmie szyfrowania;
– brak wskaźnika informującego użytkownika o poziomie uaktywnionych zabezpieczeń;
– brak kontroli danych wykorzystywanych do zabezpieczeń stosowanych po stronie sieci wizytowej;
– słaba elastyczność systemu zabezpieczeń, ograniczająca jego rozbudowę;
– brak otwartości specyfikacji algorytmów (złamanie zasady Kerckhoffsa);
– zbyt krótki klucz, którego wydłużenie stanowi problem ze względu na ograniczenia implementacyjne, co jest wynikiem tajności algorytmu.

Rozwiązanie tych problemów jest dużym wyzwaniem dla nowo powstających technologii. Aby osiągnąć ten cel, należy stworzyć listę możliwych zagrożeń, których obecnie można być świadomym, a następnie, na jej podstawie, zdefiniować mechanizmy bezpieczeństwa. Na liście tej można wyróżnić podstawowe grupy zagrożeń, takie jak:

• nieautoryzowany dostęp do danych przesyłanych przez sieć, który obejmuje:
– przechwycenie przez intruza przesyłanych danych (ang. *eavesdropping*), zarówno danych użytkownika, jak i danych sterujących;
– wykorzystanie podstawionych przez intruza urządzeń systemu w celu zdobycia poufnych danych użytkownika, podszywanie się pod użytkownika autoryzowanego w celu korzystania z usług systemu lub poufnych danych systemowych (ang. *masquerading*);
– analizę przesyłanych od/do użytkownika sygnałów w celu określenia jego położenia;
– przeszukiwanie pamięci, w której dane są przechowywane (ang. *browsing*);
– wyszukiwanie możliwych wycieków informacji (ang. *leakage*);
– obserwowanie przez intruza reakcji systemu na wysyłane zapytania lub wybrane sygnały;
• naruszenie integralności przesyłanych danych (ang. *violation of integrity*):
– manipulacja danymi (ang. *manipulation of messages*), która może dotyczyć ruchu generowanego przez użytkownika oraz danych sygnalizacyjnych i sterujących, przez wstawianie, modyfikację lub kasowanie odpowiedzi przez intruza;
• naruszenie lub nieprawidłowe użycie usług sieciowych (doprowadzanie do odrzucania żądań obsługi lub do ograniczeń w realizacji usług):
– wywoływanie zaburzenia pracy w sieci przez zakłócanie odbioru (ang. *intervention*);
– powodowanie przeciążeń sieci (ang. *resource exhaustion*);
– korzystanie z usług niezgodnie z przeznaczeniem (ang. *misuse of privileges*);
– nadużycie usług (ang. *abuse of services*);
• wypieranie się, odrzucanie (ang. *repudiation*) – możliwość wyparcia się korzystania z usług, odbioru informacji itp.;
• nieautoryzowany dostęp do usług (ang. *unauthorised access to services*):
– podawanie się za autoryzowanego użytkownika lub fragment sieci;
– zmiana praw dostępu do usług, przez co użytkownicy i jednostki sieciowe nie mogą prawidłowo przeprowadzić procesu uwierzytelnienia.

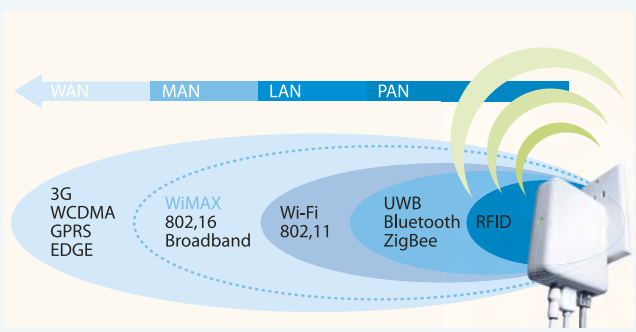
2. Rodzaje sieci

Aby ułatwić zrozumienie istoty zabezpieczeń sieci bezprzewodowych, poniżej zostaną wprowadzone definicje poszczególnych grup sieci. Bazując na ich pokryciu, możemy sklasyfikować ich rodzaje (rys. 1).

Prywatne sieci PAN (ang. *Personal Area Network*) są doraźnie tworzonymi sieciami komputerowymi o małym zasięgu. Typowe parametry pracy sieci PAN są następujące: zasięg – poniżej 10 m, przepustowość – rzędu kilkuset Mbps (megabitów na sekundę). Do grupy sieci PAN można zaliczyć: Bluetooth (802.15.1), UWB (802.15.3) z przepustowością około 100 Mbps oraz sieć ZigBee (802.15.4) z przepustowością około 250 kbps.

Lokalne sieci LAN (ang. *Local Area Network*) są sieciami komputerowymi składającymi się z grupy komputerów znajdujących się na niedużym obszarze, np. w budynku biura. Sieci LAN są wykorzystywane do współdzielenia takich zasobów, jak pliki czy drukarki. Typowe parametry pracy sieci LAN są następujące: zasięg – poniżej 100 m, przepustowość – około 11–54 Mbps. W bezprzewodowych sieciach lokalnych najczęściej używaną technologią jest WLAN, zwana także WiFi, określona standardami ETSI 802.11.

Miejskie sieci MAN (ang. *Metropolitan Area Network*) są sieciami umożliwiającymi komunikację przy dalekich



Rys. 1. Technologie sieci bezprzewodowych

odległościach. Typowe parametry pracy sieci MAN są następujące: zasięg – poniżej 5 km, przepustowość – około 70 Mbps. Do bezprzewodowych miejskich sieci MAN można zaliczyć wszystkie technologie definiowane w rodzinie standardów 802.16.

Rozległe sieci WAN (ang. *Wide Area Network*) są sieciami, których zasięg działania obejmuje duże geograficzne powierzchnie, np. obszar kraju. Sieci WAN często łączą ze sobą mniejsze sieci, takie jak LAN oraz MAN. Najbardziej popularną na świecie siecią WAN jest Internet. Ponadto do grupy sieci WAN można zaliczyć także sieci komórkowe, wykorzystujące systemy GSM lub UMTS.

W następnej części artykułu spróbujemy przeanalizować bezpieczeństwo wyżej wymienionych grup, bazując na konkretnych przykładach/technologiach.

3. Kryptograficzne mechanizmy zabezpieczeń stosowane w sieciach bezprzewodowych

3.1. Prywatne sieci PAN (np. Bluetooth)

Bezprzewodowy standard Bluetooth opisuje technologię komunikacyjną krótkiego zasięgu, której przeznaczeniem jest wyeliminowanie konieczności stosowania kablowych połączeń pomiędzy urządzeniami elektronicznymi, takimi jak telefony komórkowe, laptopy, komputery stacjonarne, drukarki czy kamery cyfrowe. Użycie technologii Bluetooth jest akceptowalne we wszystkich sytuacjach, w których co najmniej dwa urządzenia elektroniczne są w swoim sąsiedztwie oraz nie wymagają wysokiego pasma przepustowości. Niestety jednak technologia Bluetooth charakteryzuje się licznymi słabościami z punktu widzenia bezpieczeństwa, co zostało przedstawione w tabeli nr 1.

3.2. Lokalne sieci LAN (IEEE 802.11)

Bezprzewodowa transmisja danych zdefiniowana w standardach IEEE 802.11 to komfortowy sposób wymiany informacji między urządzeniami komputerowymi. Obok licznych zalet posiada jedną zasadniczą wadę. Jest nią nieograniczony dostęp do medium transmisyjnego, który niekorzystnie odbija się na poziomie bezpieczeństwa zarówno infrastruktury sieciowej, narażonej na nieautoryzowane wykorzystanie, jak i przesyłanych danych, ulegających podsłuchowi. Przeznaczeniem sieci bezprzewodowych WLAN jest przede wszystkim rozszerzenie zakresu działania ich kablowych odpowiedników. Sieć WLAN jest tworzona poprzez dołączanie urządzeń do punktu dostępowego AP, który jest fragmentem sieci przewodowej. Klienci komunikują się z AP, używając bezprzewodowego sieciowego adaptera, podobnego do adaptera stosowanego w Ethernecie. Ze względu na bezpieczeństwo nieautoryzowani klienci nie mogą mieć dostępu do zasobów sieci WLAN. Dlatego też bardzo ważny w działaniu takiej sieci jest problem bezpieczeństwa. Pierwsze standardy należące do rodziny 802.11 zabezpieczone były mechanizmem WEP. Okazał się on jednak mało skuteczny, dlatego w kolejnych wersjach standardu 802.11 wprowadzono takie zabezpieczenia, jak WPA oraz WPA2.

Historię standardu 802.11 z uwzględnieniem bezpieczeństwa można przedstawić następująco. W roku 1997 zatwierdzono pierwszy standard 802.11 (2,4 GHz, 2 Mbps), definiujący m.in. protokół WEP. Dwa lata później, w roku 1999, zatwierdzono standardy 802.11a (5 GHz, 54 Mbps) oraz 802.11b (2,4 GHz, 11 Mbps). W roku 2003 wszedł w użycie bardziej bezpieczny standard z rodziny 802.11, a mianowicie 802.11g (2,4 GHz, 54 Mbps), w którym po raz pierwszy zastosowano protokół bezpieczeństwa WPA. Ze względu na wykorzystanie algorytmu RC4, podobnie jak w protokole WEP, wymiana sprzętu nie była konieczna. Rok później zatwierdzono standard 802.11i, charakteryzujący się nowym protokołem bezpieczeństwa WPA2, który zaczął wykorzystywać nowy standard AES. Rozwiązanie to wymusiło jednak

Atrybuty bezpieczeństwa	Słabości protokołu WEP
Poufność	Strumień RC4 jest niedostosowany do transmisji pakietowej. Dla każdej ramki należy generować strumień szyfrujący od nowa.
Poufność	Stały klucz – specyfikacja protokołu WEP nie przewiduje użycia mechanizmu zarządzania kluczami; zabezpieczenie realizowane jest przy użyciu pojedynczego klucza współdzielonego pomiędzy wielu użytkowników.
Poufność	Zbyt krótki wektor początkowy IV (ang. Initial Vector) – 24-bitowy wektor IV protokołu WEP dostarcza tylko 16777216 różnych strumieni szyfrujących RC4 dla danego klucza WEP. Dodatkowo specyfikacja WEP nie określa, w jaki sposób wektor IV powinien być wybrany ani jak często powinien być zmieniany.
Poufność	Ze względu na sposób tworzenia klucza oraz jego długość pojawiają się słabe klucze, które dodatkowo są rozpoznawalne po zawartości wektora IV.
Poufność	Brak wbudowanej metody aktualizacji kluczy. Klucz zdefiniowany w standardzie 802.11 jest bardzo krótki: 40-bitowy.
Integralność danych	1) Niekryptograficzna kontrola integralności: funkcja CRC-32 (ang. Cyclic Redundancy Check-32). 2) Kontrola integralności danych nie obejmuje całości ramki (np. nagłówka), co przyczynia się do umożliwienia łatwej modyfikacji danych, bez konieczności rozszyfrowywania ramki czy odtworzenia wcześniej zapisanego ruchu sieciowego. Dodatkowo protokół WEP nie przewiduje użycia innych mechanizmów zabezpieczających przeciwko atakom powtórzeniowym.
Uwierzytelnianie	Brak wzajemnego uwierzytelniania.

Tab. 2. Słabości protokołu WEP

Właściwość \ Protokół	WEP	WPA	WPA2
Algorytm	RC4	RC4	AES
Długość klucza	40 bitów	128 bitów (szyfrowanie) 64 bity (uwierzytelnianie)	128 bitów
Długość wektora początkowego	24 bity	48 bitów	48 bitów
Kontrola integralności pakietów	CRC32	Michael	CCMP
Kontrola integralności nagłówków	Brak	Michael	CCMP
Ataki powtórzeniowe	Brak	Sekwencja IV	Sekwencja IV
Zarządzanie kluczem	Brak	Rozwiązanie bazujące na protokole EAP	Rozwiązanie bazujące na protokole EAP

Tabela 3. Zabezpieczenia WLAN

wymianę sprzętu sieciowego. W 2006 roku zatwierdzono szkic standardu 802.11n (2,4; 5 GHz, 600 Mbps).

Jak już wyżej wspomniano, w standardzie 802.11 wyróżniamy trzy następujące sposoby zabezpieczeń: WEP, WPA, WPA2. Poniżej zostanie przedstawiona ich krótka charakterystyka, ze szczególnym uwzględnieniem słabości w zabezpieczeniach.

Protokół WEP (ang. *Wired Equivalent Privacy*)

Podstawowym celem protokołu WEP była ochrona informacji w warstwie łącza danych oraz zapewnienie bezpieczeństwa na poziomie porównywalnym z bezpieczeństwem sieci przewodowych. Algorytm WEP uwzględnia następujące elementy bezpieczeństwa: uwierzytelnienie, integralność, poufność oraz niezaprzeczalność. Jeżeli chodzi o zapewnienie poufności, generowany jest, z wykorzystaniem szyfru RC4, strumień klucza. Następnie, przy wykorzystaniu strumienia informacji jawnej oraz klucza, przeprowadzana jest operacja XOR (ang. *eXclusive OR*). Integralność zabezpieczana jest poprzez dołączenie 32-bitowej sumy kontrolnej CRC-32.

Gdy protokół WEP jest użyty w sieci WLAN, każdy pakiet jest szyfrowany oddzielnie, za pomocą algorytmu RC4, używającego 64- lub 128-bitowego klucza RC4. Klucze te składają się odpowiednio z 40 lub 104 bitów oraz z generowanej przez system dodatkowej 24-bitowej wartości, zwanej wektorem początkowym IV (ang. *Initialization Vector*). Zaszyfrowany pakiet jest generowany z oryginalnego pakietu i strumienia RC4 przez wykonanie operacji XOR na obu strumieniach. Dodatkowo 4-bajtowa wartość ICV (ang. *Integrity Check Value*) jest wyliczana tylko na niezaszyfrowanej zawartości pakietu 802.11 przy użyciu funkcji CRC-32. Następnie wartość ta jest dodawana na końcu danej ramki. WEP jako protokół bezpieczeństwa jest szeroko krytykowany za wiele słabości. Niektóre z nich zostały krótko opisane w tabeli 2.

Dodatkowo możemy wyróżnić następujące typy ataków:
ataki pasywne
– FMS (atak Fluhrera, Mantina i Shamira),
– SNAP header (atak wykorzystujący dane zawarte w nagłówku SNAP – ang. *Subnetwork Access Protocol*),
– IV reuse (atak z ponownym użyciem wektora początkowego)
i ataki aktywne
– Replay attack (fałszowanie ruchu z wykorzystaniem metody „Traffic reply", polegającej na ponownym wysyłaniu już wcześniej wysłanych wiadomości),

Atrybuty bezpieczeństwa	802.16 -2001	802.16 -2004	802.16 -2005
Uwierzytelnianie	Brak wyraźnej definicji: 1) za pomocą struktury SA nie możemy rozróżnić procedur uwierzytelniania; 2) struktura SA nie zawiera danych dotyczących identyfikatora używanej stacji	Brak danych	Problem rozwiązany
Uwierzytelnianie	Brak certyfikatu BS; potrzeba obustronnego uwierzytelnienia	Jak dla standardu z 2001 roku	Problem rozwiązany
Uwierzytelnianie	Klucz uwierzytelniający budowany jest tylko przez stację bazową – użytkownik musi ufać, że stacja bazowa zawsze generuje nowy klucz uwierzytelniający	Nie do końca bezpieczny sposób tworzenia kluczy	Problem rozwiązany
Poufność	Użycie algorytmu DES w trybie CBC wymaga losowego IV (brak gwarancji ze strony standardu IEEE 802)	Brak danych	Problem rozwiązany (wykorzystanie szyfru AES)
Kontrola integralności	Funkcja CRC (fałszerstwo i powtórzenia)	Problem rozwiązany	Problem rozwiązany

Tab. 4. Słabości standardu 802.16 w zakresie bezpieczeństwa

– MAC address forging (fałszowanie adresu MAC),
– identity hijacking (podszywanie się pod innego użytkownika),
– man-in-the-middle (atak spotkania w środku),
– bit-flipping (fałszowanie danych w ramce),
– header modification (modyfikacja nagłówka).

Protokoły WPA i WPA2
(ang. *Wi-Fi Protected Access*)

Rodzina protokołów WPA, składająca się z dwóch protokołów WPA i WPA2, jest klasą rozwiązań, która jest odpowiedzialna za bezpieczeństwo bezprzewodowych sieci komputerowych. Protokoły te zostały stworzone w odpowiedzi na wiele poważnych słabości, które zostały odkryte w poprzednich systemach, tj. słabości znalezionych w protokole WEP. Standard WPA jako mechanizm zabezpieczeń został zaimplementowany w standardach IEEE 802.11g i IEEE 802.11i. Dodatkowo został zaprojektowany w taki sposób, aby był całkowicie kompatybilny ze swoim poprzednikiem, który mógł pracować ze wszystkimi interfejsami sieci bezprzewodowej oprócz rozwiązań pochodzących z pierwszej generacji tej klasy systemów. W klasie WPA możemy znaleźć nowe rozwiązania bezpieczeństwa, takie jak nowa procedura uwierzytelniania, nowy sposób tworzenia wektorów początkowych, nowy sposób kontroli integralności, wprowadzony w zamian za niekryptograficzną funkcję CRC-32 z protokołu WEP. Ponadto w protokołach tych zostały zaimplementowane nowe metody tworzenia kluczy szyfrujących oraz mechanizmy zarządzania nimi.

Porównanie zabezpieczeń stosowanych w bezprzewodowych sieciach WLAN zostało przedstawione w tabeli 3.

3.3. Miejskie sieci MAN (ang. *Metropolitan Area Network*) IEEE 802.16 WiMAX

Technologia WiMAX (ang. *World Interoperability for Microwave Access*), bazująca na standardzie IEEE 802.16, oferuje połączenie między urządzeniami przy odległości dochodzącej nawet do kilkunastu kilometrów. Sieci WiMAX mogą działać w dwóch podstawowych trybach: trybie stacjonarnym (połączenia punkt – punkt) oraz trybie zapewniającym pełną mobilność. W odróżnieniu od sieci o mniejszym zakresie, przede wszystkim sieci WiFi, standard IEEE 802.16 od początku swojego istnienia oferował wysoki poziom zabezpieczeń. Chociaż początkowo specyfikacja odnosiła się jedynie do bezpieczeństwa

Atrybuty bezpieczeństwa	Algorytm w GSM	Algorytm w UMTS	Zagrożenie
Uwierzytelnienie stacji ruchomej	+ [A3]	[f2]	Możliwość podszycia się pod stację ruchomą w komunikacji z siecią
Uwierzytelnienie sieci	-	[f1*]	Możliwość podrobienia tokenu ponownej synchronizacji
Uwierzytelnienie sieci	-	[f1]	Możliwość podszycia się pod sieć w komunikacji ze stacją ruchomą
Uwierzytelnienie sieci	-	SQN	Użycie przedawnionego lub wykorzystanego tokenu uwierzytelnienia w celu podszycia się pod sieć
Uwierzytelnienie sieci	-	[f5]	Możliwość przejęcia licznika sekwencji
Uwierzytelnienie sieci	-	[f5*]	Możliwość wykorzystania odesłanego licznika sekwencyjnego wraz ze starym tokenem
Uwierzytelnienie sieci	-	Odesłanie parametrów zabezpieczeń (sieć->SR)	Możliwość podmiany parametrów przed zastosowaniem kontroli integralności
Kontrola integralności	-	[f4]	Kompromitacja pojedynczego klucza pozwala na ciągłą i nieautoryzowaną modyfikację komunikatów
Kontrola integralności	-	[f9]	Możliwość nieautoryzowanego modyfikowania, wstawiania, powtarzania lub usuwania transmitowanych danych
Szyfrowanie (sieć radiowa)	+ [A8]	[f3]	Kompromitacja pojedynczego klucza pozwala na prowadzenie ciągłego podsłuchu
Szyfrowanie (sieć szkieletowa)	+ [A5]	[f8]	Możliwość prowadzenia podsłuchu
Użycie tymczasowych identyfikatorów	+	Stosowanie tymczasowych identyfikatorów	Możliwość śledzenia abonenta
Szyfrowanie w sieci szkieletowej	-	IPSec	Możliwość prowadzenia podsłuchu w sieci szkieletowej

Tab. 5. Zagrożenia sieci WAN

kontroli dostępu oraz szyfrowania łącza danych, późniejsze rozwiązania wypełniły wszystkie krytyczne luki w zabezpieczeniach.

