CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 3/4(61/62)/2008

ZABEZPIECZENIA

10 lat za nami

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

W NUMERZE:

- CRT czy LCD?
- Ciągłość działania w życiu codziennym
- Kompresja obrazów ruchomych zgodna ze standardem H.264
- Rozproszony system bezpieczeństwa dla dużego rozległego obiektu w aspekcie zdalnego zarządzania

NASTĘPNA GENERACJA SYSTEMÓW ZABEZPIECZEŃ PRZYBYŁA

FIKCJA STAŁA SIĘ FAKTEM ...
SYSTEMY ZABEZPIECZEŃ I-PRO PANASONIC.

Panasonic opanował najnowszą technologię IP, aby stworzyć naprawdę futurystyczny system zabezpieczeń i-pro, zawierający pełną gamę produktów. Pozwala on powstrzymać nie tylko inwazję intruzów, ale także znacząco redukuje koszty związane z użytkowaniem systemu, między innymi poprzez zmniejszenie ilości kabli oraz kosztów obsługi. Ponieważ posiadamy specjalistyczną wiedzę w tej dziedzinie, jesteśmy w stanie zaproponować najlepsze z możliwych rozwiązań.

Więcej informacji o produktach i-pro uzyskasz pod numerem telefonu (22) 33 81 177
lub odwiedzając stronę pss.panasonic.eu

i-pro

Panasonic
ideas for life

CZASOPISMO ZABEZPIECZENIA

3/4/2008

w numerze

WYDARZENIA INFORMACJE 4

WYWIAD

10 pytań na 10 lat systemu SEVEN GUARD, z Mirosławem Wandzelem, prezesem firmy System 7 Security, rozmawia Teresa Karczmarzyk 32

BEZPIECZEŃSTWO IT

Ciągłość działania w życiu codziennym, Krzysztof Białek 37

PUBLICYSTYKA

Strefa Schengen – czyli co trzeba wiedzieć o SIS, VIS i ESI, Marek Blim, Andrzej Dobosz 42

SYSTEMY ZINTEGROWANE

Commend – profesjonalne centrum nadzoru, Marek Katarzyński, C&C Partners Telecom 52

TELEWIZJA DOZOROWA

Kompresja obrazów ruchomych zgodna ze standardem H.264, Andrzej Walczyk 56

CRT czy LCD?, Sławomir Janiso, Radioton 60

Telemetria – bezprzewodowy system transmisji sygnału telemetrycznego (868 MHz) firmy 3D z Bydgoszczy, Jowita Kuczyniecka, 3D 63

KONTROLA DOSTĘPU

Oblicza RFID (cz.3), Przemysław Mierzwiak, IISB 66

OCHRONA INFORMACJI

System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001, Cz. 2. Procesy zarządzania bezpieczeństwem informacji, Andrzej Wójcik 74

SSWiN

Rozproszony system bezpieczeństwa dla dużego rozległego obiektu w aspekcie zdalnego zarządzania, Waldemar Szulc, Andrzej Szmigiel 78

Nowoczesne technologie w detektorach firmy RISCO Group, RISCO Group 86

Nowa seria czujek OPTiMAL, Jarosław Gibas, Optex Security 90

PORADY

Projektant a wykonawca, Piotr Murawski, Geo-kat 94

KARTY KATALOGOWE 97

SPIS TELEADRESOWY 108

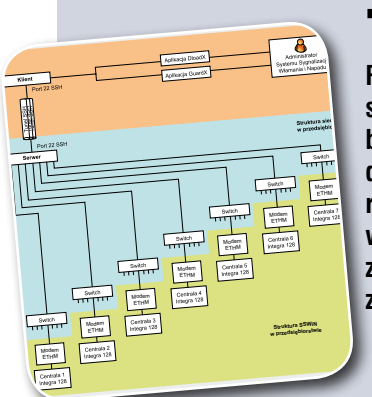
CENNIK REKLAM 118

SPIS REKLAM 118

37
Ciągłość działania w życiu codziennym

56
Kompresja obrazów ruchomych zgodna ze standardem H.264

60
CRT czy LCD?



78
Rozproszony system bezpieczeństwa dla dużego rozległego obiektu w aspekcie zdalnego zarządzania

Securex 2008
– reminiscencje

Tegoroczna Międzynarodowa Wystawa Zabezpieczeń „Securex", z uwagi na zmianę cyklu odbywania się na dwuletni, była dłużej oczekiwana niż poprzednim razem, w 2006 roku. Warto było poczekać – organizowane po raz siedemnasty targi okazały się rekordowe pod względem liczby zwiedzających (należy wziąć jednak pod uwagę fakt, że liczba zwiedzających dotyczy nie tylko Securexu, ale również Instalacji i SAWO), a liczba wystawców, zwłaszcza zagranicznych, znacząco wzrosła w porównaniu z liczbą czynnych uczestników poprzedniej edycji.

Dokładne dane liczbowe dotyczące tej imprezy zostały opublikowane przez jej organizatora i są dostępne m.in. na naszym portalu www.zabezpieczenia.com.pl. Poniżej kilka uwag i spostrzeżeń dotyczących targów Securex 2008, niekoniecznie traktujących o zagadnieniach najważniejszych, ale być może także wartych uwagi.

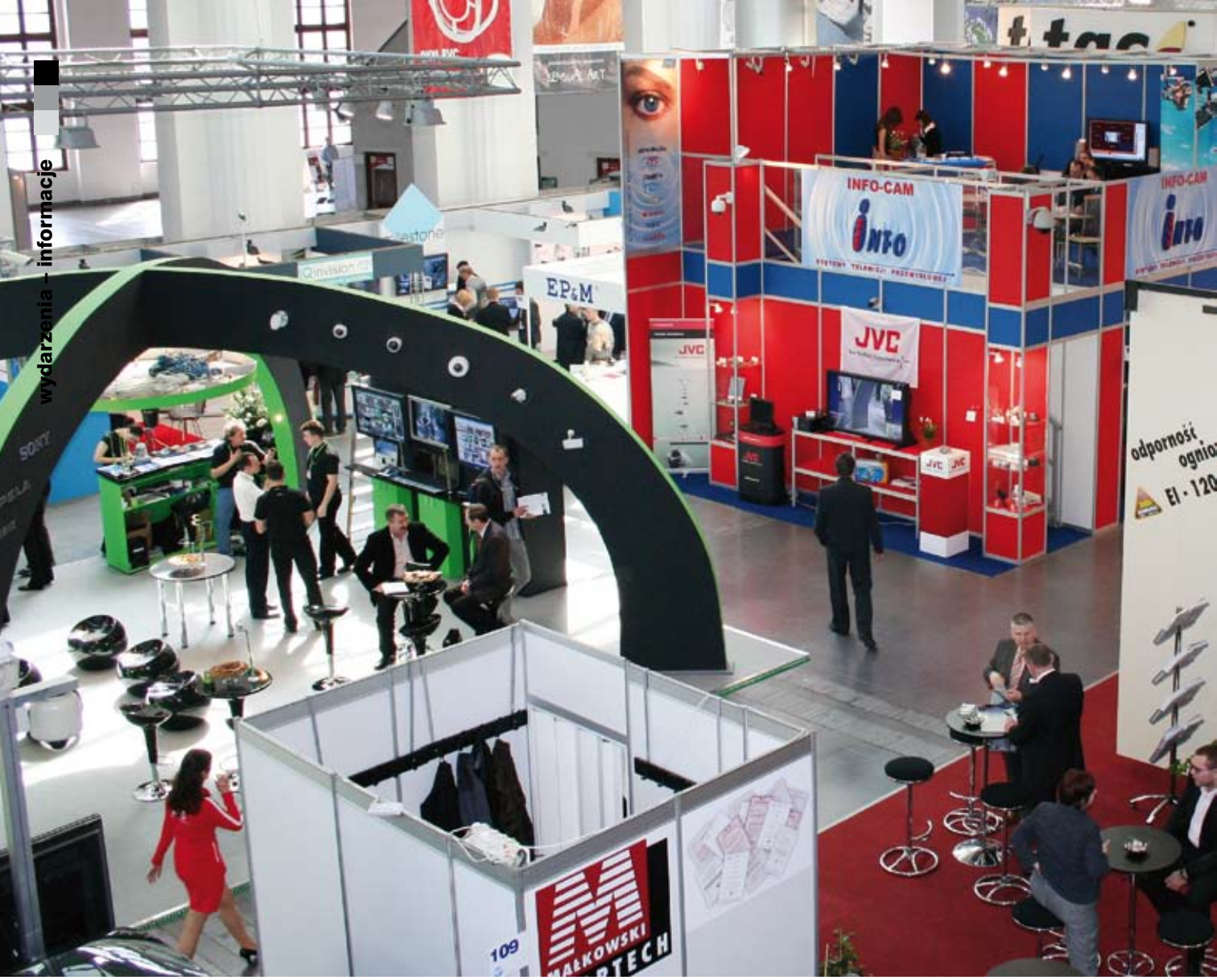
Zdaniem wielu ekspertów w branży zabezpieczeń cykl dwuletni gwarantuje, że wielu wystawców będzie miało do zaprezentowania prawdziwe nowości. Nie każdy producent w tej branży przygotowuje co roku warte zaprezentowania rozwiązania, a więc i nie każdy dystrybutor, nawet z pierwszej krajowej dziesiątki, decydował się dotychczas na czynne uczestnictwo w targach odbywających się co roku. Przed kilku laty można było wręcz zaobserwować trend wystawiania się na targach Securex co dwa lata. Decyzja organizatora targów rozwiąże w wielu przypadkach potencjalnie występujący dylemat – czy przygotowywać się jako wystawca na bieżącej imprezie, czy dopiero następnym razem. Być może następne targi okażą się znów rekordowe?

Z pewnością istnieją dziedziny przemysłu zabezpieczeń, które rozwijają się bardzo dynamicznie i w ciągu roku są w stanie wprowadzić na rynek interesujące i nowatorskie rozwiązania. Przykładem może być telewizja dozorowa. W epoce masowego rozwoju otwartych rozwiązań bazujących na protokole internetowym (IP) tempo jej rozwoju dostosowało się

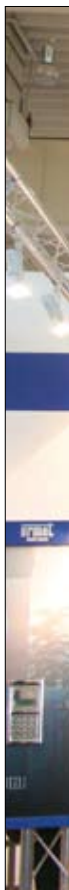
do szybkości zmian, jakie zachodzą w technologiach komputerowych. A przecież nowości w zakresie telewizji dozorowej dotyczą nie tylko sposobu przesyłania obrazu i jego analizy.

Jeszcze w co najmniej dwóch dziedzinach systemów zabezpieczeń widać wyraźnie ekspansję rozwiązań IP. Jedna z nich to systemy sygnalizacji włamania i napadu (SSWiN). Wprawdzie główny nurt nowości związany jest raczej z technologiami bezprzewodowymi, ale już od kilku lat każdy szanujący się producent tego typu systemów ma w swojej ofercie moduły współpracujące z centralami alarmowymi, umożliwiające monitorowanie przez Internet. Pojawiają się także systemy kontroli dostępu (SKD), w których kontrolery mogą być łączone ze sobą nie tylko za pomocą „tradycyjnych" interfejsów szeregowych, ale i przez Ethernet. W wielu przypadkach ułatwia to prowadzenie instalacji, a w przypadku systemów rozległych pozwala na łatwe ominięcie ograniczeń, jakie narzucają interfejsy szeregowe. Rozwiązania sieciowe zaczynają również dominować w zintegrowanych systemach nadzoru, zarówno przeznaczonych do integracji urządzeń i systemów różnych producentów, jak i obejmujących całościowe propozycje jednego producenta. W systemie zintegrowanym, z którym można było zapoznać się podczas targów Securex 2008, m.in. podczas oddzielnej, obszernej prezentacji, zarządzanie systemem odbywa się z wykorzystaniem przeglądarki internetowej, poprzez sieć. Głównym kierunkiem rozwoju SKD wydają się jednak nie rozwiązania komunikacyjne, ale biometria, oferująca coraz doskonalsze rozwiązania w zakresie identyfikacji osób na podstawie ich unikatowych cech osobistych.

W związku z członkostwem naszego kraju w Unii Europejskiej (UE) renesans przeżywają systemy zabezpieczeń zewnętrznych. Zgodnie z dyrektywami UE ochronie podlegają obiekty szczególnie ważne w organizacji życia społecznego, tzw. obiekty infrastruktury krytycznej, np. porty lotnicze i morskie, zakłady przemysłowe, elektrownie itp. Takim obiektom należy zapewnić obecnie nie tylko ochronę obwodową (zwaną też perymetryczną), co było dotychczasowa praktyką, ale i to, co znajduje się na terenie chronionego obiektu (samoloty, statki, pociągi, magazyny, zbiorniki itd.). Trendy techniczne i technologie stosowane w ochronie infrastruktury krytycznej były tematem dwóch referatów, wygłoszonych podczas odbywającej się podczas targów Securex 2008 konferencji „Urządzenia i sposoby zabezpieczenia mienia" (*Zabezpieczenia* były patronem medialnym konferencji, która już od 17 lat towarzyszy Międzynarodowej Wystawie Zabezpieczeń i, jak zapewnia Kazimierz Skrzypczak, przewodniczący komitetu organizacyjnego, należy do jednej z największych imprez w kraju, poświęconych


INFO-CAM
INFO
JVC
EP&M
109

AAT
DSC
UNITON



szeroko rozumianemu bezpieczeństwu, ochronie osób i zabezpieczeniu mienia). Przejawem zainteresowania się Polską, jako potencjalnym rynkiem zbytu systemów zabezpieczeń zewnętrznych, jest pojawienie się na targach przedstawicieli rosyjskiego producenta takich systemów. Istniejąca i od lat ustabilizowana oferta sprzętowa w tym zakresie ma szanse poszerzenia się o urządzenia nieznane wcześniej na polskim rynku.

Jak co roku *Zabezpieczenia* były również patronem medialnym Konkursu „Polski Mistrz Techniki Alarmowej 2008". Podczas targów Securex 2008 uroczyście ogłoszono wyniki i wręczono nagrody laureatom XII edycji konkursu. Wielkim zwycięzcą, a zarazem laureatem głównej nagrody – Złotej Zbroi – za agentowe systemy roju, czyli nową architekturę systemów alarmowych, przedstawioną na przykładzie systemu Novator, jest firma Alarmtech Polska z Gdańska.

Wszystkim nagrodzonym serdecznie gratulujemy.

Z przyjemnością objęliśmy również patronatem medialnym rozgrywane po raz pierwszy w historii Securexu I Mistrzostwa Polski Instalatorów Systemów Alarmowych (I MPISA), których organizatorami były Międzynarodowe Targi Poznańskie i Polska Izba Systemów Alarmowych.

Jesteśmy pod wielkim wrażeniem wiedzy i kunsztu instalatorskiego ekip, które zakwalifikowały się do finału. Gratulacje w imieniu całej redakcji! Szersze omówienie przebiegu mistrzostw znajdą Państwo w relacji Henryka Dąbrowskiego, dyrektora Biura Organizacyjnego I MPISA.

Wszystkich zainteresowanych fotoreportażami z imprez targowych i wystawy zapraszamy na naszą stronę: www.zabezpieczenia.com.pl.

W imieniu całego zespołu redakcyjnego dziękujemy prezesowi Międzynarodowych Targów Poznańskich, Przemysławowi Trawie, oraz dyrektorowi Projektu Securex, Bartoszowi Zeidlerowi, za serdeczne gratulacje z okazji 10-lecia redakcji *Zabezpieczeń* i za dotychczasową współpracę.

Teresa Karczmarzyk
Adam Bułaciński

Targi Securex 2008 – zakończone

Rekordowa liczba zwiedzających, ponad 180 nowości technologicznych i kompleksowa oferta dotycząca ochrony mienia, informacji, systemów alarmowych, monitoringu wizyjnego czy zabezpieczeń – to główne atrybuty zorganizowanej po raz siedemnasty Międzynarodowej Wystawy Zabezpieczeń „Securex".

Securex – najważniejsze wydarzenie dla branży

Securex to największe targi branży zabezpieczeń w Polsce. Ekspozycja o powierzchni ponad 9000 m^2 zgromadziła 216 wystawców (wzrost o ponad 19% w porównaniu z poprzednią edycją w 2006 roku), w tym przedstawicieli z 18 krajów, m.in. z Austrii, Danii, Holandii, Niemiec, Szwecji, Wielkiej Brytanii i Korei Płd. (o 38% więcej niż dwa lata temu). Na szczególną uwagę zasługuje fakt, że w Poznaniu obecne były niemal wszystkie najważniejsze polskie firmy z branży zabezpieczeń (w tym wiele firm działających na rynku globalnym), a także wiele małych i średnich przedsiębiorstw. Zarówno pod względem wynajętej powierzchni, jak i liczby firm uczestniczących w targach, tegoroczna edycja była rekordowa. O dobrej koniunkturze na rynku oraz dynamicznym rozwoju branży świadczy imponująca liczba zwiedzających. Ekspozycję Securex, odbywającą się równolegle z targami instalacyjnymi Instalacje oraz Międzynarodowymi Targami Ochrony Pracy, Pożarnictwa i Ratownictwa „Sawo", odwiedziło blisko 28 tysięcy osób.

Securex to forum prezentacji najnowszych rozwiązań w zakresie usług ochrony, monitoringu wizyjnego, zabezpieczeń antywłamaniowych, systemów alarmowych obejmujących sygnalizatory, czujki, stacje monitorujące oraz systemy kontroli dostępu. Szczególną uwagę zwiedzających przyciągnęła w tym roku imponująca liczba nowości technologicznych, których zaprezentowano ponad 180.

Spora dawka wiedzy i emocji

W ramach programu wydarzeń towarzyszącego ekspozycji przygotowano ciekawe prelekcje, konferencje, spotkania ze specjalistami. We wtorek wręczono nagrody w prestiżowym konkursie Polski Mistrz Techniki Alarmowej, przygotowanym przez Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „Polalarm". W uroczystości wzięli udział przedstawiciele dystrybutorów, producentów i projektantów systemów zabezpieczeń oraz prasa branżowa, pełniąca patronat medialny nad konkursem. Liczną publiczność zgromadziły odbywające się po raz pierwszy Mistrzostwa Polski Instalatorów Systemów Alarmowych, organizowane wspólnie z Polską Izbą Instalatorów Alarmowych pod honorowym patronatem Ministra Spraw Wewnętrznych i Administracji. Po trudnych eliminacjach do finału ostatecznie zakwalifikowano 9 zespołów prezentujących bardzo wysoki poziom umiejętności i przygotowania zawodowego. Zwycięskie trzy drużyny odebrały z rąk Zbigniewa Adamowicza, dyrektora Departamentu Bezpieczeństwa Publicznego MSWiA, gratulacje i dyplomy.

Dużym zainteresowaniem cieszyła się odbywająca się w środę 17. Konferencja Securex – „Urządzenia i sposoby zabezpieczenia mienia" (patronat medialny – czasopismo *Zabezpieczenia* – przyp. red.), zorganizowana dla przedstawicieli uczelni, instytutów, banków, policji, firm ochrony, a także handlu i usług. Konferencja dostarczyła wiedzy z zakresu metod zapobiegania przestępczości zalecanych w normach europejskich EN, bezpieczeństwa kont bankowych, monitorowania bezpieczeństwa wewnątrz instytucji finansowych czy ewolucji w systemach sygnalizacji pożarowej.

Strzałem w dziesiątkę okazała się prelekcja przygotowana przez firmę Dipol na temat monitoringu miejskiego i monitoringu obiektów sportowych. Duże zainteresowanie tematem świadczy o potrzebie pogłębienia wiedzy z tej dziedziny i jednocześnie jest motywacją do przygotowania podobnego spotkania podczas kolejnej edycji targów.

Profesjonalną publiczność zgromadziła konferencja „Nadzór wizyjny – nowe technologie", nad którą patronat objęła firma S.P.S. Trading. Przygotowane we współpracy z Politechniką Poznańską spotkanie cieszyło się dużym zainteresowaniem, a poruszana tematyka dostarczyła fachowej wiedzy na temat telewizji dozorowej IP.

Nagrody i konkursy

Podczas tegorocznej edycji Securex wręczono 18 Złotych Medali za najlepsze produkty, wyróżniające się nowoczesnością, jakością i funkcjonalnością. Ponadto na targach wyróżniono stoiska najlepiej realizujące założenia strategii marketingowej firmy. Nagrodami Acathus Aureus odznaczono 5 wystawców.

Ważny temat – duże zainteresowanie

Tegoroczna Międzynarodowa Wystawa Zabezpieczeń „Securex" odniosła duży sukces. Świadczą o tym pozytywne opinie wystawców oraz znacząca frekwencja zwiedzających.

O coraz większej świadomości społeczeństwa w zakresie poziomu bezpieczeństwa oraz ciągłej potrzebie zwiększania wiedzy na ten temat świadczy duże zainteresowanie mediów targami Securex. Na targach obecni byli wszyscy czołowi przedstawiciele prasy branżowej. Najważniejsze wydarzenia i rozmowy z liderami rynku były również na bieżąco relacjonowane w telewizji.

Securex 2010

Za nami siedemnasta już edycja targów Securex. Nadchodząca edycja w związku z przejściem na cykl dwuletni odbędzie się dopiero **w 2010 roku**. Już dziś zapraszamy do Poznania w dniach **26–29 kwietnia**.

Bezpośr. inf. MTP

Złote medale

targów SECUREX 2008

LISTA PRODUKTÓW NAGRODZONYCH ZŁOTYM MEDALEM MTP

Centrala sygnalizacji włamania i napadu INTEGRA 128 -WRL
Satel, Gdańsk

System sygnalizacji pożarowej INTEGRAL EVOLUTION
SCHRACK SECONET, Austria
Zgłaszający: SCHRACK SECONET Polska, Warszawa

Sieć trzymaczy drzwiowych SALAMANDER
Stephenson Gobin, Wielka Brytania
Zgłaszający: Małkowski – Martech, Poznań

System SECU-MEDIA
Optiguard, Toruń

System OBSERVISION
OBSERVISION BV, Holandia
Zgłaszający: C&C Partners Telecom, Leszno

Optyczna dualna czujka ruchu IR0840T
SIEMENS Schweiz, Building Technologies, Szwajcaria
Zgłaszający: Siemens, Warszawa

BIOSTATION (BIOSTACJA) WIRELESS RF – wersja bezprzewodowa + biometria + czytnik kart
SUPREMA, Korea
Zgłaszający: Cardco, Łódź

Sejf jubilerski TG-GB kl. I
Metalkas, Bydgoszcz

Kamera IP Mobotix M12-Sec-R8
MOBOTIX, Niemcy
Zgłaszający: LINC, Poznań

System sterowania ruchem TCS
IPP, Warszawa

Dyspenser z zamkniętym obiegiem gotówki RECYCLER RZ-100
GLORY EUROPE, Niemcy
Zgłaszający: Kłos Zbigniew Nowoczesne Technologie Bankowe, Mościska

System zarządzania dostępem do bankomatu
Sargent and Greenleat, USA
Zgłaszający: POL-ITAL, Warszawa

Multisensorowa czujka pożarowa optyczno-termiczna ESSER IQ O 2 T
NOVAR, Niemcy
Zgłaszający: Honeywell Life Safety, Austria

Multisensorowa czujka pożarowa optyczno-termiczna ESSER IQ OT blue
NOVAR, Niemcy
Zgłaszający: Honeywell Life Safety, Austria

Rejestrator obrazu AVERMEDIA AVERDiGi S.A. 6000E PRO
AVERMEDIA INFORMATION, Taiwan
Zgłaszający: Alpol, Katowice

Nadruk UV na kartach plastikowych w technologii wnikania
Digital Identification Solutions, Niemcy
Zgłaszający: EDP Support Polska, Warszawa

Multisejf XS
Konsmetal, Warszawa

Dyspenser
Konsmetal, Warszawa

Przewodniczący Sądu Konkursowego: prof. dr hab. inż. Bogdan Branowski

NAGRODY ACANTHUS AUREUS

Siemens, Warszawa
Projektant: LABUDA DESIGNE, Anna Labuda
Wykonawca: LABUDA DESIGNE, Anna Labuda

S.P.S. TRADING, Warszawa
Projektant: Agnieszka Dryl, EXPO – SYSTEM
Wykonawca: EXPO – SYSTEM

Satel, Gdańsk
Projektant: Szymon Wanatowicz, Satel
Wykonawca: Meliński Minuth

Schrack Seconet Polska, Warszawa
Projektant: Aleksandra Wójcik, Amarina
Wykonawca: Aleksandra Wójcik, Amarina

Konsmetal, Warszawa
Projektant: Międzynarodowe Targi Poznańskie
Wykonawca: Międzynarodowe Targi Poznańskie

Bezpośr. inf. MTP

Polski Mistrz Techniki Alarmowej 2008

Komisja konkursowa Ogólnopolskiego Stowarzyszenia Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „Polalarm" w dniu 4 kwietnia 2008 r. wyłoniła laureatów XII edycji Konkursu „Polski Mistrz Techniki Alarmowej 2008".

Komisja przyznała następujące nagrody i wyróżnienia w poszczególnych kategoriach konkursu:

1. Urządzenia i systemy sygnalizacji włamania i napadu

- I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2008 za agentowy system roju – nową architekturę systemów alarmowych na przykładzie systemu Novator – firmie Alarmtech Polska z Gdańska
- wyróżnienie za rodzinę barier aktywnej podczerwieni PB-IN 50/100/200 HF Takex firmie ICS Polska z Warszawy

- wyróżnienie za INTEGRĘ 128 – WRL, bezprzewodową centralę alarmową, zintegrowaną z dwukierunkowym bezprzewodowym interfejsem ABAX 868 MHz, i komunikator GSM/GPRS firmie Satel z Gdańska
- wyróżnienie za rodzinę (typoszereg) aktywnych radarów 360 st., chroniących rozległe tereny zewnętrzne, wraz z softwarem umożliwiającym automatyczne kierowanie kamerami CCTV firmie KABE z Mikołowa
- wyróżnienie za czujkę serii Professional z systemem wielopunktowego antymaskingu ISC-PDL1-WA18G firmie Robert Bosch z Warszawy

2. Urządzenia i systemy sygnalizacji pożarowej

- I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2008 za centralę sygnalizacji pożarowej FPA5000 w wersji sieciowej firmie Robert Bosch z Warszawy

3. Urządzenia i systemy nadzoru telewizyjnego i rejestracji obrazów

- I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2008 za MatriVideo – sieciowy system monitoringu i zarządzania wizyjnego w megapikselowej rozdzielczości firmy Instek Digital firmie Ultrak Security Systems ze Szczecina
- wyróżnienie za CMS – centralną stację monitorującą CCTV – sieciowy (hybrydowy) system nadzoru CCTV firmie Protector Polska ze Szczecina
- wyróżnienie za cyfrowy rejestrator Vista BLADE firmie Norbain Polska z Warszawy
- wyróżnienie za inteligentną kamerę PTZ AutoDome serii 500i firmie Robert Bosch z Warszawy

4. Urządzenia i systemy kontroli dostępu

- I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2008 za system kontroli dostępu ACCO firmie Satel z Gdańska

5. Zintegrowane systemy sygnalizacji zagrożeń

– I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2008 za rodzinę (typoszereg) aktywnych radarów 360 st., chroniących rozległe tereny zewnętrzne, wraz z softwarem umożliwiającym automatyczne kierowanie kamerami CCTV firmie KABE z Mikołowa
– wyróżnienie za system powiadamiania wizualizacji i wspomagania decyzji SWD firmie Noma z Katowic

6. Urządzenia i systemy transmisji alarmu oraz monitoringu

– I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2008 za system wizyjnej weryfikacji alarmów – rozwiązanie sprzętowe i programowe firmy HeiTel – firmie Linc z Poznania
– wyróżnienie za zintegrowany system monitoringu infrastruktury technicznej obiektów telekomunikacyjnych i informatycznych firmie Electronic Power and Market ze Szczecinka
– wyróżnienie za stację monitorowania sygnałów alarmowych Stam-2 firmie Satel z Gdańska
– wyróżnienie za LX komunikacja poprzez GPRS/GSM firmie EBS z Warszawy

7. Systemy zabezpieczenia przeciwkradzieżowego pojazdów

– I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2008 za autoalarm Q-SAFE Multi CAN firmie ETS Polska z Warszawy
– wyróżnienie za profesjonalny system zabezpieczenia antykradzieżowego pojazdów SAT – DOG ProSafe firmie ProSafe z Warszawy

8. Inne urządzenia i systemy technicznej ochrony oraz wspomagające ochronę fizyczną

– I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2008 za system depozytariuszy kluczy i skrytek firmie Protector Polska ze Szczecina
– wyróżnienie za system Active Guard firmie Active Guard z Warszawy

Ponadto komisja przyznała specjalne wyróżnienie. Wyróżnienie specjalne komisji za rodzinę (typoszereg) aktywnych radarów 360 st., chroniących rozległe tereny zewnętrzne, wraz z softwarem umożliwiającym automatyczne kierowanie kamerami CCTV otrzymała firma KABE z Mikołowa.

Spośród zdobywców I miejsc w poszczególnych kategoriach komisja wyłoniła zwycięzcę konkursu, któremu przyznała główną nagrodę. Laureatem głównej nagrody **Złota Zbroja** w Konkursie „Polski Mistrz Techniki Alarmowej 2008” za agentowe systemy roju – nową architekturę systemów alarmowych na przykładzie systemu Novator – jest firma Alarmtech Polska z Gdańska.

Bezpośr. inf. Polalarm

Zapraszamy do obejrzenia fotoreportażu na stronie: www.zabezpieczenia.com.pl

Złota Zbroja dla firmy Alarmtech Polska

Znana dotychczas z projektowania i produkcji detektorów firma Alarmtech przedstawiła podczas targów Securex 2008 całkowicie nową ofertę systemów alarmowych. Oferta ta zrywa z tradycyjnym podejściem w projektowaniu, prowadzącym do silnie zhierarchizowanych konstrukcji, i proponuje nową, opracowaną przez Alarmtech architekturę agentowych systemów roju. Alarmtech poprzez nową architekturę sięga do nowoczesnych rozwiązań, wywodzących się z dziedziny sztucznej inteligencji. Uzyskał tą drogą ważne dla instalatorów cechy systemu, niedostępne w starszych rozwiązaniach obecnych na rynku.

Opracowany system Novator zapewnia:

- całkowitą swobodę topologii budowanych systemów – dowolne typy komórek mogą być łączone w dowolny sposób celem zmniejszania czasu i kosztów okablowania systemu,
- autokonfigurację systemów bez względu na topologię – maksymalne uproszczenie procesu uruchamiania systemu,
- automatyczne rozpoznanie i programowanie konfiguracji linii wejściowych – dla umożliwienia instalatorowi szybkiego sprawdzenia systemu,
- to, że wszystkie linie wejściowe mogą pracować w dowolnej konfiguracji NC, NO, EOL, 2EOL i 3EOL,
- to, że linie w konfiguracji mogą pracować z różnymi wartościami rezystorów parametryzujących,
- bezpieczeństwo przez kodowanie wszystkich transmisji międzykomórkowych i sprawdzanie poprzez podpis cyfrowy,
- elastyczność i liniową skalowalność systemów w zakresie funkcjonalności, bezpieczeństwa i kosztów,
- samonaprawialność uszkodzeń,
- skalowalną redundancję systemu zasilania.

Opracowana architektura oparta jest na silnych podstawach – do łączności pomiędzy modułami – komórkami zastosowano niezawodne, sprawdzone w praktyce automatyki przemysłowej 4-punktowe trakty, przenoszące zasilanie (12 V_{DC}) oraz dane (RS485). Oprogramowanie komórek stworzone jest w technologii agentowej – na poziomie abstrakcji programistycznej wyższym od programowania obiektowego. Zapewniło to m.in. możliwość automatycznego nawiązywania współpracy dowolnego zestawu komórek między sobą.