Architektura bezpieczeństwa IEEE 802.16 używa pięciu następujących komponentów:

– struktura SA (ang. *Security Associations*) – używana do utrzymania stanu bezpieczeństwa odpowiedniego do połączenia;

– certyfikat X.509 – certyfikuje tożsamość komunikujących się urządzeń;

– uwierzytelnianie PKM – dystrybuuje token uwierzytelniający w celu uwierzytelnienia stacji abonenckiej;

– mechanizm zarządzania kluczami;

– szyfrowanie.

W standardzie IEEE 802.16 z roku 2001 odkryto kilka słabości, które zostały opisane w tabeli 6. Słabości te zostały wyeliminowane w kolejnych wersjach standardu, dlatego obecnie standard charakteryzuje się dużym poziomem bezpieczeństwa.

3.4. Rozległe sieci WAN – sieci PLMN (ang. *Public Land Mobile Network*), np. GSM, UMTS

Sieć PLMN to sieć telefonii mobilnej ustanowiona i zarządzana przez operatora telekomunikacyjnego, oferującego usługi w publicznej ofercie na pewnym obszarze, zazwyczaj znajdującym się na terenie jednego kraju. W punkcie tym rozważać będziemy bezpieczeństwo dwóch systemów należących do sieci PLMN, mianowicie systemów GSM i UMTS.

Bezpieczeństwo systemu GSM jest osiągane dzięki:

1. uwierzytelnieniu stacji ruchomej (mechanizm wyzwanie – odpowiedź bazujący na algorytmie A3 zwanym generatorem podpisu cyfrowego);
2. poufności tożsamości stacji ruchomej (użycie tymczasowego identyfikatora do realizacji usług zamiast jego stałego odpowiednika);
3. szyfrowaniu interfejsu radiowego (mechanizm szyfrowania oparty na szyfrze strumieniowym A5);
4. modułowi tożsamości abonenta SIM (ang. *Subscriber Identity Module*), który jest wymienialnym elementem sprzętu terminala.

Na bezpieczeństwo systemu UMTS wywodzącego się z systemu GSM ma dodatkowo wpływ:

1. obustronne uwierzytelnienie, zabezpieczające przed podszywaniem się pod stacje bazowe;
2. rozszerzenie zakresu, w którym wykorzystuje się szyfrowanie, z sieci dostępowej na sieć szkieletową;
3. zabezpieczenie baz danych przechowujących istotne informacje;
4. zaprojektowanie mechanizmu uaktualniania modelu bezpieczeństwa.

Zagrożenia dotyczące obu systemów i proponowane rozwiązania zostały przedstawione w tabeli 5.

4. Ocena bezpieczeństwa bezprzewodowych technologii

W tym punkcie zostanie dokonana próba porównania poszczególnych technologii w kontekście zaimplementowanych w nich zabezpieczeń. Tabela 6 przedstawia wyniki oceny stanu bezpieczeństwa w odniesieniu do najbardziej znanych zagrożeń sieci bezprzewodowych, zdefiniowanych na początku tego artykułu. Zagrożenia wynikające ze współpracy różnych sieci zostały pominięte. Tabela 6 zawiera tylko opisy problemów na poziomie protokolarnym. Problemy takie, jak wyczerpanie zasobów, utrata przywilejów, odrzucenie usług itp. zostały pominięte. Każde zagrożenie zostało opatrzone subiektywną oceną autora, odnoszącą się do rozwiązania danego problemu i charakteru danego systemu. Dane zagrożenie może nie dotyczyć systemu, może nie mieć wpływu na bezpieczeństwo systemu w ogóle, może mieć krytyczne skutki, może mieć pośredni wpływ na bezpieczeństwo systemu lub też dane zabezpieczenie odnoszące się do określonego zagrożenia może być uznane za skuteczne.

Przyjęto następujące określenia stanu bezpieczeństwa:

– bezpieczny: można uznać, że zaimplementowane mechanizmy na chwilę obecną zabezpieczają całkowicie przed danym atakiem, lub nie jest znany atak mogący skompromitować zabezpieczenie;

– pośredni: można uznać że zaimplementowane mechanizmy na chwilę obecną zabezpieczają przed danym atakiem wystarczająco; znane ataki nie są realizowane praktycznie;

– krytyczny: zabezpieczenie nie jest wystarczające.

5. Podsumowanie

Poziom bezpieczeństwa dostarczanego przez nowe technologie bezprzewodowe jest z roku na rok coraz wyższy. Jeżeli jednak rozważymy aspekty bezpieczeństwa bezprzewodowych technologii komunikacyjnych z punktu widzenia specyficznego charakteru sieci, możemy powiedzieć, że bezpieczeństwo sieci powinno być i generalnie jest tym większe, im szerszy jest zasięg jej użycia. Jest to wynikiem przede wszystkim komercyjnego podejścia: im więcej płacimy, tym więcej oczekujemy. Niemniej jednak, co jest oczywiste, zapewnienie wysokiego poziomu bezpieczeństwa większych systemów jest dużo trudniejsze niż w przypadku ich mniej skomplikowanych odpowiedników. Odnosząc się do oceny bezpieczeństwa, za najmniej bezpieczną technologię możemy uznać standard Bluetooth. Z punktu widzenia odległości

Sieć / Zagrożenie	Bluetooth 802.15.1 (PAN)	WiFi 802.11 (LAN)	WiMAX 802.16 (MAN)	GSM, UMTS (WAN)
Nieautoryzowany dostęp do istotnych danych przesyłanych przez sieć				
Podsłuch łącza radiowego	Bez znaczenia (mechanizm szyfrowania nie jest obowiązkowy)	WEP: Krytyczny WPA, WPA2: Pośredni	2001: Pośredni (użycie DES oraz przewidywalnych wektorów IV, głównie wyprowadzanych z numeru ramki) Obecny stan: Bezpieczny	GSM: Krytyczny (tylko łącza niechronione) lub Pośredni (łącza chronione za pomocą A5) UMTS: Bezpieczny
Maskarada (Masquerading)	Bez znaczenia (głównie brak wzajemnego uwierzytelnienia)	Krytyczny (brak wzajemnego uwierzytelnienia)	2001: Krytyczny (brak wzajemnego uwierzytelnienia) Obecny stan: Bezpieczny	GSM: Krytyczny (brak wzajemnego uwierzytelnienia) UMTS: Bezpieczny
Analiza ruchu sieci	Nie dotyczy	Krytyczny (szyfrowany tylko MAC PDU payload, pozostałe pola pakietu nieszyfrowane)	2001: Krytyczny (szyfrowany tylko MAC PDU payload, pozostałe pola pakietu nieszyfrowane) Obecny stan: Bezpieczny	GSM, UMTS: Bezpieczny (użycie tymczasowych identyfikatorów)
Przeglądanie baz danych	Nie dotyczy	Nie dotyczy	Nie dotyczy	GSM: Pośredni (niezabezpieczone bazy danych) UMTS: Bezpieczny (zabezpieczone bazy danych)
Wpływ zewnętrzny na transmisję	Nie dotyczy	WEP: Krytyczny WPA,WPA2: Pośredni (sekwencje IV)	2001: Krytyczny (użycie funkcji CRC, brak numeru sekwencyjnego) Obecny stan: Bezpieczny	GSM: Krytyczny (brak kontroli integralności) UMTS: Bezpieczny (kontrola integralności + numery sekwencyjne)
Nieautoryzowane manipulacje istotnych danych				
Manipulacje wiadomości	Nie dotyczy	WEP: Krytyczny WPA,WPA2: Pośredni (sekwencje IV)	2001: Krytyczny (użycie funkcji CRC, brak numeru sekwencyjnego) Obecny stan: Bezpieczny	GSM: Krytyczny (brak kontroli integralności) UMTS: Bezpieczny (kontrola integralności + numery sekwencyjne)

Tab. 6. Ocena stanu bezpieczeństwa sieci bezprzewodowych (Uwaga! Dla WiMAX podano w pierwszej części tabeli po dwa stany: dla wersji WiMAX z roku 2001 oraz wersji obecnej)

i kosztów zestawianych połączeń wszystkie problemy, choć krytyczne, przestają jednak mieć jakiekolwiek znaczenie praktyczne. Technologia WiFi od początku swojego istnienia borykała się z trudnościami w dziedzinie bezpieczeństwa. Pomimo prób poprawienia początkowej sytuacji wielu problemów nie rozwiązano, choć ogólnie stan bezpieczeństwa tych sieci można uznać za stabilny. Z kolei sieci WiMAX oraz UMTS charakteryzują się wysokim poziomem bezpieczeństwa. Dodatkowo należy zauważyć, że problemy, jakie można zdefiniować dla dwóch najbardziej rozległych typów sieci, wynikają generalnie ze skomplikowanego zarządzania takimi sieciami. Aby zagrożenia te były realne, musi zaistnieć wiele warunków.

Sebastian Rogawski
Politechnika Gdańska,
Adva Optical Networking

Bibliografia:

[1] ARIB STD-T63-21.133 V3.2.0 Security Threats and requirements.
[2] 3GPP TS 33.102 V7.1.0 (2006-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 7)
[3] On Bluetooth. Security, Nikos Mavrogiannopoulos December 16, 2005
[4] Wireless Network Security 802.11, Bluetooth and Handheld Devices - NIST Special Publication 800-48
[5] Bluetooth Security White Paper - Bluetooth SIG Security Expert Group 2002
[6] Wireless Network Security 802.11, Bluetooth and Handheld Devices -Tom Karygiannis, Les Owens; Natialn Institute of Standards and Technology, Technology Administration U.S. Department of Commerce
[7] Transmit Simulation and Receive Optimization for 802.11b Networks by Pascal F. Rettig
[8] Overview of IEEE 802.16 Security – David Johnson, Jeske Walker, Intel
[9] IEEE Std. 802.16-2001, IEEE Standard for Local and Metropolitan Area Networks, part 16, "Air Interface for Fixed Broadband Wireless Access Systems", IEEE Press, 2001.
[10] GSM and GPRS Security - Chengyuan Peng - Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology
[11] ETS 300 506. Digital Cellular Telecommunication System (Phase 2); Security Aspects.
European Telecommunications Standards Institute, August 2000.

Bezprzewodowa technologia wLSN

Bezprzewodowa lokalna sieć bezpieczeństwa wLSN firmy Bosch zastosowana w systemach SSWiN wykorzystuje wiele oryginalnych, autorskich i opatentowanych technologii, dzięki czemu system sygnalizacji włamania i napadu jest niezawodny nawet w niesprzyjających warunkach

Obserwowane w ostatnich latach bardzo duże zapotrzebowanie na systemy ochrony powoduje ich coraz bardziej dynamiczny rozwój. Rozwój ten wynika również z potrzeby spełnienia rosnących oczekiwań rynku systemów zabezpieczeń. Już wiele lat temu na rynku pojawiły się systemy bezprzewodowe. Początkowo były one dość zawodne. Charakteryzowały się małą skutecznością wykrywania intruzów i posiadały słabą odporność na fałszywe alarmy. Były podatne na zakłócenia komunikacji, a do tego miały spory „apetyt" na energię elektryczną, dlatego wymagały częstej wymiany baterii, co wiązało się znacznym wzrostem kosztów eksploatacji. Z tego powodu wiele firm przestało zajmować się ich dystrybucją, a jeśli nawet posiadały te systemy w swojej ofercie, to przeważnie były one zawodne i nie spełniały dobrze swojej roli. Na szczęście nie wszystkie!

Na podstawie wieloletnich doświadczeń oraz najnowszych wyników badań Centrum Badawczo-Rozwojowego firmy Bosch dział Security Systems stworzył bezprzewodowy system alarmowy, który zaprzecza istniejącym stereotypom odnoszącym się do systemów bezprzewodowych.

Po co system bezprzewodowy?

W wielu obiektach z różnych względów nie jest możliwe przeprowadzenie standardowej instalacji, która wiąże się z wierceniem czy kuciem, np. ze względu na estetykę obiektu lub jego wartość historyczną. Trudno wyobrazić sobie prowadzone w korytach przewody w zabytkowym kościele na freskach czy płaskorzeźbach. Podobnie problematyczna jest rozbudowa istniejącego systemu w eleganckim mieszkaniu. Jak wytłumaczyć właścicielowi, że nie będzie śladu na fachowo zaszpachlowanej ścianie, którą zresztą można przecież odmalować. Tego typu trudności może być znacznie więcej. Poza tym instalacja przewodowa bywa po prostu nieopłacalna. W odpowiedzi na takie problemy stworzony został system bezprzewodowy, który eliminuje trud standardowej instalacji, pozwala zaoszczędzić czas i często okazuje się bardziej ekonomiczny niż tradycyjny system przewodowy.

Komunikacja między urządzeniami

Komunikacja bezprzewodowa w technologii wLSN (*wireless Local Security Network* – bezprzewodowa lokalna sieć bezpieczeństwa) wymaga koncentratora wLSN, który stanowi łącze pomiędzy urządzeniami bezprzewodowymi a centralą alarmową. Pracuje on jako nadrzędne urządzenie sieciowe, które dostarcza sygnały taktowania i synchronizacji. Pełni rolę administratora bezprzewodowej sieci LSN, odpowiada za dobór czasu dokonywania i synchronizacji operacji w sieci, monitorowanie stanu czujek w sieci oraz wysyłanie danych konfiguracyjnych do odpowiednich węzłów czujek. Zapewnia łączność z urządzeniami przy odległości dochodzącej nawet do 1000 m w przestrzeni otwartej. Komunikacja z centralą alarmową odbywa się za pośrednictwem czterożyłowej magistrali.

Bezpieczny przez co bezkonkurencyjny

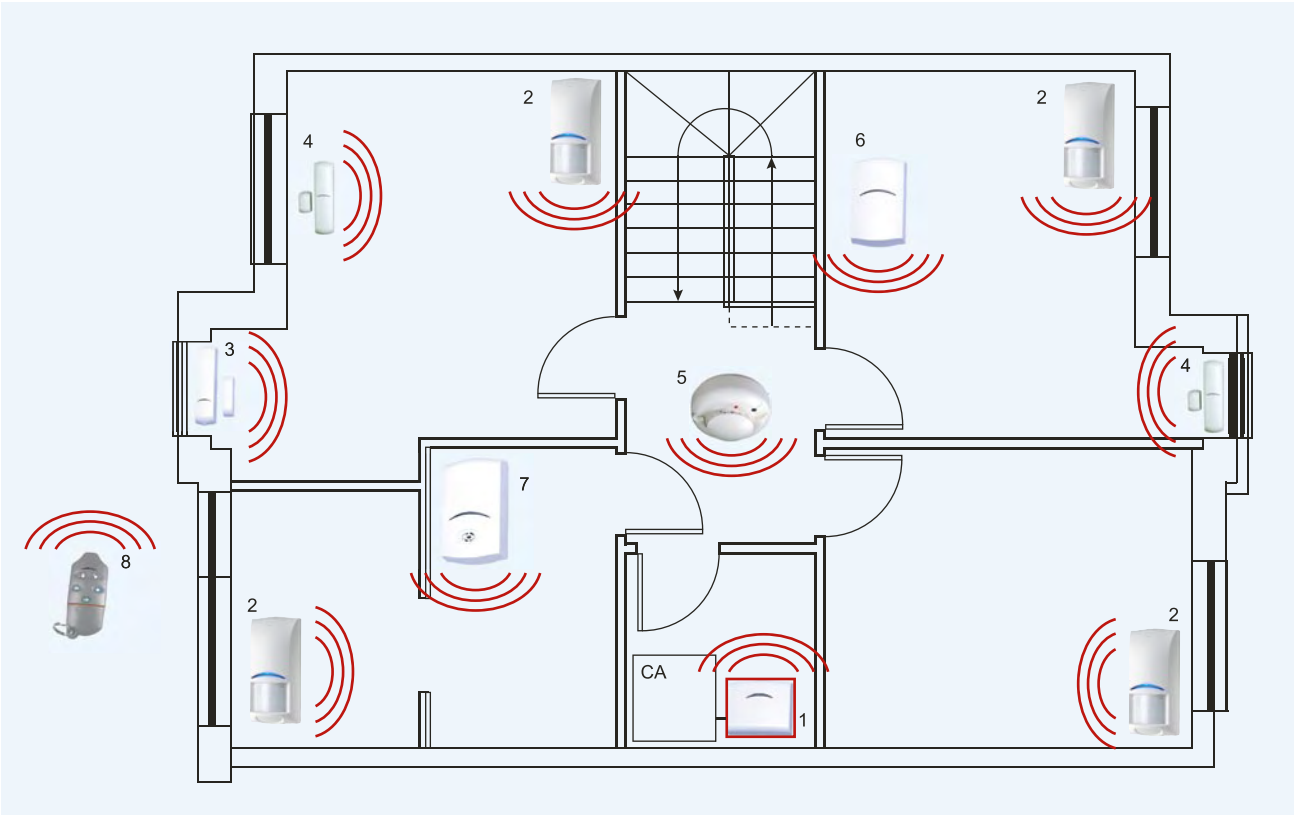
Technologia wLSN pracuje w europejskim paśmie bezpieczeństwa 868 MHz zarezerwowanym wyłącznie dla systemów sygnalizacji włamania i napadów oraz dla systemów sygnalizacji pożaru. Ograniczone pasmo komunikacji oraz zastosowane protokoły sieciowe uniemożliwiają zakłócenia innymi urządzeniami radiowymi, np. domowego użytku, takimi jak bezprzewodowe słuchawki czy wszelkiego rodzaju piloty sterujące.

Tryb wyszukiwania – sam przeprowadzi instalację urządzeń w systemie

Podczas instalacji w trybie wyszukiwania koncentrator wyszukuje urządzenia i automatycznie zapisuje ich adresy. Z ośmiu dostępnych kanałów o wąskim paśmie częstotliwościowym wynoszącym 25 kHz koncentrator wybiera i zapisuje podczas wyszukiwania dwa, dla których komunikacja bezprzewodowa jest najlepsza. Po wyszukaniu i zapisaniu wszystkich urządzeń koncentrator w czasie normalnej pracy komunikuje się tylko z wcześniej zapisanymi urządzeniami. Dzięki temu możliwe jest działanie kilku systemów w tym samym obiekcie i nie dochodzi do wzajemnego zakłócania pracy.

Dwukierunkowa komunikacja

Komunikacja w technologii wLSN jest dwukierunkowa, co ma olbrzymi wpływ na niezawodność działania całego systemu. Koncentrator wLSN wysyła komunikaty do czasu ich potwierdzenia. Jeżeli takiej odpowiedzi nie dostanie, automatycznie przełącza się na drugą częstotliwość, która została zapisana w trybie wyszukiwania. System wLSN potwierdza stan systemu i komunikuje gotowość bądź brak gotowości do dalszej pracy. W przypadku komunikacji jednokierunkowej wysłane komunikaty nie dają odpowiedzi i nie ma żadnej pewności, czy zostały odebrane.