Opracowana architektura oraz przedstawiony system są całkowicie polskim rozwiązaniem – opracowane zostały od podstaw przez zespół projektantów firmy Alarmtech, pracujący pod kierunkiem byłego wieloletniego pracownika naukowego Politechniki Gdańskiej. Opracowanie jest w 100% dziełem zespołu, łącznie z wieloaplikacyjnym, wieloprocesorowym i wielozadaniowym systemem czasu rzeczywistego, pracującym w środowisku rozproszonych procesorów.

Wykonany w technologii agentowego systemu roju system alarmowy Novator został po raz pierwszy zaprezentowany publicznie podczas targów Securex 2008 w Poznaniu w dniach 22–25.04.2008. Rozwiązanie spotkało się z bardzo dużym zainteresowaniem zwiedzających. Otrzymało też I nagrodę w Konkursie „Polski Mistrz Techniki Alarmowej 2008" organizowanym przez Polalarm w kategorii „urządzenia i systemy sygnalizacji włamania i napadu" oraz zdobyło w tym konkursie główną nagrodę – Złotą Zbroję.

Bezpośr. inf. Polalarm

Zapraszamy do obejrzenia fotoreportażu na stronie www.zabezpieczenia.com.pl

List Intencyjny o współpracy

W dniu 23 kwietnia 2008 r., na targach **Securex 2008** w Poznaniu, został podpisany **List Intencyjny** o współpracy pomiędzy Ogólnopolskim Stowarzyszeniem Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „**Polalarm**", a **Ukraińską Federacją Przemysłu Bezpieczeństwa**.

Ukraińska Federacja Przemysłu Bezpieczeństwa jest nową społeczną organizacją, mającą siedziby w 14 regionach Ukrainy. Cele Federacji są bardzo zbliżone do realizowanych przez Stowarzyszenie Polalarm. Do Zarządu Federacji wybrano kierowników znanych ukraińskich spółek – liderów na rynku technicznych środków ochrony.

List Intencyjny o współpracy podpisali: z ramienia Stowarzyszenia Polalarm – prezes Zarządu, Bogdan Tatarowski, oraz wiceprezes Andrzej Ryczer; z ramienia Ukraińskiej Federacji – Anatolii Dolynnyi oraz Bogdan Kupowicz.

W liście Stowarzyszenie Polalarm oraz Federacja wyrażają wolę współpracy mającej na celu udział firm reprezentowanych przez obie organizacje w realizacji zadań związanych z organizacją w Polsce i na Ukrainie Mistrzostw Europy w Piłce Nożnej Euro 2012. Obie organizacje zobowiązały się do realizacji wspólnych przedsięwzięć związanych z udziałem ich członków

w przygotowaniach i realizacji Euro 2012 oraz do ułatwienia wzajemnych kontaktów firm polskich i ukraińskich.

Bezpośr. inf. Polalarm

Zapraszamy do obejrzenia zdjęć na naszej stronie: www.zabezpieczenia.com.pl

ABI-TECH z Zielonej Góry Mistrzem Polski Instalatorów Systemów Alarmowych 2008

W drugim dniu Międzynarodowej Wystawy Zabezpieczeń **„Securex 2008"** odbyły się **eliminacje, a następnie finał I Mistrzostw Polski Instalatorów Systemów Alarmowych**.

Organizatorami mistrzostw, rozgrywanych po raz pierwszy w historii Securexu i branży zabezpieczeń technicznych, były Międzynarodowe Targi Poznańskie (MTP) i Polska Izba Systemów Alarmowych (PISA).

Rangę mistrzostw podkreślił minister spraw wewnętrznych i administracji, wicepremier RP **Grzegorz Schetyna**, obejmując nad nimi **honorowy patronat**.

Patronat medialny nad mistrzostwami zapewniły redakcje czasopism branżowych: *Systemy Alarmowe*, *Twierdza* i *Zabezpieczenia*.

KROK PO KROKU PO MISTRZOWSKIE TYTUŁY

10 października 2007 r.

MTP i PISA podpisały porozumienie o współpracy w sprawie organizacji, w ramach programu Międzynarodowej Wystawy Zabezpieczeń „Securex", Mistrzostw Polski Instalatorów Systemów Alarmowych (MPISA).

11 grudnia 2007 r.

Organizatorzy powołali niezależną Komisję Konkursową w składzie: Włodzimierz Cieślak (przewodniczący), Włodzimierz Matlak, Stefan J. Siudalski.

11 stycznia 2008 r.

Rozpoczęła się twórcza praca na potrzeby kwalifikacji i eliminacji mistrzostw. Nad pytaniami i odpowiedziami (trzy odpowiedzi, tylko jedna prawidłowa) pracowali indywidualnie doświadczeni wykładowcy Ośrodka Szkoleniowego Polskiej Izby Systemów Alarmowych (OS PISA): Maksymilian Majerski, Andrzej Tomczak, Stefan J. Siudalski, Włodzimierz Matlak. Prezes PISA Mirosław Krasnowski wybrał na potrzeby kwalifikacji 20 pytań. Na dwa dni przed rozpoczęciem eliminacji zdecydował, które z prawie stu pytań weszły do zestawu 50 pytań eliminacyjnych.

12 lutego 2008 r.

Prezesi MTP i PISA zwrócili się do prezesów organizacji branżowych z prośbą o życzliwe zainteresowanie inicjatywą i jak najszerszy udział firm członkowskich ich organizacji w tym nowatorskim przedsięwzięciu.

19 lutego 2008 r.

Wiceprezes Rady Ministrów RP, minister spraw wewnętrznych i administracji Grzegorz Schetyna objął patronat honorowy nad mistrzostwami.

21 lutego 2008 r.

Kilkaset znanych firm branży ochrony, wykonujących zadania zabezpieczenia technicznego, otrzymuje komunikaty o organizacji mistrzostw i rodzajach konkurencji

wraz z propozycjami udziału w rywalizacji i współpracy technicznej.

6 marca 2008 r.

W skład Komitetu Honorowego mistrzostw wchodzą: Przemysław Trawa – prezes Zarządu MTP, Mirosław Krasnowski – prezes Zarządu PISA, Marta Dynakowska – z-ca red. naczelnego *Systemów Alarmowych*, Mirosława Rulińska – red. naczelna *Twierdzy*, Teresa Karczmarzyk – red. naczelna *Zabezpieczeń*, Marek Bielski – przewodniczący Rady Programowej OS PISA.

2 kwietnia 2008 r.

Zakończenie kwalifikacji. Dziewięć spośród kilkunastu zespołów, które uzyskały najlepsze wyniki z testów kwalifikacyjnych (każdy zawodnik odpowiadał na 10 pytań technicznych), otrzymuje potwierdzenie udziału w eliminacjach i zaproszenie do przyjazdu do Poznania. Jest wśród nich zespół ABI-TECH Grzegorz Walacik z Zielonej Góry w składzie: Jacek Marcinkiewicz i Wojciech Pawlak. W kwalifikacjach zajmują drugie miejsce. Organizatorzy zwracają uwagę na **Wojciecha Pawlaka**, który **jako jedyny spośród wszystkich uczestników kwalifikacji odpowiedział bezbłędnie na wszystkie pytania**.

Pierwsze miejsce w kwalifikacjach zdobywa zespół Microsystem z Sopotu w składzie: Jacek Zieliński i Mariusz Waś. Trzecie miejsce, na tym etapie rywalizacji, wywalczył zespół Spółdzielni Usługowej Uniwersum z Warszawy w składzie: Jakub Dziedzic i Andrzej Sypuła. Przyszły finalista – zespół Dyskam z Krakowa – zdobył tylko jeden punkt mniej od zespołu Uniwersum i dwa punkty mniej od przyszłego mistrza.

Zaproszenie na eliminacje otrzymują także zespoły: Expert B.C. z Warszawy (problemy rodzinne jednego z zawodników uniemożliwiły zespołowi dalszą rywalizację), Skorpion Grupa z Warszawy, Komages z Gorzowa Wielkopolskiego, Safe System z Poznania, ARES – Agencja Detektywistyczna i Ochrony z Bydgoszczy.

8 kwietnia 2008 r.

Znane są wszystkie firmy, które zadeklarowały pomoc techniczną przy realizacji finałów mistrzostw i które otrzymały od organizatorów tytuł partnera technicznego. Opiekę nad konkurencją nr 1 (zmontowanie zewnętrznego punktu kamerowego i ustawienie zadanych parametrów) przejmuje AAT Trading Company z Warszawy, nad konkurencją nr 2 (zmontowanie przewodowego systemu sygnalizacji włamania i napadu) – Satel z Gdańska, nad konkurencją nr 3 (zaprogramowanie bezprzewodowego systemu sygnalizacji włamania i napadu) – Siemens z Warszawy. Wyposażenie parku mistrzostw w urządzenia do transmisji wizyjnej przebiegu finałów zapewniło GE Security Polska z Gdańska. Microsystem z Sopotu podejmuje się zadania instalacji systemu telewizyjnego i przekazu obrazu z kilku kamer na zamontowany staraniem MTP pokaźnych rozmiarów telebim. Pronal ze Szczecina zbuduje i obsłuży stację monitorowania na potrzeby konkurencji związanych z systemami alarmowymi.

17 kwietnia 2008 r.

Rozpoczyna się budowa i aranżacja kilkusetmetrowego parku mistrzostw. Dyrektor wystawy Securex Bartosz Zeidler wraz z Zespołem Organizacji Targów i Marcinem Jędrzejczykiem, wielce aktywnym, we współpracy z PISA i jej partnerami technicznymi w przygotowaniu organizacyjno-technicznym mistrzostw, dbają o każdy szczegół mający znaczenie dla przebiegu eliminacji i konkurencji finałowych.

22 kwietnia 2008 r.

W parku mistrzostw trwają ostatnie prace instalacyjne urządzeń stanowisk konkursowych oraz próby techniczne mikrofonów i współdziałania kamer systemu telewizji dozorowej z telebimem.

23 kwietnia 2008 r.

Godz. 10.30. Na antresolę pawilonu 3A, gdzie zbudowano salę szkoleniową, służącą eliminacjom mistrzostw, wchodzą zawodnicy. Punktualnie o godz. 10.45 prezesi MTP i PISA, w towarzystwie innych członków Komitetu Honorowego i Komisji Konkursowej, witają zespoły i dokonują oficjalnego otwarcia I MPISA. Tuż po tym przewodniczący komisji otrzymuje koperty z pięćdziesięcioma pytaniami testowymi dla każdego z zawodników. Komisja nie zna tych pytań, nie zna również odpowiedzi. Na potrzeby oceny prawidłowości rozwiązań otrzymuje tylko specjalne szablony. Zestaw pytań

pozostał do końca tajemnicą prezesa PISA i dyrektora Biura Organizacyjnego Mistrzostw.

Godz. 10.55. Komisja rozdała koperty z pytaniami. Zawodnicy są gotowi. Za dwoma stolikami stoją dwa puste foteliki. Brakuje zespołu Uniwersum z Warszawy. Przewodniczący Komisji decyduje, że na otwarcie kopert wszyscy oczekiwać będą do zaplanowanej w scenariuszu i oficjalnych komunikatach godziny 11.00. Sześćdziesiąt sekund przed tym czasem na antresolę wbiega zespół Uniwersum. Zdążyli. Zabytkowy stoper zaczął odmierzać regulaminowe 25 minut.

Godz. 11.25. Koniec testu. Zawodnicy opuszczają antresolę. Przed wszystkimi godzina niepewności i oczekiwania na wyniki. W tym czasie na teren targów przybywa dyrektor Departamentu Bezpieczeństwa Publicznego MSWiA Zbigniew Adamowicz, reprezentujący patrona honorowego mistrzostw – ministra Grzegorza Schetynę.

Godz. 12.20. Na antresoli przed zawodnikami kula z tulejami do losowania stanowisk finałowych, identyfikatory i żółte koszulki finalistów. Na dole w parku mistrzostw podium dla trzech najlepszych zespołów. Obok podium stolik z pucharami i nagrodami. To wszystko dla zwycięzców eliminacji, zespołów: Dyskam (68 pkt.), ABI – TECH (56 pkt.) i Microsystem (53 pkt.). Punkty zdobyte w eliminacjach będą istotne przy braku rozstrzygnięć w konkurencjach finałowych. Dalsze miejsca w eliminacjach, w kolejności, zdobyły zespoły: Skorpion Grupa (51 pkt.), ARES (50 pkt.), Uniwersum (49 pkt.), Safe System (47 pkt.), Komages (45 pkt.).

Indywidualnie największą wiedzą wykazał się **Czesław Boroń z Dyskamu**, uzyskując 39 pkt. na 50 możliwych. **Drugi był Jacek Zieliński z Microsystemu** (32 pkt.), **a trzeci Andrzej Sypuła z Uniwersum** (30 pkt.). Pozostali zawodnicy zdobyli od 19 do 29 pkt.

Godz. 13.00. Do parku mistrzostw wchodzą finaliści, Komisja Konkursowa i prowadzący finały Georgis Bogdanis (z wyboru członek Rady Nadzorczej PISA), który po zakończeniu mistrzostw zostanie nieoficjalnie uznany przez organizatorów, wielu obserwatorów i przedstawicieli mediów branżowych za najlepszego prezentera w branży zabezpieczeń technicznych i najlepszego znawcę tej branży wśród prezenterów. Prowadzący uroczystość zakończenia mistrzostw dyrektor Biura Organizacyjnego zapomniał z wrażenia podziękować Georgisowi Bogdanisowi za jego nieprzeciętną sprawność prezenterską i wyrazić uznanie dla ujawnionego publicznie talentu.

Godz. 13.30. Przewodniczący Komisji Konkursowej daje sygnał do rozpoczęcia pierwszej konkurencji. Czas regulaminowy wykonania zadania – 20 minut. Zawodnicy montują punkt kamerowy i „ustawiają" obiektywy. Wzorcem do oceny jakościowej jest stojący na podwyższeniu w odległości kilkunastu metrów Rotakin – specjalnie na tę okoliczność zakupiony w Wielkiej Brytanii przez PISA. Zadowolenia nie kryją wykładowcy zagadnień CCTV OS PISA, dla których Rotakin stanie się narzędziem edukacyjnym.

Limitu czasowego nie wykorzystuje zespół ABI – TECH. Zgłaszają wykonanie zadania przed czasem. ABI – TECH wykazuje najwyższą sprawność także w drugiej konkurencji. Zespoły Dyskam i Microsystem czują presję rywala. Komisja nie może ujawniać wyników poszczególnych konkurencji. Trzecia konkurencja sprawia wszystkim największą trudność. Limit czasowy, tym razem 25 minut, okazał się niewystarczający dla zaprogramowania wszystkich elementów systemu.

W trakcie zmagań zawodników ze sprzętem oglądamy na telebimie obrazy ze stanowisk konkursowych, przyglądamy się publiczności, poznajemy prezentację wizyjną partnerów technicznych mistrzostw. Z parkietu parku mistrzostw wielokrotnie startuje i krąży nad publicznością i zawodnikami miniatu-

rowy śmigłowiec z zamontowaną kamerą, którego zręczność i nieograniczone możliwości manewrowe pozwalają dotrzeć w każdy zakątek i obserwować, a następnie pokazywać na telebimie wybrane przez operatora osoby i obiekty.

Godz. 15.15. Po prawie dwóch godzinach zmagań finaliści opuszczają stanowiska konkursowe. Komisja ocenia wykonanie ostatniego zadania, podsumowuje wyniki zapisane w kartach ocen i sporządza protokół z finałów. Kolejny raz startuje śmigłowiec. Prezenter finałów przypomina publiczności uczestników konkursów finałowych. Podnosi napięcie w oczekiwaniu na ogłoszenie ostatecznych rozstrzygnięć. Do parku mistrzostw przybywa dyrektor Departamentu Bezpieczeństwa Publicznego MSWiA Zbigniew Adamowicz w towarzystwie prezesa MTP Przemysława Trawy, prezesa PISA Mirosława Krasnowskiego i pozostałych członków Komitetu Honorowego Mistrzostw. W centralnym miejscu parku zajmują miejsca wszyscy uczestnicy eliminacji, przedstawiciele partnerów technicznych i finaliści – główni bohaterowie uroczystości.

Godz. 15.50. Dyrektor Biura Organizacyjnego otwiera uroczystość zakończenia mistrzostw. Do uczestników rywalizacji, partnerów technicznych, patronów medialnych, organizatorów i obserwatorów zwraca się dyrektor Zbigniew Adamowicz. W imieniu patrona honorowego – wicepremiera Grzegorza Schetyny przekazuje wszystkim serdeczne gratulacje i życzenia pomyślności w kontynuacji przedsięwzięcia – ważnego zarówno dla branży ochrony, jak i dla realizacji programów związanych z szeroko rozumianym bezpieczeństwem. Podobne słowa wyrażają prezesi MTP i PISA, którzy następnie przekazują uczestnikom eliminacji i partnerom technicznym mistrzostw okolicznościowe dyplomy.

Wreszcie chwila, na którą oczekiwano najbardziej – ogłoszenie wyników mistrzostw. W finale każdy zespół mógł zdobyć maksymalnie 36 pkt. Na podium, w pierwszej kolejności, staje zespół Microsystem z Sopotu (20,7 pkt.) w składzie: Mariusz Waś i Jacek Zieliński – zdobywcy tytułu II Wicemistrza Polski. Na wyższy stopień podium wchodzi następnie zespół Dyskam z Krakowa (22,3 pkt.) w składzie: Czesław Boroń i Grzegorz Masłowski – zdobywcy tytułu I Wicemistrza Polski. W tym momencie unoszą się w górę ręce zwycięzców. Najwyższy stopień podium zajmuje **Mistrz Polski Instalatorów Systemów Alarmowych '2008** – zespół **ABI – TECH z Zielonej Góry** (27 pkt.) w składzie: **Jacek Marcinkiewicz** i **Wojciech Pawlak**.

Finaliści mistrzostw odbierają z rąk dyrektora Departamentu Bezpieczeństwa Publicznego MSWiA Zbigniewa Adamowicza puchary oraz indywidualne i zespołowe dyplomy Ministra, a od prezesów MTP i PISA indywidualne nagrody rzeczowe w postaci komputerów przenośnych Toshiba Satellite A200-1SN, systemów nawigacji GPS NavRoad NR750F i aparatów cyfrowych Canon PowerShot SX 100 IS. Otrzymują także upominki od partnerów technicznych mistrzostw.

Godz. 16.20. Przy błysku fleszy aparatów patronów medialnych dyrektor Zbigniew Adamowicz wyraża życzenie spotkania za dwa lata, podczas drugiej edycji mistrzostw, i ogłasza zakończenie I Mistrzostw Polski Instalatorów Systemów Alarmowych.

Godz. 16.30. W tym momencie rozpoczyna się czas podsumowań, dyskusji nad zdobytymi doświadczeniami, czas przygotowań do organizacji **w 2010 roku II Mistrzostw Polski Instalatorów Systemów Alarmowych**.

Chwilę po zakończeniu mistrzostw organizatorzy dowiadują się, że partnerzy techniczni – opiekunowie konkurencji finałowych (AAT-T, Satel i Siemens) zaproszą do siebie finalistów mistrzostw, aby – już bez emocji – poznać ich opinie o urządzeniach i systemach wykorzystywanych do zadań konkurencji finałowych, porozmawiać o potrzebach, możliwościach i warunkach doskonalenia technik instalatorskich.

Biuro Organizacyjne I MPISA wyraża wielkie podziękowanie za wsparcie i współpracę kierownictwu MTP, dyrektorowi Projektu targów Securex, pracownikom Zespołu Organizacji Targów, Komisji Konkursowej, patronom medialnym, partnerom technicznym, wykładowcom OS PISA i prezenterowi finałów. Firmom branży *security* uczestniczącym w mistrzowskich rywalizacjach, ich Zespołom i Zawodnikom przekazujemy raz jeszcze gratulacje i wyrazy szacunku i uznania za gotowość poddania wiedzy i umiejętności zawodowych pod publiczną ocenę.

Henryk Dąbrowski
dyrektor Biura Organizacyjnego I MPISA
Bezpośr. inf. PISA

Zapraszamy do obejrzenia fotoreportażu na stronie: www.zabezpieczenia.com.pl

Securex 2008

wczoraj i dziś

Po raz kolejny na terenie MTP (Międzynarodowych Targów Poznańskich) w Poznaniu, w dniach 22–25 kwietnia 2008 r., odbyła się Międzynarodowa Wystawa Zabezpieczeń Securex 2008, a w dniu 23 kwietnia towarzysząca jej konferencja „Urządzenia i sposoby zabezpieczenia mienia".

Konferencja została zorganizowana przez Stowarzyszenie Inżynierów i Techników Przemysłu Materiałów Budowlanych – oddział w Poznaniu, MTP, przy współpracy z Ogólnopolskim Stowarzyszeniem Inżynierów i Techników Systemów Zabezpieczeń „Polalarm" oraz Polską Izbą Przemysłowo-Handlową Budownictwa w Poznaniu.

Wystawa Securex odbyła się po raz pierwszy w poznańskim Domu Technika w roku 1988. W roku 1986 niżej podpisany wystąpił z ramienia Narodowego Banku Polskiego do COBR „Metalplast"(obecnie Instytut Techniki Budowlanej, ITB – przyp. red.) z prośbą o wykonanie szaf pancernych dla NBP w zakładzie doświadczalnym w Buku. Bazował przy tym na dokumentacji konstrukcyjnej banku i rozwiązaniu mechanizmu centralnego swojego indywidualnego pomysłu, na które otrzymał patent Urzędu Patentowego. COBR „Metalplast" wykonał dla NBP partię ok. 200 szaf pancernych. Był to jeden z czynników inicjujących zorganizowanie przez kolegów z COBR i MTP międzynarodowych targów Securex.

Securex gromadzi wytwórców, sprzedawców i użytkowników z dużych i małych firm międzynarodowych i obecnie daje pełny przegląd zabezpieczeń technicznych mienia, pokazując nowe trendy i rozwiązania. Niżej podpisany od początku współpracuje z organizatorami i bierze udział we wszystkich kolejnych konferencjach Securex od roku 2005 jako przedstawiciel Stowarzyszenia Inżynierów i Techników Mechaników Polskich (SIMP) oraz jako prezes Sekcji Mechanicznych Urządzeń Zabezpieczających (MUZ).

Wśród wielu firm międzynarodowych, prezentujących swoje oferty w zakresie zabezpieczeń, niżej podpisany z satysfakcją odnotował obecność wytwórców mających styczność bądź zaprzyjaźnionych z Sekcją MUZ SIMP. Wymienić tu trzeba firmy :

- ZM Kłos – Zdzisława (ojciec) i Zbigniewa (syn) Kłosów, członków zwyczajnych Sekcji MUZ SIMP. Firma ZM Kłos od lat 60-tych, początkowo na podstawie dokumentacji konstrukcyjnej NBP, wykonuje różne rodzaje mechanicznych urządzeń zabezpieczających, sukcesywnie je modernizując i wprowadzając nowe uruchomienia (np. wrzutnie, multisejfy, dyspensery) na światowym poziomie, nasycone elektroniką zapewniającą wykonywanie wielu rozmaitych funkcji.
- Pol-Ital – prowadzona od roku 1989 przez Ryszarda Karniewskiego, członka wspierającego Sekcji MUZ SIMP. Firma Pol-Ital jest wyłącznym dystrybutorem mechanicznych i sterowanych elektronicznie (co umożliwia

realizację wielu funkcji) doskonałych zamków skarbcowych i zabezpieczeniowych amerykańskiej firmy Sargent&Greenleaf, zamków zabezpieczeniowych jedno- i wielopunktowych i okuć przeciwpanicznych włoskiej firmy S.A.B. Serrature oraz pojemników zbiorczych i walizek wyposażonych w elektronikę zapewniającą bezpieczny transport pojemników i kaset (np. do bankomatów), a także depozytorów elektronicznych gotówki niemieckiej firmy Villiger.
- Metalkas, w której oddziale lubelskim pracuje członek zwyczajny Sekcji MUZ SIMP – Artur Wysocki. Firma Metalkas od 1957 roku, poczynając od kaset, rozwija produkcję różnych typów sejfów gabinetowych, meblowych, ściennych, kas pancernych, kłódek, wyposażenia stanowisk kasjerskich, szaf na broń i na dokumenty niejawne oraz biurowe i różnorodnego wyposażenia biurowego i dodatkowego.
- Konsmetal, jeszcze przed momentem powstania w roku 1991 – w latach 80-tych, jako Konsbud – konsultujący z niżej podpisanym wyposażenie w mechaniczne urządzenia zabezpieczające siedziby powstałego Banku Ziemskiego przy ul. Parkingowej w Warszawie. Firma jest od początku zaprzyjaźniona z Sekcją MUZ SIMP. Konsmetal od początku działalności rozwija wytwórstwo szeregu typów sejfów, kas pancernych, szaf, skarbców, drzwi skarbcowych i całej gamy produktów depozytowo-bankowych wyposażonych w elektronikę, jak multisejfy, multikasy, dyspensery, wrzutnie etc.
- Systemy Zabezpieczeń – Józef Matyjas prowadzone przez Józefa Matyjasa, czołowego eksperta polskiego od otwarć awaryjnych, wraz z synem i we współpracy ze znaną na świecie niemiecką firmą Adalberta Wendta. Józef Matyjas, z inicjatywy niżej podpisanego, od lat 80-tych prowadził szereg szkoleń mechaników zamknięć skarbcowych NBP w zakresie otwarć awaryjnych, a w styczniu br. prezentował dorobek w tym zakresie na konferencji zorganizowanej przez Sekcję MUZ SIMP. Firma wystawiła obecnie nową i bogatą ofertę ciągle doskonalonych narzędzi, przyrządów i urządzeń do awaryjnych otwarć MUZ.

Spośród innych firm prezentujących swoje oferty odnotować trzeba takie, jak:
- Kaba – międzynarodowa grupa przemysłowa, skupiająca wiele firm wytwarzających zabezpieczenia techniczne, w tym MUZ, zajmująca jedną z czołowych pozycji w branży w skali światowej. Przedstawiciele firmy prezentowali jej działalność na jednej z konferencji organizowanych przez Sekcję MUZ SIMP.
- Gunnebo – międzynarodowa grupa przemysłowa, podobnie skupiająca wiele firm wytwarzających zabezpieczenia techniczne, w tym powstałą w roku 1856 w Göeteborgu, firmę Rosengrens, znaną na całym świecie z najwyższej jakości drzwi skarbcowych i szaf pancernych oraz wyposażenia dla banków.
- Habeco – prowadząca działalność w obszarze zabezpieczeń od 1954 roku, a w Polsce od 2001 roku. Habeco jest jedną z największych firm europejskich w branży i wyróżnia się najwyższą jakością oraz oryginalnością konstrukcji i wzornictwa produkowanych wyrobów, takich jak różne typy sejfów, szaf, drzwi zabezpieczeniowych i skarbcowych, skarbców oraz różnorodne wyposażenie dodatkowe dla przedsiębiorstw i banków.
- Chubb safes – znana na świecie od XVIII wieku firma angielska, wyróżniająca się tradycyjną najwyższą jakością swoich sejfów.
- J&W – firma polska, zajmująca się od 1990 roku wytwórstwem i instalacją drzwi o zwiększonej odporności na włamanie, zwanych potocznie w handlu drzwiami antywłamaniowymi. J&W, jako pierwsza w tej branży, uzyskała w 1992 roku atest na drzwi o zwiększonej odporności na włamanie klasy „C", a od roku 1994 wszystkie jej wyroby mają certyfikaty klasy wydawane przez Zakład Certyfikacji MUZ działający przy Instytucie Mechaniki Precyzyjnej. Jest jedynym w Polsce producentem Panelu Kancelaryjnego do wydzielania pomieszczeń kancelarii tajnych.
- ISS – z Gorzowa Wlkp., oferująca ognioodporne sejfy i szafy na dokumenty.
- Odyniec – z Uzdowa, oferująca niestandardowe, o dowolnej konfiguracji, szafy na broń.
- Dyspenzer – oferująca różne typy multisejfów dla stanowisk kasjerskich z bogatą elektroniką zapewniającą kontrolę dostępu i funkcje opóźnień czasowych.
- Bastion – zajmująca się od 1991 roku sprzedażą nowych oraz używanych i odnawianych sejfów i kas pancernych, a także renowacją zabytkowych kas pancernych stanowiących arcydzieła rzemiosła z ubiegłych wieków.
- Fana – (obecnie DAD Polska) – któż nie pamięta zamków i okuć Fany z Poznania, występujących „etatowo" w drzwiach mieszkań w domach i blokach odbudowywanych i budowanych w „planie 3-letnim" i w „planie 6-letnim" po II wojnie światowej. Firma przedstawiła bogatą ofertę nowych typów zamków bezpośredniego ryglowania (w tym wielopunktowego) wierzchnich, wpuszczanych, wkładek bębenkowych, kluczy, zamków przemysłowych (zakrętkowych i rygli), przytrzymywaczy, zaczepów elektromagnetycznych, samozamykaczy, zapornic i wielu innych rodzajów okuć drzwiowych.
- Satel – z Gdańska, prezentująca ciekawą ofertę inteligentnych systemów alarmowych: sygnalizacji włamania i napadu, kontroli dostępu, monitoringu i telewizji dozorowej.

Spośród referatów wygłoszonych na konferencji „Urządzenia i sposoby zabezpieczenia mienia" na wyróżnienie zasługuje referat inż. Zbigniewa Czajki z ITB O/Poznań, omawiający szczegółowo wymagania w zakresie bezpieczeństwa okien i drzwi, wynikające z nowowprowadzanych norm europejskich.

Kończąc, należy zwrócić uwagę na to, jak ważną pozycję w branży osiągnęły z upływem lat wystawa, targi i konferencja, i to zarówno dla producentów, jak i dla użytkowników. Securex bez wątpienia przyczynia się do generowania nowych pomysłów i nowych technologii, do podnoszenia standardów i poziomu jakości wyrobów i usług.

Opracował:
Józef Rudziński
prezes Sekcji MUZ SIMP

Axis, Bosch i Sony
podejmują strategiczną współpracę

Firmy Axis Communications, Bosch Security Systems oraz Sony Corporation, liderzy rynku sieciowych rozwiązań wideo, podjęły strategiczną współpracę w celu standaryzacji interfejsu cyfrowych urządzeń wizyjnych. Nowy standard oznacza większą elastyczność zarówno dla instalatorów, jak i użytkowników sieciowego sprzętu wizyjnego.

Firmy Axis Communications, Bosch Security Systems i Sony Corporation ogłosiły podjęcie współpracy nad powołaniem otwartego forum, którego celem będzie opracowanie standardu interfejsu sieciowych urządzeń wizyjnych. Dotąd nie było jednego standardu definiującego sposób komunikacji pomiędzy sieciowymi urządzeniami wizyjnymi, takimi jak kamery, nadajniki wizyjne czy systemy zarządzania sygnałem wizyjnym. Nowy standard ma objąć interfejsy dla nadawania sygnału wizyjnego, wykrywania urządzeń, metadanych itp. Podstawy standardu, w tym kluczowe elementy współpracy pomiędzy sieciowymi urządzeniami wizyjnymi, zostaną przedstawione w październiku 2008 roku na pokazie systemów zabezpieczeń w Essen w Niemczech.

Podstawowym celem wdrożenia nowego standardu jest ułatwienie integracji sieciowych urządzeń wizyjnych różnych marek oraz pomoc producentom, programistom i niezależnym dostawcom oprogramowania w zapewnieniu współpracy pomiędzy urządzeniami. Ujednolicony otwarty standard to również większa swoboda wyboru dla użytkowników końcowych, którzy dzięki możliwości zakupu urządzeń różnych producentów będą mogli stworzyć system, który w pełni odpowiada ich potrzebom. Inicjatywa stworzenia wspólnego standardu pokazuje też silne zaangażowanie firm Axis, Bosch i Sony w przejście od rozwiązań analogowych do cyfrowych.

W powołanym przez Axis, Bosch i Sony forum będą mogły wziąć udział wszystkie firmy i zainteresowane grupy, które pragną wnieść swój wkład w rozwój interfejsu cyfrowych urządzeń wizyjnych. Forum zostanie powołane w czwartym kwartale 2008 roku.

– *Z radością ogłaszam nawiązanie współpracy pomiędzy naszymi firmami* – powiedział Ray Mauritsson, prezes Axis Communications. – *Otwarty standard znacząco ułatwi instalatorom i użytkownikom końcowym korzystanie z możliwości, jakie oferuje dozór wizyjny oparty na sieci IP.*

– *Ta współpraca to ogromy krok w kierunku ustanowienia międzynarodowego otwartego forum poświęconego sieciowemu dozorowi wizyjnemu* – powiedział Gert van Iperen, wiceprezes Bosch Security Systems. – *Dla producentów sieciowego sprzętu wizyjnego i oprogramowania forum oraz stworzony przez nie standard to skuteczny sposób na zapewnienie kompatybilności produktów.*

– *Punktem wyjścia dla naszej współpracy było wspólne przekonanie, iż otwarty standard przyniesie ogromne korzyści użytkownikom i wszystkim osobom z branży zabezpieczeń* – powiedział Yoshinori Onoue, starszy wiceprezes i kierownik korporacji Sony. – *W tej chwili trwają intensywne prace przedstawicieli firm Axis, Bosch i Sony nad opracowaniem podstaw standardu oraz wytycznych dla forum standaryzacyjnego.*

Bezpośr. inf. Mmd
Corporate Public Affairs&Public Relations Consultants

Firma Bosch rozszerza funkcjonalność bezprzewodowego, cyfrowego systemu dyskusyjnego DCN Wireless

Nowe udogodnienia związane z tłumaczeniami i większe możliwości połączeń

Firma **Bosch Security Systems** wprowadziła istotne rozszerzenia funkcjonalności bezprzewodowego, cyfrowego systemu dyskusyjnego **DCN Wireless**. Bezprzewodowe moduły dyskusyjne mogą być teraz łączone z przewodowymi modułami dyskusyjnymi DCN NG, w prosty i efektywny sposób rozbudowując wielkość każdego przewodowego systemu konferencyjnego DCN Next Generation. Oprócz tego, wraz z funkcjami dyskusyjnymi i głosowania, bezprzewodowy system DCN Wireless oferuje obecnie obsługę 10 języków tłumaczeń symultanicznych, umożliwiając uczestnikom śledzenie dyskusji w ich własnych językach, wybieranych przy pomocy przełącznika wyboru kanałów w bezprzewodowych modułach dyskusyjnych.

Wprowadzony w roku 2006 bezprzewodowy system dyskusyjny DCN Wireless został zaprojektowany z myślą o wielofunkcyjnych pomieszczeniach, szczególnie gdy istnieje konieczność szybkiego montażu i demontażu urządzeń na potrzeby różnych konfiguracji i zmiennych liczb uczestników. Aby dopasować się do zmian konfiguracji, do dyspozycji jest 150 atrakcyjnie zaprojektowanych stołowych pulpitów uczestników, które można w każdej chwili dowolnie rozmieszczać i przestawiać. System może być instalowany, przestawiany i obsługiwany praktycznie bez wpływu na integralność zabytkowych wnętrz, co oznacza, że nie trzeba się martwić o naruszenie bezcennych dekoracji czy estetyki wystroju wytwornych sal. Pojedynczy moduł bezprzewodowego punktu dostępowego (WAP), który może być montowany na ścianie, suficie lub statywie, ma efektywny zasięg 30 m. Jest to z reguły więcej niż potrzeba w pomieszczeniu konferencyjnym z maks. 150 uczestnikami, zależnie od rozkładu siedzeń.

Bezpośr. inf. Robert Bosch Security Systems

IDC IT Security Roadshow 2008
– relacja z konferencji

Tegoroczna, szósta edycja **konferencji IT Security Roadshow** odbyła się pod hasłem „**Chronić Biznes: Technologia i Ludzie**" w hotelu Marriott w Warszawie 20 marca 2008 r. Między 13 lutego a 18 listopada 2008 r. przewidziano łącznie 23 takie konferencje, organizowane przez IDC w większości stolic Europy Środkowej, a także na Bliskim Wschodzie i w Afryce. Siódma z nich miała miejsce w Warszawie.

Uczestnikami konferencji byli profesjonaliści w dziedzinie bezpieczeństwa informatycznego, głównie dyrektorzy ds. informatyki i ds. bezpieczeństwa informacji oraz szefowie działów informatycznych instytucji i przedsiębiorstw. Referaty konferencyjne (łącznie 20, nie licząc wystąpień przedstawicieli IDC) przygotowali zarówno partnerzy IDC, wśród których znaleźli się światowi liderzy w dziedzinie oprogramowania i rozwiązań informatycznych, także wspomaganych sprzętowo, jak i zaproszeni eksperci. Na stoiskach, usytuowanych w oddzielnej sali oraz w kuluarach, można było zapoznać się bliżej z ofertą partnerów IDC oraz spotkać się z ich przedstawicielami. Nasze czasopismo było jednym z partnerów medialnych konferencji.

Pierwsze dwie sesje, które odbyły się po krótkim powitaniu przybyłych gości, miały charakter plenarny. Dwie sesje popołudniowe odbywały się równolegle, z możliwością wyboru przez uczestników konferencji interesujących ich tematów. Tematy sesji były następujące:

Sesja I: Bezpieczeństwo informacji, trendy w branży oraz ich skutki,
Sesja II: Nowości w zakresie ochrony przedsiębiorstw,
Sesja III: Zawód – Szef ds. Bezpieczeństwa,
Sesja IV: Rozwiązania z dziedziny zabezpieczeń.

Zgodnie z zapowiedzią IDC wszystkie prezentacje z konferencji będą dostępne do pobrania z witryny www.ide-cema.com. Do najbardziej interesujących wystąpień należały trzy omówione poniżej.

Tom Vavra z IDC CEMA wygłosił wykład wprowadzający na temat zmian w branży bezpieczeństwa informacji oraz ich skutków dla głównych specjalistów ds. zabezpieczeń. Przedstawił m.in. dziesięć przewidywań na 2008 rok dotyczących bezpieczeństwa informatycznego oraz sześć zaleceń dla szefów bezpieczeństwa IT.

Główny doradca ds. bezpieczeństwa firmy Microsoft w Wielkiej Brytanii, **Edward P. Gibson** (były agent specjalny FBI z dwudziestoletnim stażem, uznany ekspert od śledztw w zakresie międzynarodowych operacji prania brudnych pieniędzy, szpiegostwa ekonomicznego oraz kradzieży wartości intelektualnej), omówił zagadnienia związane z dynamicznie rozwijającą się przestępczością internetową.

Gość specjalny konferencji – **Simon Singh** – brytyjski pisarz, dziennikarz, producent telewizyjny, autor książki *Księga szyfrów – od starożytnego Egiptu do kryptografii kwantowej* przywiózł ze sobą i zaprezentował podczas swojego wystąpienia działający egzemplarz niemieckiej maszyny szyfrującej Enigma, co stanowiło niewątpliwą atrakcję konferencji. Wart podkreślenia jest fakt, że w odkryciu tajemnicy Enigmy i rozszyfrowaniu zakodowanych za jej pomocą wiadomości najbardziej znaczący udział mieli polscy matematycy.

Sesje popołudniowe rozpoczęły się od prezentacji przez przedstawicieli IDC Polska wyników ankiet zebranych podczas ubiegłorocznej edycji konferencji (IDC IT Security 2007). Za rok, podczas następnej konferencji z tego cyklu, zostaną omówione ankiety tegoroczne.

Adam Bułaciński
Redakcja

System inteligentnego domu EIB
w krakowskim apartamentowcu

DG Elpro, wspólnie z Przedsiębiorstwem Budownictwa Przemysłowego Budostal-3, realizuje system automatyki budynków w jednym z największych apartamentowców w Krakowie.

Apartamenty Ludwinów będą spełniać wymagania stawiane **budynkom inteligentnym**. Zainstalowany zostanie **zintegrowany system zarządzania budynkiem BMS**. Części wspólne będą wyposażone w systemy oszczędzania energii, automatyczne systemy sterowania basenem i częścią rekreacyjną, a także systemy zarządzania wentylacją. Oprócz automatyki sterowania, budynek będzie wyposażony w rozbudowany system monitorowania i alarmowania. Dla zapewnienia mieszkańcom bezpieczeństwa każdy apartament będzie miał zintegrowany system sygnalizacji włamania, kontroli dostępu oraz telewizji dozorowej.

W ramach technologii inteligentnego domu EIB wewnętrzne instalacje będą funkcjonować dzięki wielofunkcyjnym przyciskom sterującym Triton.

Pozwolą one na stosowanie funkcji:
– sterowania oświetleniem lokalnego i centralnego,
– sterowania roletami,
– sterowania selektywnym i centralnym ogrzewaniem,
– wybierania scen świetlnych,
– sterowania klimatyzacją.

Nowoczesne technologie w połączeniu z prestiżową lokalizacją Apartamentów Ludwinów znajdą zapewne uznanie nawet najbardziej wymagających mieszkańców.

Bezpośr. inf. DG Elpro

Nagłe awarie elektryczne
i sposoby przeciwdziałania ich skutkom

Skutki postępującego ocieplenia klimatu w postaci coraz częstszych i coraz bardziej gwałtownych burz stają się coraz bardziej odczuwalne również w Polsce. Niedawna **awaria sieci energetycznej w Goleniowie pokazuje**, jak ważne jest **zapewnienie zasilania awaryjnego** – nie tylko w szpitalach i bankach, gdzie takie rozwiązania są w zasadzie standardem, ale też w innych instytucjach, w firmach, a nawet w domach. Niespodziewane odcięcie zasilania albo zakłócenia w sieci elektrycznej, które są dużo częstszym zjawiskiem, mogą nie tylko przerwać pracę w najmniej spodziewanym momencie, ale także spowodować utratę cennych danych lub doprowadzić do uszkodzenia sprzętu komputerowego. Warto więc zawczasu przygotować się i zadbać o zabezpieczenie zasilania awaryjnego dla sprzętu wspierającego działanie krytycznych dla firmy procesów i aplikacji. Energia elektryczna, nad której dostępnością większość z nas na co dzień się nie zastanawia, staje się dobrem coraz cenniejszym. Coraz więcej kwestii w naszym życiu jest uzależnionych od elektryczności, co sprawia, że jej wartość rośnie. Dostępność do energii jest dla nas sprawą oczywistą. Nie zastanawiamy się nad konsekwencjami jej braku, dopóki nie usłyszymy w mediach, że szpitale odwołują zaplanowane operacje, bo zabrakło prądu.

Co roku wydarzenia w czasie miesięcy letnich udowadniają nam, jak bardzo nasze życie zależy od energii elektrycznej. Rok 2006 to fala upałów, jakich w Polsce nie było od dwustu lat. Polski PSE-Operator postanowił na kilka dni wstrzymać eksport energii elektrycznej, uzależniając to od pogody w następnych dniach. Zużycie energii elektrycznej było o 10 proc. wyższe niż rok wcześniej. Rozwój gospodarki powoduje coraz większe zużycie energii elektrycznej. Coraz więcej osób korzysta z klimatyzacji i urządzeń chłodzących. Nie zapominajmy, że tradycyjnie na lato planuje się wiele prac remontowych przed sezonem grzewczym. Wzrasta niebezpieczeństwo wystąpienia problemów z dostawą energii. Energia elektryczna staje się towarem deficytowym.

Przerwa w dostawie prądu w Warszawie 17 listopada 2006 r. uświadomiła nam, że dostawcy energii elektrycznej nie zawsze są w stanie chronić przed negatywnymi skutkami nagłego zaniku napięcia. Obok skrajnych warunków pogodowych, przestarzała sieć elektroenergetyczna i błąd ludzki stanowią najczęstsze powody niestabilności zasilania, których nie da się przewidzieć i którym nie sposób zapobiec. Każdy jest w nieunikniony sposób narażony na ryzyko uszkodzenia sprzętu, utraty danych i przestojów związanych z ponownym rozruchem w wypadku np. systemów informatycznych.

Bezpośr. inf. APC Polska

Extreme CCTV zapewnia nieprzerwany podgląd wideo Eurotunelu

Mierzący ponad 50 km długości Eurotunel, biegnący 37,8 km pod Kanałem La Manche (zwanym w Wielkiej Brytanii Kanałem Angielskim – przyp. red.), jest najdłuższym tunelem podwodnym na świecie. Przez międzynarodowych ekspertów w dziedzinie budowli lądowych w USA i w Europie jest uważany za „największy sukces infrastruktury XX wieku". Od czasu otwarcia wiosną 1994 roku przeprawiło się przez niego 212 milionów pasażerów i 196 milionów ton towarów.

Firma Extreme CCTV nie bez dumy dowiedziała się od operatora tunelu – grupy Eurotunnel, posiadającej koncesję na swoją działalność do 2086 roku, że zintegrowane kamery dzienno-nocne EX82 (IDN) tej firmy zapewniły ponad pięcioletni nieprzerwany podgląd wideo Eurotunelu.

Zgodnie ze wszelkimi standardami tunel ten jest środowiskiem ekstremalnym, z uwagi na wysokie ciśnienie powietrza, wilgotność i zasolenie otoczenia, ale kamery Extreme CCTV EX82 zdały tam egzamin.

– *Kamery Extreme CCTV zapewniły do chwili obecnej ponad pięcioletni nieprzerwany obraz Eurotunelu spod ziemi. Ze względu na lokalizację kamer jest dla nas ważne, że sprzęt ten wymaga stosunkowo niewiele serwisowania i jest zarówno odporny, jak i niezawodny* – twierdzi Richard Howkins, lider zespołu ds. utrzymania i sygnalizacji w grupie Eurotunnel.
– *Kamery wykonały fantastyczną robotę, działając przez ostatnie pięć lat bez usterek w tak trudnym otoczeniu, i jest to świadectwo wbudowanej w nasze produkty jakości* – powiedział Ian Crosby z Extreme CCTV.

EX82 zawiera kamerę, obiektyw oraz oświetlacz podczerwieni w jednej obudowie środowiskowej i zapewnia prawdziwie przyjazne dla instalatora rozwiązanie „*Plug and Play*" (ang. „podłącz i używaj"). Kamera została ostatnio zmodernizowana przez zastosowanie technologii podczerwieni Black Diamond i jest teraz znana jako EX82 Infrared Imager, dostarczając wysokiej jakości (nazwa handlowa: *High-Fidelity*) oświetlenie do obrazów nocnych o wysokiej rozdzielczości.

Kamery, które sprawdziły się praktycznie w wymagających zastosowaniach z zakresu bezpieczeństwa na całym świecie, odgrywają krytyczną rolę w systemie transportującym codziennie 300 pociągami średnio ponad 26000 pasażerów i 50000 ton produktów.

Redakcja

Źródło: Extreme CCTV

Kontrola granic będzie dominować na wystawie i konferencji ISNR 2008

Rozpoczęcie w kwietniu br. działalności nowej zunifikowanej Agencji Granicznej Wlk. Brytanii podkreśla znaczenie odpierania zagrożeń dla bezpieczeństwa narodowego, wynikających z terroryzmu, nielegalnej imigracji oraz przestępczości zorganizowanej.

Podczas **międzynarodowej wystawy i konferencji ISNR** (*International Security and National Resilience*) z zakresu bezpieczeństwa, która odbędzie się w londyńskim centrum wystawienniczym Olimpia 2 i 3 grudnia br., będą wystawiane technologie wymagane do optymalizacji efektywności zabezpieczania granic. Kluczowymi graczami z tego sektora zabezpieczeń, którzy już wpisali się na listę wystawców, są **Thales, EADS i Senstar-Stellar**.

Kontrola granic będzie także jednym z głównych tematów tegorocznej konferencji ISNR. Impreza ta, dotycząca także transportu oraz zabezpieczenia infrastruktury krytycznej, zgromadzi wiodące postacie z tej branży z całego świata w celu wymiany poglądów i doświadczeń. Na tym samym poziomie co wystawa będą także odbywać się bezpłatne seminaria, które pozwolą wystawcom na zademonstrowanie teorii i praktyki najnowszych technologii służących do zabezpieczania granic i innych, związanych z bezpieczeństwem.

Zgodnie z opinią ISNR sektor bezpieczeństwa staje się coraz bardziej zintegrowany, gdyż przedstawiciele zagranicznych jednostek oceny ryzyka, oficerowie łącznikowi linii lotniczych, pracownicy urzędów imigracyjnych i celnych współpracują z policją, aby granice stawały się coraz bardziej bezpieczne. W świetle tego organizatorzy ISNR zachęcają do nawiązywania indywidualnych kontaktów z kluczowymi agencjami i stowarzyszeniami w celu informowania ich o dominujących tematach wystawy i konferencji i zapewnienia, że odpowiadają one bieżącym potrzebom rynkowym.

Redakcja

Źródło: www.securityworldhotel.com

III Kongres Gospodarki Elektronicznej – relacja

III Kongres Gospodarki Elektronicznej odbył się 19 maja 2008 roku w Centrum Konferencyjnym Wojska Polskiego w Warszawie pod hasłem **„Technologia a nowoczesne i bezpieczne państwo – doświadczenia biznesu, które warto wykorzystać”**. Kongres został zorganizowany przez **Związek Banków Polskich** wraz z działającym przy nim **Forum Technologii Bankowych**. Partnerem merytorycznym imprezy była firma **NASK**. Udział w kongresie potwierdziło ok. 250 osób, głównie przedstawicieli instytucji bankowych (w tym 32 banków), biznesu (ponad 115 osób z 75 firm), środowisk naukowych, samorządów i różnych organizacji.

Wykład inauguracyjny wygłosili prezes Związku Banków Polskich **Krzysztof Pietraszkiewicz**, który przedstawił m.in. perspektywy rozwoju gospodarki elektronicznej i zagadnienia związane z jej **bezpieczeństwem**, oraz **Wojciech Cellary** z Akademii Ekonomicznej w Poznaniu, który omówił rolę innowacyjności w rozwoju gospodarki. Następnie odbyły się trzy sesje, dotyczące trendów w rozwoju gospodarki elektronicznej, płatności bezgotówkowych oraz baz danych jako podstawy **bezpiecznego obrotu gospodarczego**. Sesje popołudniowe rozpoczął **Dariusz Bogdan**, podsekretarz stanu w Ministerstwie Gospodarki, omawiając zamierzenia rządu w zakresie gospodarki elektronicznej.

Kolejna i ostatnia już sesja pt. **„Standardy bezpieczeństwa gospodarki narodowej”** obejmowała dwa bloki referatów. Pierwszy dotyczył nowych wyzwań biometrii i obejmował trzy wystąpienia.

Adam Czajka z NASK omówił **zalety i zagrożenia biometrii w bankowości** z dwóch różnych punktów widzenia: klienta i banku. **Tadeusz Woszczyński** z firmy Hitachi dokonał **przeglądu technologii biometrycznych** pod kątem ich **wykorzystania w bankowości od strony klienta i w bezpieczeństwie wewnętrznym banku** oraz przedstawił przykład udanego ich wykorzystania w bankowości japońskiej. **Włodzimierz Sosnowski** z firmy WASKO omówił natomiast dwa **projekty dokumentów elektronicznych**: Europejskiego Dokumentu Tożsamości oraz Paszportowego Systemu Informacyjnego, zwracając też uwagę na konieczność **zabezpieczania baz danych biometrycznych**.

Drugi blok był poświęcony niewykorzystanej – jak dotąd – szansie podpisu elektronicznego w Polsce i rozpoczął się od referatu **Elżbiety Włodarczyk** z Krajowej Izby Rozliczeniowej. Przedstawiono w nim korzyści płynące ze stosowania **podpisu elektronicznego jako jednego certyfikatu do wielu zastosowań**. W drugim referacie **Wacław Iszkowski** z Polskiej Izby Informatyki i Telekomunikacji zaprezentował różne poglądy na temat **celowości stosowania podpisu elektronicznego oraz zagadnienia praktyczne**, związane z wdrażaniem tej technologii w Polsce.

Podsumowania kongresu dokonał Krzysztof Pietraszkiewicz, zachęcając m.in. do stosowania w gospodarce elektronicznej wyłącznie rozwiązań najlepszych, ale nie tych, które są „mniejszym złem” i zwracając uwagę na **pierwszoplanową dla obrotu elektronicznego kwestię bezpieczeństwa**, którego poziom należy stale podnosić. Następnie odbyło się, po raz pierwszy w historii Kongresu Gospodarki Elektronicznej, wręczenie przedstawicielom instytucji zasłużonych dla rozwoju gospodarki elektronicznej w Polsce statuetek i dyplomów uznania Związku Banków Polskich (w trzech kategoriach). W kategorii „**Ambasador Gospodarki Elektronicznej**” nagrodzono prof. **Michała Kleibera**, prezesa PAN, i wyróżniono **Krzysztofa Rybińskiego** oraz **Sławomira Lachowskiego**, znanych ze swojej działalności bankowej. „**Partnerem Roku**” została **Krajowa Izba Rozliczeniowa**; jest to jednocześnie wyraz uznania dla wszystkich banków, które KIR założyły. Statuetkę i dyplom odebrał prezes KIR, **Kazimierz Małecki**. W tej kategorii wyróżniono także firmę **Blue Media** i jej prezesa **Sebastiana Ptaka**. Trzecią kategorią był „**Projekt Roku**”, a zwycięzcą **ING Bank Śląski**. Nagrodzonym pogratulował minister Dariusz Bogdan, po czym zebrani mieli okazję do nieformalnych rozmów i wymiany poglądów podczas uroczystego bankietu.

Adam Bułaciński
Redakcja

Spotkanie partnerów JVC Professional

relacja

Drugie już spotkanie partnerów JVC Professional, zorganizowane przez oficjalnego dystrybutora JVC Professional na terenie Polski, firmę Radioton z Krakowa, odbyło się w dniach 26–28 maja w Hotelu Turówka w Wieliczce.

To wyjątkowy hotel, można by rzec z duszą. Jego historia sięga roku 1811, gdy budynek pełnił funkcję warzelni soli. Budynek został wzniesiony na gruntach należących do miasta Wieliczka, na obszarze średniowiecznego folwarku zwanego „Tur". Stąd też pochodzi obecna nazwa obiektu – „Turówka".

Sąsiedztwo Kopalni Soli w Wieliczce (najstarszej funkcjonującej kopalni soli kamiennej na świecie, obiektu unikatowego na skalę światową, który jest obiektem zabytkowym a zarazem funkcjonującym zakładem górniczym, wpisanym na listę Światowego Dziedzictwa Kultury i Przyrody UNESCO), najbardziej znanego zabytku Wieliczki, było niewątpliwie dodatkową atrakcją. Przedstawiciele Radiotonu zorganizowali dla wszystkich chętnych wycieczkę do kopalni, podczas której można było dowiedzieć się między innymi, że w wyniku wydobywania przez górników soli kamiennej pod powierzchnią miasta wykształcił się podziemny labirynt górniczych wyrobisk na głębokości 9 poziomów – od 64 do 327 metrów w głąb ziemi.

Przyjazny, komfortowy, o wysokim standardzie hotel był idealnym miejscem do zapoznania się z nowościami w ofercie JVC, w szczególności w zakresie urządzeń IP, ale również do oderwania się od codziennych obowiązków.

Pierwszego dnia, po zwiedzaniu kopalni, Paweł Trojak, dyrektor Radiotonu, zaprosił gości na uroczystą integracyjną kolację.

Drugiego dnia zorganizowana była konferencja, podczas której Manager Systems Group JVC Professional Europe, Jochen Hahn, zaprezentował strategię firmy i funkcjonowanie jej struktur w Europie oraz tzw. *Case Studies* – ciekawe realizacje systemów CCTV wykorzystujących rozwiązania JVC. Na produkty CCTV przypada 35% obrotu JVC. Produkty CCTV są coraz tańsze, a rynek cały czas powiększa się. W ubiegłym roku zaszło w JVC wiele zmian. JVC kładzie bardzo duży nacisk na jakość i niezawodność swoich produktów.

O najnowszych produktach JVC opowiedział Alexander Wodok, Area Sales Manager, zwracając przy tym uwagę na korzyści finansowe, wynikające ze stosowania najnowszych rozwiązań. Przykładowo – krosownica, czyli element systemu CCTV, który w telewizji analogowej kosztował bardzo dużo, obecnie jest zastąpiony przez znacznie prostsze i bardziej elastyczne rozwiązanie cyfrowe. Podczas tegorocznej wystawy IFSEC zaprezentowano pierwszą megapikselową kamerę JVC – model VX35. Zapewnia ona 1,3 mln pikseli i będzie dostępna w sprzedaży pod koniec lata br. Oprócz kamer JVC jest też producentem monitorów. Należy podkreślić, że wszystkie modele są montowane w metalowych obudowach, co wpływa bezpośrednio na ich trwałość i niezawodność. Odnośnie niezawodności – JVC jako jeden z nielicznych producentów podaje parametry niezawodnościowe swoich produktów – tzw. MTBF, czyli średni czas między uszkodzeniami (ang.: *Mean Time Between Failures*). Wynoszą one od 60 do 80 tysięcy godzin i są nawet (jak twierdzi Alexander Wodok) kilkukrotnie lepsze niż w przypadku produktów konkurencyjnych. Inni producenci z reguły nie podają tych danych, traktując je jako poufne. Z uwagi na wysoką jakość i niezawodność produktów JVC są one stosowane, podobnie jak produkty innych uznanych marek światowych, takich jak Panasonic czy Pelco, w prestiżowych obiektach na terenie Chin, mimo że kraj ten jest jednym z głównych producentów światowych kamer i innego sprzętu CCTV.

Kolejną dynamiczną prezentację (bardzo nam się podobała) poprowadzili Sławomir Janiso, Key Account Manager, i Łukasz Klepacki, Key Account Manager. Dotyczyła ona rozwiązań sieciowych w produktach telewizji dozorowej (Wideo IP) i możliwości technicznych, jakie niesie ta nowoczesna i stale rozwijająca się technologia.

W kolejnym wystąpieniu, po raz pierwszy w Polsce, Alexey Mayorov zaprezentował kanadyjską firmę z korzeniami w Rosji – AxxonSoft. Na rynku światowym zajmuje ona drugie miejsce po firmie Milestone w dziedzinie rozwiązań Wideo IP. Posiada tzw. rozwiązania inteligentne wideo, np. systemy rozpoznawania tablic rejestracyjnych, detekcji twarzy itp. Firma Radioton będzie wyłącznym przedstawicielem tej firmy w Polsce, uznając, że rozwiązania sprzętowe, jakimi dysponuje, to jeszcze nie wszystko, aby zapewnić elastyczność rozwiązań w zakresie telewizji dozorowej.

Zorganizowanie tego typu imprezy biznesowej wcale nie jest łatwe. Założenie, że w przyjaznej i luźnej atmosferze słuchacze szybciej przyswoją serwowaną im wiedzę, jest z gruntu właściwe. Jeżeli nawet tak nie jest, to kto nie będzie pamiętał wszystkich dodatkowych atrakcji, jakich dostarczyli gospodarze spotkania partnerów JVC Professional. Poza wymianą doświadczeń z zakresu urządzeń IP uczestnicy spotkania mieli zagwarantowaną dobrą zabawę, spędzenie czasu w miłym towarzystwie, a także (oprócz wspomnianej wycieczki do kopalni): rozlosowanie wśród obecnych biletów na mecze Euro 2008 (JVC jest od wielu lat sponsorem Mistrzostw Europy w Piłce Nożnej), występy zawodowych artystów, grę w gigantyczne piłkarzyki (tym razem w wykonaniu uczestników zjazdu), konkurs rzutu chińską kamerą do kosza, jazdę na seagwayu oraz konkurs dla bardziej zaawansowanych – jazdę na seagwayu przy jednoczesnym trzymaniu jedną ręką rakietki do ping ponga z piłeczką, konkurs karaoke dla miłośników śpiewu, bankiet, podczas którego wystąpiła kapela, której wokalistki mógłby pozazdrościć niejeden znany zespół.

Na zakończenie uroczystej kolacji wszyscy ruszyli w tany. Zabawa trwała do białego rana.

Jak zapewniali organizatorzy, kolejne spotkanie partnerów JVC Professional już za rok.

Teresa Karczmarzyk

Kamera Panasonic z serii Super Dynamic

osiąga 2 miliony sztuk sprzedaży

15 maja 2008 roku firma **Panasonic System Solutions** świętowała osiągnięcie historycznego kamienia milowego – 2 milionów sprzedanych sztuk kamer z dynamicznej, inteligentnej serii SD od czasu wprowadzenia ich na rynek w 1997 roku.

Technologia Super Dynamic została opracowana przez Panasonic, aby umożliwić połączenie w kamerach najlepszych scen z obrazów uzyskanych przy dwóch różnych otworach przysłony w celu jednoczesnego odtworzenia zarówno jasnych, jak i ciemnych powierzchni, co jest nieosiągalne w kamerach konwencjonalnych z uwagi na ich ograniczony zakres dynamiki.

Obecnie trzecia generacja kamer **Super Dynamic III (SDIII)** zapewnia bezprecedensowy poziom inteligencji i właściwości. To nie tylko robiący wrażenie zakres dynamiki (128 x), ale i bardzo dynamiczny procesor sygnału cyfrowego, automatyczna ostrość, naturalna reprodukcja kolorów, detekcja zmian sceny i automatyczna stabilizacja obrazu. Co więcej, technologię SDIII znajdziemy zarówno w kamerach analogowych serii WV-CP480, jak i w nagradzanych kamerach sieciowych i-Pro z ostatnio wprowadzonych na rynek serii WV-NS950 i WV-NW960.

Wraz z nowymi produktami zaplanowanymi do wprowadzenia na rynek w najbliższej przyszłości Panasonic System Solutions będzie kontynuować sprzedaż kamer z serii Super Dynamic i planuje w dalszym ciągu opracowanie nowych produktów, w których będą zastosowane postępy technologii Super Dynamic.

W celu uzyskania dodatkowych informacji prosimy odwiedzić witrynę pss.panasonic.eu.

Bezpośr. inf. Panasonic System Solutions Europe

Opracowanie: Redakcja

Sagem Sécurité koordynatorem projektu badawczego z zakresu biometryki i kryptografii

Firma Sagem Sécurité została wybrana do koordynowania europejskiego projektu badawczego TURBINE (*Trusted Revocable Biometric Identities*). Ten trwający 3 lata projekt ma na celu rozwinięcie zaawansowanych rozwiązań z zakresu tożsamości cyfrowej, łączących automatyczne rozpoznawanie odcisków palców z innowacyjnymi technikami kryptograficznymi.

Wysiłki badawcze skupią się na ukryciu informacji tajnej wewnątrz opisu odcisków palców w taki sposób, aby informacja ta mogła być odczytana jedynie przez osobę z takimi samymi odciskami palców. Wykorzystując techniki kryptograficzne, projekt ten może prowadzić do fundamentalnych zmian w zabezpieczaniu danych osobowych bazującym na odciskach palców. Byłoby na przykład możliwe zaprojektowanie takich biometrycznych plików z danymi osobowymi, do których dostęp byłby możliwy jedynie po nie budzącej wątpliwości autoryzacji posiadacza tych prywatnych danych.

– *Te badania są podstawą obietnicy stworzenia technologii zabezpieczania systemów informatycznych bazujących na technologiach biometrycznych* – mówi Jean-Paul Jainsky, szef Sagem Sécurité.

Konsorcjum TURBINE obejmuje głównych graczy w tym sektorze, w tym Philips Research Europe, Sagem Orga, Precise Biometrics w Szwecji, Cryptolog and ARTTIC we Francji oraz 3D-GAA w Grecji, jak również laboratoria badawcze K.U. Leuven w Belgii i Gjovik University College w Norwegii.