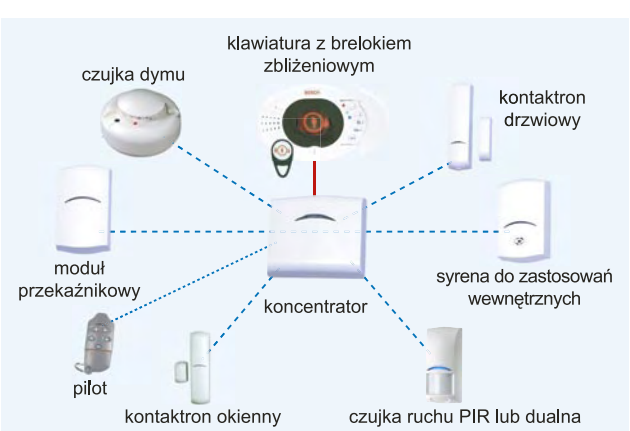
Rys. 1. Przykładowe zastosowanie systemu bezprzewodowego w domku jednorodzinnym gdzie: 1 - Koncentrator wLSN, 2 - Czujka ruchu PIR i dualna, 3 - Kontaktron drzwiowy, 4 - Kontaktron okienny, 5 - Czujka dymu, 6 - Czujka stłuczenia szkła, 7 - Sygnalizator do zastosowań wewnętrznych, 8 - Pilot uzbrajający/rozbrajający/napadowy

System wLSN spełnia europejską normę EN 50131-5-3 w zakresie bezprzewodowej transmisji alarmów. To kolejny bardzo istotny element, podkreślający zalety systemu Bosch.

Czas pracy na baterii nawet do pięciu lat!

Zmorą wszystkich urządzeń bezprzewodowych jest pojemność akumulatora. Wiele wciąż dostępnych na rynku systemów bezprzewodowych nie jest w stanie zagwarantować długiej i niezawodnej pracy, często nawet nie wskazując potrzeby wymiany baterii w czujkach, co doprowadza do tego, że system staje się bezużyteczny.

Innowacyjność technologii wLSN dzięki zastosowaniu najnowszych technik komunikacji bezprzewodowej pozwala na wydłużenie czasu pracy na akumulatorach nawet do pięciu lat. Tak długi czas pracy znacznie ogranicza koszty eksploatacji. Ponadto system sygnalizuje potrzebę wymiany akumulatorów w poszczególnych elementach należących do systemu.



Rys. 2. Zestawienie urządzeń w technologii wLSN

Duże możliwości

Bosch Security Systems, wprowadzając na rynek system wLSN, zadbał o bardzo duży asortyment urządzeń współpracujących: czujki PIR, dualne, kontaktrony drzwiowe i okienne, czujki zbicia szkła, czujki inercyjne, czujki dymu, pilot umożliwiający uzbrajanie i rozbrajanie systemu, syreny do zastosowań wewnętrznych, dodatkowy moduł przekaźnikowy do sterowania oświetleniem lub drzwiami garażowymi. Daje to kompletny zestaw do zabezpieczenia obiektów, zapewnia dużą elastyczność i możliwość przyszłego rozwoju systemu.

Bezprzewodowa technologia wLSN dowodzi, że system bezpieczeństwa może z powodzeniem wykorzystywać łączność bezprzewodową. Jednocześnie zaprzecza istniejącym do tej pory stereotypom. System wLSN spełnia pod względem funkcjonalności oczekiwania nawet najbardziej wymagających klientów, a przy tym jest całkowicie niezawodny i bezpieczny. Dzięki prostej instalacji oraz niskim kosztom eksploatacyjnym stał się również systemem ogólnie dostępnym. Bosch jest marką wiodącą, gwarantującą najwyższą jakość wykonania i niezawodność wszystkich swoich produktów.

Krzysztof Kostecki
Bosch Security Systems

INFO-CAM

Wyłączny dystrybutor **AVerMedia Technologies, Inc.** www.infocam.com.pl

PŁOCK Al. Kilińskiego 5, tel. (024) 266 97 12, tel./fax (024) 266 97 13, handlowy@infocam.com.pl

NeoTech J2000D-16T2DVAU

- Rejestrator cyfrowy typu Stand Alone
- 16 przelotowych wejść kamer
- 4 wejścia i 1 wyjście **audio RCA**
- Prędkość wyświetlania **400 kl./sek.**
- Zapis obrazu z prędkością **100 kl./sek.** w rozdzielczości **720x288**, 200 kl./sek. w rozdzielczości 360x280
- Algorytm kompresji **JPEG2000** (wysoka jakość zapisanego obrazu, mały rozmiar pliku)
- Kompresja **H.264** dla podglądu w sieci LAN, WAN
- Praca w trybie **Triplex** (Odtwarzanie, Nagrywanie, Praca w sieci)
- Zdalny podgląd obrazu dobrej jakości przez TCP/IP (obsługa **DDNS**)
- Automatyczne wykrywanie ustawień sieciowych DHCP
- Wbudowane wyjście **VGA** (obsługa monitorów TFT LCD)
- Możliwość podłączenia myszki PS/2
- Backup danych poprzez wbudowaną nagrywarkę **DVD-RW** lub port **USB 2.0**
- Programowa detekcja ruchu
- Menu ekranowe w języku polskim
- Obsługa 2 dysków twardych **S-ATA** bez limitu pojemności
- Pilot zdalnego sterowania
- Możliwość podłączenia pulpitu sterującego J2000-KB485

4 545,00 zł

3 575,00 zł **NeoTech J2000D-08T2DVAU - 8ch**

AVerDiGi NV7000H

AVerMedia

- Karta PCI + oprogramowanie w języku polskim
- 8 wejść video BNC, 8 wejść audio RCA
- Prędkość wyświetlania i zapisu **200 kl./sek.**
- Praca w OS Windows 2000 / XP / **Vista**
- Maks. rozdz. wyświetlania i zapisu 720x576
- **Sprzętowa kompresja obrazu H.264**
- 2 tryby deinterlacji graficznej dla scen statycznych i dynamicznych
- Możliwość podłączenia kamer IP PAL i IP Megapixelowych
- Funkcja automatycznej redukcji szumów NRF
- Wbudowane wyjście TV-OUT
- Praca w sieci LAN, WAN, ISDN, SDI, ADSL
- Wyszukiwanie archiwum po dacie, czasie, zdarzeniach alarmowych, detekcji ruchu, inne
- Transmisja na odległość (WebCam, zdalna konsola, PDA, GSM, CMS)
- Obsługa dynamicznych nazw domen DDNS
- Możliwość zdalnej zmiany ustawień i podglądu archiwum
- Zoom cyfrowy w podlądzie na żywo i w archiwum
- Programowa detekcja ruchu z możliwością ustawienia masek detekcji
- Funkcja inteligentnego i wizualnego wyszukiwania zdarzeń
- Wizualizacja operacji kasowych POS
- Znak wodny i 5 poziomów zabezpieczeń hasłami
- Możliwość rejestracji dźwięku do 16 kanałów
- Możliwość łączenia w system: 16ch – 400 kl./sek.

3 799,00 zł

AVerMedia AVerDiGi EB1304 NET

- Rejestrator cyfrowy typu Stand Alone
- Kompresja obrazu **MPEG4**
- 4 wejścia kamer BNC
- Wyjście wizyjne composite BNC i **VGA**
- 1 wejście i 1 wyjście **audio** RCA
- Prędkość wyświetlania 100 kl./sek.
- Prędkość zapisu 100 kl./sek. (tryb QUAD), **50 kl./sek.** (tryb EACH)
- Rozdzielczość zapisu **720x576** (tryb EACH), 360x288 (tryb QUAD)
- Programowa detekcja ruchu
- Praca w trybie **Triplex**
- Praca w sieci **LAN**, WAN
- Wbudowany serwer HTTP, zdalny podgląd przez PDA, CMS
- Obsługa 1 dysku twardego bez limitu pojemności
- Technologia pomijania uszkodzonych sektorów dysku
- Graficzne menu ekranowe w języku polskim
- Złącze **USB 2.0** do komunikacji z komputerem PC
- 4 wejścia alarmowe, 1 wyjście przekaźnikowe
- Brak ruchomych elementów chłodzących
- Pilot zdalnego sterowania
- Wymiary: 290 x 180 x 50 mm

1 625,00 zł

CAMSTAR CAM-640C/OSD

- Kamera kolorowa typu **Dzień/Noc**
- Przetwornik 1/3" **Sony** CCD Nextchip DSP
- Rozdzielczość **520 linii TV**
- Czułość 0.1 luxa przy F1.2 (low illumination mode)
- Sterowanie AutoIris Video i DC
- Menu ekranowe **OSD**
- 64 pola detekcji ruchu
- 4 strefy prywatności
- Regulacja: ostrości/jasności/kontrastu/saturacji
- Cyfrowa redukcja szumów DNR
- Migawka ręczna lub automatyczna
- Automatyczny balans bieli AWB/ATW
- Zasilanie 12VDC
- Wymiary: 125 x 60 x 53 mm

395,00 zł

CAMSTAR CAM-430IV2B/OSD

- Kamera kolorowa typu **Dzień/Noc wodoodporna**
- Przetwornik 1/3" **Sony** CCD Nextchip DSP
- Rozdzielczość **450 linii TV**
- Wbudowany promiennik podczerwieni IR, zasięg do 40 m
- Czułość 0 luxa przy aktywnym prominniku IR
- Wbudowany obiektyw o zmiennej ogniskowej 4-9 mm
- Menu ekranowe **OSD**
- 64 pola detekcji ruchu
- 4 strefy prywatności
- Regulacja: ostrości/jasności/kontrastu/saturacji
- Cyfrowa redukcja szumów DNR
- Migawka ręczna lub automatyczna
- Automatyczny balans bieli AWB/ATW
- Uchwyt z przepustem kablowym w komplecie
- Zasilanie 12VDC
- Wymiary: 195 x 165 x 84 mm

480,00 zł

CAMSTAR CAM-430C/OSD

- Kamera kolorowa typu **Dzień/Noc**
- Przetwornik 1/3" **Sony** CCD Nextchip DSP
- Rozdzielczość **450 linii TV**
- Czułość 0.1 luxa przy F1.2 (low illumination mode)
- Sterowanie AutoIris Video i DC
- Menu ekranowe **OSD**
- 64 pola detekcji ruchu
- 4 strefy prywatności
- Regulacja: ostrości/jasności/kontrastu/saturacji
- Cyfrowa redukcja szumów DNR
- Migawka ręczna lub automatyczna
- Automatyczny balans bieli AWB/ATW
- Zasilanie 12VDC
- Wymiary: 125 x 60 x 53 mm

295,00 zł

CAMSTAR CAM-432D/OSD

- Kamera kolorowa typu **Dzień/Noc** kopułowa
- Przetwornik 1/3" **Sony** CCD Nextchip DSP
- Rozdzielczość **450 linii TV**
- Czułość 0.1 luxa przy F1.2 (low illumination mode)
- Wbudowany obiektyw 3.6 mm
- Menu ekranowe **OSD**
- 64 pola detekcji ruchu
- 4 strefy prywatności
- Regulacja: ostrości/jasności/kontrastu/saturacji
- Cyfrowa redukcja szumów DNR
- Migawka ręczna lub automatyczna
- Automatyczny balans bieli AWB/ATW
- Zasilanie 12VDC
- Wymiary: ϕ 135 x 80 mm

299,00 zł

Zestaw obserwacyjny

- Rejestrator cyfrowy **AVerDiGi EB1304 MD** (kompresja MPEG4, wyjście VGA, 4ch video, 1ch audio, 100kl./sek., rozdz. 720x576, detekcja ruchu, USB 2.0)
- Dysk twardy **250GB**
- Kolorowy monitor CRT 17" **GATEWAY VX750**
- 4 x kamera kolorowa typu **CAMSTAR CAM-210D** (1/4" Sharp CCD; 420 linii TV; 1,0 luxa przy F 1.2; wbudowany obiektyw 3.6 mm)

1 800,00 zł

atrakcyjne rabaty dla firm instalacyjnych i dystrybutorów

%

Podane ceny nie zawierają podatku VAT 22%.
Oferta promocyjna obowiązuje do wyczerpania zapasów.
Niniejsza oferta nie stanowi oferty handlowej w rozumieniu art. 66 par. 1 KC oraz innych właściwych przepisów prawnych.

artykuł sponsorowany

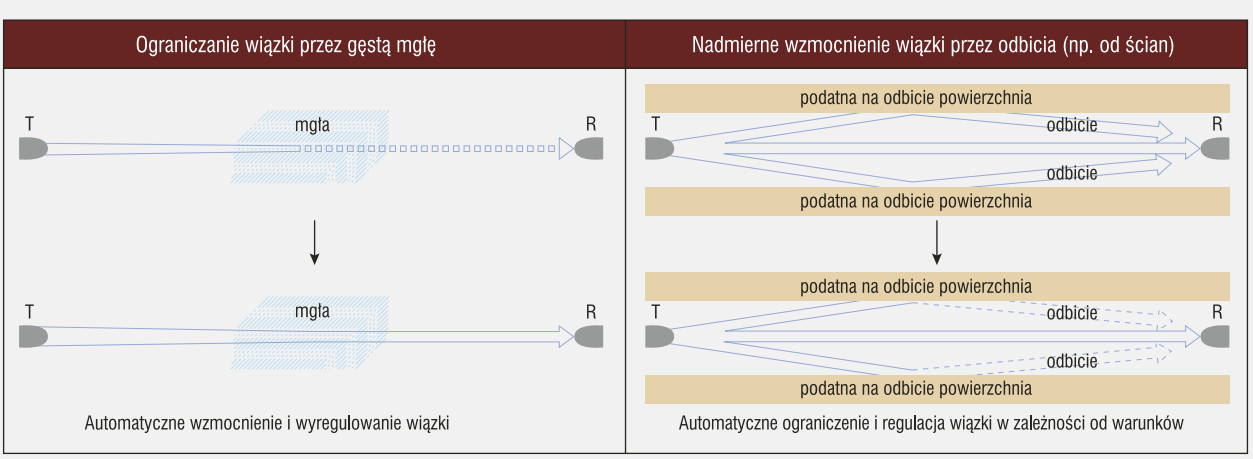
Cyfrowe bariery podczerwieni

serii AX-350/650DH MKIII

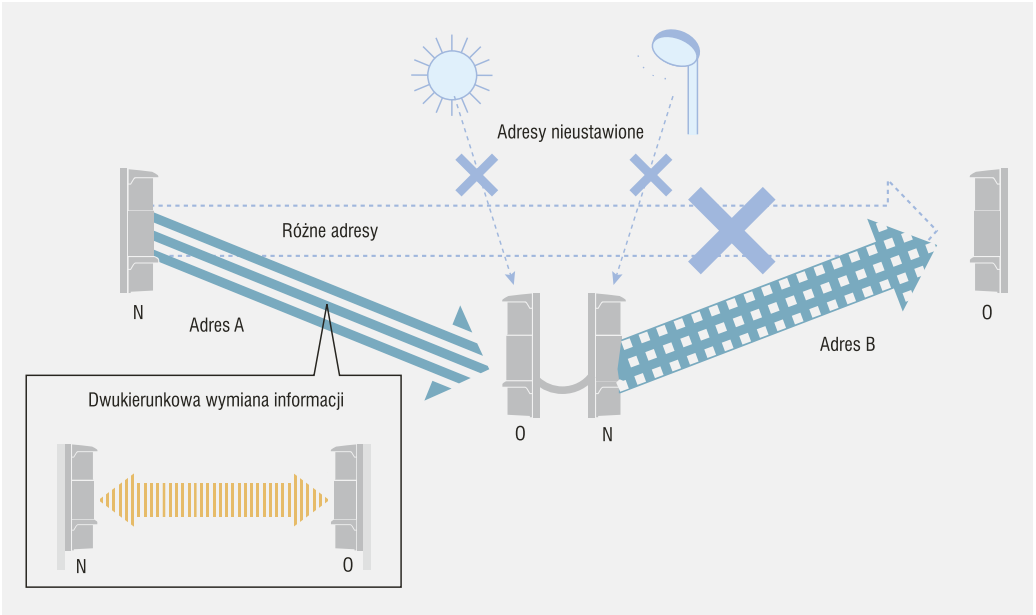
Przedstawiamy Państwu pierwszą w pełni cyfrową barierę podczerwieni. To wyjątkowe urządzenie wprowadza zupełnie nowe podejście do problematyki wykorzystania tego typu sprzętu w systemach zabezpieczeń. Prostota obsługi, przejrzyste i proste zasady projektowania oraz wyjątkowa odporność na warunki pracy umożliwiają szybką i bezproblemową realizację nawet najbardziej skomplikowanych instalacji

Detekcja intruza za pomocą przerwanej wiązki światła znana jest w technice zabezpieczeń od bardzo dawna. Ewolucja działających w ten sposób urządzeń doprowadziła do powstania szeregu produktów o różnych własnościach użytkowych. Dostępne są czujki krótkiego i dalekiego zasięgu, o dwu lub więcej wiązkach, modulowane jedną lub kilkoma częstotliwościami itd. Stabilność oferty potwierdza niewielka liczba nowych produktów w tym segmencie rynku. Ewentualne nowości polegają raczej na zastosowaniu zdobyczy technologii materiałowych bądź nowych rozwiązań z dziedziny elektroniki lub inżynierii komputerowej niż na istotnych zmianach w sposobie funkcjonowania czujek. Firma Optex, lider w dziedzinie rozwiązań z zakresu ochrony zewnętrznej, postanowiła zmienić *status quo* i zaproponować zupełnie nowe rozwiązanie. Jest nim pierwsza cyfrowa bariera podczerwieni AX-350/650DH. Zastosowano w niej serię nowatorskich rozwiązań technicznych, które na zawsze zmienią podejście do zagadnienia ochrony obwodowej przy użyciu barier podczerwieni.

Istotą tego rozwiązania jest realizacja informacyjnego sprzężenia zwrotnego pomiędzy nadajnikiem i odbiornikiem. Modulowanie wiązki podczerwieni, wykorzystywane powszechnie w standardowych produktach do identyfikacji nadajnika przez odbiornik, wykorzystano jako nośnik informacji o stanie nadajnika, warunkach pracy oraz innych istotnych danych. Sprzężenie zwrotne, czyli informacja zwrotna z odbiornika do nadajnika, jest również realizowane za pomocą wiązki podczerwieni. Stworzono w ten sposób bezprzewodowy, dwukierunkowy kanał informacyjny, który wykorzystano do realizacji nowatorskich technologii, takich jak System Optymalizacji Natężenia Wiązki (ATPC – *Auto Transmit Power Control*), automatyczne rozpoznawanie adresu urządzeń czy Funkcja Synchronizacji Pionowej



Rys. 1. Optymalizacja natężenia emitowanej wiązki - ATPC



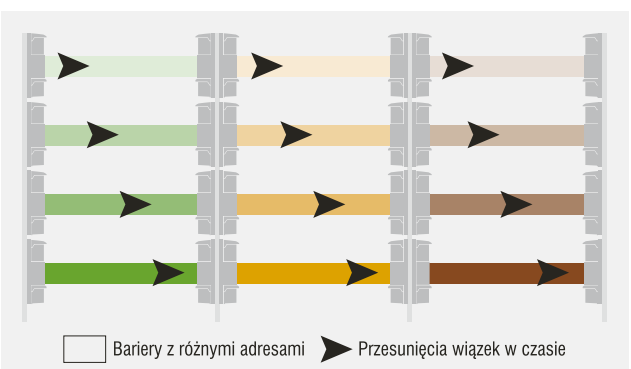
Rys. 2. Identyfikacja źródła wiązki

(*Time Division Multiplex*). To właśnie opracowanie i zastosowanie tych technologii świadczy o wyjątkowości urządzeń systemu AX-350/650DH.