Redakcja

Źródło: www.securityworldhotel.com

Nowe brytyjskie centrum oświetlenia CCTV firmy Raytec

Po kolejnym roku zwiększonego zapotrzebowania na energooszczędne rozwiązania w zakresie oświetlenia podczerwienią i światłem białym do zastosowań CCTV firma Raytec dokonała otwarcia nowego obiektu produkcyjnego i technologicznego w Wansbeck (Northumberland, Wlk. Brytania). To posunięcie jest częścią rozleglejszych inwestycji w zakresie infrastruktury sprzedaży, inżynieryjnej oraz produkcyjnej. Nowy obiekt zawiera największą w przemyśle tej branży dedykowaną ciemnię.

Bezpośr. inf. Raytec

Securitas Systems kupuje G4S Sicherheitssysteme

Firma **Securitas Systems** przejęła niemiecką działalność operacyjną **G4S Sicherheitssysteme**. Cena nabycia wynosi 10 milionów euro.

G4S Sicherheitssysteme jest jedną z pięciu największych firm na rynku *security* w Niemczech. Firma zatrudnia ok. 300 osób i ma 20 filii w całym kraju. Skupia się na bankowości i sektorze finansowym, jak również na sektorze handlowym. Roczna sprzedaż w 2007 roku wyniosła ok. 34 miliony euro, z jedną trzecią dochodu z umów serwisowych. Działalność niemieckiej części Securitas Systems przyniesie po konsolidacji obroty rzędu 64 milionów euro przy 500 zatrudnionych.

Połączenie firm nastąpi do maja 2008 r., w terminie zależnym od czasu rozpatrywania transakcji przez niemieckie władze antytrustowe.

– *W wyniku tego połączenia będziemy graczem numer trzy i największym niezależnym produktowo integratorem systemów na rynku niemieckim. Będziemy umacniać nasze portfolio usług i uzyskamy zasięg ogólnokrajowy na największym rynku Europy kontynentalnej* – twierdzi Juan Vallejo, prezes firmy Securitas Systems AB.

Redakcja

Źródło: www.securityworldhotel.com

Megapikselowe bezpieczeństwo Axis 209 MFD-R

Softex Data, autoryzowany dystrybutor Axis Communications, przedstawia nowe megapikselowe wcielenie kamery Axis 209. Płaski *design*, idealny do najbardziej wymagających środowisk, i progresywne skanowanie w rozdzielczości megapikselowej to tylko niektóre zalety nowej kamery.

Axis 209 MFD-R została zaprojektowana specjalnie do pracy w trudnych warunkach, gdzie wymagana jest wysoka odporność na warunki środowiskowe, takie jak kurz, wilgotność i wstrząsy. Niewielka, mierząca jedynie cztery centymetry kamera może być z łatwością zainstalowana nawet w trudno dostępnych miejscach i na nierównym podłożu, np. w pociągach i autobusach. Urządzenie jest zasilane poprzez sieć Ethernet w standardzie PoE. Axis oferuje kamerę 209 MFD-R z dwoma rodzajami konektorów: RJ-45 oraz M12.

Bezpośr. inf. Softex Data

Szwajcarskie stadiony wybierają telewizję dozorową Geutebruck na EURO 2008

Dwa szwajcarskie stadiony, na których odbędą się w czerwcu mecze mistrzostw Europy w piłce nożnej UEFA EURO 2008, wybrały sprzęt telewizji dozorowej niemieckiej firmy **Geutebruck** do zapewnienia bezpieczeństwa i zarządzania tłumem na terenie stadionów oraz handlowych i rozrywkowych obiektów towarzyszących, a także wokół nich.

Systemy hybrydowe, zainstalowane ostatnio przez **Eotec AG** na stadionie Św. Jakuba w Bazylei (40 tysięcy miejsc) i stadionie Letzigrund w Zurichu (30 tysięcy miejsc), integrują istniejące kamery analogowe z nowymi megapikselowymi kamerami IP, zapisem cyfrowym i matrycami wirtualnymi, aby uzyskać elastyczność, dużą funkcjonalność oraz efektywność.

Operatorzy stadionów wybrali Geutebruck, ponieważ otwarte interfejsy tej firmy, wraz z jej rodzimym sprzętem i oprogramowaniem, zapewniają całkowitą kompatybilność w obrębie całego systemu telewizji dozorowej, jak również łatwość połączenia z innymi systemami, np. takimi jak z Schneider Intercom. Nowa instalacja pozwala także personelowi na wyświetlanie obrazów „na żywo" na wielu ekranach, pobieranie indywidualnych portretów do celów identyfikacji i archiwizację całego meczu po naciśnięciu jednego przycisku. Systemy monitorują się samodzielnie dzięki wbudowanym funkcjom diagnostycznym i systemom alarmowym. Zajmują bardzo niewielkie pasmo, gdyż technologia DLS (*dynamic live streaming*) zapewnia to, że strumienie danych płyną przez sieć tylko wtedy, gdy obrazy są rzeczywiście potrzebne.

Redakcja

Źródło: www.securityworldhotel.com

Ogólnopolskie Warsztaty Zacisze 2008
– relacja

Wiodącą tematyką szesnastych Ogólnopolskich Warsztatów – Systemy Sygnalizacji Pożarowej Zacisze 2008 była integracja instalacji bezpieczeństwa pożarowego. Takie instalacje obejmują dziś już nie tylko centralę systemu sygnalizacji pożarowej (SSP) wraz z czujkami, ręcznymi ostrzegaczami pożarowymi i urządzeniami służącymi do transmisji pożarowych sygnałów alarmowych, ale i systemy oddymiania, gaszące czy dźwiękowe systemy ostrzegawcze (DSO). Powiązane z nimi mogą być systemy oświetlenia awaryjnego, sygnalizacji włamania i napadu, kontroli dostępu, telewizji dozorowej, a także dźwigi osobowe lub schody ruchome i systemy wentylacji oraz klimatyzacji. W związku z tym istotny staje się problem kompatybilności współpracujących ze sobą urządzeń, które wchodzą w skład tego rodzaju instalacji. Temu zagadnieniu był poświęcony jeden z referatów, a kolejny – możliwościom i ograniczeniom integracji instalacji bezpieczeństwa pożarowego. Dwa inne także dotyczyły współpracy różnych systemów z SSP. W jednym z nich omówiono zadania systemów kontroli dostępu i telewizji dozorowej w sytuacji zagrożenia pożarowego, wynikające z zasad ogólnych, opracowanych dla zintegrowanych systemów bezpieczeństwa i zebranych w Specyfikacji Technicznej CLC/TS 50398:2002. W drugim – problematykę praktycznej integracji systemów DSO i SSP.

W wielu referatach odnoszono się do obowiązujących w zakresie bezpieczeństwa pożarowego przepisów, które ulegają szybkiemu rozwojowi. Przykładowo, w grupie norm EN 54 pojawiły się już normy dotyczące urządzeń transmisji alarmów pożarowych i sygnałów uszkodzeniowych oraz central i głośników używanych w DSO.

Problemy wynikające
z integracji systemów
DSO z instalacjami

Podczas warsztatów przedstawiono także produkty związane z ich tematyką: wielodetektorowe czujki Polon-Alfa, optyczne bezkomorowe czujki dymu Bosch (wraz z licznymi wynikami badań porównawczych), system oświetlenia awaryjnego firmy Hybryd, ssący system bardzo wczesnej detekcji dymu VESDA oraz oprogramowanie InPro BMS do wizualizacji stanu systemów bezpieczeństwa i ich integracji.

W dniach 29–31.05.2008 na zaproszenie organizatorów, Zakładu Urządzeń Dozymetrycznych Polon-Alfa, których reprezentował Jerzy Karczewski, do Ośrodka Doskonalenia Kadr Służby Więziennej w Suchej przyjechali zaproszeni goście, wybitni specjaliści, wśród których znaleźli się między innymi mgr inż. Janusz Sawicki, mgr inż. Jerzy Ciszewski, dr Waldemar Wnęk, dr Jerzy Sobstel i dr Andrzej Ryczer.

Wygłoszono jedenaście referatów:

1. Efektywność instalacji SAP w świetle obowiązujących przepisów – Lech Światły, Polon-Alfa
2. Kompatybilność urządzeń tworzących pożarowe instalacje bezpieczeństwa – Janusz Sawicki, ITB
3. Integracja instalacji bezpieczeństwa pożarowego – możliwości i ograniczenia – Jerzy Ciszewski, ITB
4. Optyczne bezkomorowe czujki dymu w świetle badań testowych – Waldemar Wnęk, SGSP
5. Urządzenia transmisji alarmów pożarowych i sygnałów uszkodzeniowych w centrali monitoringu pożarowego – Jerzy Sobstel, Noma 2
6. Problemy wynikające z integracji systemów DSO z instalacjami SAP – Leszek Demidowicz, Ambient System
7. Zadania systemów kontroli dostępu i telewizji dozorowej w sytuacji zagrożenia pożarowego – Andrzej Ryczer, Politechnika Warszawska
8. Demonstracje generatorów dymu i symulatorów pożaru – Janusz Jagodziński, Compact
9. Funkcjonowanie oświetlenia awaryjnego w razie pożaru – Andrzej Krzesiński, Hybryd
10. Problemy wizualizacji i nadzoru instalacji bezpieczeństwa pożarowego – Jerzy Taczalski, Ifter
11. Systemy wczesnej detekcji dymu – integracja z systemem sygnalizacji pożarowej – Mariusz Konik, Vision Polska

W kuluarach warsztatów odbywały się zwyczajowe dyskusje, a kilka firm zaprezentowało swoje produkty. Wśród nich znalazły się:

- Ambient System – dystrybutor, producent i projektant systemów obiektowych: nagłośnieniowych, pożarowych i komunikacyjnych,
- Compact – firma zajmująca się serwisem i sprzedażą gaśnic, znaków ewakuacyjnych, węży hydrantowych itp.,
- Hybryd – producent opraw i systemów oświetlenia awaryjnego,
- IPS – firma zajmująca się zagadnieniami związanymi z przemysłowymi instalacjami palnikowymi oraz systemami detekcji i zwalczania zagrożeń gazowych i pożarowych w przemyśle,
- Vision Polska – firma specjalizująca się w dostarczaniu kompleksowych rozwiązań w zakresie bardzo wczesnej detekcji dymu, opartych na technologii VESDA,
- Polon-Alfa – obecnie największy w Polsce producent systemów sygnalizacji pożarowej.

Organizatorzy tradycyjnie już zadbali o dostarczenie uczestnikom warsztatów wiedzy, a w czasie wolnym dużej dawki zabawy i relaksu.

Do stałych punktów programu należą uroczysta kolacja z tańcami do białego rana, rejs polonowską Nivą oraz ognisko, podczas którego każdy ma okazję do zaprezentowania swoich zdolności wokalnych.

W „pojedynku gladiatorów" – konkursie dla odważnych – oprócz panów udział wzięły jak zwykle nieustraszone i waleczne panie. Ogłoszenie wyników i wręczenie nagród nastąpiło podczas wieczornego ogniska.

Cel warsztatów – integracja instalacji bezpieczeństwa pożarowego oraz integracja zaproszonych gości – został osiągnięty.

Dziękujemy organizatorom za wspólnie spędzony czas i... do zobaczenia za rok. Mamy nadzieję, że pogoda i dobry humor dopiszą.

Teresa Karczmarzyk

SEVEN GUARD

10 pytań na 10 lat systemu

Z Mirosławem Wandzelem, prezesem firmy System 7 Security, rozmawia Teresa Karczmarzyk

Czy SEVEN GUARD sprawdził się w ciągu tych dziesięciu lat?

Niech przemówią fakty. Przed dziesięciu laty, gdy z naszym pierwszym rejestratorem wkraczaliśmy na rynek, był on pełen konkurencyjnych produktów „zachodnich" i dalekowschodnich, służących do kontroli wartowników. Jednak niespotykana odporność rejestratorów SEVEN GUARD, prostota obsługi i oczywiście niska cena sprawiły, że obecnie tego typu konkurentów praktycznie trudno znaleźć na naszym polskim rynku. Również poziom naszego serwisu był wyższy niż u zagranicznej konkurencji. W stosunkowo krótkim czasie dopracowaliśmy się też chyba najlepszego na rynku, wielojęzycznego, wielodostępowego i darmowego programu komputerowego, opartego na doskonałej, bezpłatnej serwerowej bazie danych (SQL). I tak, w ciągu tych dziesięciu lat sprzedaliśmy kilkadziesiąt tysięcy urządzeń kilku tysiącom użytkowników w kraju i za granicą. Początkowo naszymi klientami były prawie wyłącznie agencje ochrony, wojsko itp. Później, w miarę rozwoju systemu, doszli też inni klienci – od dużych przedsiębiorstw i instytucji (np. poczta, wyższe uczelnie), aż po małe firmy, wykorzystujące nasze urządzenia do celów, których nigdy byśmy nie przewidzieli.

Oczywiście obecnie mamy liczącą się krajową konkurencję, dopinguje nas to jednak do pracy i dalszego rozwoju, nie pozwala poprzestać na osiągniętej już pozycji.

Co z nowościami zaprezentowanymi na targach Securex 2008?

Faktycznie było ich wiele. Obecnie przechodzą ostanie testy i badania w laboratoriach oraz są wdrażane do produkcji. Myślę, że warto je wymienić:

Po pierwsze: cała rodzina rejestratorów SG3

Tym, co łączy cztery produkty z tej rodziny, jest hermetyczna, stalowo-kompozytowa obudowa o niewielkich rozmiarach i niespotykanej odporności. W każdym z nich zastosowano również nowatorski układ „inteligentnego" zarządzania ładowaniem wewnętrznego akumulatora polimerowego, chroniący go przed błędami użytkowników i wydłużający jego żywotność. Niestety, żaden z rejestratorów SG3 nie posiada wibratora, charakterystycznego dla SG2.

Pierwszy reprezentant – SG3ECO – to „ekonomiczny" przedstawiciel tej rodziny. Może pracować wyłącznie ze stałokodowymi punktami stykowymi w trybie odczytu dowolnych punktów. Nie obsługuje bezpośrednio podłączonej drukarki i harmonogramów wewnętrznych, posiada niekasowalną pamięć ostatnich 1850 zdarzeń. Funkcjonalnie jest podobny do większości dostępnych na rynku urządzeń tego typu, chociaż, jak każdy rejestrator SEVEN GUARD, jest odporny na wodę, udary, zabrudzenie, zakłócenia elektromagnetyczne i nie posiada żadnych wyłączników, gniazd itp.

Drugi – SG3 – to podstawowy przedstawiciel rodziny SG3. Od SG3ECO jest bogatszy o możliwość pracy w trybie zaprogramowanych punktów, obsługę bezpośredniej drukarki i harmonogramów wewnętrznych. Ponadto posiada innowacyjny układ, sprawiający, że jego styki są „nieczułe" na większość możliwych do podłączenia napięć zewnętrznych. Obsługuje stało- i zmiennokodowe punkty stykowe. Niekasowalna pamięć mieści 5600 ostatnich zdarzeń.

Trzeci produkt z tej rodziny to SG3PROX. Funkcjonalnie jest podobny do SG3. Różnica polega na tym, że odczytuje wyłącznie punkty zbliżeniowe, zarówno stałokodowe, jak i zmiennokodowe. Jest to nasza odpowiedź na zapotrzebowanie niektórych klientów, chcących odczytywać punkty kontrolne również przez szybę. Wprawdzie jesteśmy przekonani o wyższości punktów stykowych w tego typu zastosowaniach (chociażby kwestia oszczędności akumulatora, odporności na zakłócenia i niewrażliwości na otoczenie), niemniej jednak bywają sytuacje, w których punkt zbliżeniowy też ma swoje zalety.

Najwyższy model w tej linii to SG3DUO. Funkcjonalnie jest podobny do poprzedników, z tym, że obsługuje stałokodowe i zmiennokodowe punkty **stykowe** oraz **zbliżeniowe**. Zatem jest to pierwszy polski rejestrator dwusystemowy.

Oczywiście popularne i sprawdzone „w boju" rejestratory **SG2** będą nadal produkowane i zapewne jeszcze długo pozostaną w sprzedaży.

Po drugie: plomby elektroniczne SGSL

Jest to absolutna nowość w systemie SEVEN GUARD. Prawdopodobnie najmniejsze w Europie plomby elektroniczne wielokrotnego użytku o przemyślanej konstrukcji i bogatej funkcjonalności.

Posiadają niekasowalną pamięć ostatnich 1344 zdarzeń (z datą i czasem wystąpienia), niepowtarzalny numer i nazwę nadawaną przez użytkownika, możliwość autoryzacji zamknięcia/otwarcia przez upoważnione osoby, sygnalizację optyczną i akustyczną, zabezpieczenie antysabotażowe i są zasilane z trwałej baterii litowej. Zdarzenia zapisane w ich pamięci mogą być odczytywane za pośrednictwem rejestratora SEVEN GUARD lub bezpośrednio, za pomocą komputera. Ponadto w systemie pełnią one funkcję zwykłego stykowego punktu kontrolnego.

Autoryzacja zdarzeń odbywa się również za pomocą zwykłych punktów personalnych.

Pierwsza przedstawicielka tej rodziny – plomba SGSL1 – to nowoczesna alternatywa dla tradycyjnych plomb metalowych lub plastikowych (o „plastelinowych" nie wspominając) w miejscach o szczególnym znaczeniu lub często plombowanych. Wyposażona jest w wytrzymałą, giętką pętlę przewlekaną (o długości od 5 do 200 cm), zakończoną stykami o specjalnej konstrukcji.

Druga plomba to SGSL2. Znajduje ona zastosowanie w nadzorowaniu drzwi, szuflad itp. Tradycyjną pętlę zastąpiono w niej czujnikiem magnetycznym, a cała plomba mocowana jest na stałe od strony wewnętrznej chronionego pomieszczenia (strefy itp.). Urządzenie to może dodatkowo rejestrować wszystkie otwarcia/zamknięcia drzwi (np. do ważnych pomieszczeń). Montaż na powierzchniach metalowych jest możliwy po zastosowaniu odpowiednich podkładek.

I ostatnia nowość w naszej ofercie: depozytory kluczy SGKEY

Jest to cała rodzina szaf do automatycznego wydawania kluczy i rejestrowania ich obiegu. Oczywiście konkretna osoba musi mieć uprawnienia do pobierania konkretnych kluczy w danym czasie. Standardowy program produkcyjny to depozytory dla **4**, **9**, **34**, **68**, **95** kluczy. Urządzenia można łączyć w grupy o dowolnej wielkości. Komunikacja wzajemna pomiędzy szafami oraz z komputerami nadzorującymi wykorzystuje sieć LAN/WAN lub RS485. Praktycznie jedynym ograniczeniem jest liczba 64000 szaf, kluczy lub użytkowników w systemie. Depozytory są obecnie na etapie testów i będą w sprzedaży dopiero po wakacjach.

Z czego wynika potrzeba aż takiego zróżnicowania modeli rejestratorów SEVEN GUARD?

Obecnie nasi klienci mogą wybrać odpowiednie urządzenie, stosownie do swoich potrzeb i możliwości finansowych. Mamy obecnie w ofercie pięć modeli rejestratorów, co stawia nas w ścisłej światowej czołówce producentów tego typu urządzeń i nie jest to nasze ostatnie słowo.

Dlaczego plomby elektroniczne nie są jeszcze w Polce powszechnie stosowane?

Myślę, że była to kwestia ceny i dostępności. Mam nadzieję, że nasze nowe produkty przełamią obie te bariery. Nie bez znaczenia jest również kwestia przyzwyczajenia. Trochę wstyd o tym wspominać, ale w wielu poważnych instytucjach w Polsce na początku XXI wieku nadal królują plomby „plastelinowe".

Czy jest zapotrzebowanie na depozytory kluczy?

Zapotrzebowanie jest ogromne, niemniej jednak dotychczas barierą stosowania była zaporowa wręcz cena (np. 40000 zł za szafę i oprogramowanie). Postanowiliśmy uzdrowić tę sytuację i mam nadzieję, że trafimy w oczekiwania tych, którzy chcą uporządkować gospodarkę kluczami za bardzo rozsądną cenę.

SEVEN GUARD nie jest chyba najtańszym systemem na rynku?

Jeżeli chodzi o rejestratory, to są one najkorzystniejszym rozwiązaniem w swojej klasie, również w odniesieniu do ceny. Trudno je jednak porównywać z wytworami, dla których każdy upadek na ziemię może skończyć się uszkodzeniem, nie mówiąc już o upadku do kałuży, lub takimi, które wymagają ładowania akumulatora co dwa dni. Nasze rejestratory były w najdrobniejszych szczegółach projektowane do zastosowania w rzeczywistych, a więc trudnych warunkach i spełniania stawianych im surowych wymagań, nie są zatem zbiorem dostępnych na rynku standardowych (tanich) elementów, jak to bywa w przypadku znacznej części „konkurencji". Pozostałe, nowe urządzenia systemu są raczej bezkonkurencyjne, jeżeli chodzi o cenę i nie tylko.

Czy to nie przesada, aby stosować zmienny kod w systemach tego typu?

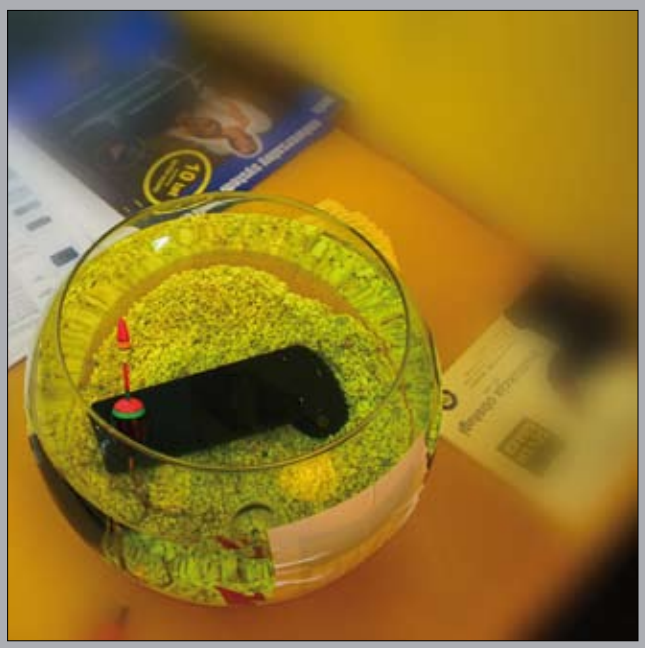
Po latach okazało się, że przy obecnym stanie techniki powstały rozwiązania pozwalające na oszukanie nawet naszego stałokodowego systemu stykowego; o konkurencyjnych systemach opartych na zbliżeniowych kartach i punktach (RFID 125 kHz) już nawet nie wspominam. Ponieważ nie chcemy sprzedawać naszym klientom „złudzeń", wdrożyliśmy do produkcji rozwiązanie praktycznie uniemożliwiające „nagrywanie" kodów punktów, i to zarówno dla naszych punktów stykowych, jak i zbliżeniowych.

Niektóre rejestratory rodziny SG3, jako prawdopodobnie **pierwsze na świecie**, mogą współpracować z punktami kontrolnymi o **pseudolosowo zmiennym** kodzie, co praktycznie uniemożliwia oszukanie systemu przez nierzetelnych pracowników.

Metoda zabezpieczenia, będąca **autorskim opracowaniem** firmy SYSTEM 7, jest skuteczniejsza w tym zastosowaniu niż standardowe kodowanie dostępu do odczytu danych z punktu i szyfrowanie komunikacji z punktem razem wzięte. W naszym systemie nawet poznanie używanego w danym rejestratorze kodu szyfrującego nie pozwala na określenie, jaki powinien być faktycznie kod danego punktu kontrolnego przy jego odczytywaniu przez konkretny rejestrator.

Z jakimi sukcesami były związane najprzyjemniejsze chwile w czasie tych dziesięciu lat?

Wprawdzie nasza firma działa już od 1990 roku, jednak w tym ostatnim czasie było ich szczególnie wiele. Poczynając od niespodziewanego tempa, w jakim SEVEN GUARD zdobywał rynek w latach 2000–2002. W tamtym czasie, pomimo nieustannego zwiększania produkcji, wciąż nie mogliśmy nadążyć za potrzebami rynku. SEVEN GUARD zdobył też tytuł Polskiego Mistrza Techniki Alarmowej. Potem był przełom lat 2002/2003 uwieńczony pierwszym, wydanym przez TUV certyfikatem ISO9001 na pełny zakres naszej działalności. Było też wiele wyrazów uznania ze strony użytkowników systemu, szczególnie doceniających odporność i prostotę obsługi systemu. Zresztą zakończenie prac nad każdym nowym rozwiązaniem jest dla nas dniem szczególnym. Niestety tylko niektóre nasze opracowania są wdrażane do produkcji. Inne zajmują miejsce w archiwum lub czekają na odpowiedni moment. Tak było na przykład z rejestratorem z wbudowanym modułem GSM/GPRS. Mieliśmy prawie gotowy prototyp, gdy dowiedzieliśmy się, że za kilka miesięcy inna polska firma zamierza wprowadzić na rynek podobne urządzenie. Ponieważ znaliśmy już takie rozwiązanie, sprzedawane przez jednego z zachodnioeuropejskich konkurentów, i wiedzieliśmy o doświadczeniach z systemem WARTA firmy CON-SPARK, który był chyba pierwszym polskim radiowym systemem kontroli pracy wartowników *online* (rok 1996), postanowiliśmy poczekać, by sprawdzić, jak rynek przyjmie tego typu rozwiązanie. Od roku zbieramy opinie naszych klientów, dotyczące możliwości szerszego zastosowania u nich rejestratorów z komunikacją GSM/GPRS. Jeżeli ich opinie potwierdzą sensowność takiego przedsięwzięcia, to wdrożymy do produkcji posiadane rozwiązanie (oczywiście cena i odporność będą godne marki SEVEN GUARD).



Wracając jednak do chwil radości, obecnie najbardziej cieszy nas, gdy wraca do naszego serwisu któryś z prawie 10-letnich rejestratorów z pierwszej partii, a klient zdecydowanie chce nadal go używać i prosi tylko o wymianę akumulatorów (których teoretyczna żywotność wynosiła 5 lat!).

Czyżby nie było żadnych trudności?

Niestety, przez te wszystkie lata mieliśmy też kilka „wpadek". Ostatnią całkiem niedawno, w 2007 r., kiedy to okazało się, że jeden z układów scalonych użytych w wyprodukowanej partii rejestratorów SG2 zaczynał działać nieprawidłowo w znaczącym odsetku urządzeń. Sprawa była o tyle skomplikowana, że rejestratory przechodziły wszelkie testy, a wada ujawniała się po paru miesiącach użytkowania w sposób dość przypadkowy. Po długim dochodzeniu ustaliliśmy jednak, co było przyczyną kłopotów, i mogliśmy temu skutecznie zaradzić. Było to dla nas jeszcze jedno trudne, ale i pouczające doświadczenie.

Jakie są plany firmy SEVEN GUARD na przyszłość?

Częściowo odpowiedziałem już na to pytanie. Może dodam tylko, że obecnie nasz dział konstrukcyjny jest prawie trzy razy większy niż cztery lata temu i pracujemy nad sześcioma zupełnie nowymi rozwiązaniami. Oczywiście nie zaniedbujemy naszej działalności dystrybucyjnej. Przecież jesteśmy również renomowanym regionalnym dystrybutorem urządzeń w branży *security*.

Patrząc jednak na naszą branżę, trudno oprzeć się wrażeniu, że nasi polscy producenci są raczej mało innowacyjni. Myślę, że na palcach obu rąk można policzyć krajowe firmy, które faktycznie zdobywają się na kreowanie nowych rozwiązań na światowym poziomie. Oczywiście z własnego doświadczenia wiemy, że osiągnięcie takiego poziomu nie jest rzeczą łatwą. Niemniej jednak uważam, że nasz prawie czterdziestomilionowy kraj z takimi tradycjami i możliwościami w dziedzinie techniki naprawdę stać na wiele, wiele więcej. Czego sobie i wszystkim życzę.

SYSTEM 7
INFOLINIA: 0801 000 307
TEL.: 033 8218777
WWW.SYSTEM7.BIZ

Skuteczna **detekcja**

wszechstronne zastosowania

IVORY - precyzyjna optyka zwierciadlana
AQUA Luna - nowatorskie rozwiązanie podświetlenia awaryjnego
AMBER - atrakcyjna, kompaktowa obudowa

Idealne rozwiązania do ochrony banków,
obiektów przemysłowych, biur,
jak również domów i mieszkań.

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

POLON-ALFA
Największy polski producent systemów sygnalizacji pożarowej
www.polon-alfa.pl
POŻAR
ODYMIANIE

TargiKielce
ALARM
5-6.11.2008, Kielce
oraz
IX OGÓLNOPOLSKA KONFERENCJA
Bezpieczne Miasto - Monitoring
Wizyjny Miast
Patronat prasowy:
Patronat internetowy:
twierdza
www.ochrona.pl
IX Konferencja i Wystawa Monitoringu Wizyjnego
Targi Kielce Sp z o.o., ul. Zakładowa 1, 25-672 Kielce,
Szczegółowe informacje: Dyrektor Produktu - Grzegorz Figarski, tel. 041 365 12 33, fax 041 345 62 61,
e-mail: figarski.g@targikielce.pl
www.alarm.targikielce.pl

Ciągłość działania
w życiu codziennym

Świat ciągle pędzi do przodu. To, co jeszcze kilka lat temu wydawało się możliwe jedynie w filmach typu *science-fiction*, coraz częściej staje się dostępne dla każdego z nas: wyszukiwanie informacji w niezliczonej ilości zbiorów bez wychodzenia z domu przy wykorzystaniu sieci Internet, możliwość dokonywania zakupów za pośrednictwem komputera czy chociażby realizacja transakcji za pomocą kawałka plastiku w postaci karty płatniczej. Dziś już nikogo nie zaskakują takie zdobycze techniki, jak komputer, bankomat czy telefon komórkowy, które na stałe wpisały się w życie codzienne i są powszechnie wykorzystywane. Wielu z nas używa takich urządzeń na co dzień, nie zastanawiając się nawet nad tym, w jaki sposób funkcjonują i jak prowadzone są działania mające na celu zapewnienie ciągłości działania każdego z systemów. Dopiero w momencie wystąpienia awarii uniemożliwiającej korzystanie z sieci Internet, pojawienia się trudności z dokonaniem płatności kartą, gdy mamy koszyk pełen zakupów, a w portfelu niewystarczającą sumę pieniędzy, w przypadku niemożności wykonania połączenia telefonicznego właśnie wtedy, gdy jest ono konieczne, jesteśmy zdenerwowani brakiem ciągłości działania systemów informatycznych w danym sektorze usług.

Stały rozwój usług elektronicznych stawia przed ich dostawcami coraz większe wyzwania. Przy bezlitosnej walce konkurencyjnej w świecie wolnego rynku nie ma miejsca na pomyłki lub podejmowanie prowizorycznych działań. Każdy – nawet najmniejszy – błąd może spowodować, iż klienci utracą zaufanie do firmy i wybiorą ofertę konkurencji. Konieczność realizacji usług na wysokim poziomie i ciągłe podnoszenie ich jakości – a co zatem idzie i bezpieczeństwa – powoduje, iż za utrzymanie poprawnej pracy urządzeń i systemów odpowiadają sztaby wykwalifikowanych specjalistów, którzy muszą być dostępni zawsze wtedy, gdy jest to niezbędne.

W zależności od stopnia krytyczności systemów informatycznych przyjmowane są różne scenariusze działań koniecznych do podjęcia w sytuacji wystąpienia zagrożenia ciągłości ich funkcjonowania, co ma swoje odbicie w sposobie organizacji pracy służb serwisowych. Zanim jednak stworzony zostanie grafik godzin pracy i dyżurów, konieczne jest wykonanie prac analitycznych, których celem będzie dobór optymalnego wariantu, który z jednej strony będzie jak najbardziej efektywny, a z drugiej pozwoli na wyeliminowanie zbędnych kosztów.