System Optymalizacji Natężenia Wiązki dzięki dwukierunkowej wymianie danych stroi parametry pracy bariery tak, aby uzyskać maksymalną wydajność urządzenia. Regulując natężenie emitowanego sygnału, urządzenie dostosowuje się do zmiennych warunków atmosferycznych, zapewniając optymalne warunki pracy w zakresie możliwości sprzętowych. Dzięki tej funkcji parametry wiązki są zawsze optymalne, co zapobiega powstawaniu fałszywych alarmów oraz powoduje wyeliminowanie zjawiska odbić wiązek o zbyt dużym natężeniu. W klasycznych urządzeniach zjawisko odbić, obserwowane na przykład w wąskich przejściach lub podczas opadów śniegu, powoduje powstanie wielu „ścieżek", którymi energia wiązki dociera do odbiornika. Może to powodować brak alarmu przy przejściu intruza. Sterowanie natężeniem emitowanej wiązki podczerwieni oznacza również oszczędność energii. Maksymalna wartość poboru prądu, podana w specyfikacji produktu, wynosi 110 mA. Należy pamiętać, że do maksymalnego poboru prądu dochodzi jedynie w wyjątkowo niekorzystnych warunkach pracy bariery oraz przy pełnej wizualizacji jej stanu diodami LED w nadajniku i odbiorniku, czyli niezwykle rzadko. Typowe wartości w normalnych warunkach pracy nie przekraczają kilkudziesięciu mA.

Automatyczne rozpoznawanie adresu zastąpiło uciążliwe w użyciu ustawianie częstotliwości modulacji wiązek podczerwieni. W systemie czujek AX-350/650DH każda z nich już na etapie produkcji jest jednoznacznie identyfikowana za pomocą jednego z 63 dostępnych w systemie adresów. Odbiornik domyślnie nie posiada żadnego adresu. Dopiero po wykonaniu niezbędnych czynności instalacyjnych oraz przeprowadzeniu wstępnego strojenia programujemy odbiornik do pracy z odpowiednim nadajnikiem przez jedno naciśnięcie przycisku. System dostaw firmy Optex gwarantuje, że dostarczone produkty będą posiadały odpowiednio zróżnicowane adresy. Poza tym każde urządzenie umożliwia szybką i wygodną zmianę adresu na adres alternatywny. Dzięki tej technologii zdjęto z projektanta i instalatora trudny obowiązek skomplikowanego planowania wykorzystania częstotliwości modulacji wiązek podczerwieni w poszczególnych czujkach.

Funkcja Synchronizacji Pionowej jest szczególnie przydatna w realizacji aplikacji wielopoziomowych. Aby zapobiec ewentualnym interferencjom oraz zapewnić każdej z czujek optymalne warunki pracy, system czujek AX-350/650DH wyposażono w funkcję multipleksowania czasu aktywacji kolejnych wiązek. W ten sposób w najbliższym sąsiedztwie transmisji dokonuje tylko jedna czujka, dzięki czemu unika się nakładania wiązek i potencjalnego zakłócania transmisji. Wykorzystując te udogodnienia, można instalować do czterech poziomów czujek. Oczywiście synchronizacja pozioma odbywa się bezprzewodowo. Czujki systemu AX-350/650DH wyposażono w oryginalną obudowę. Wykonana z wysokiej jakości materiałów jest w pełni szczelna, zapewniając wyjątkowo wysoki stopień ochrony – IP65. Charakterystyczne „daszki" na pokrywie czujki stanowią jej zabezpieczenie przed szronem, który mógłby zakłócić pracę urządzenia. Kolejne udogodnienia odnajdujemy w konstrukcji głowic roboczych. Pozycjonowania dokonuje się bez użycia narzędzi, za pomocą specjalnie zaprojektowanych pokręteł, które umożliwiają precyzyjne dostrojenie wiązek. Dzięki dwukierunkowej transmisji danych zrealizowano dokładną wizualizację stanu dostrojenia obu wiązek, zarówno w nadajniku jak i odbiorniku. Kolejnym udogodnieniem dla instalatora jest wykorzystanie możliwości sterowania natężeniem emitowanej wiązki w systemie strojenia czujki. Przekraczając kolejne poziomy dostrojenia, urządzenie zmniejsza natężenie emitowanych wiązek, umożliwiając wyjątkowo dokładne i szybkie pozycjonowanie układów optycznych nadajnika i odbiornika. Umożliwia to strojenie czujek przez jedną



Rys. 3. Synchronizacja pionowa czujek - TDM

osobę oraz wykonanie pełnego cyklu wzajemnego pozycjonowania wiązek bez użycia multimetru. Wysiłek i czas poświęcone na tym etapie instalacji barier podczerwieni zawsze procentują niezawodną pracą urządzeń w trudnych warunkach atmosferycznych.

Wszystkie rozwiązania i technologie zastosowane w systemie barier AX-350/650DH są owocem pracy inżynierów firmy Optex. Ich celem było stworzenie nowego systemu czujek, który będzie bardziej przystępny dla projektanta i instalatora zabezpieczeń obwodowych. Zaproponowany system jest bardzo nowatorski, ponieważ wprowadza daleko idące zmiany w ogólnie przyjętym schemacie dla tego typu urządzeń. Firma Optex podjęła ryzyko związane z wprowadzeniem takiego systemu na rynek z bardzo dobrym skutkiem. Zaproponowane rozwiązania umożliwiają nawet mniej doświadczonej kadrze szybkie i sprawne wykonanie systemu ochrony obwodowej. Uruchomienie czy serwis systemu nie wymagają posiadania specjalistycznych narzędzi i mogą być dokonane przez jedną osobę. Wszystkie te udogodnienia oznaczają duże oszczędności dla firm realizujących projekty inwestycyjne z wykorzystaniem czujek serii AX-350/650DH. Wszystkie produkty opisane w niniejszym artykule można nabyć w firmie AAT-T – polskiego dystrybutora firmy Optex.

Jarosław Gibas
Optex Security

Kolorowe drukarki do kart identyfikacyjnych PVC

MAGICARD

HoloKote™ - znak wodny drukowany na całej powierzchni karty. Widoczny przy patrzeniu pod kątem.

Nadruk od krawędzi do krawędzi z jakością 300 dpi.

HoloPatch™ - okno w rogu karty, w którym znak wodny jest bezpośrednio widoczny (opcja karty).

Możliwość kodowania pasków magnetycznych (opcja).

Dwustronny nadruk – tylko drukarka Avalon Duo.

Taśmy kolorowe nadruk 250, 300 lub 350 kart. Taśmy monochromatyczne nadruk 1000 kart. Kolory taśm monochromatycznych: czarny, czerwony, niebieski, zielony, złoty, srebrny, biały oraz taśma typu scratch-off (zdrapka).

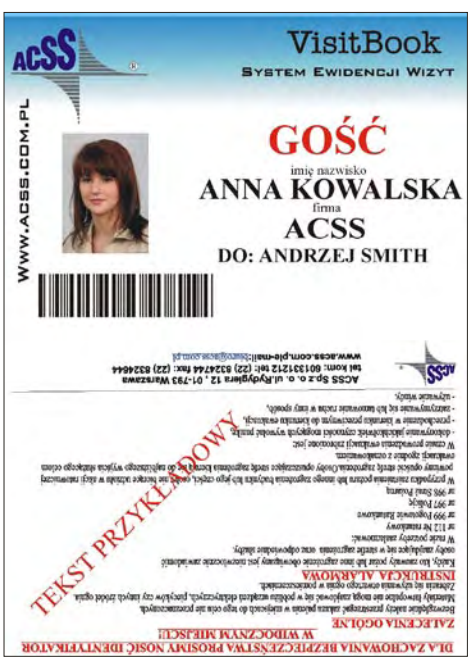
Specyfikacja techniczna
Prędkość nadruku
Wydruk karty w kolorze od krawędzi do krawędzi w 35 sekund
Monochromatyczny wydruk karty w 6 sekund
Cykl działania
Ciągły
Wbudowane zabezpieczenia
HoloKoteTM anty-coping – znak wodny na całej powierzchni karty
Typ taśmy
AV1: YMCKO nadruk 250 kart
LC1: YMCKO nadruk 350 kart
LC3: Monochromatyczny nadruk 1000 kart
LC8: YMCKOK nadruk dwustronny 300 kart (tylko Avalon Duo)
Karty
Drukuje na wszystkich standardowych kartach PCV ISO CR80 o grubości od 0,38 mm do 1,6 mm, kartach magnetycznych, zbliżeniowych, samoprzylepnych
Dostępne karty z HoloPatchTM
Pojemność magazynków kart
Podajnik 100 kart
Zasobnik kart nadrukowanych 50 sztuk
Głowica
300 dpi (wymienna)
Interfejs do PC
USB rev. 1.1. (kompatybilny z USB 2.0)
Sterowniki
Windows 2000, XP, VISTA
Kompatybilność elektromagnetyczna i certyfikat
EN 50 081-1 i EN 50 082-1 (Europa)/CE
Zasilanie
90-265 V / 47-63 Hz
Wymiary
Avalon (445 x 200 x 220) mm
Avalon Duo (470 x 200 x 220) mm
Waga
Avalon około 7,2 kg
Avalon Duo około 8,3 kg
Kolor
Srebrny metalik (fioletowe ścianki boczne)
Temperatura pracy
10-30°C
Gwarancja
2 lata

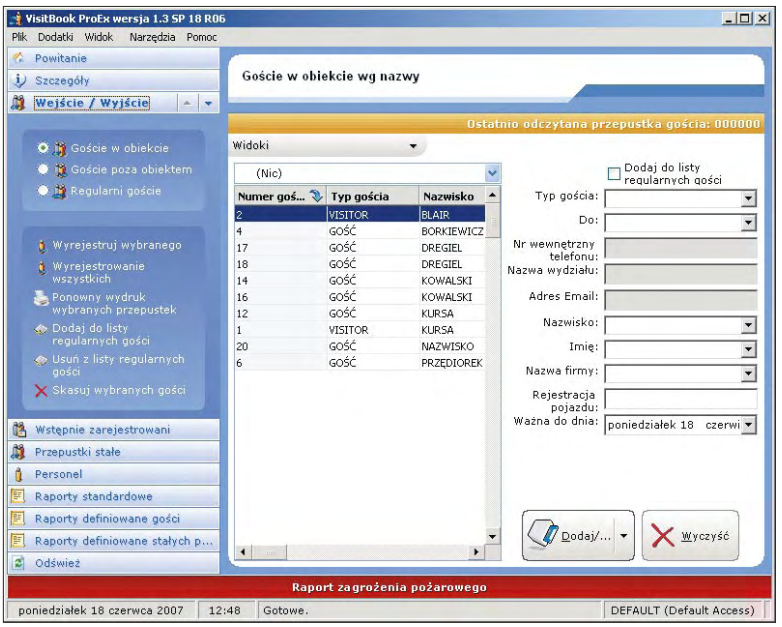
Dystrybutor w Polsce:

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

System rejestracji gości VisitBook

System rejestracji gości VisitBook jest narzędziem służącym do wspomagania pracy recepcji. Zastępuje papierową księgę gości jej elektronicznym odpowiednikiem. System umożliwia rejestrację danych gości 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 przez użycie czytnika kodów kreskowych. Program VisitBook został stworzony w trzech wersjach: Lite, Pro i ProEx.





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.

Ostatnia z nich – wersja ProEx jest wersją najbardziej rozbudowaną. Umożliwia ona wydruk przepustki wraz ze zdjęciem oraz zawiera między innymi funkcję projektowania własnych wzorów przepustek. Wydruk przepustek możliwy jest na standardowych drukarkach biurowych oraz drukarkach termosublimacyjnych do kart PVC (tylko wersja ProEx).

Zasadniczą zaletą użycia systemu jest możliwość raportowania w czasie rzeczywistym np. raport pożarowy, raport gości w obiekcie, raport ruchów gości itp. Program dodatkowo zawiera kilka użytecznych funkcji takich jak: manager personelu, manager kontrahentów, obsługa konferencji.

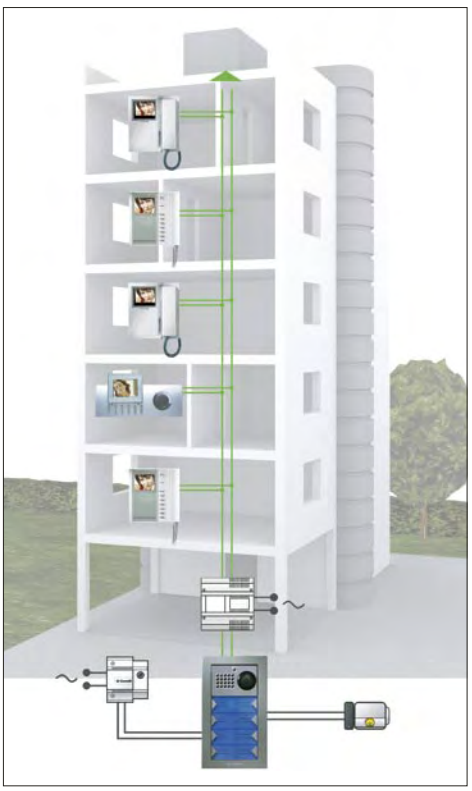
Wybrane funkcje systemu VisitBook	wersja LITE	wersja PRO	wersja PRO EX
Kontrola gości, Kontrahentów, Personelu	tak	tak	tak
Rejestracja wstępna	–	tak	tak
Lista regularnych gości	–	tak	tak
Pobieranie zdjęcia	–	–	tak
Czytnik kodów kreskowych	–	tak	tak
Elektroniczny podpis	–	–	tak
Przepustka pojazdu	–	–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

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

tel. 022 832 47 44,faks 022 832 46 44
e-mail: biuro@acss.com.pl
http://www.acss.com.pl

2-przewodowy, kolorowy system wideodomofonowy

firmy COMELIT



SBC SIMPLEBUS COLOR

Cechy systemu:

- kolorowe monitory z ekranami LCD;
- 2 przewody łącznie z zasilaniem monitora;
- 4 magistrale na zasilacz (np. 4 piony w budynku mieszkalnym);
- do 8 monitorów z funkcją interkomu na każdy apartament;
- do 240 użytkowników;
- do 600 m maksymalnej odległości pomiędzy panelem wejściowym, a ostatnim monitorem;
- nieograniczona liczba paneli głównych i dodatkowych;
- centralny moduł portiera;
- proste programowanie za pomocą przełączników;
- możliwość tworzenia systemów mieszanych audio i wideo.

Aparaty wewnętrzne dostępne w systemie Simplebus Color

GENIUS

BRAVO

DIVA

UNIFON STYLE

Panele wejściowe

W systemie Simlpebus2 można zastosować panele wejściowe serii Powercom jak i wandaloodporne Vandalcom. Oba panele występują w wersji cyfrowej z elektronicznym spisem nazwisk oraz z indywidualnymi przyciskami wywołania. Ramki zewnętrzne paneli dostępne są w różnych kolorach.

Dystrybutor w Polsce:

alarmnet®

Alarmnet Sp.j.
ul. Karola Miarki 20c
01-496 Warszawa
tel. (22) 663 40 85, fax (22) 833 87 95

e-mail: biuro@alarmnet.com.pl
www.alarmnet.com.pl
www.comelit.com.pl

System wideodomofonowy serii 480

GDE POLSKA wprowadza do sprzedaży nowy system wideodomofonowy przeznaczony do instalacji w biurowcach, budynkach mieszkalnych i osiedlach zamkniętych. System może obsłużyć do 480 abonentów.

System charakteryzuje się bardzo prostą instalacją i programowaniem.

W skład systemu wchodzą:
- kamery DRC-480L
- monitory APV-480L
- unifony AP-480AL
- centrale portierskie CDS-480L

System umożliwia tworzenie zaawansowanych struktur łącząc maksymalnie 99 kamer DRC-480L i 480 monitorów APV-480L. Zamiast monitora (lub równolegle z monitorem) może pracować unifon AP-480AL. Jeśli u jednego lokatora jest zainstalowanych kilka odbiorników (monitorów, unifonów) możliwe jest takie skonfigurowanie systemu aby z kamery wywołać jednocześnie wszystkie odbiorniki lub każdy osobno (kilka kodów użytkowników).

Wywołanie monitorów/unifonów jest możliwe z klawiatury numerycznej na panelu z kamerą. Klawiatura ta umożliwia także otwieranie drzwi wejściowych (system indywidualnych kodów). Opcjonalnie istnieje możliwość otwierania drzwi kartą (czytnik kart zamontowany w kamerze).

Po zainstalowaniu centrali portierskiej mamy możliwość kontroli dostępu osób wchodzących/wychodzących poprzez portiera. Osoba odwiedzająca może nawiązać komunikację bezpośrednio z danym lokatorem wybierając kod abonenta lub (jeśli np. nie znamy kodu abonenta) poprzez portiera, który nawiąże połączenie z danym lokatorem.

W systemie tym jest także możliwość nawiązania rozmowy pomiędzy lokatorami (funkcja interkomu). W tym celu lokator dzwoni do portiera, który nawiązuje połączenie z kolejnym lokatorem.

◄ Przykładowy schemat podłączenia

DRC-480L ►

GDE POLSKA
Global Distributor of Electronics

GDE Polska
ul. Koniecznego 46
32-040 Świątniki Górne

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

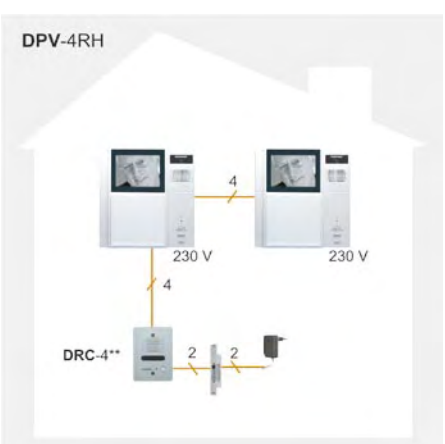
DPV-4RH / DRC-4BG
Monitor głośnomówiący czarno-biały z kamerą

DPV-4RH uzupełnia ofertę firmy GDE POLSKA o monitor głośnomówiący do zastosowań w systemach wideodomofonowych. Monitor współpracuje z kamerami 4-przewodowymi typu DRC-4*** firmy COMMAX (np. DRC-4BG).

Charakterystyka monitora:
- monitor czarno-biały
- wbudowane głośniki
- kineskop 4", 480 linii
- obsługa jednego wejścia
- możliwość podłączenia dodatkowego monitora
- instalacja czteroprzewodowa + obwód elektrozamka
- współpracuje z kamerami analogowymi czteroprzewodowymi
- zasilanie 230V

Okablowanie	4 przewody spolaryzowane
Zasilanie	100-240V AC; 50/60 Hz
Pobór mocy	Czuwanie: 2,5W Praca: 15W
Temperatura pracy	0°C do 40°C
Wymiary (szer. x wys. x gł.)	211mm x 226mm x 52mm
Masa	1,7 kg

Charakterystyka kamery:
- kamera czarno-biała
- obudowa żeliwna, montaż podtynkowy
- ukryty obiektyw typu PIN-HOLE
- doświetlenie podczerwienią
- instalacja czteroprzewodowa + obwód elektrozamka
- współpracuje z monitorami czteroprzewodowymi
- głębokość tylko 18 mm



Przykładowy schemat podłączenia

GDE POLSKA
Global Distributor of Electronics

GDE Polska
ul. Koniecznego 46
32-040 Świątniki Górne

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

Rejestrator hybrydowy z technologią IP – SymSafe

Rejestrator cyfrowy SymSafe wykorzystuje „hybrydową" technologię nagrywania, umożliwiającą pracę zarówno z konwencjonalnymi kamerami analogowymi, jak i z urządzeniami z nowej rodziny cyfrowych produktów sieciowych firmy GE. Ta unikalna platforma pozwala na płynne przejście do nagrywania w technologii cyfrowej – technologii przyszłości w dziedzinie zapisu wideo – przy jednoczesnym wykorzystaniu istniejącego sprzętu analogowego. Rejestrator SymSafe umożliwia rejestrowanie obrazów w rozdzielczości 720*576, w czasie rzeczywistym dla każdego z zapisywanych kanałów. Urządzenie wykorzystuje technologię kompresji MPEG-4, pozwalającą na nagrywanie obrazu z prędkością 25 klatek na sekundę z każdego kanału – w rozdzielczości CIF. Dzięki temu możliwe jest uzyskanie niewielkich plików z zachowaniem doskonałej jakości obrazu. Urządzenie SymSafe łączy w sobie funkcję Triplex pozwalającą na jednoczesny podgląd, odtwarzanie oraz rejestrowanie obrazu wideo. SymSafe zapisuje 16 kanałów analogowych oraz 2 kanały cyfrowe w rozdzielczości D1 (720 x 576). Urządzenie SymSafe umożliwia wyszukiwanie wg następujących kryteriów: czasu, daty oraz wystąpienia ruchu lub alarmu. Umożliwia obsługę alarmów, zapisanych w rejestrze zdarzeń oraz przesyłanie wiadomości o wystąpieniu alarmu na skrzynkę e-mail. Urządzenie to umożliwia wygodną pracę w sieci oraz zdalny podgląd zarejestrowanych obrazów za pomocą sieci Ethernet (10/100/1000 BaseT). Rejestratory z tej rodziny wykorzystują funkcję dynamicznego nadawania adresów IP (DHCP) oraz obsługują funkcję dynamicznego nadawania nazw domen (DDNS). Oprogramowanie firmy GE Security umożliwia przeglądanie bieżących i zarejestrowanych obrazów z wielu rejestratorów SymSafe 16 jednocześnie. Rejestrator jest dostępny w kilku wariantach o różnej pojemności dysku twardego, od 160 GB do 1 TB. Dyski te są lepiej chłodzone dzięki zastosowaniu wyjątkowej technologii Cooling Tunnel, dzięki czemu wzrasta ich niezawodność. Wymiary rejestratora SymSafe pozwalają na łatwą instalację w standardowej 19-calowej szafie typu rack.

Specyfikacja

Wideo	
Wejścia	16 wejść typu BNC, NTSC/EIA lub PAL/CCIR, autoterminacja
Zakres	AGC – od 0,7 do 1,4 V pp
Rozdzielczość pozioma	720 pikseli
Rozdzielczość pionowa	576 linii
Standard kompresji wideo	MPEG-4
Wyjście monitora A typu composite	podział ekranu, złącze BNC, kompatybilność z NTSC/EIA lub PAL/CCIR
VGA	wyświetla ten sam obraz co monitor A
Wyjście monitora B typu composite	podział ekranu, złącze BNC, kompatybilność z NTSC/EIA lub PAL/CCIR
Nagrywanie	
Prędkość	nagrywanie w czasie rzeczywistym z wszystkich kanałów w rozdzielczości CIF
Rozdzielczość	do pełnej rozdzielczości D1
Ustawienia jakości obrazu	6 stopni
Szerokość pasma	do 1 Mbit/sek dla każdego kanału, skalowalna
Sieć	
Typ	port 10/100/1000 Ethernet RJ-45
Protokół	TCP/IP, UDP, DHCP
Archiwizowanie	
Zewnętrzne	dysk USB ThumbDrive
Wewnętrzne	nagrywarka DVD
Łącza	
Port szeregowy RS-232	1 DB-9
RS-485/422	2
USB	2 (1 z przodu i 1 z tyłu)
Obsługa alarmów	
Wejście alarmowe	16 programowalnych wejść alarmowych NO/NC
Wyjście alarmowe	wyjścia przekaźnikowe (2)
Detekcja ruchu	
Stref na kamerę	256, siatka 16 x 16
Rejestrowanie obrazu	
Twarde dyski	2 dyski twarde S-ATA, z technologią Cooling Tunnel zwiększającą ich żywotność
Obsługa	
Liczba języków	7
Sterowanie	mysz USB, pokrętło typu Jog/Shuttle, pilot na podczerwień
	Przyciski
Wskazywanie alarmu	
	wskaźnik alarmu
Potwierdzenie alarmu	Tak
Pozostałe informacje	
Napięcie zasilania	od 120 do 240 VAC, autodopasowanie
Temperatura pracy	od 0 do 40°C
Wymiary (wys./szer./gł.)	89 x 395 x 420 mm
Waga	11 kg
Standardy i normy	
	FCC, CE, UL
Wilgotność względna	od 10 do 95%, bez kondensacji

GE Security

GE Security
ul. Sadowa 8
80-771 Gdańsk

tel. (58) 301 38 31
fax (58) 301 14 36
www.gesecurity.pl

Rejestrator hybrydowy z technologią IP – SymSafe Pro

Rejestrator cyfrowy SymSafe Pro wykorzystuje „hybrydową" technologię nagrywania, umożliwiającą pracę zarówno z konwencjonalnymi kamerami analogowymi, jak i z urządzeniami z nowej rodziny cyfrowych produktów sieciowych firmy GE. Ta unikalna platforma pozwala na płynne przejście do nagrywania w technologii cyfrowej – technologii przyszłości w dziedzinie zapisu wideo – przy jednoczesnym wykorzystaniu istniejącego sprzętu analogowego. Rejestrator SymSafe Pro umożliwia rejestrowanie obrazów w rozdzielczości 720*576 w czasie rzeczywistym oraz sygnałów audio towarzyszących zapisywanym obrazom. Urządzenie wykorzystuje technologię kompresji MPEG-4, pozwalającą na nagrywanie obrazu z prędkością 25 klatek na sekundę z każdego kanału w rozdzielczości CIF. Dzięki temu możliwe jest uzyskanie niewielkich plików z zachowaniem doskonałej jakości obrazu. Urządzenie SymSafe Pro łączy w sobie funkcję Triplex pozwalającą na jednoczesny podgląd, odtwarzanie oraz rejestrowanie obrazu wideo. SymSafe Pro zapisuje 16 kanałów analogowych oraz 2 kanały cyfrowe w rozdzielczości D1 (720 x 576). Urządzenie SymSafe Pro umożliwia wyszukiwanie wg następujących kryteriów: czasu, daty oraz wystąpienia ruchu lub alarmu. Umożliwia obsługę alarmów, zapisanych w rejestrze zdarzeń oraz przesyłanie wiadomości o wystąpieniu alarmu na skrzynkę e-mail. Urządzenie to umożliwia wygodną pracę w sieci oraz zdalny podgląd zarejestrowanych obrazów za pomocą sieci Ethernet (10/100/1000 BaseT). Rejestratory z tej rodziny wykorzystują funkcję dynamicznego nadawania adresów IP (DHCP) oraz obsługują funkcję dynamicznego nadawania nazw domen (DDNS). Oprogramowanie firmy GE Security umożliwia przeglądanie bieżących i zarejestrowanych obrazów z wielu rejestratorów SymSafe Pro jednocześnie. Rejestrator jest dostępny w kilku wariantach o różnej pojemności dysku twardego, od 160 GB do 1 TB. Dyski te są lepiej chłodzone dzięki zastosowaniu wyjątkowej technologii Cooling Tunnel, dzięki czemu wzrasta ich niezawodność. Wymiary rejestratora SymSafe Pro pozwalają na łatwą instalację w standardowej 19-calowej szafie typu rack.

Specyfikacja

Wideo	
Wejścia	4, 8 lub 16 wejść typu BNC, NTSC/EIA lub PAL/CCIR, autoterminacja
Zakres	AGC – od 0,7 do 1,4 V pp
Rozdzielczość pozioma	720 pikseli
Rozdzielczość pionowa	576 linii
Standard kompresji wideo	MPEG-4
Wyjście monitora A typu composite	podział ekranu, złącze BNC, kompatybilność z NTSC/EIA lub PAL/CCIR
VGA	wyświetla ten sam obraz co monitor A
Wyjście monitora B typu composite	podział ekranu, złącze BNC, kompatybilność z NTSC/EIA lub PAL/CCIR
Audio	
Wejście audio	315 mV, 400 kiloomów, RCA (2)
Wyjście audio	315 mV, 600 omów, RCA (1)
Standard kompresji audio	MPEG-1
Nagrywanie	
Prędkość	nagrywanie w czasie rzeczywistym z wszystkich kanałów w rozdzielczości CIF
Rozdzielczość	do pełnej rozdzielczości D1
Ustawienia jakości obrazu	6 stopni
Szerokość pasma	do 2 Mbit/sek dla każdego kanału, skalowalna
Sieć	
Typ	port 10/100/1000 Ethernet RJ-45
Protokół	TCP/IP, UDP, DHCP
Archiwizowanie	
Zewnętrzne	dysk USB ThumbDrive
Wewnętrzne	nagrywarka DVD
Łącza	
Port szeregowy RS-232	1 DB-9
RS-485/422	2
USB	2 (1 z przodu i 1 z tyłu)
Obsługa alarmów	
Wejście alarmowe	4, 8 lub 16 programowalnych wejść alarmowych NO/NC
Wyjście alarmowe	wyjścia przekaźnikowe (2)
Detekcja ruchu	
Stref na kamerę	256, siatka 16 x 16
Rejestrowanie obrazu	
Twarde dyski	2 dyski twarde S-ATA, z technologią Cooling Tunnel zwiększającą ich żywotność
Obsługa	
Liczba języków	7
Sterowanie	mysz USB, pokrętło typu Jog/Shuttle, pilot na podczerwień
	Przyciski
Wskazywanie alarmu	
	wskaźnik alarmu
Potwierdzenie alarmu	Tak
Pozostałe informacje	
Napięcie zasilania	od 120 do 240 VAC, autodopasowanie
Temperatura pracy	od 0 do 40°C
Wymiary (wys./szer./gł.)	89 x 395 x 420 mm
Masa	11 kg
Standardy i normy	
	FCC, CE, UL
Wilgotność względna	od 10 do 95%, bez kondensacji

GE Security

GE Security
ul. Sadowa 8
80-771 Gdańsk

tel. (58) 301 38 31
fax (58) 301 14 36
www.gesecurity.pl

ALARMTECH POLSKA Sp. z o.o.

Detektor sejsmiczny VD 400 firmy ALARMTECH

Dane techniczne	
Napięcie zasilania	9-15 V DC
Tętnienia max	2 Vpp
Pobór prądu w stanie czuwania	10 mA
Pobór prądu w stanie alarmu	11 mA
Rodzaj wyjścia alarmowego	przekaźnik
-rezystancja szeregowa pętli zabezpieczającej	20-30 Ohm
-obciążalność	500 mA/35 V
-czas podtrzymania alarmu w trybie AUTO	2 sek
-sygnalizacja alarmu w trybie MONITOR	dioda LED
-kasowanie alarmu	wyłączenie zasilania lub zdalny reset na wejściu D/N
Styk zabezpieczający	NC
-obciążalność	max 35 V/50 mA
-temperatura pracy	-10 do +70°C
-temperatura przechowywania	-40 do +70°C
-wilgotność, DIN 40040	max. 95% RH, klasa F
-kategoria ochronna obudowy IEC 529	IP 31

Montowany na stalowym i betonowym podłożu zapewnia skuteczną ochronę sejfów, kas pancernych, szaf na akta lub broń, ścian budynków, itp. Sygnalizowane są wszelkie próby sforsowania obiektu za pomocą ładunków wybuchowych oraz narzędzi takich jak wiertarki, obcinarki tarczowe, szlifierki oraz niektóre narzędzia termiczne. Trzy niezależne kanały detekcji, monitorowane przez dodatkowy kanał kontroli wewnętrznej pracy systemu gwarantują skuteczność działania.

1. **Kanał integracji** - wykrywa sygnały o małej amplitudzie, wysokiej częstotliwości oraz długim czasie trwania. Czułość regulowana za pomocą potencjometru.
2. **Kanał zliczania** - można go ustawić na zliczanie 4 kolejnych zdarzeń lub odłączyć, gdy nie jest potrzebny.
3. **Kanał wykrywający eksplozję** - wykrywa sygnały o bardzo dużej amplitudzie i krótkim czasie trwania. Sygnał z tego kanału jest priorytetowy w stosunku do pozostałych.
4. **Kanał kontroli wewnętrznej** - do kontroli pracy systemu i wykrywania wszelkich prób sabotażu.

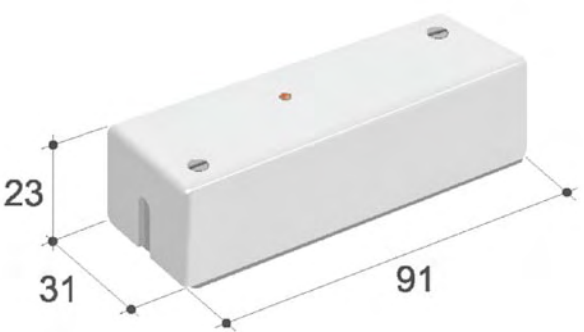
Montaż detektora na betonowych i ceglanych ścianach powinien być przeprowadzany przy użyciu płyty montażowej **MP 400**.

Promień detekcji, w zależności od rodzaju powierzchni chronionego obiektu wynosi do 5 m.

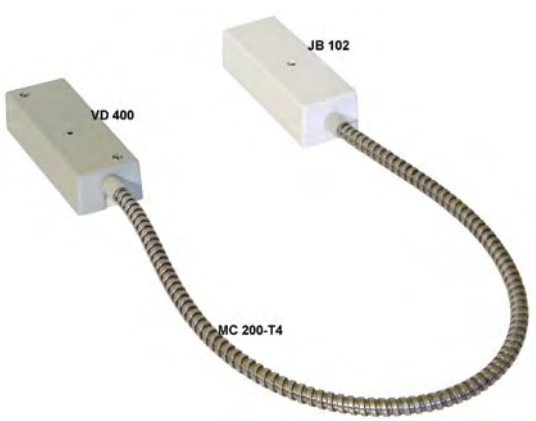
Przy montażu na wolnym powietrzu w niedogodnych warunkach atmosferycznych lub w chłodnych pomieszczeniach, należy skorzystać z obudowy **WH 400**. Obudowa wyposażona jest w element grzewczy utrzymujący odpowiednią temperaturę otoczenia detektora, wilgotność poniżej wartości krytycznej.

Detektor sejsmiczny VD 400 jest wyposażony w sygnalizator alarmu w postaci diody LED, zabezpieczenie przed zdjęciem pokrywy oraz posiada wewnętrzny rejestrator zdarzeń - „**czarną skrzynkę**".

Posiada atest Techom w klasie S.....39/06



VD 400 oferowany jest także w zestawach VD 400-Z1 oraz VD 400-Z2, z puszką przyłączeniową JB 102.

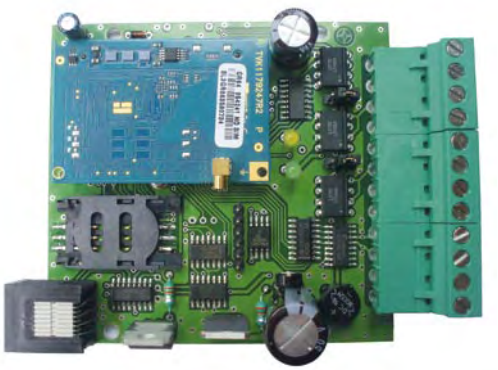


Standardowy zestaw **VD 400-Z1** – do ochrony kas, sejfów, szaf na broń, ścian budynków i innych, zawiera:
- detektor sejsmiczny VD 400
- stalową osłonę przewodów MC 200-T4
- puszkę przyłączeniową JB 102

80-299 Gdańsk – Osowa, ul. Kielnieńska 115
tel. (58) 340 24 40, fax (58) 340 24 49
http://www.alarmtech.pl, e-mail: info@alarmtech.pl

Moduły GSM/GPRS

Urządzenia TX404, TX800,TX1000 przeznaczone są do monitoringu, komunikacji i powiadamiania o stanach alarmowych chronionych obiektów wykorzystując sieć telefonii komórkowej dowolnego operatora GSM. Monitoring stanów alarmowych możliwy jest za pomocą zwykłej wiadomości tekstowej SMS lub z wykorzystaniem funkcji Clip do stacji monitoringu.



Urządzenia służą również do zdalnego sterowania innymi urządzeniami wykonawczymi w dowolnych systemach. Każdy z modeli serii TX jest zintegrowany z modułem komunikacyjnym GSM/GPRS i wymaga tylko włożenia aktywnej karty SIM. Poprzez dołączone w zestawie oprogramowanie konfiguracyjne należy urządzenie odpowiednio zaprogramować.
Urządzenia przeznaczone są do zastosowań profesjonalnych w systemach zabezpieczeń i automatyce przemysłowej.

Model urządzenia	TX406	TX800	TX1000
Wejścia binarne			
Ilość wejść	6	8	8
Optoizolacja wejść	Tak	Tak	Tak
Typ wejść	NO-NC / napięciowe	NO-NC / napięciowe	NO-NC / napięciowe
Możliwość blokowania wejść	Tak	Tak	Tak
Wyjścia			
Ilość wyjść	2	8	8
Czasowe przełączanie wyjść	Tak	Tak	Tak
Wiadomości SMS			
Ilość numerów telefonów	8	8	8
Dynamiczne formatowanie treści SMS	Tak	Tak	Tak
Programator czasowy			
Ilość programowalnych zdarzeń	4	8	8
Rodzaj zdarzeń czasowych	Odstępy czasowe Dokładna godzina	Odstępy czasowe Dokładna godzina	Odstępy czasowe Dokładna godzina
Polecenia SMS			
Polecenia standardowe [1]	Tak	Tak	Tak
Max. ilość poleceń użytkownika [2]	8	8	8
Wyjścia analogowe			
Ilość wejść	0	0	2 lub 4
Rozdzielczość wejść	-	-	10 lub 16 bit
Zakres pomiaru napięcia	-	-	0 do 10 V
Transmisja danych na serwer FTP	-	-	Tak

[1] Polecenia standardowe - wbudowane polecenia do zdalnej zmiany stanu wyjść, zapytania o stan urządzenia
[2] Polecenia użytkownika - polecenia o dowolnie konfigurowalnej treści i rodzaju czynności do wykonania przez urządzenie

inter-Kompas

inter-Kompas s.c.
33-300 Nowy Sącz
ul. Grottgera 3

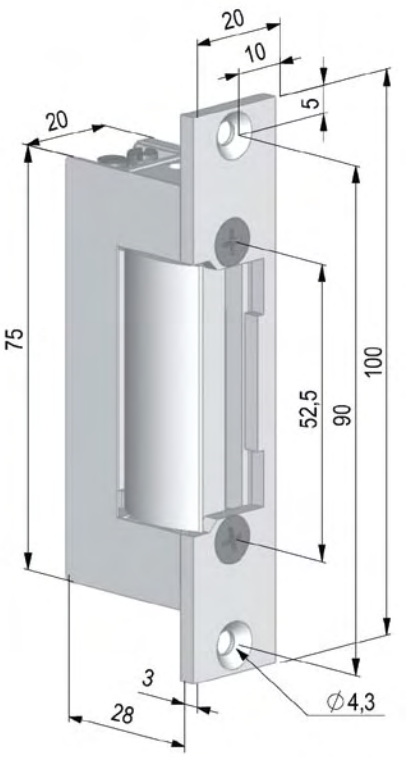
tel. (18) 547 40 11, fax (18) 547 40 09
www.interkompas.com.pl
interkompas@interkompas.com.pl

Elektrozaczepy symetryczne BeFo DUAL

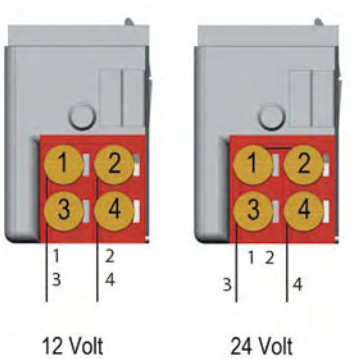
BeFo DUAL to nowa seria elektrozaczepów wygodnych w instalacji. Dzięki zastosowaniu dwóch niezależnych cewek, mamy możliwości podłączenia jednego rygla na dwa sposoby.
Cewki elektromagnesu można połączyć w taki sposób, aby możliwe było zasilanie w dwóch zakresach wartości napięcia 6-12V lub 12-24V. Elektrozaczepy charakteryzuje niski pobór prądu.
Dzięki możliwości wyboru wartości napięcia zasilającego (6-12V lub 12-24V) można łatwo dostosować elektrozaczep do istniejącego zasilacza.
Elektrozaczepy posiadają regulowaną zapadkę w granicach 3mm oraz wyposażone są standardowo w okucie 100x20x3 mm lub 250x25x3 mm.
Dostępne są w różnych opcjach:

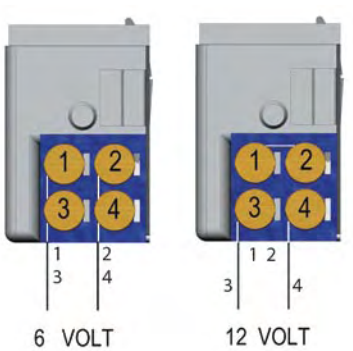
- pamięć otwarcia,
- sygnalizacja NO/NC,
- mechaniczna blokada

oraz wszystkie możliwe kombinacje powyższych rozwiązań.