Podstawowym zadaniem, które należy wykonać przed stworzeniem harmonogramu pracy, jest konieczność przeprowadzenia identyfikacji ryzyk, czyli po pierwsze inwentaryzacji systemów i usług objętych serwisem, po drugie określenia stopnia krytyczności każdego z nich. Stopień krytyczności może być wyznaczony na podstawie wielu zmiennych, ale najważniejszy jest czas w funkcji kosztu (rzeczywistego lub założonego) ewentualnego przestoju danego systemu, a także wyznaczenie granicy, po której przekroczeniu koszt ten wzrasta lawinowo. Na jego wykres składają się nie tylko straty wymierne, wynikające z braku możliwości zrealizowania operacji klientów – które można wyliczyć w prosty sposób,

mnożąc średnią liczbę operacji dokonywanych w ciągu godziny przez zysk z tych operacji generowany w sytuacji poprawnego funkcjonowania systemów – ale również koszty niewymierne (niepoliczalne), związane z utratą zaufania klientów do firmy oraz ryzykiem ich przejścia do konkurencji. Im krótszy jest czas od wystąpienia awarii do momentu przekroczenia poziomu akceptowalnej wartości strat, tym system jest bardziej krytyczny.

Po przeprowadzeniu takiej analizy systemy informatyczne dzieli się – według przyjętych w danym podmiocie kryteriów – na grupy ryzyka (krytyczności). Na potrzeby artykułu przyjmiemy podział na trzy grupy krytyczności systemów, zależny od wartości granicznej akceptowalnych strat:

I – systemy, które wartość graniczną osiągają przed upływem jednej godziny od momentu wystąpienia awarii,

II – systemy, które wartość graniczną osiągają w czasie pomiędzy jedną godziną a czterema godzinami od wystąpienia awarii,

III – systemy, które wartość graniczną osiągają w czasie powyżej czterech godzin od momentu wystąpienia awarii.

Dla systemów z każdej z tych grup przyjmowane są inne założenia do opracowania planu pracy służb serwisowych odpowiedzialnych za przywrócenie systemów do poprawnej pracy. Dla systemów grupy III wystarczający jest jednozmianowy system pracy z zastosowaniem uzupełnienia w postaci ustalenia dyżurów, czyli gotowości pracowników do przyjazdu na miejsce wystąpienia awarii. Przy wyborze konkretnego pracownika przyjmuje się zazwyczaj, by miejsce jego zamieszkania nie znajdowało się dalej niż dwie godziny drogi od miejsca wystąpienia potencjalnej awarii. Oczywiście pracownicy pełniący taki dyżur powinni zostać odpowiednio wcześniej wyposażeni w środki łączności, umożliwiające odebranie informacji o awarii danego systemu. Przy obecnym poziomie rozwoju techniki informacja o wystąpieniu zagrożenia niekoniecznie musi być przekazana przez człowieka. Coraz częściej wykorzystywane są skrypty, powodujące automatyczne wysłanie informacji tekstowej za pomocą wiadomości SMS. Wiele systemów jeszcze przed wystąpieniem awarii potrafi wykryć anomalie i automatycznie wysłać informację pocztą elektroniczną na wskazany adres serwisowy, dzięki czemu administrator może zjawić się na miejscu zagrożenia jeszcze przed wystąpieniem samej awarii, a podjęte przez niego działania mogą jej zapobiec. Na rynku dostępne są, w coraz bardziej korzystnych cenach, usługi umożliwiające odbieranie wiadomości e-mail za pomocą zwykłych telefonów komórkowych lub dedykowanych urządzeń, które umożliwiają zarówno wykonywanie połączeń telefonicznych, jak również odbieranie poczty elektronicznej w podobny sposób, jak dzieje się to w przypadku wiadomości SMS, bez konieczności każdorazowego łączenia się z siecią Internet. Takie rozwiązania znacząco skracają czas od momentu otrzymania informacji do jej przeczytania przez administratora.

Systemy z grupy ryzyka II powinny być objęte większym reżimem czasowym. Administratorzy odpowiedzialni za te systemy, oprócz narzędzi wymienionych przy okazji systemów klasy trzeciej, powinni mieć również możliwość zdalnego połączenia z siecią wewnętrzną firmy, by móc możliwie w jak najkrótszym czasie rozpocząć działania mające na celu likwidację nieprawidłowości i przywrócenie poprawności pracy systemów. Najczęściej wykorzystywanym narzędziem jest bezpośrednie połączenie zewnętrznego komputera pracownika serwisu z siecią wewnętrzną firmy przy wykorzystaniu zdalnego pulpitu. Aby było ono bezpieczne (zabezpieczone przed możliwością podsłuchania przesyłanych informacji lub ewentualnym przechwyceniem nazw użytkowników i haseł), stosuje się szereg rozwiązań bazujących na połączeniach wykorzystujących tunele VPN (ang. *Virtual Private Network* – wirtualna sieć prywatna). Dane przesyłane w ten sposób pomiędzy komputerem serwisanta a administrowanym zdalnie serwerem są szyfrowane i bardzo trudne do podsłuchania przez nieuprawnione osoby. Ponadto odpowiednio skonfigurowany VPN pozwala na uruchomienie odpowiednich polityk na komputerze, z którego są wykonywane połączenia z siecią wewnętrzną firmy, i na czas trwania połączenia możliwe jest zablokowanie niektórych usług, co chroni zasoby firmy przed potencjalnym wypływem danych (np. GG, możliwości przeglądania stron WWW, odbierania i wysyłania prywatnej poczty elektronicznej). Dla zwiększenia poziomu bezpieczeństwa, oprócz uwierzytelnienia w postaci loginu – nazwy użytkownika – i hasła, stosowane są fizyczne lub programowe tokeny do generacji haseł dynamicznych (zmiennych w czasie). Dodatkową zaletą rozbudowanych systemów, umożliwiających połączenie poprzez tunel VPN, jest możliwość monitorowania i zdalnej weryfikacji pracy administratorów zarówno pod kątem operacji wykonywanych w obsługiwanych systemach, jak również bezpieczeństwa (sposób i czas logowania, informacja, do jakich systemów dany użytkownik próbował się zalogować, czy wyłącznie do tych, do których ma uprawnienia, itp.). Funkcjonalności te mają szczególne znaczenie w sytuacji, gdy opieka nad systemami sprawowana jest przez pracowników podmiotu zewnętrznego, świadczącego usługi wsparcia dla naszej firmy. Możliwość zdalnego połączenia z siecią wewnętrzną firmy powoduje, iż komputer połączony w ten sposób staje się praktycznie równoważny komputerom wewnętrznym, a wykonanie przez zalogowanego do sieci użytkownika niepożądanych operacji może spowodować zagrożenie dla pracy innych systemów wewnętrznych lub wypływ wrażliwych informacji na zewnątrz.

Dla systemów z grupy krytyczności I najczęściej stosowany jest ciągły, całodobowy system pracy administratorów, którzy prowadzą działania na miejscu, dbając na bieżąco o poprawność pracy systemów. Jest to system pracy najbardziej kosztowny, jednak – biorąc pod uwagę konieczność zapewnienia stałej dostępności usług dla klientów – w konsekwencji najbardziej opłacalny.

Reasumując, należy również pamiętać o bardzo ważnej zasadzie, mającej ogromny wpływ na skrócenie czasu wyeliminowania zagrożenia. Zadania dla każdej z omówionych grup ryzyka winny być przeprowadzone efektywnie w sytuacji wystąpienia awarii, dla każdego z systemów, każdy z procesów powinien być opisany i na bieżąco aktualizowany. Dla jak największej liczby mogących wystąpić zdarzeń należy przygotować szczegółowe procedury informowania i reakcji, by pod presją czasu w sytuacji wystąpienia zagrożenia pracownik mógł podejmować trafne decyzje i realizował w pierwszej kolejności takie działania, które zminimalizują czas przestoju systemów.

Krzysztof Białek

15 LAT DOŚWIADCZENIA

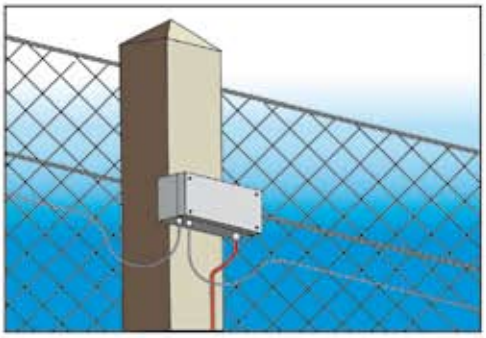
firma ATLine®

Firma ATLine sp.j. K. Cichulski, S. Pruski
91-845 Łódź, ul. Franciszkańska 125
tel: +48 (0) 42 657 30 80, fax: +48 (0) 42 655 20 99
info@atline.pl
biuro@atline.com.pl
www.atline.pl

AN 303
liniowy czujnik wibracyjny na ogrodzenie

ANIKOM

zewnętrzny czujnik wibracyjny AN303 z kablem sensorycznym, instalowany na ogrodzeniu; 2 strefy po 300m każda;



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

Protech

zewnętrzne czujki dualne; kombinacja mikrofal wykorzystujących efekt Doppler'a i pasywnej podczerwieni;

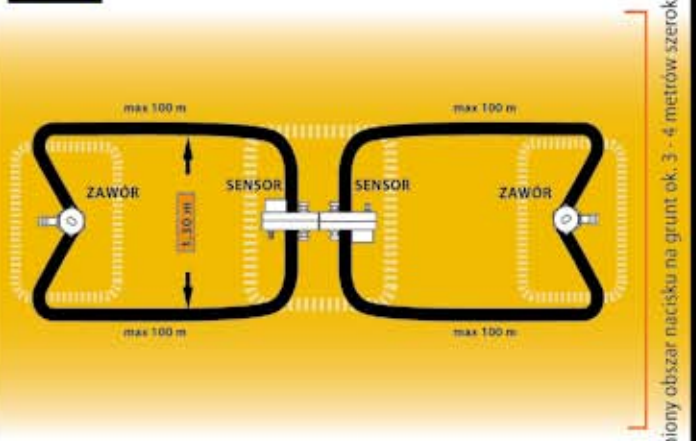
MANTA
zewnętrzna cyfrowa bariera mikrofalowa

CIAS

- zasięg 50 lub 80m
- 16 kanałów modulacji częstotliwości
- cyfrowa regulacja parametrów pracy
- zapis zdarzeń poprzez port RS485/232 i oprogramowanie

GPS (Ground Perimeter System)
zewnętrzny zakopywany system peryferyjnej ochrony obiektów z kablem ciśnieniowym; dostępny w wersji sieciowej lub STAND-ALONE

GPS STANDARD



NOWE BARIERY PODCZERWIENI ELKRON

OPTYMALNA OCHRONA

4 częstotliwości działania do wyboru
łatwa i szybka instalacja

EL50RT4PH-250m 4 wiązki, zasięg wew. 500m/ zew. 250m
EL50RT2PH-150m 2 wiązki, zasięg wew. 300m/ zew. 150m
EL50RT2PH-60m 2 wiązki, zasięg wew. 120m/ zew. 60m

ELKRON

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

PAG

the Art of PROTECTION

Szczegóły oferty, lista dystrybutorów na stronie:
www.pag.com.pl

ALARMTECH

AGENTOWY SYSTEM ROJU

NOVATOR

NOWA ARCHITEKTURA SYSTEMÓW ALARMOWYCH

- architektura systemów sztucznej inteligencji
- łatwość budowy, autokonfiguracja
- wysoki poziom bezpieczeństwa
- elastyczność - brak ograniczeń
- wszechstronność zastosowań
- skalowalność systemu
- optymalizacja kosztów
- samonaprawialność
- odporność na ataki
- niezawodność

I miejsce w kategorii urządzeń dla SSWiN

Polski Mistrz Techniki Alarmowej 2008

Laureat Nagrody Głównej "Złota Zbroja"

www.alarmtech.pl

Alarmtech Polska Sp. z o.o., ul. Kielnieńska 115, 80-299 Gdańsk, tel. 058 340 24 40, fax 058 340 24 49, info@alarmtech.pl

Strefa Schengen

– czyli co trzeba wiedzieć o SIS, VIS i ESI

Artykuł jest zarazem „pokłosiem" i uzupełnieniem problematyki funkcjonowania w warunkach polskich Konwencji Wykonawczej Schengen, prezentowanej przez autorów w ramach konferencji Securex 2008. Zgłaszane w kuluarach pytania i wątpliwości co do zakresu niezbędnych zmian, wynikających z kontroli bezpieczeństwa w ramach Systemu Informacyjnego Schengen, w połączeniu z zadaniami wizowymi oraz zobowiązaniami wobec EUROPOLU są przyczynkiem do tak szerokiego wyjaśniania tych spraw, bowiem ich znajomość jest ciągle w naszym społeczeństwie zbyt powierzchowna. W artykule autorzy omawiają podstawowe rozstrzygnięcia problemu i wskazują dostępne materiały źródłowe

1. Budowa strefy Schengen i Systemu Informacyjnego Schengen (SIS)

Problem „Wspólnot Europejskich bez wewnętrznych granic" został podniesiony w momencie, gdy okazało się, że istniejące transgraniczne układy handlowe, będące środkiem przyśpieszonego rozwoju, są niepotrzebnie spowalniane w wyniku rekonwersji pracy i pieniądza. Po analizie okazało się, że źródłem zaburzeń stały się formalności i opłaty celne –zwracane w trybie późniejszym zgodnie z funkcjonującymi już zobowiązaniami wzajemnymi, ograniczały szybkość przepływu pieniądza i generowały straty (finansowe i czasowe).

Rozwiązania EOG/EEA (Europejskiego Obszaru Gospodarczego/*European Economic Area*) nie pozwalały na szersze zmiany gospodarcze bez wprowadzenia niezbędnych zmian politycznych – pojawiła się idea wspólnie kontrolowanej strefy wewnętrznej o swobodnym przepływie ludzi i informacji, zapewniającej wspólną politykę informacyjną w zakresie bezpieczeństwa osobowego i wizowego. Podjęty wysiłek zaowocował powołaniem strefy Schengen.

1.1. Strefa Schengen i jej umocowania prawne

Strefa Schengen jest obszarem, na którym zniesiona została kontrola graniczna na granicach wewnętrznych oraz stosowane są ściśle określone jednolite zasady dotyczące:

- kontroli na granicach zewnętrznych,
- wzoru wiz wydawanych cudzoziemcom,
- wzajemnej współpracy pomiędzy służbami państw – sygnatariuszy, w szczególności w zakresie współpracy policyjnej i sądowej w sprawach kryminalnych, jak również działania tzw. Systemu Informacyjnego Schengen (SIS).

Strefa Schengen powstała jako rezultat wprowadzenia drogą międzynarodowej umowy swobody przemieszczania się ludzi i ułatwień handlowych. Ciągle rozszerzany Układ z Schengen jest umową międzynarodową, zawartą 14 czerwca 1985 r. między Belgią, Francją, Holandią, Luksemburgiem i Niemcami. Zakłada ona stopniowe znoszenie kontroli na wspólnych granicach, mające na celu zapewnienie swobody przepływu osób na obszarze składającym się z terytoriów państw – sygnatariuszy, czyli w tzw. strefie Schengen.

1.1.1. Konwencja Wykonawcza Schengen (KWS)

Konwencja Wykonawcza do Układu z Schengen (powstała w 1990 r.) ustanawia jednolite zasady kontroli na granicach zewnętrznych, jednakże jej zasadniczą treść stanowią przepisy wprowadzające tzw. środki wyrównawcze, których celem miało być wyrównanie „deficytu bezpieczeństwa" powstałego na skutek zniesienia kontroli na granicach wewnętrznych.

Do najważniejszych z nich należą:

- ujednolicenie standardów kontroli na granicach zewnętrznych (art. 3–27), w tym wymogów wizowych (art. 9–18) oraz postępowania wobec obcokrajowców;
- harmonizacja przepisów w dziedzinie polityki azylowej (art. 28–38);
- ściślejsza współpraca pomiędzy narodowymi służbami policyjnymi (art. 39–47), w szczególności w zakresie pościgu (tzw. *hot pursuit*) i obserwacji transgranicznej;
- współpraca sądowa i administracyjna, dotycząca między innymi ekstradycji (art. 59–66) oraz wykonywania wyroków w sprawach karnych (art. 67–69);
- jednolita polityka wobec handlu narkotykami i innymi środkami odurzającymi (art. 70–76), a także posiadania i obrotu bronią palną oraz amunicją (art. 77–91);
- stworzenie elektronicznego Systemu Informacji Schengen (SIS), zapewniającego dostęp do danych umożliwiających identyfikację konkretnych osób i rzeczy (art. 92–119).

Konwencja Wykonawcza weszła w życie w roku 1995, a następnie została włączona do systemu prawnego Unii

Europejskiej na mocy Traktatu Amsterdamskiego z 1997 r., który ustanowił cały dorobek Schengen (tzw. *acquis* Schengen) częścią wspólnotowego porządku prawnego. Traktat Amsterdamski wszedł w życie w maju 1999 r. i od tego czasu stosowane są w ramach porządku wspólnotowego przepisy dorobku Schengen, który jest nadal rozwijany w prawnych i instytucjonalnych ramach Unii Europejskiej.

1.2. Dorobek prawny i reżim wykonawczy strefy Schengen

W skład dorobku prawnego Schengen, poza samym Układem z Schengen i Konwencją Wykonawczą, wchodzą również:

- protokoły akcesyjne i porozumienia do układu z 1985 r.;
- protokoły Porozumienia Wykonawczego z 1990 r., zawarte z Włochami (podpisane w Paryżu 27 listopada 1990 r.), Hiszpanią i Portugalią (podpisane w Bonn 25 czerwca 1991 r.), Grecją (podpisane w Madrycie 6 listopada 1992 r.), Austrią (podpisane w Brukseli 28 kwietnia 1995 r.) oraz z Danią, Finlandią i Szwecją (podpisane w Luksemburgu 19 grudnia 1996 r.), wraz z odnoszącymi się do nich Aktem Końcowym i Wspólnymi Oświadczeniami;
- decyzje i oświadczenia przyjęte przez Komitet Wykonawczy ustanowiony na podstawie postanowień Porozumienia Wykonawczego z 1990 r.;
- akty przyjęte przez organy, którym Komitet Wykonawczy udzielił kompetencji decyzyjnych dla wdrażania Porozumienia Wykonawczego (łącznie około 3000 stron).

Treść Konwencji Wykonawczej do Układu z Schengen, wynikająca z Traktatu Wspólnot Europejskich i uzupełniona Jednolitym Aktem Europejskim, jest dostępna w języku polskim w Dzienniku Urzędowym Wspólnot Europejskich z 2000 r., wolumin 19, t. 2, s. 9, poz. L 239/19 z dnia 22 września 2000 roku.

Obecnie (od 28 października 2007 r.) strefa Schengen obejmuje następujące państwa: Austrię, Belgię, Czechy, Danię, Estonię, Finlandię, Francję, Grecję, Hiszpanię, Holandię, Litwę, Luksemburg, Łotwę, Maltę, Niemcy, Polskę, Portugalię, Słowację, Słowenię, Węgry oraz Włochy.

Państwami stowarzyszonymi, stosującymi reżim Schengen, są Norwegia i Islandia.

Państwami członkowskimi UE, które nadal pozostają poza obszarem Schengen, są Wielka Brytania i Irlandia. Kraje te podjęły decyzję o zachowaniu kontroli granicznych na granicach z innymi państwami członkowskimi UE, jednakże mogą one stosować niektóre postanowienia dotyczące współpracy policyjnej i sądowej w sprawach kryminalnych (EUROPOL).

Ponadto zawarto specjalne umowy dotyczące ułatwień w ruchu granicznym na obszarze Schengen dla obywateli państw Europejskiego Obszaru Gospodarczego (EOG/EEA) oraz Szwajcarii.

1.2.1. SIS jako baza wykonawcza strefy Schengen

Strefa Schengen jest obszarem, na którym zniesiona została kontrola graniczna na wspólnych granicach i zapewniona została swoboda przepływu osób. Swoboda przemieszczania się osób wewnątrz dotyczy nie tylko obywateli państw – sygnatariuszy, ale wszystkich osób dowolnej narodowości i o dowolnym obywatelstwie, które przekraczają granice wewnętrzne na obszarze objętym układem. W strefie Schengen stosowane są ściśle określone jednolite zasady postępowania dotyczące: kontroli na granicach zewnętrznych, wprowadzenia wspólnej polityki wizowej, wzajemnej współpracy pomiędzy służbami państw – sygnatariuszy, w szczególności w zakresie współpracy policyjnej i sądowej w sprawach kryminalnych, jak również działania tzw. Systemu Informacyjnego Schengen (SIS).

SIS jest wspólną elektroniczną bazą danych o poszukiwanych osobach i przedmiotach, składającą się z modułów krajowych oraz jednostki centralnej, usytuowanej w Strasburgu. Dane wprowadzone do systemu przez jedno państwo członkowskie dostępne są dla służb i organów pozostałych państw w niezbędnym dla nich zakresie. System ten zapewnia wymianę informacji pomiędzy służbami odpowiedzialnymi za:

- ochronę granic,
- wydawanie wiz,
- bezpieczeństwo publiczne.

Podczas przekraczania granic zewnętrznych lub podczas standardowej kontroli policyjnej przy użyciu SIS następuje sprawdzenie, czy dany przedmiot (np. samochód) albo osoba figurują we wspólnej bazie danych. SIS może zawierać następujące dane osobowe: imię, nazwisko, ew. pseudonimy, stałe cechy wyglądu zewnętrznego, inicjały drugich imion, miejsce i datę urodzenia, płeć, narodowość, oznaczenie „uzbrojony", „groźny", powód wpisania do SIS oraz jakie kroki należy przedsięwziąć wobec danej osoby. W ramach traktatu z Schengen istnieją dwa zestawy reguł dotyczących przetwarzania danych osobowych: pierwszy dotyczy danych osobowych przetwarzanych w SIS, a drugi danych osobowych przetwarzanych w ramach współpracy policji i wymiaru sprawiedliwości z krajów objętych obszarem Schengen.

W przypadku, gdy dana osoba jest poszukiwana przez służby państwa – strony Układu, stosowana jest odpowiednia procedura, która może polegać np. na odmówieniu danej osobie prawa wjazdu na obszar strefy Schengen lub podjęciu odpowiednich działań policyjnych.

Specjalny organ kontroluje przetwarzanie danych osobowych w tym obszarze, a instytucje w poszczególnych krajach są kontrolowane przez krajowe organy ds. ochrony danych osobowych. One też rozpatrują wszelkie skargi.

OBECNI CZŁONKOWIE

1995: Belgia, Francja, Holandia, Niemcy, Luksemburg, Hiszpania, Portugalia
1997: Austria, Włochy
2000: Grecja
2001: Dania, Finlandia, Szwecja oraz Islandia, Norwegia pozostające poza Unią Europejską

ROZSZERZENIE W 2007

Czechy, Estonia, Litwa, Łotwa, Malta, Polska, Słowacja, Słowenia, Węgry

PAŃSTWA, KTÓRE ZAMIERZAJĄ PRZYSTĄPIĆ DO STREFY SCHENGEN

2008: Szwajcaria (włączając Lichtenstein)
2009: Cypr
2011: Bułgaria, Rumunia

Rys. 1. Państwa strefy Schengen

1.2.2 Zobowiązania Polski wobec danych SIS w strefie Schengen

Zgodnie z ustawą z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej polskim administratorem danych przetwarzanych w Systemie Informacyjnym Schengen jest Komendant Główny Policji i do niego należy zgłaszać wnioski o udostępnienie lub modyfikację danych. Należy mieć na uwadze, że wykorzystywanie danych systemu SIS może następować bez wiedzy i zgody osób, których dane dotyczą, oraz bez obowiązku ujawniania faktycznego celu zbierania danych. Aby zapewnić odpowiednią ochronę prawną osób, których dane są przechowywane w systemie SIS, Generalny Inspektor Ochrony Danych Osobowych sprawuje kontrolę nad tym, czy wykorzystywanie danych nie narusza praw osób, których dane te dotyczą. Kontrola ta jest sprawowana zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Za szkody wyrządzone przez niezgodne z prawem wykorzystywanie danych SIS odpowiada Skarb Państwa. Organem reprezentującym Skarb Państwa w sprawach odszkodowawczych jest Prokuratoria Generalna Skarbu Państwa.

2. Mechanizmy bezpieczeństwa budowy i użytkowania systemu Schengen

W Polsce kluczowym dokumentem strategicznym, poświęconym kwestiom wdrażania dorobku prawnego Schengen, był *Plan Działania w zakresie wdrażania dorobku prawnego Schengen w Polsce (Poland – Schengen Action Plan)*, który został przyjęty w dniu 15 sierpnia 2001 roku przez Komitet Integracji Europejskiej. Ten corocznie aktualizowany dokument określał zarówno priorytety, jak i instrumenty wdrażania dorobku (*acquis*) Schengen w Polsce, wyznaczając również terminy wykonania poszczególnych działań.

Instytucja sprawdzająca dane w SIS	Zakres sprawdzanych danych
Minister Spraw Wewnętrznych i Administracji	Art. 100
Prezes Urzędu ds. Repatriacji	Art. 96, 100 (dokumenty tożsamości)
Wojewoda	Art. 96, 100 (dokumenty tożsamości)
Policja	Art. 95, 96, 97, 98, 99, 100
Straż Graniczna	Art. 95, 96, 97, 98, 99, 100
Minister Sprawiedliwości	Art. 95, 96, 97, 98, 99, 100
Sąd	Art. 95, 96, 97, 98, 99, 100
Prokurator	Art. 95, 96, 97, 98, 99, 100
Służby celne	Art. 95, 96, 97, 98, 99, 100
Generalny Inspektor Informacji Finansowej	Art. 98, 100
Generalny Inspektor Kontroli Skarbowej	Art. 98, 99, 100
Agencja Bezpieczeństwa Wewnętrznego	Art. 99
Minister Spraw Zagranicznych	Art. 96
Konsul	Art. 96

Tab. 1. Instytucje w Polsce uprawnione do korzystania z SIS i zakres ich uprawnień

Szczegółowa prezentacja projektu budowy polskiego komponentu Systemu Informacyjnego Schengen została zawarta w dokumencie *Program dla uczestnictwa Rzeczypospolitej Polskiej w realizacji tytułu IV Konwencji Wykonawczej Schengen (MASTERPLAN SIS II PL)*. Definiuje on zadania, których wykonanie jest niezbędne dla pełnego stosowania przez Polskę części dorobku prawnego Schengen, uregulowanego Tytułem IV Konwencji Wykonawczej.

W dniu 24 sierpnia 2007 r. Sejm Rzeczypospolitej Polskiej przyjął „ustawę o udziale RP w Systemie Informacyjnym Schengen (SIS) i Systemie Informacji Wizowej (VIS)". Ustawa określa zasady i tryb udziału Rzeczypospolitej Polskiej w tych systemach, w tym obowiązki organów dokonujących wpisów oraz organów uprawnionych do dostępu do danych poprzez Krajowy System Informatyczny.

Polska od przystąpienia do UE w dniu 1 maja 2004 roku jest odpowiedzialna za zabezpieczenie jednego z najdłuższych odcinków wspólnej lądowej granicy zewnętrznej, o czym warto i trzeba pamiętać.

2.1. Dorobek Konwencji Wykonawczej Schengen (KWS)

Jednym z głównych celów działania Unii Europejskiej jest utrzymanie i rozwijanie Unii jako przestrzeni wolności, bezpieczeństwa i sprawiedliwości, w której zagwarantowana jest swoboda przepływu osób, w powiązaniu z właściwymi środkami stosowanymi w odniesieniu do kontroli granic zewnętrznych, azylu, imigracji oraz zapobieganie i zwalczanie przestępczości.

Genezy współpracy państw w III filarze Unii Europejskiej należy się doszukiwać w utworzeniu w 1976 r. Grupy TREVI (ang. *Terrorism, Radicalism, Extremism, Violence International*, czyli Terroryzm, Radykalizm, Ekstremizm, Przemoc Międzynarodowa). Ta forma współpracy państw zakładała głównie walkę z terroryzmem i międzynarodowymi grupami przestępczymi.

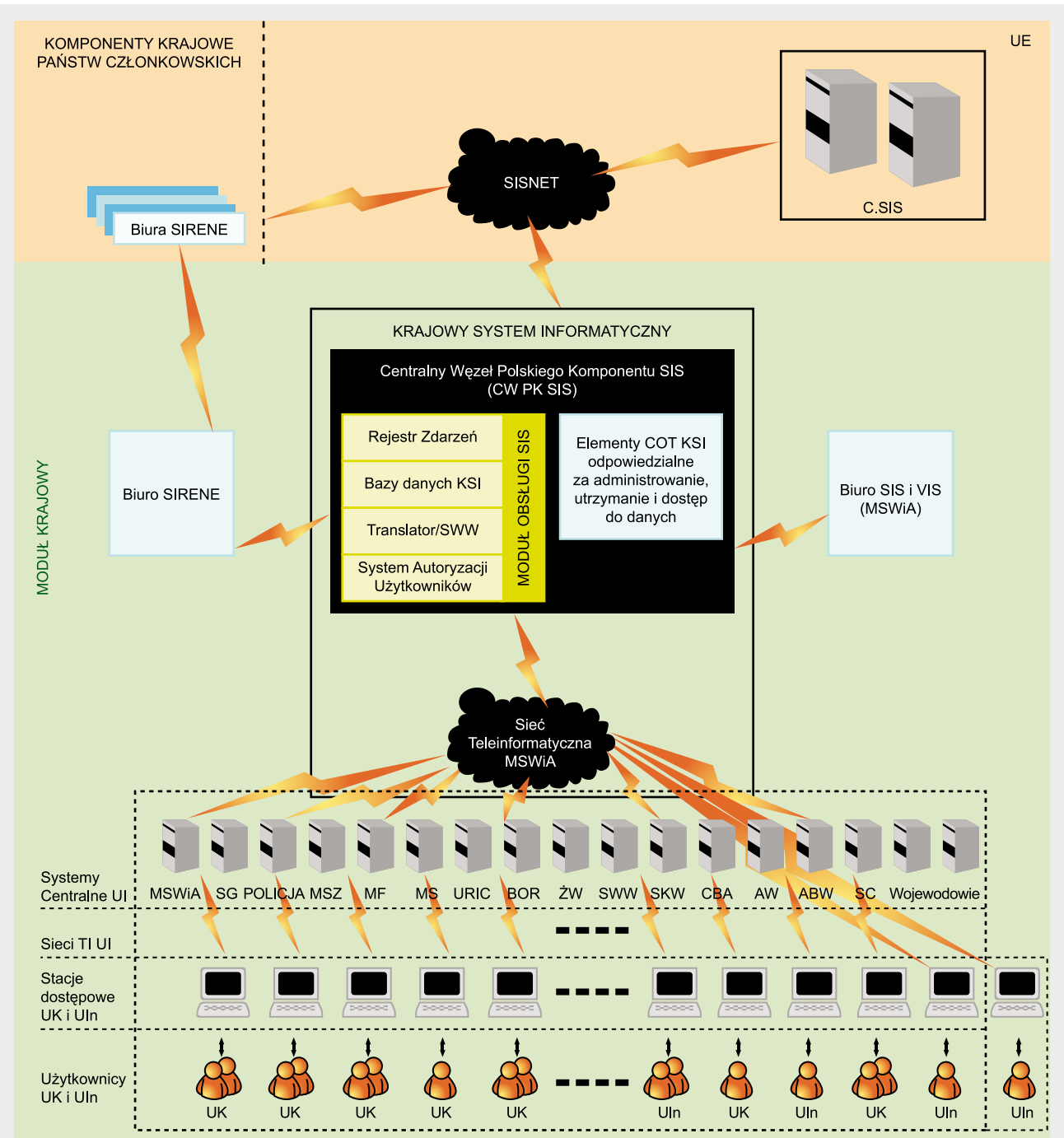
Działalność oparta była na współpracy międzyrządowej (były to spotkania ministrów spraw wewnętrznych i sprawiedliwości oraz wysokich urzędników, odbywające się dwa razy do roku, a także spotkania grup roboczych). W ramach Grupy TREVI rozszerzano współpracę dotyczącą: zwalczania terroryzmu, wspólnych działań policji, zwalczania międzynarodowej przestępczości zorganizowanej, ochrony i bezpieczeństwa instalacji i urządzeń nuklearnych, przeciwdziałania klęskom żywiołowym oraz stworzenia systemu komputerowego na potrzeby policji. Ta pozainstytucjonalna forma współpracy z czasem przyniosła efekty w postaci powołania krajowych centrów spotkań, wymiany informacji, komputeryzacji baz danych oraz wprowadzenia nowych metod i technik szkolenia policji.