DRZWI	LEWE / PRAWE
DRZWI MATERIAŁ	DREWNO, PLASTIK, STAL, ALUMINIUM
NACISK NA DRZWI PRZED OTWARCIEM	DO 4 KG
USZKODZENIE TRWAŁE	PRZY OBCIĄŻENIU 1500N
MATERIAŁ OBUDOWA	ALUMINIUM (ODLEW) + CYNK
MATERIAŁ ZAPADKA	MOSIĄDZ (ODLEW)
SZYLD	STAL 20X3
POKRYCIE SZYLDU	CYNK + CHROM
TOLERANCJA NAPIĘCIA	± 1V
KONSTRUKCJA	SYMETRYCZNY 75 X 28 X 20
TEMP. PRACY	-15°C ~ +50°C





NAPIĘCIE	WYKONANIE 12 - 24	
	ZMIENNE ~ V	STAŁE = V
12 V	160 mA	195 mA
24 V	75 mA	95 mA

NAPIĘCIE	WYKONANIE 6 - 12	
	ZMIENNE ~ V	STAŁE = V
6 V	325 mA	405 mA
12 V	165 mA	205 mA

Micronix Sp. z o.o.
ul. Spółdzielcza 10
58-500 Jelenia Góra

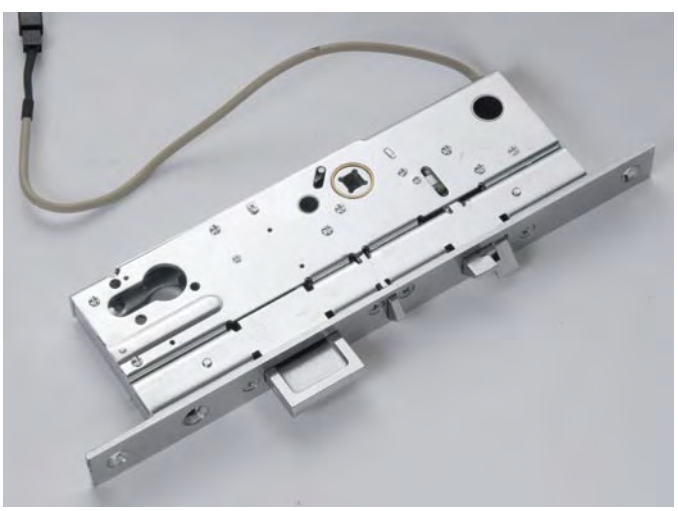
tel. (75) 755 78 78, 642 45 35, fax (75) 642 45 25
e-mail: info@micronix.pl
www.micronix.pl

Elektromechaniczny zamek BERA

Opis działania:
Z zewnętrznej strony drzwi zamek można otworzyć kluczem (standardowa wkładka) lub klamką wyzwalaną elektrycznym impulsem. Impuls podawany jest na elektromagnetyczną cewkę, która zwalnia odpowiedni mechanizm blokujący w zamku, dzięki temu można otworzyć drzwi zewnętrzną klamką w standardowy sposób. Impuls ten można podać na kilka sposobów z różnych urządzeń wchodzących w skład systemu kontroli dostępu: domofonu,wideodomofonu, kodowanej klawiatury z czytnika kart magnetycznych itp. Bez wyzwolenia zamka impulsem zewnętrzna klamka pracuje jałowo tzn. można nacisnąć ją jak każdą standardową klamkę ale nie spowoduje to otwarcia zamka. Klamka po stronie wewnętrznej drzwi działa standardowo i za każdym razem umożliwia otwarcie drzwi. Każde zamknięcie otwartych drzwi powoduje automatyczne dwupunktowe ryglowanie drzwi. Zamek spełnia normy: EN 12209:2004, ENV 1627 - odporność na włamanie, trzeci stopień bezpieczeństwa.

Funkcje:
- Podwójne ryglowanie przy każdorazowym zamknięciu drzwi;
- Swobodne każdorazowe otwarcie drzwi od wewnątrz. Funkcja PANIC (drzwi ewakuacyjne);
- Możliwość kontroli wejścia z dowolnego urządzenia kontroli dostępu oraz wyjścia (np. za pomocą centrali p.poż), zamki V, W;
- Możliwość otwarcia drzwi po zamontowaniu standardowej wkładki euro;

Napięcie	12V/DC
Prąd	220 mA
Prąd Max	900 mA
Max. Czas obciążenia cewki	120 min.
Sygnalizacja LED	Czerwona / Zielona
długość kabla zasilającego	30 cm
Liczba otwarcia/zamknięcia	1,5 mil
liczba dziennych przejść	Nieograniczona
Wkładka cylindryczna	Standardowa (norma euro)
czworokąt klamki	8 x 8
Orientacja zamka	Lewy lub prawy
Gwarancja	24 mc.
Okucia	Chrom / Tytan, (lśniący / mat)

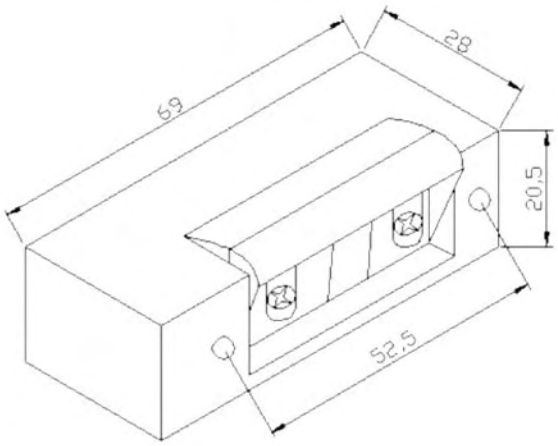


Wykonanie (typ zamków):
E – standardowy uzbrajanie klamki,
D + sygnalizacja optyczna i akustyczna,
M + sygnalizacja optyczna i akustyczna - kontrola funkcji *,
V - sterowanie obu klamek,
W - sterowanie obu klamek + sygnalizacja optyczna i akustyczna + kontrola funkcji,
R - rewersyjny – zamknięty po podaniu napięcia. Wszystkie stopnie funkcjonalności E, D, M, V i W, bez akustycznej sygnalizacji,

* kontrola naciśnięcia klamki, położenia zamka (wysunięty/schowany), pętla sabotażowa / dezaktywacja systemu

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

Elektrozaczepy IST – FT Drzwi przeciwpożarowe



- Regulowana zapadka, 5 pozycji - 4 mm, sygnalizacja otwarcia/zamknięcia w opcji;
- Wytrzymałość 10.000 N oraz wysoka odporność na temperaturę;
- Zasilanie 6-24 V AC DC ± 15% lub 12-48 V AC DC ± 15%;
- Ochrona przepięciowa;
- Certyfikat MPA;
- Zastosowanie w drzwiach przeciw pożarowych dla wydzielonych stref pożarowych, przegrody przeciwpożarowe ograniczające rozprzestrzenianie się ognia;
- Wytrzymałość rygla umożliwia jego zastosowanie w drzwiach antywłamaniowych.

Strojírenský zkušební ústav, s. p., autorizovaná osoba 202
Hudcova 56b, Brno, Česká republika
Rozhodnutí o autorizaci č. 27/2006 ze dne 29. 08. 2006

CERTIFIKÁT VÝROBKU

č. AO 202/C5/2007/reg. č: J-30-20123-07

V souladu s ustanovením § 5 odst. 2 nařízení vlády č. 163/2002 Sb., kterým se stanoví technické požadavky na vybrané stavební výrobky, ve znění nařízení vlády č. 312/2005 Sb., autorizovaná osoba potvrzuje, že u stavebního výrobku

výrobek: elektrický otvírač dveří určený pro únikové protipožární a protikouřové uzávěry, modelová řada FT
typové označení: FT 201 A
varianty: FT 200 A; FT 200 B; FT 201 B; FT 500 A; FT 501 A; FT 500 B; FT 501 B

dovozce: BERA s.r.o.
Šestajovická 488
198 00 Praha 9
identifikační číslo: 44797800

výrobce: IST Systems GmbH
Kohlmeiserweg 5, D-72458 Albstadt, Německo

přezkoumala podklady předložené dovozcem, provedla počáteční zkoušku typu výrobku na vzorku a posoudila způsob kontroly výrobků dovozcem a zjistila, že uvedený výrobek splňuje základní požadavky nařízení vlády č. 163/2002 Sb., ve znění nařízení vlády č. 312/2005 Sb.

Při posuzování shody použila autorizovaná osoba ČSN 16 6014:1992.

Autorizovaná osoba zjistila, že způsob kontroly výrobků dovozcem odpovídá příslušné technické dokumentaci podle § 5 odst. 1 písm. d) a zabezpečuje, aby výrobky uváděné na trh splňovaly požadavky stanovené shora uvedenou určenou normou a odpovídaly technické dokumentaci podle § 4 odst. 3.

Nedílnou součástí tohoto certifikátu je závěrečný protokol č. 30-7010 ze dne 22. března 2007, který obsahuje závěry zjišťování, ověřování, výsledky zkoušek, základní popis a zobrazení, nezbytné pro identifikaci certifikovaného výrobku.

Tento certifikát zůstává v platnosti po dobu, po kterou se požadavky stanovené určenou normou, na kterou byl uveden odkaz, nebo způsob kontroly výrobků dovozcem výrazně nezmění.

Autorizovaná osoba provádí nejméně jedenkrát za 12 měsíců dohled nad řádným fungováním kontroly výrobků u dovozce, odebírá vzorky výrobků, provádí jejich zkoušky a posuzuje, zda vlastnosti výrobku odpovídají určené normě podle ustanovení § 5 odst. 5 výše uvedeného nařízení vlády.

V Brně dne 22. března 2007

Ing. Jiří Rozsíval
zástupce ředitele

J-30-20123-07.doc Strana 1 (1)

NAPIĘCIE	WYKONANIE 12 - 48		NAPIĘCIE	WYKONANIE 6 - 24	
	Prąd	Czas		Prąd	Czas
12 V	0,30 A	∞	6 V	0,6 A	∞
18 V	0,45 A	3 min.	9 V	0,9 A	3 min.
24 V	0,60 A	1 min.	12 V	1,1 A	1 min.
24 V	0,15 A	∞	12 V	0,30 A	∞
36 V	0,22 A	3 min.	18 V	0,45 A	3 min.
48 V	0,30 A	1 min.	24 V	0,60 A	1 min.

Micronix Sp. z o.o.
ul. Spółdzielcza 10
58-500 Jelenia Góra

tel. (75) 755 78 78, 642 45 35, fax (75) 642 45 25
e-mail: info@micronix.pl
www.micronix.pl

2M ELEKTRONIK
ul. Majora 12a
31-422 Kraków
tel. (12) 412 35 94
faks (12) 411 27 74
e-mail: 2m@2m.pl
www.2m.pl

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

---

4 COM Sp. z o.o.
ul. Adama 1
40-467 Katowice
tel. (32) 609 20 30
faks (32) 609 20 30 wew. 103
e-mail: biuro@4.com.pl
www.4.com.pl

AAT Trading Company Sp. z o.o.
ul. Puławska 431
02-801 Warszawa
tel. (22) 546 05 46
faks (22) 546 05 01
e-mail: aat_wawa@aat.pl
www.aat.pl

Oddziały:
ul. Racławicka 82, 60-302 **Poznań**
tel. (61) 662 06 60
faks (61) 662 06 61

ul. Mieszczańska 18, 30-313 **Kraków**
tel. (12) 266 87 95
tel./faks (12) 266 87 97

Al. Niepodległości 659, 81-855 **Sopot**
tel. (58) 551 22 63
tel./faks (58) 551 67 52

ul. Zielona 42, 71-013 **Szczecin**
tel. (91) 483 38 59, 489 47 23
faks (91) 489 47 24

ul. Na Niskich Łąkach 26, 50-422 **Wrocław**
tel./faks (71) 348 20 61
tel./faks (71) 348 42 36

ul. Ks. W. Siwka 17, 40-318 **Katowice**
tel. (32) 351 48 30
tel. (32) 256 69 34
tel./faks (32) 256 60 34

ul. Dowborczyków 25, 90-019 **Łódź**
tel./faks (42) 674 25 45
tel./faks (42) 674 25 48

ul. Łęczycka 37, 85-737 **Bydgoszcz**
tel./faks (52) 342 91 24, 342 98 82

ACIE Polska Sp. z o.o.
ul. Poleczki 21
02-822 Warszawa
tel./faks (22) 894 61 63
e-mail: info@acie.pl
www.acie.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 POLAND Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. (22) 430 8 414
faks (22) 430 8 302
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. H. Krahelskiej 7
40-285 Katowice
tel. (32) 790 76 56
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. Portowa 14, 44-100 **Gliwice**
tel. (32) 790 76 23
faks (32) 790 76 65
e-mail: gliwice@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. Pachońskiego 2a, 31-223 **Kraków**
tel. (32) 790 76 46
faks (32) 790 76 73
e-mail: krakow@e-alpol.com.pl

ul. Os. Na Murawie 10/2, 61-655 **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: anb@anb.com.pl
www.anb.com.pl

Zakład Produkcyjno-Usługowo-Handlowy
ANMA s.c. Tomaszewscy
ul. Ostrowskiego 9
53-238 Wrocław
tel. (71) 363 38 93
faks (71) 363 17 53
e-mail: anma@anma-pl.eu
www.anma-pl.eu

ATLine Spółka Jawna
Krzysztof Cichulski, Sławomir Pruski
ul. Franciszkańska 125
91-845 Łódź
tel. (42) 657 30 80
faks (42) 655 20 99
e-mail: info@atline.com.pl
www.atline.com.pl

AVISmedia
ul. żeromskiego 10
64-200 Wolsztyn
tel. (68) 347 09 25
faks (68) 347 09 26
e-mail: office@merlaud.com.pl
www.merlaud.com.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

ROBERT BOSCH Sp. z o.o.
Security Systems
ul. Poleczki 3
02-822 Warszawa
tel. (22) 715 41 01
faks (22) 715 41 05/06
e-mail: securitysystems@pl.bosch.com
www.boschsecurity.com.pl

P.W.H. BRABORK Laboratorium Sp. z o.o.
ul. Postępu 2
02-676 Warszawa
tel. (22) 257 68 12
faks (22) 257 68 95
e-mail: brabork@braborklab.pl
www.braborklab.pl

---

bt electronics Sp. z o.o.
ul. Dukatów 10 b
31-431 Kraków
tel. (12) 410 85 10
faks (12) 410 85 11
e-mail: saik@saik.pl
www.saik.pl

MARKA GRUPY LEGRAND
LEGRAND POLSKA Sp. z o.o.
Al. Wyścigowa 8
02-681 Warszawa
Infolinia 0 801 133 084
faks (22) 843 94 51
e-mail: info@legrand.com.pl
www.legrand.pl

C&C PARTNERS TELECOM Sp. z o.o.
wyłączny autoryzowany dystrybutor
samsung techwin w Polsce
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

CAMSAT
ul. Prosta 32
86-050 Solec Kujawski
tel. (52) 387 36 58
faks (52) 387 54 66
e-mail: camsat@camsat.com.pl
www.camsat.com.pl

CBC (Poland) Sp. z o.o.
ul. Morcinka 5 paw. 6
01-496 Warszawa
tel. (22) 638 44 40
faks (22) 638 45 41
e-mail: info@cbcpoland.pl
www.cbcpoland.pl

CCX
ul. Ligocka 103
Budynek 9.2
40-568 Katowice
tel. (32) 609 90 80
faks (32) 609 90 81
e-mail: biuro@ccx.pl
www.ccx.pl

CENTRUM MONITOROWANIA
ALARMÓW Sp. z o.o.
ul. Puławska 359
02-801 Warszawa
tel. (22) 546 08 88
faks (22) 546 06 19
e-mail: mail@cma.com.pl
www.cma.com.pl

Oddział:
ul. Świętochłowicka 3, 41-909 **Bytom**
tel. (32) 388 09 50
faks (32) 388 09 60

CEZIM Jolanta Podrażka
ul. Partyzantów 1
96-500 Sochaczew
tel./faks (46) 863 56 50
e-mail: cezim@cezim.pl
sklep@cezim.pl
www.cezim.pl

COM-LM
ul. Ściegiennego 90
25-116 Kielce
tel. (41) 368 71 90
faks (41) 368 71 12
e-mail: biuro@com-lm.pl
www.com-lm.pl

CONTROL SYSTEM FMN Sp. z o.o.
Al. Komisji Edukacji Narodowej 96 Lok. U15
02-777 Warszawa
tel. (22) 855 00 17÷19
faks (22) 546 19 78
e-mail: cs@cs.pl
www.cs.pl, www.ckp.com.pl

D+H Polska Sp. z o.o.
ul. Polanowicka 54
51-180 Wrocław
tel. (71) 323 52 50
faks (71) 323 52 40
Dział SAP: tel. (71) 323 52 47
e-mail: biuro@dhpolska.pl
www.dhpolska.pl

Oddziały:
ul. Hagera 41, 41-800 **Zabrze**
tel. (32) 375 05 70
faks (32) 375 05 71

ul. Kielnieńska 134A, 80-299 **Gdańsk**
tel. (58) 554 47 46
faks (58) 552 45 24
ul. Płochocińska 19 lok. 43
03-191 **Warszawa**
tel. (22) 614 39 52
faks (22) 614 39 64

ul. Narutowicza 59, 90-130 **Łódź**
tel. (42) 678 01 32
faks (42) 678 09 20

DANTOM s.c.
ELEKTRONICZNE SYSTEMY ALARMOWE

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

DAR–ALARM
ul. Nieszawska 3C
03-382 Warszawa
tel. (22) 498 60 62
tel./faks (22) 814 10 30

ul. Polnej Róży 2/4
02-798 **Warszawa**
tel./faks (22) 649 27 97
e-mail: handlowy@darsystem.pl
www.darsystem.pl
www.tvtech.com.pl

DELTA BUSINESS SERVICE
ul. Ciepła 15/50
50-524 Wrocław
tel. (71) 367 06 16, 364 78 64
faks (71) 367 06 16
e-mail: biuro@delta-dbs.pl
www.delta-dbs.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
faks (12) 278 48 91
e-mail: biuro@dpksystem.pl
www.dpksystem.pl
www.jablotron.pl