Zrozumiały jest cały szereg wykonywanych działań krajowych i międzynarodowych, ukierunkowanych na zapewnienie bezpieczeństwa uzyskiwanych i przechowywanych informacji, niezależnie od ich postaci oraz nośników, na których zostały one zapisane, oraz przedsięwzięcia podjęte dla ochrony całości bazy danych, przy zapewnieniu

szybkiego i jednoznacznego weryfikowania zapytań i informacji jednostkowych.

Funkcjonujący od początku sierpnia 2007 r. System Informacyjny Schengen (SIS 1+) jest nowym instrumentem do walki z przestępczością zorganizowaną oraz nielegalną migracją. Dane zawarte w bazie systemu wykorzystywane są podczas kontroli policyjnej, granicznej, celnej oraz przy wydawaniu wiz i zezwoleń na pobyt w stosunku do obywateli krajów trzecich. Dzięki SIS 1+ polski wymiar sprawiedliwości ma stały dostęp do informacji o przestępcach zatrzymywanych w innych krajach, co zwiększa szanse na sprowadzenie i ukaranie tych, którzy uciekli za granicę. Oto kilka przykładów z materiałów KGP (źródło – biuletyn z dn. 27 września 2007 r.).

I/ Wydział Kryminalny Komendy Mokotów (23.08.07). Funkcjonariusze otrzymali poufną informację, z której wynikało, że pewna mieszkanka ich dzielnicy zakupiła ostatnio srebrnego mercedesa klasy R i że pochodzi on prawdopodobnie z kradzieży. Policjanci natychmiast udali się do mieszkania kobiety. Katarzyna P. zapewniała policjantów, że auto nabyła 21 czerwca w Niemczech od pewnej 26-latki. Twierdziła, że samochód nie do końca odpowiadał ofercie zamieszczonej w Internecie, w związku z czym cenę auta obniżono do 30000 euro. Jeszcze tego samego dnia zakupionym właśnie samochodem wróciła do kraju. Kobietę oraz jej znajomego przesłuchano, a mercedesa zabezpieczono na policyjnym parkingu i sprawdzono dane pojazdu



Rys. 2. Infrastruktura systemu SIS 1+ (UE – Unia Europejska, UI – Użytkownik Instytucjonalny, UIn – Użytkownik Indywidualny, C.SIS – Centralny SIS, SieciCOT KSI – Centralny Organ Techniczny, Sieci TI UI – Sieci Teleinformatyczne Użytkowników Instytucjonalnych). Źródło: MasterPlan SIS i VIS PL wer. 4.0.

w nowym Systemie Informacyjnym Schengen (SIS 1+). Szybko okazało się, że auto zostało skradzione 18 czerwca br. we Włoszech i poszukiwane jest przez komisariat policji w Neapolu.

II/ W ubiegłym tygodniu (17.09.07) policjanci z Marek zatrzymali poszukiwanego przez niemiecką policję 29-letniego Macieja W. Mężczyzna poszukiwany był w związku z podejrzeniem dokonania wielu oszustw i wyłudzeń na terenie Niemiec. Było to pierwsze zatrzymanie w powiecie wołomińskim osoby zarejestrowanej jako poszukiwana w nowym systemie SIS 1+. W Warszawie to drugi taki przypadek.

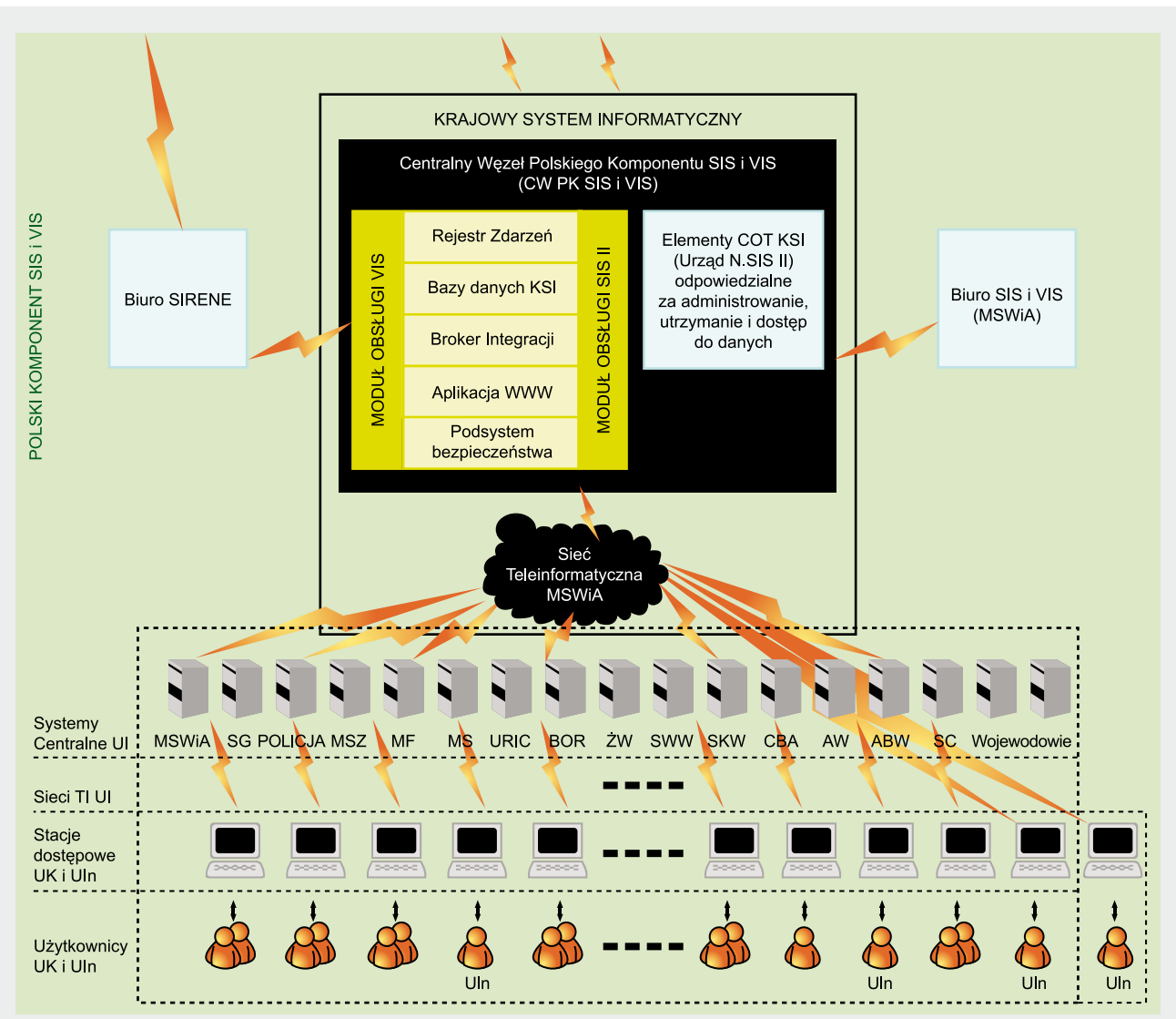
III/ 26.09.07 około 9.15 policjanci z tarnobrzeskiej drogówki zwrócili uwagę na jadący bez świateł samochód. Siedzący w nim mężczyzna nie miał zapiętych pasów bezpieczeństwa. Zatrzymali auto do kontroli. W trakcie sprawdzenia w policyjnej bazie informacyjnej SIS 1+ okazało się, że mężczyzna poszukiwany jest przez holenderską prokuraturę za rozbój w 2004 r. Na 35-letniego mieszkańca Tarnobrzega wydano Europejski Nakaz Aresztowania. Mężczyzna został zatrzymany. O jego losach zadecyduje sąd. Holenderski wymiar sprawiedliwości ma możliwość wystąpienia o ekstradycję mężczyzny.

Tabela 1 dotyczy Konwencji Wykonawczej Schengen, która obejmuje wraz ze swoimi aktualizacjami wszystkie warianty SIS (SIS stary – zwany także SIS I; pośredni – SIS 1+; oraz docelowy SIS II razem z VIS). Należy pamiętać, że baza danych SIS może zawierać tylko i wyłącznie informacje przewidziane przez KWS (Art. 94.3).

2.2. Zasady i zobowiązania narodowe w zakresie bezpieczeństwa

Dla zachowania bezpieczeństwa systemu obowiązują zasady ochrony informacji zgodne z wymaganiami UE (załączniki X i XI do Traktatu Amsterdamskiego), uzupełnione wymaganiami Komisji Europejskiej z dnia 29 listopada 2001 r. (dyrektywa EC 1041/2001).

Zobowiązania narodowe w zakresie bezpieczeństwa obejmują Polski Komponent SIS (PK SIS) – system informacyjny obejmujący CW PK SIS, użytkowników indywidualnych,



Rys. 3. Infrastruktura systemu SIS II z modułem VIS (UE – Unia Europejska, UI – Użytkownik Instytucjonalny, UIn – Użytkownik Indywidualny, CS-SIS – Centralny System SIS, CS-VIS – Centralny System VIS, NI-SIS – Narodowy Interfejs systemu SIS, NI-VIS – Narodowy Interfejs systemu VIS, COT KSI – Centralny Organ Techniczny, Sieci TI UI – Sieci Teleinformatyczne Użytkowników Instytucjonalnych). Źródło: MasterPlan SIS i VIS PL wer. 4.0.

sieć teleinformatyczną MSWiA, systemy centralne użytkowników instytucjonalnych, w tym sieci teleinformatyczne UI i stacje dostępowe wraz z użytkownikami końcowymi, oraz infrastrukturę teleinformatyczną polskiego Biura SIRENE oraz Biura SIS i VIS, włączając w to ich wzajemne relacje. Polski Komponent SIS jest rozumiany jako całość infrastruktury technicznej, prawnej i organizacyjnej wraz z niezbędnym personelem, uczestniczącym w wymianie informacji z centralnym systemem SIS (realizowanym jako moduł krajowy).

Zobowiązania narodowe obejmują etap SIS 1+ oraz docelowy (2009) SIS II i VIS, określają uprawnienia osób funkcyjnych oraz użytkowników końcowych (instytucjonalnych i indywidualnych).

Za zasadę główną uważa się **pośredni dostęp do danych**. Uprawnieni użytkownicy instytucjonalni mają dostęp bezpośredni w celu uzupełniania i aktualizowania danych w KSI.

Pośredni dostęp do danych wykorzystywanych poprzez Krajowy System Informatyczny jest realizowany:

1. w celu wglądu do danych SIS dotyczących przedmiotów do celów ich zajęcia lub wykorzystania jako dowodów w postępowaniu karnym, wskazanych w art. 100 ust. 3 lit. a, b i f Konwencji Wykonawczej z dnia 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 r. między rządami państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach, i przysługuje organom samorządowym właściwym w sprawach rejestracji pojazdów;
2. w celu wglądu do danych VIS, który przysługuje: sądowi, prokuraturze, policji, Straży Granicznej, Służbie Celnej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnemu Biuru Antykorupcyjnemu, organom kontroli skarbowej, Biuru Ochrony Rządu, Służbie Kontrwywiadu Wojskowego, Żandarmerii Wojskowej oraz Służbie Wywiadu Wojskowego;

jeżeli:

3. dostęp jest konieczny w celu zapobiegania, wykrywania lub ścigania przestępstw wymienionych w art. 607 w kodeksu postępowania karnego (Dz. U. z 1997 r., nr 89, poz. 555 z późn. zm.);
4. jest to niezbędne w związku z określoną sprawą;
5. istnieją uzasadnione powody do uznania, że wgląd do danych VIS ma istotne znaczenie dla zapobiegania, wykrywania lub ścigania przestępstw, o których jest mowa w pkt. 1., przy zachowaniu warunków wynikających z zasad krajowych ochrony informacji.

2.3. Biuro SIRENE – nadzór nad działaniem systemu

SIRENE to anglojęzyczny skrót terminu *Supplementary Information Request at the National Entry* – tłumaczony dosłownie oznacza „wniosek o informacje uzupełniające na wejściu krajowym", a dotyczy weryfikacji bezpieczeństwa stałych informacji bazowych. Na poziomie całości systemu w UE biuro SIRENE zapewnia nadzór nad terminowością odświeżania i weryfikacji podstawowej kopii krajowych (min. co kwadrans) oraz eliminuje zapisy uzupełniające, pozostające bez wtórnej weryfikacji danych uzupełniających (maks. 14 dni).

W warunkach krajowych biuro SIRENE to wyodrębniona organizacyjnie komórka w ramach struktury Komendy Głównej Policji, zapewniająca w szczególności wymianę informacji uzupełniających w trybie i zgodnie z zasadami określonymi w Załączniku Nr 1 do Decyzji Komisji 2006/758/WE z dnia 22 września 2006 r. w sprawie zmiany podręcznika SIRENE (Dz. Urz. WE L 317 z dnia 16.11.2006, s. 41).

Biuro krajowe SIRENE realizuje dwa główne zadania w ramach systemu:

- koordynowanie i nadzór nad polityką bezpieczeństwa krajowej sieci użytkowników SIS (Art. 118),
- zapewnienie przestrzegania Konwencji oraz przepisów prawa polskiego w zakresie ochrony danych osobowych (ODO).

Biuro krajowe SIRENE kontroluje istotne elementy bezpieczeństwa SIS:

- rejestr zdarzeń,
- czas wzorcowy,

a także inne (wynikające ze struktury systemu KSI – CW PK SIS) na styku z CS SIS.

2.4. Zarządzanie granicami zewnętrznymi UE – agencja FRONTEX

Agencja FRONTEX z siedzibą w Warszawie powołana została Rozporządzeniem Rady (WE) Nr 2007/2004 z dnia 26.10.2004, ustanawiającym Europejską Agencję Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach Państw Członkowskich Unii Europejskiej.

Zadania agencji związane są z nadzorowaniem udostępniania danych i poprawności funkcjonowania systemów SIS II i VIS wobec konieczności zachowania bezpieczeństwa strefy Schengen.

Agencja FRONTEX, poprzez kontrolę czasu napływu informacji i zapytań, wykorzystując stempel czasu, nadzoruje system antykorupcyjny w obszarze wizowym oraz weryfikuje:

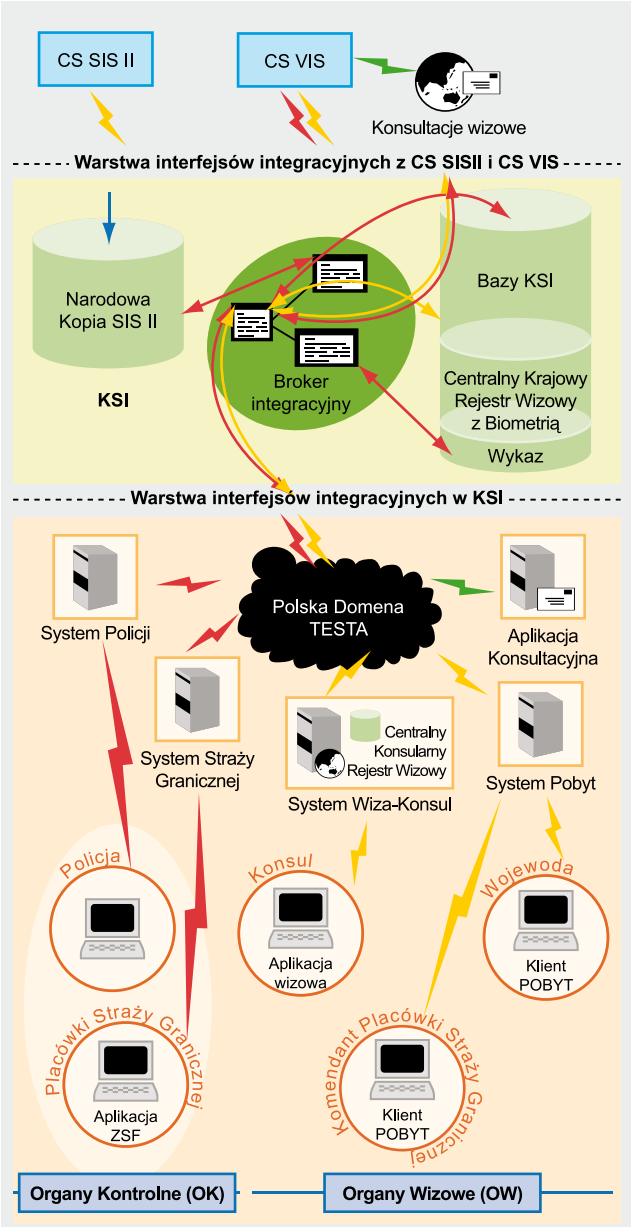
- rejestr zdarzeń,
- czas wzorcowy,
- paszporty biometryczne,
- wizy,

współpracując z Komisją Europejską ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych.

Działania agencji są szczególnie istotne w odniesieniu do „kraju przyjęcia" dla osób posiadających wizy „C" a udających się na czasowy pobyt w strefie Schengen.

3. Teleinformatyczne aspekty bezpieczeństwa systemu i danych w nim zawartych

Całość systemu informacyjnego strefy Schengen oparta jest na wykorzystaniu wspólnych zasobów informacyjnych, aktualizowanych w trybie ciągłym i nadzorowanych co do aktualności ich wprowadzenia (potwierdzanie w sprawie i przymusowa eliminacja przy jego braku). System funkcjonuje na bazie serwerów wykonujących czynności gromadzenia, rejestrowania i udostępniania całej zawartości bazy informacyjnej przy zachowaniu dostępności komponentu krajowego pod kątem zmian realizowanych przez upoważnionego użytkownika (tzn. uzupełnień, modyfikacji stanu – włącznie z usunięciem danego pliku).



Rys. 4. Schemat funkcjonowania SIS II i VIS po roku 2009

Bezpieczeństwo informacji w systemie jest zachowywane na zasadach zbliżonych do warunków klauzuli „*confidential*" i odpowiada polskiemu poziomowi ochrony danych osobowych wynikających z obowiązującej ustawy z 1997 roku (tekst jednolity: Dz. U. z 2002 r., nr 101, poz. 926 z późn. zm.) oraz jej rozporządzeniom wykonawczym (w szczególności: Dz. U. z 2004 r., nr 100, poz. 1024).

Bezpieczeństwo informacji chronionych na poziomie UE jest oparte na zasadach przewidzianych w regulaminie Komisji Europejskiej i przez nią nadzorowane co do zakresu i sposobu stosowania. Aktualnie SIS 1+ wykorzystuje rozwiązania przedstawione przez Portugalię w ramach systemu narodowego N.SIS, udostępnionego dla nowych członków UE (SISone4ALL).

Docelowo SIS II będzie posiadał podwyższoną ochronę kryptograficzną (Crypto-Intranet) i specjalizowaną infrastrukturę PKI w obszarze ponadnarodowym przy zachowaniu narodowych wymagań ochrony kryptograficznej w kopiach krajowych (KSI).

3.1. Infrastruktura systemu SIS – cechy podstawowe

Obecnie na obszarze państw, które przystąpiły do strefy Schengen w 2007r., mamy sytuację pośrednią, określaną jako system SIS 1+, którą obrazuje poniższy schemat.

Sytuacja taka wynikła z opóźnień we wdrażaniu docelowego systemu SIS II (termin planowany, 2007 r., nie mógł być dotrzymany ze względu na opóźniający się przetarg na system łączności s-TESTA), a realizacja tak okrojonej wersji systemowej odbyła się wyłącznie dzięki decyzji Portugalii. Projekt zaproponowany przez Portugalię polegał na opracowaniu i przekazaniu kopii oprogramowania portugalskiego N.SIS państwom, które przystąpiły do UE w 2004 r. Ponadto w ramach tego projektu zawarte zostały również szkolenia, koordynowanie testów krajowych oraz zarządzanie projektem globalnym. Decyzja o przyjęciu do realizacji projektu SISone4ALL została podjęta podczas posiedzenia Rady Wymiaru Sprawiedliwości i Spraw Wewnętrznych w dniach 4–5 grudnia 2006 r.

Uruchomiona dla potrzeb systemu SIS 1+ sieć SISNET dla celów przesyłania danych w procesie konsultacji wizowych VISION i dla potrzeb komunikacji pomiędzy Biurami SIRENE jest uzupełnieniem dotychczasowego „starego SIS", opartego na korzystaniu z przestarzałego protokołu X400.

Tymczasem nowe technologie, oparte na *Web Services* i języku XML, w łatwy sposób umożliwiają integrację różnego typu systemów oraz zarządzanie danymi w wielu formatach, a właśnie taki ma być nowy SIS II (2009), mogący przetwarzać dane multimedialne – zdjęcia, dane biometryczne – nie tylko tekstowe, jak dotąd. Prace nad tym systemem rozpoczęły się w 2001 r., ale poprzedzone były dyskusjami toczącymi się już od 1998 r., zanim jeszcze zapadły decyzje o wielkim rozszerzeniu. Ich pełne zrealizowanie znacząco zmienia infrastrukturę Krajowego Systemu Informatycznego w obszarze Centralnego Węzła Polskiego Komponentu SIS i VIS.

Wprowadzone moduły obsługi SIS II i VIS pozwalają na przekazywanie pakietów informacyjnych, a nie tylko danych tekstowych (SIS I), zarazem zapewniając bezpieczeństwo wprowadzanych plików (nie tylko tekstowych), transportowanych w obszarze sieci TI MSWiA oraz przekazywanych do bazy danych KSI.

Należy podkreślić obowiązkowe zachowanie wymogów kryptograficznego zabezpieczania transmisji danych we wszystkich relacjach – stosownie do ustaleń KWS.

3.2. Infrastruktura techniczna systemów

Infrastruktura systemów wchodzących w skład CW PK SIS i VIS składa się z komponentów krajowych (sieć TI MSWiA, sieci użytkowników instytucjonalnych) oraz udostępnionych lub zakupionych w UE integratorów systemowych i stacji dostępowych (stacjonarnych oraz mobilnych), których docelowa ilość przekroczy 8 tys. sztuk.

Specyfikacja techniczna poszczególnych urządzeń wynika z założonych zadań (określonych potrzeb zadaniowych wg załączonej dokumentacji SIS II i VIS) przy możliwości współpracy z kolejnymi systemami. System SIS II współpracuje bezpośrednio z systemem VIS oraz będzie dysponował integratorem systemowym dla potrzeb rozbudowywanego

systemu informacyjnego policji europejskiej (EIS – *EUROPOL Information System*).

W ramach specjalizowanej infrastruktury technicznej przewidywane są stanowiska dostępowe użytkowników indywidualnych o wyodrębnionych uprawnieniach.

Infrastruktura techniczna systemu uniemożliwia nieautoryzowany dostęp do jego elementów oraz wszelkich przechowywanych zapisów, zapewniając rejestrację i identyfikację wszystkich realizowanych czynności.

3.3. Rejestracja i transmisja danych

Całość informacji/danych przechowywanych i przekazywanych w systemie podlega ustawowej ochronie (wg prawa RP).

Informacje w SIS II nie mają klauzuli tajności, ale właśnie ze względu na ochronę danych osobowych są oznaczone klauzulą zbliżoną do „*confidential*", co wymaga stosowania certyfikowanych urządzeń kryptograficznych i kontroli dostępu, aby wiedzieć, kto, kiedy, do czego miał dostęp i jakie były zapytania kierowane do systemu.

Wszystkie transmisje są chronione programowo i objęte zabezpieczeniami.

Krajowa kopia danych systemu (BD KSI) jest odnawiana w cyklu piętnastominutowym względem danych zgromadzonych w CS SIS. Czas dostępu dla użytkowników końcowych (zapytanie – odpowiedź) nie powinien docelowo przekraczać 15 sekund dla danych podstawowych (przekazanie zdjęcia – od 30 do maks. 90 sekund).

3.4. Bezpieczeństwo teleinformatyczne w systemie

W procesie przyjmowania zapytania i przekazywania danych bezpieczeństwo teleinformatyczne jest gwarantowane wobec każdego:

- **UI** – użytkownika instytucjonalnego – jest to uprawniona instytucja administracji publicznej
- **UK** – użytkownika końcowego – jest to osoba fizyczna, posiadająca określone prawa dostępu i korzystająca z uprawnionej stacji/terminala
- **UIn** – użytkownika indywidualnego – jest to UK korzystający z aplikacji dostępowych otrzymanych bezpośrednio z CW PK SIS II i VIS

pod warunkiem zachowania założonych wymagań procedur dostępowych (warunki sesji).

System wyklucza (znacznik i sygnatura czasu) posłużenie się wtórne wartościami sesji uprawnionej, uruchamia automatycznie blokadę informacyjną i procedury bezpieczeństwa.

4. Perspektywy i zagrożenia dla SIS II i VIS

Docelowo systemy SIS II i VIS będą zintegrowane z EIS (EUROPOL IS) i na bazie protokołu VISION będą współpracować z poszczególnymi służbami krajowymi, zapewniając bezpieczeństwo.

W praktyce przewidywany jest dostęp nadzoru informacyjnego EIS wobec grupy danych.

Opracowali:
dr inż. Marek Blim
mgr inż. Andrzej Dobosz

Bibliografia:

Akty prawne i dokumenty polskie (PL)

Pełnomocnik Rządu ds. SIS II i VIS

- Rozporządzenie Rady Ministrów z dnia 20.12.2004 w sprawie ustanowienia Pełnomocnika Rządu do spraw Przygotowania Organów Administracji Państwowej do Współpracy z Systemem Informacyjnym Schengen II (SIS II) i Systemem Informacji Wizowej (VIS) – Dz. U. z 2004 r., nr 281, poz. 2788, zm., Dz. U. z 2005 r., nr 48, poz. 449, Dz. U. z 2005 r., nr 196, poz. 1629, Dz. U. z 2006 r., nr 227, poz. 1659, Dz. U. z 2007 r., nr 62, poz. 420
- Decyzja Nr 103 Ministra Spraw Wewnętrznych i Administracji z dnia 1 czerwca 2006 r. w sprawie zakresu czynności Sekretarzy Stanu oraz Podsekretarzy Stanu w Ministerstwie Spraw Wewnętrznych i Administracji
- Zarządzenie Nr 141 Prezesa Rady Ministrów z dnia 12 września 2006 r. w sprawie Międzyresortowego Zespołu do spraw Informatyzacji
- Zarządzenie nr 75 Prezesa Rady Ministrów z dnia 12 sierpnia 2004 r. (z późn. zm.) w sprawie Międzyresortowego Zespołu do spraw Wykorzystania Środków w Ramach Funduszu Schengen oraz Norweskiego Mechanizmu Finansowego
- Zarządzenie Nr 24 Prezesa Rady Ministrów z dnia 7 marca 2007 r. w sprawie Komitetu Rady Ministrów do spraw Informatyzacji i Łączności
- Zarządzenie Nr 26 Ministra Spraw Wewnętrznych i Administracji z dnia 7 marca 2007 r. w sprawie zmiany nazwy państwowej jednostki budżetowej Władza Wdrażająca Program Współpracy Przygranicznej PHARE na Władza Wdrażająca Programy Europejskie oraz nadania jej statutu

Programy dla uczestnictwa Rzeczypospolitej Polskiej w realizacji Tytułu IV Konwencji Wykonawczej Schengen

- Program dla uczestnictwa Rzeczypospolitej Polskiej w realizacji Tytułu IV Konwencji Wykonawczej Schengen, MasterPlan SIS II PL wersja 2.4, zatwierdzony przez Radę Ministrów dnia 2 listopada 2004 r.
- Program dostosowania Organów Administracji Państwowej do współpracy z Systemem Informacyjnym Schengen (SIS II) i Systemem Informacji Wizowej (VIS), MasterPlan SIS II i VIS PL wersja 3.0, zaakceptowany przez Komitet Europejski Rady Ministrów dnia 13 września 2005 r.
- Program dostosowania Organów Administracji Państwowej do współpracy z Systemem Informacyjnym Schengen II (SIS II) i Systemem Informacji Wizowej (VIS), MasterPlan SIS II i VIS PL wersja 3.1, przyjęty przez Radę Ministrów dnia 27 czerwca 2006 r.
- Suplement VIS do programu dostosowania Organów Administracji Państwowej do współpracy z Systemem Informacyjnym Schengen (SIS II) i Systemem Informacji Wizowej (VIS), MasterPlan SIS II i VIS PL w. 3.1, przyjęty przez Radę Ministrów w dniu 30 kwietnia 2007 r.

Raporty

- Raport o postępach prac w ramach przygotowań Organów Administracji Państwowej do współpracy z Systemem

Informacyjnym Schengen II (SIS II) i Systemem Informacji Wizowej (VIS) z dnia 12 grudnia 2005 r., wersja 2.0
– Raport o stanie przygotowań Organów Administracji Państwowej do współpracy z Systemem Informacyjnym Schengen II (SIS II) i Systemem Informacji Wizowej (VIS) z dnia 25 lipca 2005 r., wersja 1.2

Ustawy
– Ustawa z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych oraz o Krajowym Systemie Informatycznym (Dz. U. z 2001 r., nr 110, poz. 1189, nr 154, poz. 1800, z 2002 r., nr 81, poz. 731, nr 89, poz. 804, z 2003 r., nr 124, poz. 1153, nr 128, poz. 1175, nr 137, poz. 1302, nr 142, poz. 1380, z 2004 r., nr 179, poz. 1842, z 2005 r., nr 183, poz. 1537)
– Ustawa z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej

Inne
– Plan działania w zakresie wdrażania dorobku prawnego Schengen w Polsce (Poland - Schengen Action Plan), sierpień 2005
– Aneks do planu działania w zakresie wdrażania dorobku prawnego Schengen w Polsce, aktualizowany w sierpniu 2005 r.
– Program Indykatywny 2005 („*Schengen Facility" Art. 35 of Accession Act Indicative Schedule 2005 of the Republic of Poland*)

Akty prawne i dokumenty unijne (UE)
System Informacyjny Schengen (SIS 1+)
– Decyzja Rady z dnia 12 czerwca 2007 r. w sprawie stosowania przepisów dorobku Schengen dotyczących Systemu Informacyjnego Schengen w Republice Czeskiej, Republice Estońskiej, Republice Łotewskiej, Republice Litewskiej, Republice Węgierskiej, Republice Malty, Rzeczypospolitej Polskiej, Republice Słowenii i Republice Słowackiej (2007/471/WE)
– Decyzja Rady z dnia 25 czerwca 2007 r. zmieniająca decyzję komitetu wykonawczego, ustanowionego na mocy konwencji Schengen z 1990 r., zmieniającą rozporządzenie finansowe w sprawie wydatków instalacyjnych i operacyjnych w celu technicznego wsparcia działania Systemu Informacyjnego Schengen (C.SIS) (2007/472/WE)
– Konwencja Wykonawcza z 19 czerwca 1990 r. do Układu z Schengen z dnia 14 czerwca 1985 roku między rządami państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach (Dz. Urz. UE L 239/19 z 22 września 2000 r.), znowelizowana Rozporządzeniem Rady (WE) 871/2004 z dnia 29 kwietnia 2004 r. oraz Decyzją Rady 2005/211/WSiSW z dnia 24 lutego 2005 r. dotyczącymi wprowadzenia kilku nowych funkcji do Systemu Informacyjnego Schengen, a także Rozporządzeniem (WE) 1160/2005 Parlamentu Europejskiego i Rady z dnia 6 lipca 2005 r. zmieniającym Konwencję Wykonawczą do Układu z Schengen w zakresie dostępu służb odpowiedzialnych w państwach członkowskich za wydawanie świadectw rejestracji pojazdów do Systemu Informacyjnego Schengen
– Decyzja Komisji z dnia 22 września 2006 r. w sprawie zmiany podręcznika SIRENE (2006/758/WE)

System Informacyjny Schengen drugiej generacji (SIS II)
– Rozporządzenie Rady (WE) nr 2424/2001 z dnia 6 grudnia 2001 r. w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji (SIS II)
– Decyzja Rady 2001/886/WSiSW z dnia 6 grudnia 2001 r. w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji (SIS II)
– Decyzja Rady 2006/1007/WSiSW z dnia 21 grudnia 2006 r. w sprawie utworzenia, działania i wykorzystania Systemu Informacyjnego Schengen drugiej generacji (SIS II)
– Sprostowanie do decyzji Rady 2006/1007/WSiSW z dnia 21 grudnia 2006 r. zmieniającej decyzję 2001/886/WSiSW w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dziennik Urzędowy Unii Europejskiej L 411 z dnia 30 grudnia 2006 r.)
– Rozporządzenie (WE) NR 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II)
– Rozporządzenie (WE) NR 1986/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie dostępu służb odpowiedzialnych w państwach członkowskich za wydawanie świadectw rejestracji pojazdów do Systemu Informacyjnego Schengen drugiej generacji (SIS II)
– Wniosek z 11.06.2007 – Decyzja Rady w sprawie instalacji i obsługi infrastruktury komunikacyjnej dla środowiska Systemu Informacyjnego Schengen (SIS) oraz zarządzania tą infrastrukturą (przedstawiony przez Komisję) {COM(2007) 311 *final*} {SEC(2007) 809} {SEC(2007) 810}
– Decyzja Rady UE z dnia 12 czerwca 2007 r. nr 2007/533/WSiSW w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji

Kodeks Graniczny Schengen
– Rozporządzenie (WE) NR 562/2006 Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. ustanawiające wspólnotowy kodeks zasad regulujących przepływ osób przez granice (Kodeks Graniczny Schengen)

Inne
– Deklaracja Ministrów Spraw Wewnętrznych Państw Grupy Wyszehradzkiej – Bruksela, dnia 19 lipca 2004 r.
– Komunikat Komisji Europejskiej do Parlamentu Europejskiego i Rady w sprawie zwiększenia skuteczności, interoperacyjności i efektu synergii wynikającego ze współdziałania europejskich baz danych w dziedzinie sprawiedliwości i spraw wewnętrznych {COM(2005) 597 *final*}

C & C

TKH GROUP

Wykryje najdrobniejszy ruch...

Rozdzielczość 560/700 TVL (kolor/bw)
Czułość 0.001 Lux (tryb sens-up)
WDR (52 dB/128x)
System redukcji szumów SSNR2
Zdalny dostęp do OSD (RS-485)
Cyfrowa stabilizacja obrazu (DIS)
Wbudowany obiektyw 3.8 ~ 9.5 mm
Inteligentna detekcja ruchu

SID-560P

SAMSUNG TECHWIN

www.ccpartners.pl

www.samsungcctv.ccpartners.pl

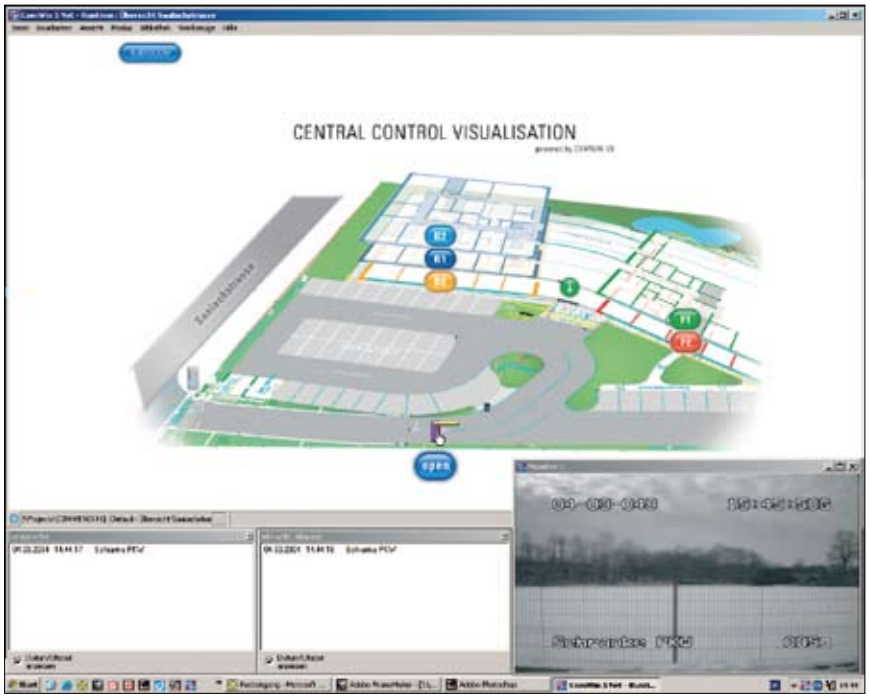
Dystrybutor w Polsce: **C&C Partners Telecom Sp. z o.o.**
Siedziba **Leszno** · Oddział **Gdańsk** · Oddział **Katowice** · Oddział **Warszawa**

Commend – profesjonalne centrum nadzoru

GUI (ang. *Graphical User Interface*), czyli Graficzny Interfejs Użytkownika, wraz z rozwojem automatyki z sukcesem zaadaptował się w aplikacjach przemysłowych, ale coraz częściej tego typu oprogramowanie trafia do obiektów niezwiązanych z obszarem produkcyjnym. Stosowanie szerokiej gamy urządzeń z branży zabezpieczeń i teletechniki sprawia, że nie sposób odczytać w kilka chwil informacji napływającej z tego typu sprzętu. W takich przypadkach niezwykle pomocny okazuje się system wizualizacji – system, który pozwoli na rejestrację zdarzeń, zdalne sterowanie urządzeniami oraz automatycznie przerzuci obraz na monitorze tak, by nic nie umknęło znużonemu oku stróża czy operatora. Rozwiązaniem przeznaczonym do integracji wielu systemów, głównie w punktach nadzoru, jest Commend – produkt firmy o tej samej nazwie, której wyłącznym przedstawicielem w Polsce jest C&C Partners Telecom

Rys. 1. Commend pozwala na integrację wybranych systemów według zapotrzebowania

Commend to jednocześnie firma i marka produktów. Ponad 30 lat doświadczenia w produkcji interkomów, rozwój elektroniki i zmiany zapotrzebowania rynku sprawiły, że Commend jest obecnie zintegrowanym systemem zarządzania i komunikacji. Oferując w pełni cyfrowe rozwiązania, bazujące na architekturze wieloprocesorowej oraz technologiach DSP, umożliwia komunikację z niespotykaną jakością dźwięku (wykorzystując pasmo 7 kHz) oraz bardzo elastyczną integrację z wieloma innymi systemami. Obecnie standardem w instalacjach budynkowych jest stosowanie przynajmniej kilku systemów teletechnicznych i zabezpieczeń, takich jak: sieć telefoniczna, komputerowa, telewizja dozorowa, system sygnalizacji pożarowej, kontrola dostępu, system łączności wewnętrznej czy rejestracji czasu pracy. Wykorzystując elastyczność rozwiązań firmy Commend, można zbudować zintegrowany system kontroli i komunikacji w obrębie całego budynku, poprawiając znacząco komfort pracy personelu i ochrony, a także zwiększając bezpieczeństwo i pewność przebywających w nim gości. Skuteczność integracji zwiększona jest dzięki oprogramowaniu wizualizacyjnemu COMWIN, które staje się sercem systemu kontrolnego.



Rys. 2. Dzięki możliwości wyświetlania kilku okien operacyjnych każde zdarzenie zostanie odpowiednio zarejestrowane

COMWIN 5

Struktura klient-serwer pakietu COMWIN (przeznaczonego dla platform MS Windows 2000/XP) oferuje funkcjonalność w zakresie wyświetlania, rejestrowania i sygnalizacji. Do projektu można wstawiać dowolną liczbę własnych podkładów tła, ograniczona jest natomiast liczba ikon (patrz informacje o licencji). Interaktywne ikony reprezentują połączenia, komunikaty o błędach lub komunikaty alarmowe i zmieniają swój wygląd zależnie od wymagań. W osobnych oknach możliwe jest wyświetlanie tekstów pomocy, rejestrowanie informacji, a także wysyłanie wiadomości pocztą elektroniczną. Wszystkie zdarzenia są przechowywane w bazie danych chronionej hasłem. Zestaw *Software Development Kit* (SDK) pozwala tworzyć własne aplikacje, np. pomiar czasu pracy, listy obecności. Pulpit wizualizacyjny może być wyświetlany na jednym lub kilku monitorach. Za pośrednictwem oprogramowania i dzięki mnogości protokołów integracja z innymi urządzeniami/systemami jest wyjątkowo prosta. Wystarcza jedno kliknięcie, aby możliwe było zestawienie połączeń głosowych, wysterowanie przekaźników, otwarcie drzwi, podniesienie barierki na parkingu, zmiana oświetlenia czy odcięcie wody. COMWIN jest systemem prostym w konfiguracji, a oferowana przez producenta pomoc oraz wsparcie techniczne pozwala na budowę najbardziej skomplikowanych, funkcjonalnych, a zarazem przyjaznych użytkownikowi aplikacji.

Sprzęt

Do poprawnej pracy pakietu wizualizacyjnego COMWIN w aktualnej wersji 5 potrzebny jest procesor klasy Pentium 500 MHz lub wyższej oraz przynajmniej 100 MB przestrzeni dyskowej i 128 MB pamięci operacyjnej. Niezbędny jest też napęd CD i port USB do podłączenia klucza sprzętowego. System Windows musi być uzupełniony o aktualizacje Service Pack, Microsoft Data Access Components, Message Queuing i .NET Framework. Komputer przez port szeregowy łączy się z centralą interkomową. Centrala GE200/GE700 musi być wyposażona w kartę abonenta o najwyższej (z 3-stopniowej skali) funkcjonalności oraz kartę programowalną V24 PRO. Idealnym komponentem systemu nadrzędnego w centrach nadzoru i kontroli jest interkomowy pulpit sterujący EE880, który można rozbudować do 504 swobodnie programowalnych przycisków z podświetleniem LED. Model ten wyposażony jest w wyświetlacz

Rys. 3. Centrum zarządzania obiektem

LCD oraz mikrofon na „gęsiej szyjce". Każdy przycisk może realizować odmienną funkcję. Stacje tego typu są dostępne w wersji nabiurkowej oraz do zabudowy.

Cechy oprogramowania:

- doskonały przegląd sytuacji dzięki wyświetlaniu okien na kilku monitorach;
- używane ikony można wcześniej definiować lub korzystać z domyślnych;
- standardowo program przewiduje 8 poziomów, np. ikon dla żądania połączenia, rozmowy, zajętości linii, przerwania itp.;
- aplikacja LogWatcher zapisuje wszystkie zdarzenia w bazie chronionej hasłem (nawet takie, jak kliknięcie myszą);
- projekt chroniony loginem i hasłem;
- COMWIN 5 standardowo korzysta z bazy MS Access, opcjonalnie dostępny jest MS SQL;
- możliwość tworzenia użytkowników z różnymi uprawnieniami (dostęp do całej lokalizacji lub jej części);
- podkłady tła przypisywane są do lokalizacji (np. parkingi), do której można dodać kilka planów (np. piętra);
- wszelkie zdarzenia mogą być wyświetlane w postaci pełnego tekstu;
- filtr zapobiegający stałemu wyświetlaniu wszystkich zdarzeń na ekranie;
- opcja wydruku;
- możliwość tworzenia systemu rozproszonego z wykorzystaniem sieci IP;
- integracja z rozwiązaniami wideo firm Axis i VCS oraz technologiami HTML i *Video-over-IP*.

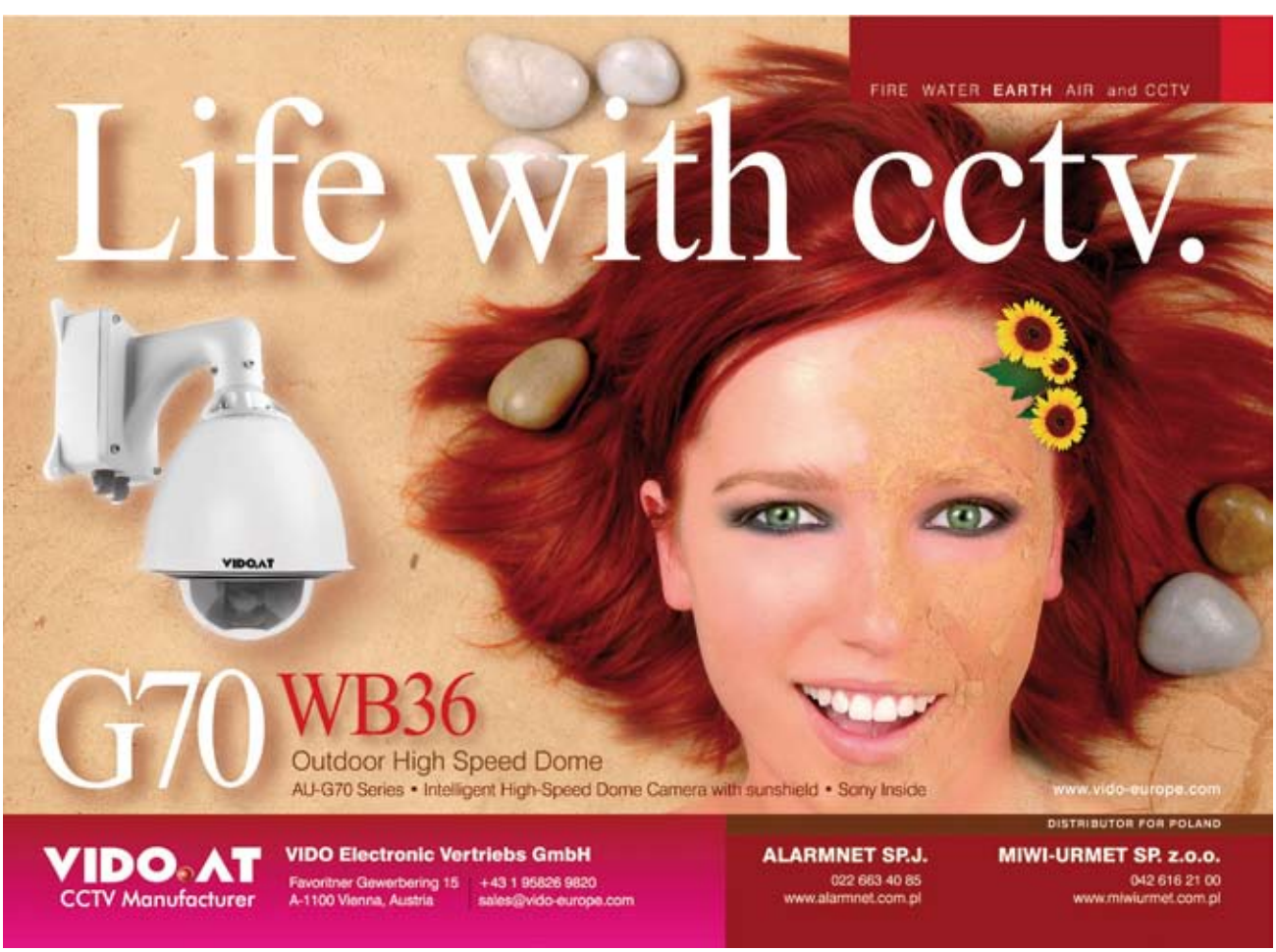
Różne potrzeby – różne licencje

Dostępne są trzy wersje oprogramowania. Najprostsza, COMWIN LIGHT, pozwala na zastosowanie 10 planów i 100 ikon i jest przydatna dla niewielkich firm bądź tylko strategicznych lokalizacji w dużych aplikacjach. COMWIN WORKSTATION to jednostanowiskowa wersja do zaawansowanych funkcji sterujących (1000 ikon i dowolna liczba planów). COMWIN NET to wersja klient-serwer podobna do poprzedniej, jednak przeznaczona dla wielostanowiskowych pulpitów, także w zdalnych lokalizacjach. Dostępne są także licencje rozszerzające (o kolejne ikony, stanowiska czy *back-up*). Dodatkowo pakiety oprogramowania zawierają narzędzia:

- REPORTER (służące do zapisywania zdarzeń oraz ich przeszukiwania i filtrowania),
- SCHEDULER (pozwalające na inicjację zdarzeń w przyszłości, np. otwieranie drzwi o zadanym czasie),
- COMVIDEO (służące do wizualizacji obrazu z różnych źródeł wideo, mogące pracować niezależnie od COMWIN) i SDK (umożliwiające, jak wcześniej napisano, tworzenie własnych aplikacji).

Aby dokładniej poznać środowisko COMWIN oraz rozwiązania produktowe Commend, najlepiej umówić się na spotkanie z lokalnym przedstawicielem tej austriackiej firmy w kraju.

Marek Katarzyński
C&C Partners Telecom



Obiektywy

które widzą więcej

computar®

Computar - synonim japońskich obiektywów, najczęściej stosowanych w systemach CCTV na całym świecie.

Funkcjonalność oferowanych obiektywów Computar pozwala na dostosowanie wybranego modelu obiektywu w dowolnej aplikacji - np. różnorodne systemy dozoru, specjalistyczne maszyny przemysłowe.

Doskonała i sprawdzona jakość obiektywów znacząco wpływa na zwiększenie efektywności systemów, w których są stosowane.

Wszystkie obiektywy Computar objęte są 3-letnią gwarancją.

CBCGROUP

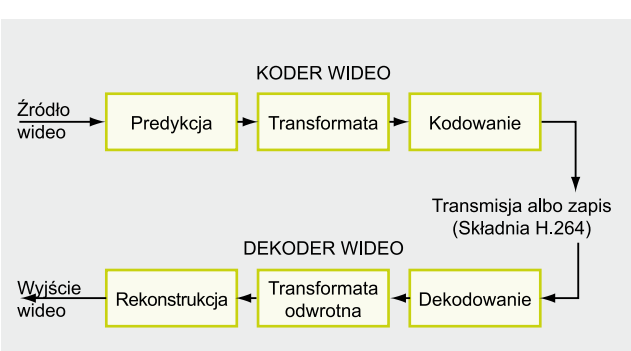
Rosnąca popularność sieciowych systemów telewizyjnych, w tym także systemów monitoringu IP, pociąga za sobą stały rozwój metod kompresji obrazów telewizyjnych. W literaturze poświęconej tej tematyce jest dostępnych wiele opracowań, których cechą wspólną jest znaczny stopień szczegółowości, a co za tym idzie brak czytelnego opisu podstaw działania tych standardów

Poniższy artykuł traktuje temat opisowo i jest adresowany do szerokiej rzeszy projektantów i instalatorów systemów monitoringu wizyjnego, dla których szczegóły skomplikowanych rozważań matematycznych nie są istotne. Został on opracowany na podstawie dokumentu *H.264/MPEG4 Part 10 White Paper* oraz licznych publikacji Iaina Richardsona, dyrektora Centre for Video Communications, profesora School of Engineering w Aberdeen. Iain Richardson uchodzi obecnie za jednego z najlepszych znawców tematyki kompresji ruchomych obrazów telewizyjnych i jest współtwórcą standardu H.264.

W dokumencie *Recommendation H.264: Advanced Video Coding*, opublikowanym w roku 2003 przez ITU i ISO/IEC, metoda H.264, pozwalająca na kompresję ruchomych obrazów telewizyjnych, została uznana za standard przemysłowy, co przyczyniło się do jej szybkiego upowszechnienia. Dotyczy to zarówno zastosowań związanych z zapisem i przekazem programów telewizyjnych, jak i zamkniętych systemów monitoringu wizyjnego. We wszystkich tych przypadkach zasada kompresji jest identyczna, różnice mogą dotyczyć jedynie specyfiki poszczególnych aplikacji.

Na rys. 1 przedstawiony jest schemat blokowy, wyjaśniający przebieg procesu kodowania i dekodowania informacji w standardzie H.264.

Spróbujmy prześledzić drogę danych kodujących obrazy telewizyjne, począwszy od źródła, aż do wyjścia dekodera.



Rys. 1. Kodowanie i dekodowanie informacji w standardzie H.264

Czym wyróżnia się ten system? W procesie kodowania mamy do czynienia z następującymi operacjami:

- predykcja, czyli przewidywanie treści kolejnych obrazów telewizyjnych,
- obliczanie transformaty kosinusowej, czyli przejście z dziedziny czasu do dziedziny częstotliwości,
- kodowanie danych wyjściowych, czyli przygotowanie danych do zapisu lub transmisji.

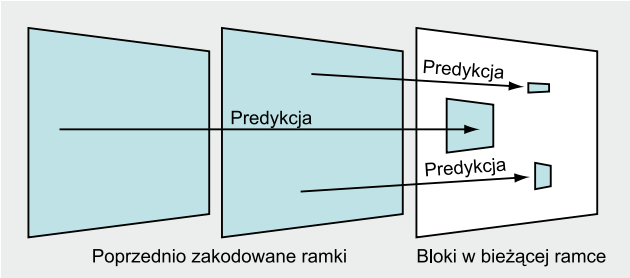
Podczas dekodowania następuje proces odwrotny, to znaczy dekodowanie danych wejściowych, obliczanie transformaty odwrotnej oraz rekonstrukcja sekwencji obrazów. Omówmy kolejno wymienione powyżej elementy.

Proces kodowania

Predykcja

Jak wiadomo, na ruchomy obraz telewizyjny składa się sekwencja następujących po sobie ramek telewizyjnych. Koder H.264 dokonuje podziału kolejnych ramek na mniejsze elementy, o rozmiarach 16x16 pikseli. Elementy te nazywają się makroblokami. Operacją mającą kluczowe znaczenie dla tego standardu jest predykcja zawartości kolejnych makrobloków, dokonywana na podstawie poprzednio zakodowanych danych. Jak rozumieć słowo „predykcja"? Chodzi o przewidywanie treści obrazów, które mają dopiero nastąpić. Tłumacząc jaśniej, jest to próba wykalkulowania, jak będzie wyglądał kolejny makroblok danych, jeśli jego poprzednicy mieli określoną treść i wygląd.

Podczas predykcji operuje się pojęciem wektorów przesunięcia, znanym już wcześniej z opisu metod kompresji MPEG-2 i MPEG-4. Wektory te określają zmiany położenia elementów obrazu na kolejnych klatkach telewizyjnych. W zasadzie przedmiotem predykcji jest nie tyle zawartość kolejnych makrobloków, co długość i kierunek wektorów przesunięcia. W przypadku H.264 przesunięcia wskazywane przez wektory mogą być mniejsze od rozmiarów pojedynczych pikseli, co znacznie poprawia reprodukcję obrazów, na których elementy składowe poruszają się z małą prędkością. We współczesnych systemach kompresji H.264 stosuje się dokładność równą 1/4 wielkości pojedynczego piksela.



Rys. 2. Istota interpredykcji

Rozróżnić należy dwa rodzaje predykcji: intrapredykcję, dokonywaną tylko na podstawie danych pochodzących z bieżącej ramki obrazowej, oraz interpredykcję, dokonywaną na podstawie danych pochodzących z wielu ramek (rys. 2). Proces interpredykcji bywa określany jako estymacja ruchu. Są to pojęcia równoznaczne.

Metody predykcji stosowane w standardzie H.264 są bardziej elastyczne niż w innych metodach kodowania, przez co precyzja ich działania jest większa. Stosowane są małe bloki danych, o rozmiarach 16x16 pikseli, które w pewnych warunkach mogą być dodatkowo zmniejszane do rozmiarów 4x4. Jest to szczególnie istotne podczas interpredykcji, gdzie dane są pobierane z pikseli z bieżącej ramki oraz z pikseli znajdujących się w podobnym obszarze ramek poprzednich.

Tworzenie różnic cząstkowych, bloki residual

Kolejną bardzo ważną operacją, związaną z kodowaniem w standardzie H.264, jest tworzenie obiektów noszących angielską nazwę *residual*, powstających w wyniku odjęcia danych pochodzących z predykcji od danych stanowiących treść bieżącego makrobloku. Obraz utworzony z elementów *residual* (rys. 3) przypomina znany z fotografii efekt reliefu, w którym widoczne na obrazie obiekty mają wyraźnie zaznaczone krawędzie, jednak większa część zdjęcia tonie w odcieniach szarości.

Operacja odjęcia danych pochodzących z interpredykcji od danych z aktualnego makrobloku jest także nazywana kompensacją ruchu. Jak łatwo się domyśleć, wszystkie te zabiegi prowadzą do określenia zmian, jakie zachodzą w kolejnych obrazach telewizyjnych, a tym samym do zmniejszenia ilości przekazywanych informacji.

Brak jest ścisłego odpowiednika terminu *residual* w języku polskim. W matematyce mówi się o residuum lub pozostałości. Słowo to należy rozumieć jako szczątkową różnicę, powstałą na skutek odjęcia od siebie elementów wykazujących duże podobieństwo. Elementami takimi są kolejne ramki obrazu telewizyjnego.

Obliczanie transformaty i kwantowanie

Na kolejnym etapie kodowania powstające w procesie predykcji bloki *residual* podlegają przekształceniu za pomocą zmodyfikowanej, dyskretnej transformaty kosinusowej, zwanej transformatą całkowitoliczbową, przy czym operuje się blokami o rozmiarach 4x4 lub 8x8 pikseli. W wyniku tej operacji powstaje zbiór współczynników, który z kolei podlega kwantyzacji, czyli zaokrągleniu do wartości całkowitych. Odbywa się to drogą dzielenia wartości współczynników przez odpowiednio dobraną liczbę całkowitą i odrzucania reszty z dzielenia.

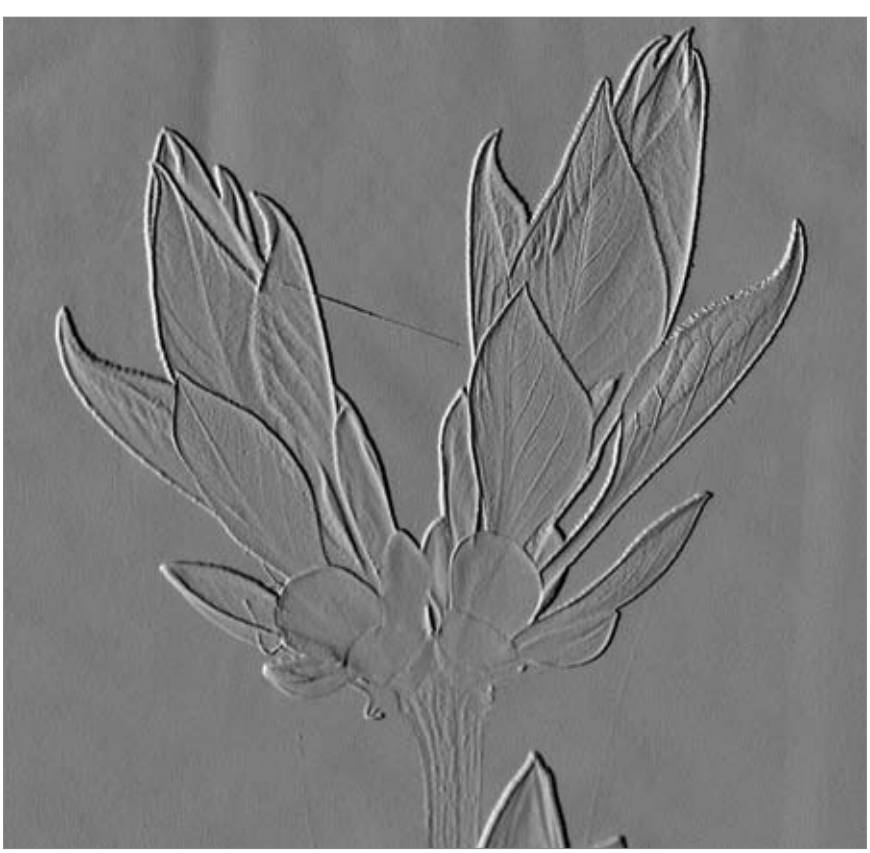
Tego typu operacja oznacza utratę pewnej części danych opisujących kompresowany obraz, dlatego też bardzo istotny jest dobór parametrów procesu kwantyzacji. Zależy od tego precyzja przekształcenia matematycznego, a tym samym równowaga między objętością danych a jakością zakodowanego obrazu.

W wyniku wszystkich opisanych dotychczas operacji powstają bloki danych składające się niemal z samych zer i jedynie niewielu elementów niezerowych. Liczba elementów niezerowych rośnie wraz z pogarszaniem stopnia kompresji, czemu towarzyszy poprawa jakości zakodowanego obrazu. Przy odpowiednim doborze parametrów procesu kwantowania można uzyskać kompromis pomiędzy wysoką jakością obrazów a skutecznością kompresji.

Kodowanie strumienia danych

Ciąg danych pochodzący z procesu kwantyzacji jest uzupełniany o dodatkowe informacje, związane z obróbką sekwencji obrazów telewizyjnych. Całość jest kodowana w jeden wspólny strumień danych, niosący następujące informacje:

- skwantowane wartości współczynników stanowiących wynik transformaty bloków *residual*,
- dane pozwalające na późniejsze przeprowadzenie odwróconego procesu predykcji,



Rys. 3. Przykładowy obraz telewizyjny, utworzony z bloków residual

– dane określające strukturę skompresowanego strumienia danych,
– dane dotyczące narzędzi użytych w procesie kompresji,
– dane pozwalające na kompletację sekwencji zdekodowanych obrazów telewizyjnych.

Opisany powyżej strumień wartości i parametrów, zwanych elementami syntaktycznymi, jest konwertowany na jednolity kod binarny, stanowiący wynik całego procesu kompresji. Na tym etapie kodowania wykorzystuje się metody matematyczne o zmiennej długości kodu lub metody kodowania arytmetycznego. Jest to proces bezstratny, prowadzący do wytworzenia skompresowanej, jednorodnej reprezentacji przesyłanych informacji. Powstały w wyniku kodowania ciąg bitów może być przetransmitowany z wykorzystaniem dowolnej metody telekomunikacyjnej, a także zapisany na odpowiednio dobranym nośniku danych celem późniejszego odtworzenia.

Proces kodowania binarnego przypomina znaną powszechnie technikę kompresji danych komputerowych. Większości czytelników znane są formaty plików skompresowanych zip czy rar. Na ostatnim etapie kompresji H.264 mamy do czynienia z podobnym procesem, prowadzonym w sposób ciągły, w czasie rzeczywistym.

Proces dekodowania

Dekodowanie strumienia danych

Dekoder H.264 odbiera strumień danych stanowiący wynik procesu kompresji i drogą dekodowania binarnego wydziela z niego opisane powyżej elementy syntaktyczne. Zachodzi tu podobieństwo do rozpakowywania plików typu zip czy rar. Odzyskane elementy syntaktyczne są poddawane dalszemu procesowi dekodowania.

Skalowanie współczynników i transformata odwrotna

Pobrane ze zbioru elementów syntaktycznych skwantowane współczynniki transformacji podlegają ponownemu przeskalowaniu, które odbywa się drogą przemnożenia ich wartości przez liczbę stałą, użytą poprzednio w procesie kwantyzacji. Proces ten jest często określany jako kwantyzacja odwrotna, jednakże nie jest to zbyt ścisłe porównanie, gdyż informacje utracone w wyniku dzielenia i odrzucania reszty nie ulegają pełnemu odtworzeniu w procesie mnożenia.

Na kolejnym etapie dekodowania przeskalowane współczynniki są poddawane odwrotnej transformacie kosinusowej, w wyniku której odtwarzane są bloki *residual*. Są one łączone w większe grupy, tworząc makrobloki *residual*.

Rekonstrukcja sekwencji obrazów

W procesie dekodowania każdy z makrobloków jest poddawany takiemu samemu procesowi predykcji, jak to miało miejsce podczas kodowania. Następuje dodawanie zawartości makrobloków *residual* do zawartości poprzednich makrobloków obrazowych, a tym samym rekonstrukcja oryginalnych fragmentów sekwencji obrazów.