Przedsiębiorstwo Usług Inżynieryjnych
DRAVIS Sp. z o.o.
ul. Gliwicka 3
40-079 Katowice
tel. (32) 253 99 10
faks (32) 253 70 85
e-mail: dravisdravis@neostrada.pl
www.dravis.pl

Dyskret Sp. z o.o.
ul. Mazowiecka 131
30-023 Kraków
tel. (12) 423 31 00
tel. kom. (0) 501 510 175
faks (12) 423 44 61
e-mail: office@dyskret.com.pl
www.dyskret.com.pl

EBS Sp. z o.o.
ul. Bronisława Czecha 59
04-555 Warszawa
tel. (22) 812 05 05
faks (22) 812 62 12
e-mail: office@ebs.pl, j.haschka@ebs.pl
www.ebs.pl

EDP Support Polska Sp. z o.o.
ul. Chłapowskiego 33
02-787 Warszawa
tel. (22) 644 53 90, 644 51 53
faks (22) 644 35 66
e-mail: edps@edps.com.pl
www.edps.com.pl

---

ela-compil sp. z o.o.
ul. Słoneczna 15a
60-286 Poznań
tel. (61) 869 38 50, 869 38 60
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, 42 30 728
faks (32) 42 30 729
e-mail: el-mont@el-mont.com
el-mont@internetdsl.pl
www.el-mont.com

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

ELTCRAC
Centrum Zabezpieczeń
ul. Ruciana 3
30-803 Kraków
tel. (12) 292 48 60 do 61
faks (12) 292 48 62
e-mail: biuro@eltcrac.com.pl
www.eltcrac.com.pl

Elza Elektrosystemy
ul. Ogrodowa 13
34-400 Nowy Targ
tel. (18) 266 46 10
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./faks (22) 836 54 05, 837 75 93
tel. kom. 0 602 222 516
e-mail: warszawa@emu.com.pl

EUREKA SOFT & HARDWARE
Rynek 13
62-300 Września
tel. (61) 437 90 15
faks (61) 436 27 14
e-mail: biuro@eureka.com.pl
www.eureka.com.pl

FES Sp. z o.o.
ul. Nałkowskiej 3
80-250 Gdańsk
tel. (58) 340 00 41÷44
faks (58) 340 00 45
e-mail: fes@fes.pl
www.fes.pl

GE Security Polska Sp. z o.o.
ul. Sadowa 8
80-771 Gdańsk
tel. (58) 301 38 31, 760 64 80
faks (58) 301 14 36
www.gesecurity.pl

Oddziały:
Al. Stanów Zjednoczonych 59
04-028 **Warszawa**
tel. (22) 810 00 03
faks (22) 810 10 55

Os. Na Murawie 11/2, 61-655 **Poznań**
tel. (61) 821 35 66
faks (61) 821 31 94

GUNNEBO POLSKA Sp. z o.o.
ul. Piwonicka 4
62-800 Kalisz
tel. (62) 768 55 70
faks (62) 768 55 71
e-mail: polska@gunnebo.com
www.rosengrens.pl
www.gunnebo.com

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. 0 693 029 278
e-mail: warszawa@gv.com.pl

ul. Lwowska 74a
33-300 **Nowy Sącz**
tel. (18) 444 35 38, 444 35 39
faks (18) 444 35 84
tel. kom. 0 695 583 424
e-mail: biuro@gv.com.pl

ul. Racławicka 60a
53-146 **Wrocław**
tel. (71) 361 66 02
faks (71) 361 66 23
tel. kom. 0 695 583 292
e-mail: wroclaw@gv.com.pl
www.gvpolska.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

ID ELECTRONICS Sp. z o.o.
ul. Przy Bażantarni 11
02-793 Warszawa
tel. (22) 649 60 95
faks (22) 649 61 00
e-mail: sales@ide.com.pl
www.ide.com.pl

INFO-CAM
Al. Kilińskiego 5
09-402 Płock
tel. (24) 266 97 12
tel./faks (24) 266 97 13
e-mail: handlowy@infocam.com.pl
www.infocam.com.pl

Oddział:
ul. Opolska 29, 61-433 **Poznań**
tel. (61) 832 48 94
tel./faks (61) 832 48 75
e-mail: biuro@infocam.com.pl

Przedsiębiorstwo Usług Technicznych
INTEL Sp. z o.o.
ul. Ładna 4–6
31-444 Kraków
tel. (12) 411 49 79
faks (12) 411 94 74
e-mail: intel@intel.net.pl
www.intel.net.pl

P.W. IRED
Kazimierzówka 9
21-040 Świdnik
tel. (81) 751 70 80
tel. kom. 0 605 362 043
faks (81) 751 71 80
e-mail: ired@exe.pl
www.ired.com.pl

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 Sp. z o.o.
ul. Waryńskiego 63
43-190 Mikołów
tel. (32) 32 48 900
faks (32) 32 48 901
e-mail: handel@kabe.pl
www.kabe.pl, www.kabe.eu

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

KOLEKTOR
K. Mikiciuk, R. Rutkowski Sp. J.
ul. Krzywoustego 16
80-360 Gdańsk-Oliwa
tel. (58) 553 67 59
faks (58) 553 48 67
e-mail: info@kolektor.pl
www.kolektor.pl

KRAK-POŻ Sp. z o.o.
Centrum Ochrony Przeciwpożarowej
i Antywłamaniowej
ul. Ceglarska 15
30-362 Kraków
tel. (12) 266 99 85, 266 52 84, 266 95 08
faks (12) 269 25 79
e-mail: biuro@krakpoz.pl
www.krakpoz.pl

PPUH Laskomex
ul. Dąbrowskiego 249
93-231 Łódź
tel. (42) 671 88 00
faks (42) 671 88 88
e-mail: marketing@laskomex.com.pl
www.laskomex.com.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

MIWI-URMET Sp. z o.o.
ul. Pojezierska 90a
91-341 Łódź
tel. (42) 616 21 00
faks (42) 616 21 13
e-mail: miwi@miwiurmet.com.pl
www.miwiurmet.com.pl

NOMA 2
Zakład Projektowania i Montażu
Systemów Elektronicznych
ul. Plebiscytowa 36
40-041 Katowice
tel. (32) 359 01 11
faks (32) 359 01 00
e-mail: systemy@noma2.com.pl
www.systemy.noma2.pl

Oddziały:
ul. Ryżowa 42, 02-495 **Warszawa**
tel./faks (22) 863 33 40
e-mail: systemy-wa@noma2.com.pl

ul. Brzozowa 71, 61-429 **Poznań**
tel./faks (61) 830 40 46
e-mail: systemy-pz@noma2.com.pl

NORBAIN POLSKA Sp. z o.o.
ul. Szczecińska 1 FA
72-003 Dobra k. Szczecina
tel. (91) 311 33 49
faks (91) 421 18 05
e-mail: info@norbain.pl
www.norbain.pl

Biuro:
ul. Ostrobramska 101 lok. 202
04-041 Warszawa
tel. (22) 465 65 81
faks (22) 465 65 80
infolinia: 0 801 055 075

OBIS CICHOCKI ŚLĄZAK Sp. J.
ul. Rybnicka 64
52-016 Wrocław
tel. (71) 341 98 54
fax, (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
poznan@omc.com.pl

PAG Sp. z o.o.
Bogdanka
21-013 Puchaczów
tel./faks (81) 462 51 36, 462 51 26
e-mail: pag@pag.com.pl
www.pag.com.pl

Oddział:
ul. Zemborzycka 112, 20-445 **Lublin**
tel. (81) 748 02 00 ÷ 09
faks (81) 744 90 62

PANASONIC POLSKA Sp. z o.o.
Al. Krakowska 4/6
02-284 Warszawa
tel. (22) 338 11 77
faks (22) 338 12 00
e-mail: dariusz.labedzki@panasonic.com.pl
www.panasonic.pl

PETROSIN Sp. z o.o.
Rynek Dębnicki 2
30-319 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
ul. Dzielna 1
00-162 Warszawa
tel. (22) 831 15 35, 831 18 97
faks (22) 831 73 36
e-mail: biuro@polital.pl
www.polital.pl

POLON-ALFA
Zakład Urządzeń Dozymetrycznych Sp. z o.o.
ul. Glinki 155
85-861 Bydgoszcz
tel. (52) 363 92 61, 363 92 60
faks (52) 363 92 64
e-mail: polonalfa@polon-alfa.com.pl
www.polon-alfa.pl

PROFICCTV
ul. Heleny Szafran 10
60-693 Poznań
tel./faks (61) 842 29 62
e-mail: biuro@proficctv.pl
www.proficctv.pl
www.dmaxcctv.pl
www.samsungcctv.pl

PROXIMA Sp. J.
ul. Filtrowa 23
87-100 Toruń
tel. (56) 660 20 00
faks (56) 660 20 03
e-mail: proxima@proxima.pl
www.proxima.pl

Filia: (alarmy do obiektów)
ul. Olbrachta 4/6
87-100 **Toruń**
tel. (56) 661 18 96
faks (56) 661 18 97
e-mail: alarmy@proxima.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

P.P.H. PULSON
ul. Czerniakowska 18
00-718 Warszawa
tel. (22) 851 12 20
faks (22) 851 12 30
e-mail: biuro@pulson.pl
www.pulson.pl

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

RAMAR s.c.
ul. Modlińska 237
03-120 Warszawa
tel./faks (22) 676 77 37
e-mail: ramar@ramar.com.pl
www.ramar.com.pl

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

Sagitta Sp. z o.o.
ul. Piekarnicza 18
80-126 Gdańsk
tel./faks (58) 322 38 45
e-mail: sagitta@sagitta.pl
www.sagitta.pl

SAMAX S.A.
ul. Mińska 25
03-808 Warszawa
tel./faks (22) 813 44 25, 870 43 80, 870 77 36
e-mail: samax@samax.pl
www.samax.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

SAWEL systemy bezpieczeństwa
ul. Lwowska 83
35-301 Rzeszów
tel. (17) 857 80 60, 857 79 80
faks (17) 857 79 99
e-mail: sawel@sawel.com.pl
www.sawel.com.pl

SCHRACK SECONET POLSKA Sp. z o.o.
ul. Wołoska 5
02-675 Warszawa
tel. (22) 60 60 614÷617
faks (22) 60 60 618
e-mail: office.warszawa@schrack-seconet.pl
www.schrack-seconet.pl

Oddział:
ul. M. Palacza 13
60-242 **Poznań**
tel. (61) 66 43 140 - 42
faks (61) 66 43 143
e-mail: office.poznan@schrack-seconet.pl

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

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

Oddział:
ul. Różyckiego 1 C
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

SOFTEX DATA S.A.
ul. Poleczki 47
02-822 Warszawa
tel. (22) 331 19 90
faks (22) 331 15 11
e-mail: softex@softex.com.pl
www.softex.com.pl

SOLAR ELEKTRO Sp. z o.o.
ul. Rokicińska 162
92-412 Łódź
tel. (42) 677 58 00
faks (42) 677 58 01
e-mail: communication@solar.pl,
security@solar.pl
www.solar.pl

Oddziały:
ul. Łużycka 3B
81-537 **Gdynia**
tel. (58) 662 00 00/04/05
tel. kom. 0 603 963 695
faks (58) 664 04 00

ul. Radzikowskiego 35
31-315 **Kraków**
tel. (12) 638 91 16
tel. kom. 0 605 366 396
faks (12) 638 91 22

ul. Witosa 3
20-330 **Lublin**
tel. (81) 745 59 00
faks (81) 745 59 05

ul. Smoluchowskiego 7
60-179 **Poznań**
tel. (61) 863 02 04
faks (61) 863 02 70

ul. Heyki 3
70-631 **Szczecin**
tel. (91) 485 44 00
tel. kom. 0 601 570 247
faks (91) 485 44 01

ul. Krakowska 141-155
50-428 **Wrocław**
tel. (71) 377 19 12
tel. kom. 0 607 038 023
faks (71) 377 19 19

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

Oddziały:
ul. Budowlanych 64E
80-298 **Gdańsk**
tel. (58) 340 77 00
faks (58) 340 77 01
e-mail: gdansk@sprint.pl

ul. Przemysłowa 15
85-758 **Bydgoszcz**
tel. (52) 365 01 01
faks (52) 365 01 11
e-mail: bydgoszcz@sprint.pl

ul. Heyki 27c
70-631 **Szczecin**
tel. (91) 431 00 04
faks (91) 462 48 95
e-mail: szczecin@sprint.pl

ul. Canaletta 4
00-099 **Warszawa**
tel. (22) 826 62 77
faks (22) 827 61 21
e-mail: warszawa@sprint.pl

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.com.pl

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

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

ul. Inflancka 6, 91-857 **Łódź**
tel. (42) 617 00 32
faks (42) 659 85 23
e-mail: lodz@spstrading.com.pl
www.aper.com.pl
www.spstrading.com.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 SECURITY
ul. Krakowska 33
43-300 Bielsko-Biała
tel. (33) 821 87 77
faks (33) 816 91 88
e-mail: biuro@s7.pl
www.s7.pl, www.sevenguard.com,
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

TAC Sp. z o.o.

Oddziały:
ul. Rzymowskiego 53
02-697 **Warszawa**
tel. (22) 313 24 10
faks (22) 313 24 11
e-mail: tac_pol@tac.com
www.tac.com/pl

ul. Stefana Batorego 28-32
81-366 **Gdynia**
tel. (58) 782 00 00
faks (58) 782 00 22

ul. Walońska 3-5
50-413 **Wrocław**
tel. (71) 340 58 00
faks (71) 340 58 02

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

TALCOMP SYSTEMY BEZPIECZEŃSTWA
Konrad Talar
ul. Fałęcka 48
30-441 Kraków
tel. (12) 655 85 85, 425 63 67
faks (12) 425 63 68
e-mail: talcomp@talcomp.pl
www.talcomp.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, (32) 357 19 21
e-mail: biuro@tayama.com.pl
www.tayama.com.pl

Zakład Rozwoju Technicznej Ochrony Mienia TECHOM Sp. z o.o.

– Centrum Kształcenia Zawodowego Instalatorów i Projektantów Systemów Alarmowych, Monitoringu oraz Rzeczoznawstwa

– Laboratorium Badawcze Elektronicznych Urządzeń Alarmowych

ul. Marszałkowska 60
00-545 Warszawa
tel. (22) 625 34 00
faks (22) 625 26 75
e-mail: techom@techom.com
www.techom.com

TECHNOKABEL S.A.
ul. Nasielska 55
04-343 Warszawa
tel. (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, 639 88 72
faks (42) 639 89 85
e-mail: teltechinfo@tpteltech.pl
www.tpteltech.pl

Oddziały:
ul. Długa 22/27
80-801 **Gdańsk**
tel. (58) 302 52 12
faks (58) 346 25 09
e-mail: michal.mikolajski@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. Rakowiecka 51
31-510 **Kraków**
tel. (12) 431 59 01
faks (12) 423 97 65
e-mail: marek.zembaty@telekomunikacja.pl

ul. Rzeczypospolitej 5
59-220 **Legnica**
tel./faks (76) 856 60 71
e-mail: marian.sitko@telekomunikacja.pl

ul. Kosmonautów 82
20-358 **Lublin**
tel. (81) 745 39 83
faks (81) 745 39 78
e-mail: zbigniew.chodkiewicz@telekomunikacja.pl

TRIKON
32-447 Siepraw 1123
tel. (12) 274 61 27
faks (12) 274 51 51
e-mail: biuro@trikon.com.pl
www.trikon.com.pl

TYCO FIRE AND INTEGRATED SOLUTIONS Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. (22) 430 8 301
faks (22) 430 8 302
e-mail: tycofis-pl@tycoint.com
www.tycofis.pl

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

Oddziały:
ul. Ratuszowa 11, 03-450 **Warszawa**
tel. (22) 619 22 04
faks (22) 818 64 67

Os. Polan 33, 61-249 **Poznań**
tel. (61) 872 92 08÷10
faks (61) 872 96 30

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

WIZJA Sp. z o.o.
ul. Zakładowa 6
62-052 Komorniki k. Poznania
tel. (61) 810 08 00
faks (61) 810 08 10
www.wizja.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

VISONIC Sp. z o.o.
ul. Smoleńskiego 2
01-698 Warszawa
tel. (22) 639 34 36, 37
faks (22) 833 48 60
e-mail: visonic@visonic.com.pl
www.visonic.com.pl

CZASOPISMO ZABEZPIECZENIA
ul. Puławska 359, 02-801 Warszawa
tel. 022 546 09 51, faks 022 546 09 59

..... , dn. ..... 2008 r.

ZAMÓWIENIE

NA WPIS DO SPISU TELEADRESOWEGO

Zamawiamy ogłoszenie reklamowe w spisie teleadresowym „Zabezpieczeń":

☐ 6 emisji = 360 zł + VAT ☐ 12 emisji = 648 zł + VAT

Nr i rok wydania: ...../.....

OŚWIADCZENIE

Oświadczamy, że firma .....
jest płatnikiem uprawnionym do otrzymywania faktur VAT zgodnie z Rozporządzeniem Ministra Finansów z dnia 18 kwietnia 1995 r. w sprawie podatku od towarów i usług (Dz. Ust. Nr 41, poz. 212 z późniejszymi zmianami).

Upoważniam firmę:
AAT Trading Company Spółka z o.o., ul. Puławska 431, 02 - 801 Warszawa,
Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy KRS, KRS 0000058658, NIP: 951-10-01-169
wysokość kapitału zakładowego 5600000,00 zł, nr rej. GIOŚ: E0001894W,
wydawcę czasopisma „Zabezpieczenia" do wystawiania faktur VAT bez podpisu odbiorcy.

Forma płatności: przelew

DANE NA FAKTURZE:

Nazwa firmy: .....

.....

Adres (ulica, nr domu) .....

.....

(kod, miejscowość) .....

.....

NIP: .....

Imię i nazwisko oraz nr telefonu osoby, z którą można uzgadniać szczegóły techniczne reklamy:

.....

.....

AKTUALNE DANE TELEADRESOWE:

Nazwa firmy: .....

.....

Adres (ulica, nr domu) .....

.....

(kod, miejscowość) .....

.....

Telefon: .....

.....

Faks: .....

E-Mail: .....

www: .....

KATEGORIE

- ☐ Systemy sygnalizacji włamania i napadu
- ☐ Systemy telewizji dozorowej
- ☐ Systemy kontroli dostępu
- ☐ Systemy sygnalizacji pożarowej
- ☐ Systemy ochrony peryferyjnej
- ☐ Integracja systemów
- ☐ Monitoring
- ☐ Zabezpieczenia mechaniczne
- ☐ Systemy nagłośnień

DZIAŁALNOŚĆ

- ☐ Produkcja
- ☐ Projektowanie
- ☐ Dystrybucja
- ☐ Instalacja
- ☐ Szkolenia

Imię i nazwisko osoby zamawiającej:

.....

.....
podpis, data i pieczęć firmy

Prosimy także o przesłanie na nośniku elektronicznym bądź e-mailem zabez@zabezpieczenia.com.pl loga Państwa firmy w CMYK-u w formacie eps, cdr, ai, tif lub jpg.

DZIAŁALNOŚĆ

firma	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
2M Elektronik	-	TAK	TAK	TAK	-
3D	TAK	TAK	-	-	TAK
4 COM	-	TAK	TAK	TAK	TAK
AAT Trading Company	-	TAK	TAK	-	TAK
ACIE	TAK	-	TAK	TAK	TAK
ACSS ID Systems	-	-	TAK	-	TAK
ADT Poland	TAK	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	-
Alarmnet Sp. J.	-	-	TAK	-	TAK
Alarmtech Polska	TAK	TAK	-	-	TAK
Aldom	-	TAK	TAK	TAK	TAK
Alkam System	TAK	TAK	TAK	TAK	-
Alpol Sp. z o.o.	-	-	TAK	-	TAK
Ambient System	TAK	TAK	TAK	TAK	TAK
ANB	-	TAK	TAK	TAK	TAK
Anma	-	TAK	-	TAK	TAK
Atline Sp. J.	-	TAK	TAK	-	TAK
AVISmedia	-	TAK	TAK	-	TAK
Bitner Zakłady Kablowe	TAK	-	-	-	-
BOSCH	-	-	TAK	-	TAK
P.W.H. Brabork - Laboratorium	-	TAK	TAK	TAK	-
bt electronics	TAK	-	TAK	TAK	-
C&C Partners	-	TAK	TAK	-	TAK
CAMSAT	TAK	TAK	TAK	-	-
CBC Poland	-	-	TAK	-	-
CCX	TAK	-	TAK	TAK	-
Cezim	TAK	TAK	TAK	-	TAK
CMA Sp. z o.o.	TAK	-	-	TAK	-
COM-LM	TAK	TAK	TAK	TAK	-
CONTROL SYSTEM FMN	-	TAK	TAK	TAK	TAK
D+H Polska	TAK	TAK	TAK	TAK	-
DANTOM	TAK	-	TAK	-	-
DAR-ALARM	-	TAK	TAK	TAK	TAK
Delta Business Service	-	TAK	-	TAK	TAK
DG Elpro	-	TAK	TAK	TAK	TAK
DOM Polska	TAK	TAK	TAK	-	-
DPK System	-	-	TAK	-	TAK
Dravis	-	TAK	-	TAK	-
Dyskret	-	TAK	TAK	TAK	TAK
EBS	TAK	-	TAK	-	-
EDP Support Polska	TAK	TAK	TAK	TAK	TAK
ela-compil	TAK	TAK	TAK	-	TAK
El-Mont	TAK	TAK	-	TAK	-
Elproma	-	TAK	-	TAK	-
Eltcrac	TAK	TAK	TAK	TAK	TAK
Elza Elektrosystemy-Instalacje	-	TAK	-	TAK	TAK
Emu	-	-	TAK	-	-
Eureka	-	TAK	-	TAK	-
FES	-	TAK	TAK	TAK	-
GE Security Polska	-	-	TAK	-	TAK
Gunnebo	TAK	TAK	TAK	TAK	TAK
GV Polska	-	-	TAK	-	TAK
HSA	-	-	TAK	-	-
ICS Polska	-	-	TAK	-	TAK
ID Electronics	-	TAK	TAK	TAK	-
Info-Cam	TAK	TAK	TAK	TAK	TAK

DZIAŁALNOŚĆ

firma	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Intel	-	TAK	TAK	TAK	TAK
Ired	TAK	TAK	TAK	TAK	-
Janex International	-	-	TAK	-	TAK
KABE	TAK	TAK	TAK	TAK	TAK
Kolektor	-	TAK	-	TAK	-
Kolektor MR	-	TAK	TAK	TAK	-
Krak-Poż	-	TAK	-	TAK	-
Laskomex	TAK	TAK	TAK	TAK	TAK
Legrand Polska	TAK	TAK	TAK	-	TAK
MAXBAT	TAK	TAK	TAK	TAK	TAK
MicroMade	TAK	-	-	-	-
Micronix	-	TAK	TAK	-	-
Miwi-Urmet	TAK	TAK	TAK	-	TAK
Noma 2	TAK	TAK	TAK	TAK	-
NORBAIN Polska	TAK	-	TAK	-	TAK
OBIS Sp. J.	-	TAK	TAK	TAK	TAK
OMC INDUSTRIAL	-	-	TAK	-	-
PAG	TAK	TAK	TAK	TAK	-
Panasonic	-	-	TAK	-	TAK
Petrosin	-	TAK	-	TAK	-
Pointel	-	TAK	-	TAK	-
POL-ITAL	-	-	TAK	-	-
Polon-Alfa	TAK	-	-	-	-
ProfiCCTV	-	TAK	TAK	-	TAK
PROXIMA Sp. J.	TAK	-	TAK	-	-
Pulsar	TAK	-	TAK	-	-
PPH Pulson	TAK	TAK	TAK	-	-
Radioton	-	-	TAK	-	-
Ramar	TAK	-	TAK	TAK	TAK
ROPAM Elektronik	TAK	-	TAK	-	-
Sagitta Sp. z o.o.	TAK	-	-	-	-
Samax	TAK	TAK	-	TAK	TAK
Satel	TAK	TAK	-	-	TAK
Sawel	-	TAK	TAK	TAK	-
Schrack Seconet Polska	TAK	-	-	-	TAK
Secural	TAK	TAK	TAK	-	TAK
S.M.A.	-	TAK	-	TAK	-
SOFTEX Data	-	-	TAK	-	TAK
Solar	-	-	TAK	-	-
Sprint Sp. z o.o.	-	TAK	-	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	-	TAK
STRATUS	-	TAK	TAK	-	TAK
SYSTEM 7 SECURITY	TAK	TAK	TAK	-	TAK
TAC	-	TAK	TAK	TAK	-
Talcomp	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	-	-	TAK	-	TAK
Tayama	TAK	TAK	TAK	TAK	TAK
Techom	-	-	-	-	TAK
Technokabel	TAK	-	-	-	-
TP TELTECH	-	TAK	TAK	TAK	-
Trikon	TAK	TAK	-	TAK	-
TYCO	TAK	TAK	TAK	TAK	TAK
UNICARD S.A.	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	-	-
Wizja	-	-	TAK	TAK	-
Vision Polska	-	TAK	TAK	-	TAK
Visonic	-	-	TAK	-	-

KATEGORIE

firma	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
2M Elektronik	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
3D	-	TAK	-	-	-	-	-	-	-
4 COM	TAK	TAK	TAK	TAK	-	TAK	TAK	TAK	-
AAT Trading Company	TAK	TAK	TAK	TAK	-	TAK	TAK	-	-
ACIE	-	-	TAK	-	-	-	-	-	-
ACSS ID Systems	systemy identyfikacji								
ADT Poland	TAK	TAK	TAK	TAK	-	TAK	TAK	-	TAK
Alarm System	TAK	TAK	TAK	-	-	-	-	-	-
Alarmnet Sp. J.	-	TAK	TAK	-	-	TAK	-	-	-
Alarmtech Polska	TAK	-	-	-	-	-	-	-	-
Aldom	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Alkam System	TAK	TAK	TAK	TAK	-	TAK	-	-	TAK
Alpol Sp. z o.o.	TAK	TAK	TAK	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	-	-	-
ATLine Sp. j.	TAK	TAK	TAK	-	TAK	TAK	-	-	-
AVISmedia	-	-	-	TAK	-	-	-	-	TAK
Bitner Zakłady Kablowe	-	TAK	-	TAK	-	-	TAK	-	TAK
BOSCH	TAK	TAK	-	TAK	-	-	TAK	-	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
bt electronics	-	-	TAK	-	-	TAK	-	TAK	-
C&C Partners	-	TAK	-	-	-	-	TAK	-	-
CAMSAT	-	TAK	-	-	-	-	-	-	-
CBC Poland	-	TAK	-	-	-	-	-	-	-
CCX	-	-	TAK	-	-	-	-	TAK	-
Cezim	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
CMA Sp. z o.o.	-	-	-	-	-	-	TAK	-	-
COM-LM	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Control System FMN	TAK	TAK	TAK	-	-	TAK	-	TAK	-
D+H	-	-	-	TAK	-	TAK	-	-	TAK
DANTOM	TAK	TAK	TAK	TAK	-	-	-	TAK	-
DAR-ALARM	TAK	TAK	TAK	TAK	-	-	TAK	-	-
Delta Business Service	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
DOM Polska	-	-	TAK	-	-	-	-	TAK	-
DPK System	TAK	TAK	-	-	-	-	TAK	-	-
Dravis	TAK	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	-	-	-	-
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Eltcrac	TAK	TAK	TAK	TAK	TAK	TAK	-	-	-
Elza Elektrosystemy-Instalacje	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Emu	akumulatory bezobs ugowe do zasilania awaryjnego urządzeń alarmowych								
Eureka	TAK	TAK	TAK	-	TAK	TAK	TAK	-	-
FES	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
GE Security Polska	TAK	TAK	TAK	TAK	TAK	TAK	-	-	-
Gunnebo	-	-	TAK	-	-	-	-	TAK	-
GV Polska	-	TAK	-	-	-	-	TAK	-	-
HSA	TAK	TAK	TAK	TAK	TAK	-	-	-	TAK
ICS Polska	TAK	TAK	TAK	-	-	-	-	-	-
ID Electronics	TAK	TAK	TAK	-	TAK	-	-	TAK	-
Info-Cam	TAK	TAK	TAK	-	-	TAK	TAK	-	TAK

KATEGORIE

firma	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
Intel	TAK	TAK	TAK	TAK	-	TAK	TAK	-	TAK
Ired	TAK	TAK	TAK	-	-	TAK	TAK	-	-
Janex International	TAK	TAK	TAK	TAK	-	-	TAK	-	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Krak-Poż	-	-	-	TAK	-	-	TAK	-	TAK
Laskomex	-	TAK	TAK	-	-	-	TAK	TAK	-
Legrand Polska	-	-	TAK	-	-	-	-	-	-
MAXBAT	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	-
MicroMade	-	-	TAK	-	Rejestracja czasu pracy			-	-
Micronix	TAK	TAK	TAK	TAK	-	-	-	TAK	-
Miwi-Urmet	TAK	TAK	TAK	-	TAK	TAK	-	-	-
Noma 2	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
NORBAIN Polska	-	TAK	-	-	-	TAK	-	-	-
OBIS Sp. J.	TAK	TAK	TAK	TAK	-	TAK	TAK	-	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	-	-	-	-	TAK	-
PAG	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
Panasonic	-	TAK	TAK	-	-	-	-	-	-
Petrosin	TAK	TAK	TAK	-	-	-	-	-	-
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
POL-ITAL	-	-	TAK	-	-	-	-	TAK	-
Polon-Alfa	-	-	-	TAK	-	-	-	-	-
ProfiCCTV	TAK	TAK	TAK	TAK	-	-	-	-	-
Proxima Sp. J.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Pulsar	TAK	TAK	TAK	-	-	-	TAK	TAK	-
PPH Pulson	-	-	-	-	-	TAK	TAK	-	-
Radioton	-	TAK	-	-	-	-	-	-	-
Ramar	TAK	TAK	TAK	-	TAK	-	TAK	-	-
ROPAM Elektronik	TAK	-	TAK	TAK	-	-	TAK	-	-
Sagitta Sp. z o.o.	-	-	-	TAK	-	-	-	-	-
Samax	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Satel	TAK	TAK	TAK	-	-	-	TAK	-	-
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	-
Schrack Seconet Polska	-	-	-	TAK	-	-	-	-	-
Secural	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.M.A.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Softex Data	-	TAK	-	-	-	TAK	TAK	-	-
Solar	TAK	TAK	TAK	TAK	-	-	-	-	TAK
Sprint Sp. z o.o.	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	TAK	-	-	-	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	-	-	-	TAK
SYSTEM 7 SECURITY	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
TAC	TAK	TAK	TAK	-	TAK	TAK	TAK	-	-
Talcomp	TAK	TAK	TAK	-	TAK	-	-	-	-
Tap – Systemy Alarmowe	TAK	-	TAK	-	TAK	-	-	-	-
Tayama	TAK	TAK	TAK	-	-	TAK	-	-	TAK
Techom	TAK	-	-	-	-	-	-	-	-
Technokabel	wszystkie rodzaje kabli								
TP TELTECH	TAK	TAK	TAK	TAK	-	-	TAK	-	-
Trikon	-	-	TAK	-	-	-	-	TAK	-
TYCO	TAK	TAK	TAK	TAK	-	TAK	-	-	TAK
UNICARD S.A.	-	-	TAK	-	-	TAK	-	TAK	-
W2	TAK	-	-	TAK	-	-	-	-	-
Wizja	-	-	-	-	-	-	-	-	TAK
Vision Polska	-	-	-	TAK	-	-	-	-	-
Visonic	TAK	-	TAK	-	-	-	TAK	-	-

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk
teresa@zabezpieczenia.com.pl

Redaktor merytoryczny
Adam Bułaciński
adam@zabezpieczenia.com.pl

Dział marketingu i reklamy
Ela Końka
ela@zabezpieczenia.com.pl

Redaguje zespół:
Marek Blim
Patryk Gańko
Norbert Góra
Ireneusz Krysowaty
Paweł Niedziejko
Edward Skiepko
Ryszard Sobierski
Waldemar Szulc
Adam Wojcinowicz

Współpraca zagraniczna
Rafał Niedzielski
rafal@zabezpieczenia.com.pl

Współpraca
Jarosław Barszcz
Krzysztof Białek
Sławomir Wagner
Marcin Pyclik

Skład i łamanie
Agnieszka Zadrożna

Korekta
Paweł Karczmarzyk

Adres redakcji
ul. Puławska 359, 02-801 Warszawa
tel. (22) 546 09 51,53
faks (22) 546 09 59
www.zabezpieczenia.com.pl

Wydawca
AAT Trading Company Sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. (22) 546 05 97
faks (22) 546 05 29

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

Cennik reklam

cała strona, pełny kolor	– 3600 zł
cała strona, czarno–biała	– 2100 zł
1/2 strony, pełny kolor	– 2200 zł
1/2 strony, czarno–biała	– 1300 zł
1/3 strony, pełny kolor	– 1700 zł
1/3 strony, czarno–biała	– 1000 zł
1/4 strony, pełny kolor	– 1300 zł
1/4 strony, czarno–biała	– 800 zł
karta katalogowa, 1 strona	– 800 zł
artykuł sponsorowany	– indywidualne negocjacje

Reklama na okładkach

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

Spis teleadresowy

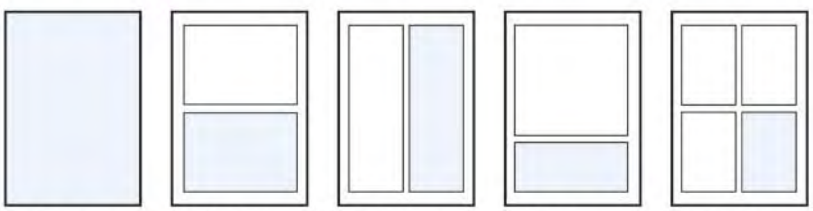
jednorazowy wpis	– 60 zł

Redakcja przyjmuje zamówienia na minimum 6 kolejnych emisji.

W przypadku zamówienia na 12 emisji – 10% rabat.

Podane ceny nie uwzględniają podatku VAT (22%).

Nr konta: **AAT Trading Company Sp. z o.o.**
PKO SA VIII Oddział/Warszawa 34124011121111000001649659



cała strona	1/2 strony	1/2 strony	1/3 strony	1/4 strony
200 x 282 mm + 3 mm spad	170 x 125 mm	81,5 x 257 mm	170 x 80,5 mm	81,5 x 125 mm

Materiały reklamowe przyjmowane są tylko w formie elektronicznej.

Redakcja przyjmuje pliki w CMYK-u w plikach:

- **tiff** – 1 warstwa, rozdzielczość 300 dpi,
- **eps, ai, pdf** – teksty zamienione na krzywe, rozdzielczość bitmap 300 dpi, PDF 1.3,
- **cdr** – do wersji 11, teksty zamienione na krzywe, rozdzielczość bitmap 300 dpi,
- **jpg** – możliwie najwyższa jakość (*maximum quality*), rozdzielczość 300 dpi.

Uwaga!

Reklamy całostronicowe muszą zawierać min. 3 mm spady z każdej strony.

Redakcja nie ponosi odpowiedzialności za zgodność kolorów w innej niż CMYK przestrzeni kolorystycznej.

Redakcja przyjmuje materiały reklamowe na płytach CD lub e-mailem (do 5 MB).

Materiały należy dostarczyć na 3 tygodnie przed planowanym zamknięciem numeru.

SPIS REKLAM

www.hardwarefair.com

INTERNATIONAL | PRACTICAL HARDWARE FAIR | WORLD

Kolonia, 9–12 marca 2008

Cztery
dni dla biznesu

12 marca 2008. W Moskwie jest godzina 20.00, w Kairze 19.00, zaś w Hongkongu jest już nawet jeden dzień później, podczas gdy w Kolonii o godzinie 18.00 czasu lokalnego dobiegło końca największe w skali światowej wydarzenie branżowe, wszyscy nieobecni stracili wiele: kompleksowy przegląd sektora narzędzi, technik zabezpieczeń oraz budownictwa. Cała branża spotyka się w Kolonii. Cztery dni dla biznesu. Obecność obowiązkowa. **Oszczędź czas i pieniądze: już od połowy grudnia możliwa rejestracja i zakup biletu wstępu dla odwiedzających online na stronie: www.hardwarefair.com**

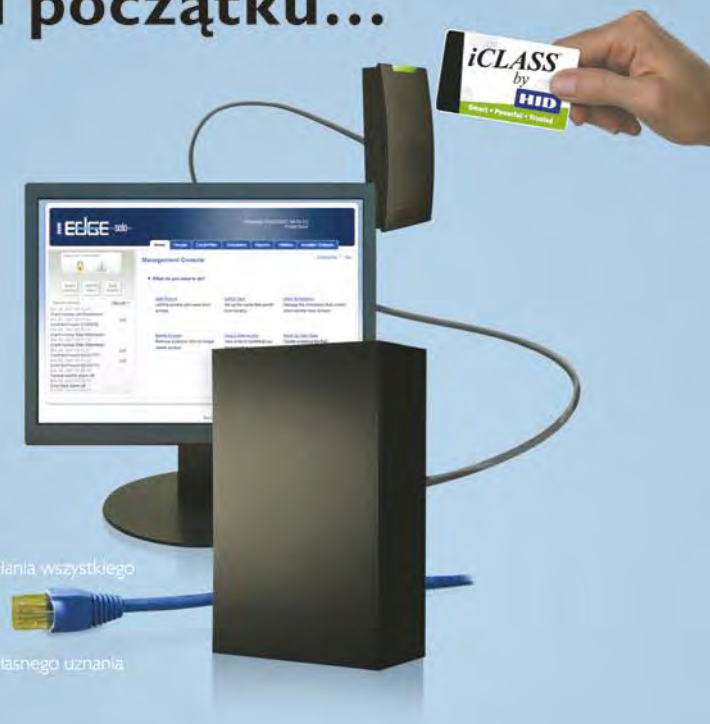
Przedstawicielstwo Targów
Koelnmesse w Polsce Sp.j.
ul. Chmielna 5/7, 00-021 Warszawa
Telefon +48 22 827 46 70, Telefax +48 22 827 34 56
info@koelnmesse.pl

koelnmesse
we energize your business

W roku 1990 firmy HID i Indala wywracają pojęcie Kontroli Dostępu do góry nogami, przedstawiając czytniki i karty zbliżeniowe…

KONTROLA DOSTĘPU

I znowu od początku…



Zmień swój sposób myślenia o kontroli dostępu.

Oparte na technologii IP
Obsługa poprzez standardową przeglądarkę internetową
Brak dodatkowego oprogramowania!

Skalowalny
Zdalna obsługa z głównej bazy czytników
Bez konieczności wprowadzania zmian przy drzwiach!

Prosty
Użycie zasilania poprzez sieć komputerową; jeden kabel do zasilania wszystkiego
Bez zasilacza!

Elastyczny
Zastosuj zintegrowany czytnik iCLASS lub każdy inny według własnego uznania
Nieograniczony wybór czytników i kart!

Edge Solo firmy HID.

Przedstawiamy Edge Solo, produkt HID opłacalny kosztowo, autonomiczny, tworzący możliwość adresowania IP pojedynczych drzwi.

HID

EDGE solo

ACCESS

Inteligencja na drzwiach

hidcorp.com