Wszystkie opisane czynności wiążą się z nieprzerwanym wykonywaniem skomplikowanych operacji matematycznych, co pociąga za sobą bardzo wysokie zapotrzebowanie na moc obliczeniową systemu kodowania, jednakże wynik końcowy w postaci znakomitej jakości obrazu oraz wydajnej kompresji danych uzasadnia użycie tak skomplikowanych metod.

Uzyskane wyniki

Działanie H.264 w praktyce

Przedstawiony powyżej opis standardu H.264 jest jedynie ilustracją zasady jego działania. Faktyczne mechanizmy kompresji obrazów są znacznie bardziej skomplikowane, a ich zrozumienie wymaga zagłębienia się w zagadnienia matematyczne. Przykładem może być zastosowanie filtrów eliminujących błędy wynikające z podziału obrazu na bloki o niewielkich rozmiarach. Filtry te stosuje się zarówno podczas kodowania, jak i podczas dekodowania sekwencji obrazów.

Projektant systemów bezpieczeństwa czy instalator kamer przemysłowych jest zainteresowany efektami praktycznymi, wynikającymi z zastosowania takiej a nie innej metody kompresji obrazów. Jakie więc wnioski wynikają z tych rozważań?

Najistotniejszą różnicą pomiędzy stosowanymi dotychczas metodami kompresji obrazów a standardem H.264 jest wysoka wydajność tego procesu. W stosunku do metod MPEG-2 i MPEG-4 H.264 zapewnia lepszą jakość obrazu przy porównywalnym strumieniu zakodowanych danych wyjściowych albo skuteczniejszą kompresję strumienia danych przy podobnej jakości obrazu.

Uważny czytelnik łatwo zauważy, że wiele mechanizmów wykorzystanych w standardzie H.264 znajduje zastosowanie w starszych metodach kompresji obrazów. Skąd więc ta zwiększona skuteczność?

Na tak postawione pytanie nie ma jednoznacznej odpowiedzi. Wspomniane powyżej podobieństwa sugerują, że H.264 jest raczej rozszerzeniem istniejących standardów niż nową, rewolucyjną koncepcją kodowania danych. Różnica polega na dalszej komplikacji działania algorytmu, na zwiększeniu różnorodności ramek pośrednich (operuje się tu pojęciem plastra – z angielskiego *slice*), a także na zastosowaniu bloków o małych rozmiarach i dynamicznie zmienianej wielkości. Uzyskuje się tym samym lepsze wykorzystanie możliwości kompresji w zależności od konkretnej treści obrazu telewizyjnego. Działając z osobna, każde ze wspomnianych usprawnień poprawia skuteczność kompresji o niewielki procent, lecz wszystkie razem, połączone w jeden system, zapewniają zauważalną poprawę.

Standard H.264 stale się rozwija. Śledząc najnowsze doniesienia prasowe, napotyka się notatki o dalszym, bardzo znacznym zwiększeniu stopnia kompresji obrazów z zachowaniem podobnego poziomu jakości. Analizując ofertę rynkową w dziedzinie kamer przemysłowych oraz sieciowych rejestratorów wizyjnych, zauważa się wzrost popularności metody kompresji H.264. Tendencja ta wiąże się między innymi ze stałym spadkiem cen elementów stanowiących dotychczas domenę rynku komputerowego, takich jak wysokowydajne mikroprocesory czy komponenty cyfrowych sieci IP.

Na zakończenie, posługując się żartobliwie terminologią zaczerpniętą z opisu H.264, można stwierdzić, że w wyniku predykcji sytuacji rynkowej na najbliższe kilkanaście miesięcy wszystkie wektory przesunięcia wskazują wzrost popularności metody H.264 i spadek zainteresowania metodami MPEG.

Andrzej Walczyk

Twoje bezpieczeństwo
jest w jego rękach.
Daj mu najlepsze narzędzia,
pogadaj z SONY.

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

SONY

www.sonybiz.net/nvm

Inteligentna analiza obrazu... bezpieczeństwo dla Ciebie.

Linia produktów SONY zawiera zarówno najlepsze kamery i rejestratory wizyjne jak i doskonałej jakości oprogramowanie do zarządzania systemami monitoringu.

Reakcja pracowników ochrony będzie natychmiastowa.

By poznać szczegóły skontaktuj się z firmą ALTRAM – autoryzowanym dystrybutorem Sony.

ALTRAM tel. +48 22 847 5505 altram@altram.com.pl www.altram.com.pl.

IPELA

CRT czy LCD?

Zadaniem systemów telewizji dozorowej jest przekazanie obrazu. Pod tym kątem wybiera się kamery, dopasowując ich parametry do warunków, w jakich będą pracowały. Nie mniej istotny jest wybór monitorów w centrum monitoringu. Aktualnie większość systemów wyposaża się w monitory LCD, rezygnując z monitorów kineskopowych. Czy słusznie?

CRT *(Cathode-Ray Tube)* to technologia monitorów kineskopowych, w których do wyświetlenia obrazu używa się wiązki elektronów, która pada na luminofor, powodując jego świecenie. Jest to technologia rozwijana od 1924 roku. W JVC pierwszy telewizor tego typu skonstruowano w 1939 roku. Monitory CRT znakomicie sprawdzają się w nowoczesnych systemach nadzoru. Z jednej strony obraz z kamer z systemu CCTV musi być ostry, z żywymi kolorami, przekaz obrazu w trybie *live* musi odbywać się bez migotania, ale z drugiej strony wymaga się, by monitor w odpowiedni sposób wyświetlał menu tekstowe, jakie jest przekazywane przez rejestratory wideo (DVR/NVR). Monitory CRT spełniają powyższe wymagania, a przy tym są atrakcyjne cenowo. Zaletami takich monitorów są:

– wysoki kontrast,
– wierne oddanie kolorów (prawidłowy poziom czerni),
– szeroki kąt widzenia,
– bardzo dobre odwzorowanie dynamicznych scen.

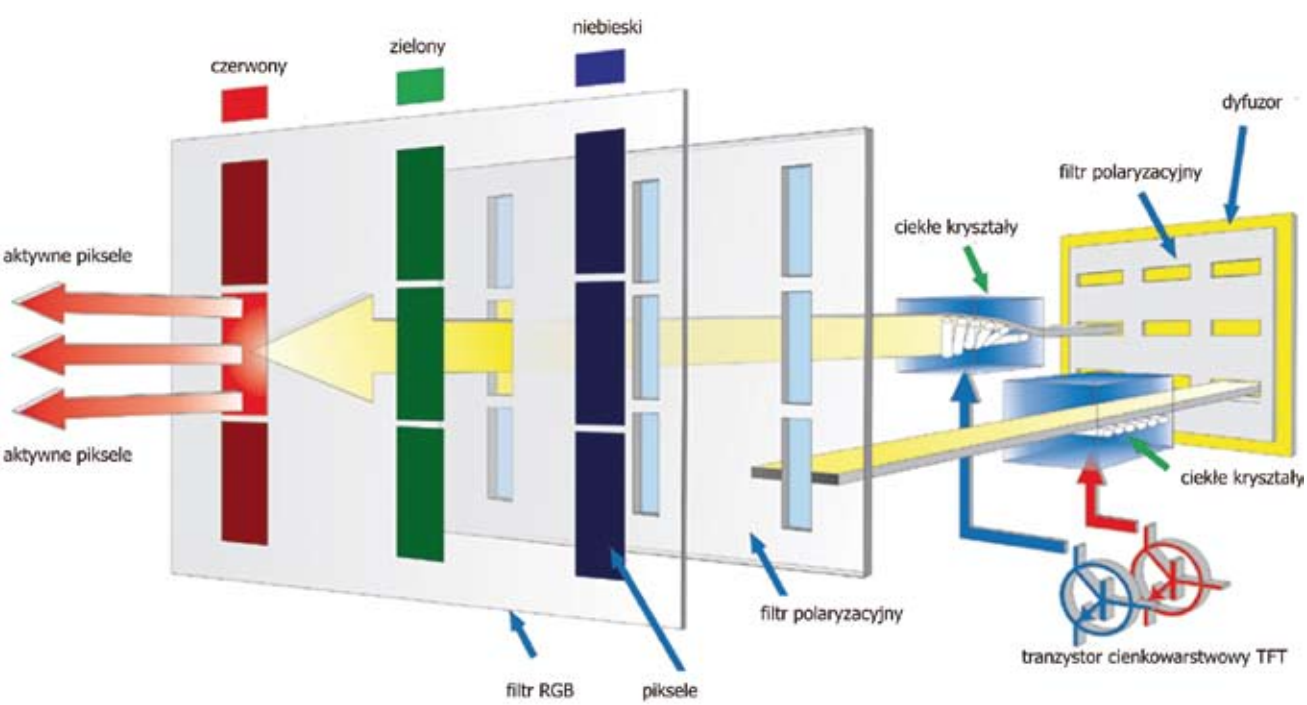
Technologia kineskopowa ma również swoje wady:

– znaczne gabaryty,
– małe niedokładności geometrii w narożnikach,
– efekt migotania,
– wyższe zużycie energii w porównaniu do LCD,
– podwyższenie temperatury w pomieszczeniu w wyniku wydzielania ciepła przez monitory.

Pomimo tych wad monitory CRT są bardzo chętnie stosowane tam, gdzie priorytetem jest uzyskanie ostrego obrazu o dużym zakresie dynamiki i wierne oddanie kolorów.

Wyświetlacz ciekłokrystaliczny, **LCD** (ang. *Liquid Crystal Display*) – to urządzenie wyświetlające obraz, którego zasada działania oparta jest na zmianie polaryzacji światła na skutek zmian orientacji cząsteczek ciekłego kryształu pod wpływem przyłożonego pola elektrycznego.

Technologia ciekłych kryształów została odkryta przez botanika T. Reinitzera w 1888 roku. Jednak dopiero w 1969 roku zjawiskiem tym zainteresowała się firma



Rys. 1. Schemat monitora LCD TFT

Radio Corporation of America, która skonstruowała wyświetlacz ciekłokrystaliczny i jako pierwsza na świecie wdrożyła w praktyce rozwiązanie wykorzystujące właściwości ciekłych kryształów. Wyświetlacze LCD działają na zasadzie rotacji płaszczyzny polaryzacji. W 1973 roku George Gray odkrył ciekłe kryształy stabilne w temperaturze pokojowej i pod normalnym ciśnieniem. Od lat 70. XX wieku stosujemy wyświetlacze LC (*liquid crystal*) w zegarkach, kalkulatorach i wielu innych urządzeniach.

Wszystkie rodzaje wyświetlaczy ciekłokrystalicznych składają się z czterech podstawowych elementów:

- komórek, w których zatopiona jest niewielka ilość ciekłego kryształu,
- elektrod, które są źródłem pola elektrycznego działającego bezpośrednio na ciekły kryształ,
- dwóch cienkich folii, z których jedna pełni rolę polaryzatora a druga analizatora,
- źródła światła.

Fot. 1. Monitor profesjonalny LCD 65" JVC GD-F65L1

Wyświetlacze LCD buduje się z ciekłych kryształów o strukturze nematycznej. Są to sztywne nitki, zmieniające położenie pod wpływem przyłożonego pola elektrycznego. Zmieniając swe ułożenie, powodują polaryzację padającego światła. LCD nie emituje światła (przeciwnie niż wyświetlacze w technologii plazmowej), ale działa jak filtr, który przepuszcza światło. Lampa fluoroscencyjna emituje światło koloru białego, które przechodzi przez ciekłe kryształy, w których przy pomocy filtra jest mu nadawany odpowiedni kolor. Efektem tego jest opóźnienie w przełączaniu obrazu. Aby poprawić jakość obrazu, zaczęto stosować technologię TFT. Tranzystor przyspiesza przełączanie obrazu oraz opóźnia rozładowywanie ładunków kondensatora. Matryce LCD/TFT nazywane są aktywnymi, a obraz wyświetlany za ich pomocą jest bardziej kontrastowy oraz bez efektu migotania.

Plusy monitorów LCD/TFT:

- małe gabaryty,
- odporność na wpływ pola elektromagnetycznego,
- niskie zużycie energii elektrycznej,
- nie powodują nagrzewania pomieszczeń,
- brak efektu migotania,
- możliwości wizualizacji wielkoformatowej.

Minusy TFT:

- niski kontrast, zależny od kąta oglądania
- obraz dynamiczny jest nieostry.

Dużą zaletą stosowania monitorów LCD jest możliwość wizualizacji wielkoformatowej. Aktualnie w ofercie firmy JVC Professional pojawiły się monitory LCD o przekątnych 46", 52" oraz 65". Ich najważniejsze cechy to rozdzielczość Full HD (1920x1080) oraz przystosowanie do pracy ciągłej. Jest to parametr niezwykle istotny w systemach CCTV.

Jaki rodzaj monitora wybrać do systemów CCTV?

Jeśli priorytetem jest uzyskanie ostrego, bardzo kontrastowego obrazu z wiernym oddaniem kolorów i prawidłową czernią, to monitory CRT są nadal niepokonane. Dodatkowo, z racji dopracowania technologii istniejącej od wielu lat na rynku, urządzenia te są bezawaryjne (średni czas pracy bezawaryjnej MTBF monitora JVC TM-A140EA to prawie 10 lat). Korzyścią dla klientów są również niższe ceny w porównaniu do monitorów LCD. Skąd zatem popularność technologii LCD? Decydują o niej głównie małe gabaryty, aktualnie istotną przewagą jest również przekątna do 65", niedostępna dla monitorów CRT. Pamiętajmy jednak, że urządzenia w systemach telewizji dozorowej muszą pracować w trybie ciągłym (24/7), więc należy wykorzystywać rozwiązanie profesjonalne, przystosowane do takiej pracy. Większość komputerowych monitorów LCD nie spełnia tego warunku.

Sławomir Janiso
Radioton

SYSTEMY

Bezprzewodowa transmisja obrazu i dźwięku

2,4 GHz

seria mini

- 4 kanały pracy
- duży zasięg
- CE 1471
- łatwy montaż i obsługa
- miniaturowe gabaryty
- dobra jakość obrazu i dźwięku

- inne wykonania systemów transmisyjnych 2,4 GHz

seria hermetyczna

seria standard

5,8 GHz

seria hermetyczna

- obudowa IP 66
- wbudowana antena
- łatwy montaż i obsługa

- 8 kanałów pracy (5,725 - 5,875 GHz)
- doskonała jakość obrazu i dźwięku
- homologacje: FCC, IC, CE

Bezprzewodowa transmisja telemetryczna

868 MHz

NOWOŚĆ!

- łatwe zarządzanie kamerami obrotowymi w standardzie RS 485
- zasięg transmisji do 2000 metrów
- prędkość transmisji 4800-38400 bit/s
- zalecany protokół sterowania Pelco-D
- opcja testowania i oceny jakości sygnału

wykonanie hermetyczne

- obudowy IP 66

CAM SAT

więcej informacji na stronie internetowej: www.3d.com.pl

producent: 3D Sp. z o.o.

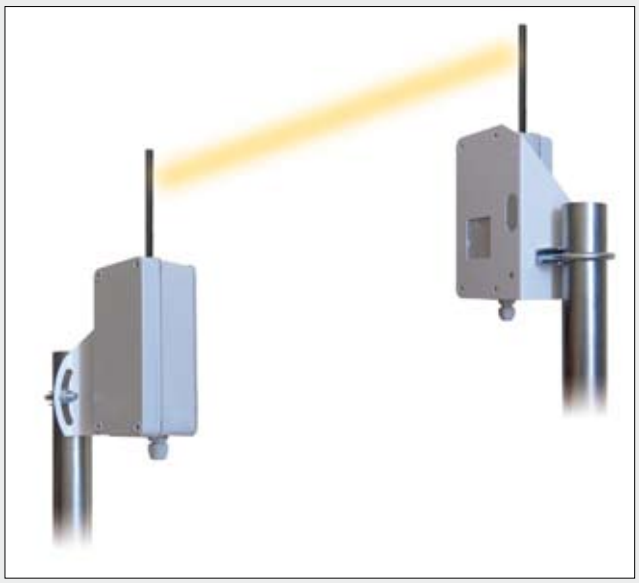
Telemetria – bezprzewodowy system transmisji sygnału telemetrycznego (868 MHz) firmy 3D z Bydgoszczy

Cieszący się dużym zainteresowaniem na minionych targach Securex 2008 nasz nowy produkt – bezprzewodowy system transmisji sygnału telemetrycznego (RTR008T-h, skonstruowany i wyprodukowany przez firmę 3D z Bydgoszczy) – zainspirował nas do napisania kolejnego artykułu. Chcemy w nim przybliżyć charakterystykę produktu oraz przedstawić, jak poprawnie zainstalować system

Bezprzewodowe kamery obrotowe, charakterystyka systemu telemetrii RTR008T-h

W wielu profesjonalnych systemach dozorowych wykorzystuje się kamery szybkoobrotowe. Stało się tak za sprawą coraz niższych kosztów ich zakupu. Przystępność cenowa kamer szybkoobrotowych, a przede wszystkim ich wybór, co mogliśmy zaobserwować na targach Securex, spowodowały duże zainteresowanie ich bezprzewodowym sterowaniem. Rozwój systemów bezprzewodowych na przestrzeni kilku lat spowodował, że inwestor/instalator nie zadaje sobie pytania czy, tylko jak zamontować system bezprzewodowy.

Nasza firma wyszła naprzeciw oczekiwaniom instalatorów i zaprojektowała system bezprzewodowego sterowania kamerami szybkoobrotowymi RTR008T-h, pracujący w paśmie 868 MHz (standard nadawania RS485). Prędkość transmisji protokołu jest regulowana przez użytkownika w zakresie od 4800 do 38400 bitów na sekundę. System składa się z nadajnika i odbiornika w wykonaniu hermetycznym, który obsługuje protokół Pelco-D, najbardziej popularny dla kamer obrotowych. Nadajnik/odbiornik zasilany jest napięciem stałym 12 V przy poborze prądu rzędu 100 mA. W wersji podstawowej system pracuje na dwóch dookolnych antenach na częstotliwości 868 MHz (w paśmie niewymagającym zezwoleń), zapewniając transmisję o zasięgu do 2000 metrów. Rodzaj zastosowanej anteny ma decydujące znaczenie dla maksymalnej odległości transmisji. Przy zastosowaniu anten kierunkowych zasięg transmisji znacząco się zwiększa. Moduły telemetryczne są zgodne z wymogami normy EN 300 220-1 oraz EN 300 220-2 dla urządzeń bliskiego zasięgu, dotyczącymi kompatybilności elektromagnetycznej EC i zagadnień widma radiowego (ERM – *Electromagnetic Compatibility and Radio Spectrum Matters*), oraz posiadają oznakowanie CE.



Fot. 1. Zestaw telemetrii pełny

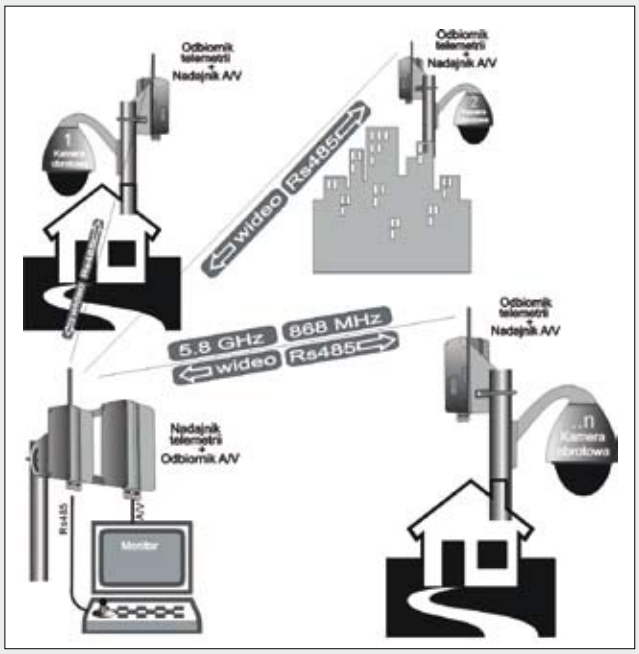
Innowacją konstrukcyjną naszego systemu jest **opcja testu**, w której instalator może sprawdzić poprawność działania urządzenia oraz jakość instalacji, a przede wszystkim brak przeszkód w transmisji, zanim przystąpi do montażu urządzenia w obiekcie. Tej bardzo potrzebnej opcji nie posiadają żadne inne systemy telemetrii, które pojawiły się na rynku. Tylko system RTR008T-h (3D Bydgoszcz) pozwoli inwestorom/instalatorom ocenić, czy system telemetrii w danym obiekcie będzie działał poprawnie i czy transmisja będzie przebiegać bez zakłóceń i przeszkód.

Kolejną konstrukcyjną innowacją jest zasilacz zintegrowany **ZTR-h PTZ**, który powstał podczas prac nad systemem telemetrii. Po stronie kamery obrotowej występują różne rodzaje zasilania: stałe 12 V i 24 V oraz zmienne 230 V. Z myślą o instalatorach, dla których łatwość montażu jest istotna, stworzyliśmy zasilacz zintegrowany w obudowie hermetycznej. Za pomocą jednego zasilacza instalator zasili nadajnik AV, odbiornik telemetrii oraz kamerę obrotową.

Konfiguracja systemu RTR008T-h

Konfiguracji systemu składającego się z jednej lub kilku bezprzewodowych kamer szybkoobrotowych nie należy się obawiać. Wiedza o montowaniu bezprzewodowych systemów transmisji AV, pracujących w paśmie 2,4 GHz i 5,8 GHz, jaką posiadł instalator, w znacznym stopniu ułatwi montaż i początkową obsługę telemetrii. Po instalacji system staje się już bezobsługowy (poza koniecznością obsługi samej kamery przez użytkownika po stronie klawiatury).

Projekt instalacji należy rozpocząć od tzw. **wizji lokalnej** w obiekcie. Należy zastanowić się nad jak najlepszą lokalizacją kamer po to, by ich obraz monitorował oczekiwany obszar, jak również zachowana była widzialność optyczna między nadajnikiem a odbiornikiem bezprzewodowej transmisji wizji oraz między nadajnikiem a odbiornikiem telemetrii. Bez widzialności optycznej urządzeń instalator może mieć poważne kłopoty z uzyskaniem obrazu oraz sterowaniem kamerą obrotową. Do przesyłu wizji nasza firma proponuje zastosowanie systemu pracującego w paśmie 5,8 GHz (RTR05-h). Pasmo 5,8 GHz charakteryzuje się oddzieleniem transmisji cyfrowych (Internet itp.) od analogowych, co w sposób zdecydowany ogranicza liczbę zakłóceń. W podstawowej wersji oba systemy przesyłają sygnał na odległość rzędu 2000 metrów, a zdecydowana większość instalacji przewiduje transmisje na takie właśnie odległości. Istnieje jednak możliwość zwiększenia zasięgu. W przypadku zestawu do przesyłu wizji wymaga to montażu eliminatora zakłóceń bocznych AK05 bądź zewnętrznej anteny kierunkowej 5,8 GHz, a w przypadku zestawu telemetrii zewnętrznej



Rys. 1. System kompleksowej bezprzewodowej obsługi n kamer obrotowych

– anteny kierunkowej 868 MHz. Zasięgi transmisji można zwiększyć w obydwu przypadkach do około 4000 metrów.

Rozpatrzmy przypadek instalacji n bezprzewodowych kamer szybkoobrotowych w jednym obiekcie z zachowaniem widzialności optycznej obsługiwanych przez jeden pulpit (Rys. 1). Konfiguracja takiego systemu składa się z jednego nadajnika telemetrii i n odbiorników telemetrii oraz n nadajników AV i n odbiorników AV. Użytkownik obsługujący pulpit sterujący wyznacza za pomocą nadajnika telemetrii, która kamera ma w danej chwili wykonać jakąś czynność. Przy zastosowaniu większej liczby pulpitów sterujących zwiększa się wymagana liczba nadajników telemetrii. Zasada jest taka, że liczba pulpitów sterujących jest równa liczbie nadajników telemetrii.

Co dalej?

Firma 3D z Bydgoszczy to wiodący producent systemów bezprzewodowych stosowanych w nowoczesnym monitoringu. Mamy za sobą blisko 20 lat doświadczeń w branży elektronicznej. Profil produkcyjny rozpoczynaliśmy od obrotnic anten satelitarnych, dekoderów itp. Od 2000 roku produkujemy bezprzewodowe systemy transmisyjne, początkowo pracujące na częstotliwości 1,2 GHz. Obecnie są to systemy transmisyjne działające na częstotliwościach 2,4 GHz, 5,8 GHz oraz telemetria (868 MHz). Rozpoczęliśmy prace nad kolejnymi produktami, rozszerzając swoją bogatą ofertę. Zachęcamy do kierowania pytań i sugestii na temat naszych produktów na adres *jowita.kuczyniecka@3d.com.pl*. Zapraszamy również do odwiedzenia naszej strony internetowej, gdzie znajdują się opisy poszczególnych produktów, karty katalogowe oraz instrukcje.

Jowita Kuczyniecka
„3D" Bydgoszcz
www.3d.com.pl

INFO-CAM
Generalny dystrybutor AVerMedia Information, Inc.
www.infocam.com.pl
PŁOCK Al. Kilińskiego 5, tel. (024) 266 97 12, tel./fax (024) 266 97 13, handlowy@infocam.com.pl

AVerDiGi SA9000E Pro

- Zapis z 16 wejść wizyjnych – 400 kl./sek. w rozdzielczości 720x576
- Obsługa kamer analogowych, IP, MegaPixel, obrotowych
- Hybrydowe wyjście Spot monitor & Dual monitor
- Wajścia TV analogowe & IP
- Integracja z systemami POS z opcją zaawansowanego wyszukiwania
- Prosty w użyciu touchpad
- Multifunkcyjny panel przedni z wyświetlaczem LCD
- Pokrętło typu jog shuttle ułatwiające przeglądanie archiwum
- Obsługa 16 wejść audio
- Wbudowana nagrywarka DVD-RW
- Wbudowane wyjścia RS-485 i e-SATA
- Obsługa do 4 dysków SATA bez limitu pojemności
- Zaawansowana sprzętowa kompresja obrazu MPEG4
- Zdalna kontrola: CM3000, Remote console, WebViewer, PDAViewer, JavaViewer, HandyViewer i SmartViewer
- Współpraca z pulpitem sterującym AVerDiGi System Controller

AVerMedia

www.avermedia.com
www.averdigi.eu

Oblicza RFID (Część 3)

Zagrożenia

Jednym z wielu bodźców stymulujących postęp cywilizacyjny dzisiejszego społeczeństwa informacyjnego jest wdrażanie nowych technologii do zastosowań w przemyśle i życiu codziennym. Mają one służyć człowiekowi i sprawiać, by mógł on swobodnie funkcjonować. Stosowanie nowych technologii niesie za sobą wiele korzyści, ale też i wiele nowych zagrożeń, na które niejednokrotnie nie jesteśmy przygotowani lub też świadomie je ignorujemy. W przypadku systemów automatycznej identyfikacji RFID są to przede wszystkim zagrożenia związane z ochroną zdrowia i prywatnością użytkowników, a także bezpieczeństwem środowisk informatycznych wykorzystujących technologie RFID.

Grupa robocza Parlamentu Europejskiego ds. oceny technologii w swym raporcie dużo uwagi poświęca zagrożeniom stwarzanym przez technologię RFID w aspekcie ochrony danych osobowych. Wiemy, że dane te stanowią szczególny rodzaj informacji i utrata ich poufności może nieść za sobą wiele przykrych następstw. Ze względu na możliwość skrytego odczytu i modyfikacji danych zawartych w identyfikatorze radiowym stosowanie RFID do wymiany i przechowywania danych osobowych nie wydaje się być dobrym pomysłem. Dlatego też raport krytykuje zalecenie Komisji Europejskiej wprowadzenia w krajach Unii paszportów z układem RFID. Miałyby one zawierać, oprócz podstawowych danych dotyczących właściciela, również jego cyfrową fotografię, a w przyszłości także dane biometryczne (profil DNA, obraz: linii papilarnych, kształtu twarzy, tęczówki oka). Sceptycy obawiają się też tego, że informacja biometryczna przechowywana w różnych systemach bazodanowych (dla celów weryfikacji) może być wykorzystywana niezgodnie z przeznaczeniem.

Problem ochrony danych osobowych dotyczy także możliwości zbierania i nadużywania różnego rodzaju wzorców zachowań przez firmy, rządy i inne instytucje, za pomocą analizy śladów, jakie pozostawiają użytkownicy w środowisku RFID. Mogą być to informacje dotyczące naszej lokalizacji, preferencji, wydajności pracy, zwyczajów, upodobań itp. Przykładem takiego działania jest umieszczenie metek RFID w kartach lojalnościowych niemieckiej sieci marketów Metro, gdzie system automatycznej identyfikacji rejestrował i analizował przemieszczanie się klientów na terenie sklepu.

Technologia RFID może także służyć zorganizowanym szajkom złodziei do namierzania w naszych domach interesujących ich przedmiotów. Za pomocą odpowiednio czułego sprzętu będzie można zeskanować cały dom i na podstawie odczytanych metek RFID ustalić, jaki sprzęt znajduje się w środku. Oczywiście podczas zakupu w kasie sklepowej identyfikatory radiowe powinny być dezaktywowane poleceniem *„kill"*, ale jak na razie nie ma aktów prawnych, które nakładałyby na sprzedawców taki obowiązek. Poza tym klient nie zawsze będzie miał świadomość obecności identyfikatora, który może być ukryty wewnątrz opakowania lub artykułu.

Innym bardzo poważnym zagrożeniem ze strony technologii RFID może być możliwość infekowania przez etykiety radiowe systemów informatycznych i bazodanowych. Wirusy przenikające ze środowiska RFID do systemów nadrzędnych mogą mieć na celu wywołanie określonych działań tychże systemów lub ich całkowity paraliż. W przypadku lotnisk wykorzystujących etykiety RFID do kontroli bagażu mogłoby to umożliwić przemyt narkotyków bądź wprowadzenie na pokład samolotu bomby. W marketach za pomocą zainfekowanych metek można byłoby wpływać na cenę lub sposób naliczania określonych towarów. To tylko dwa przykłady scenariuszy z opublikowanego w 2007 roku uniwersyteckiego raportu *RFID Viruses and Worms*. Jego autorzy ostrzegają, że pojawienie się wirusów zagnieżdżonych w etykietach RFID to tylko kwestia czasu.

Metodę wprowadzenia wirusa do identyfikatora RFID opracował już zespół naukowców z holenderskiego Vrije Universiteit. Udało się to na razie w specyficznych warunkach, które stworzono na potrzeby napisania wirusa. Holenderscy badacze twierdzą, iż założenie przez twórców technologii radiowej, że podczas pobierania informacji z identyfikatora nie będzie możliwa modyfikacja oprogramowania kontrolującego cały proces jest dużym błędem. Badania prowadzone przez naukowców mają na celu opracowanie odpowiednich zabezpieczeń, które w przyszłości pozwolą skutecznie chronić systemy wykorzystujące technologię RFID przed atakami z zewnątrz.

Przed możliwością złamania haseł standardowych metek radiowych ostrzega też znany izraelski informatyk, kryptograf, współtwórca algorytmu RSA, profesor Adi Shamir. Przeprowadził on eksperyment, w którym za pomocą anteny kierunkowej podłączonej do oscyloskopu monitorował fluktuacje energii podczas transmisji pomiędzy czytnikiem a identyfikatorem. Okazało się, że charakterystyka emitowanego sygnału jest zależna od tego, czy chip otrzymywał poprawne, czy niepoprawne hasło. Metoda ta pozwoliła określić, które z transmitowanych bitów informacji są rozpoznawane jako właściwe elementy hasła. Naukowiec przyznał, że wszystkie funkcje i składniki potrzebne do przeprowadzenia podobnego eksperymentu są dostępne w standardowym telefonie komórkowym. Możliwość włamywania się do identyfikatorów radiowych może okazać się przydatna złodziejom sklepowym. Uzbrojeni w czytnik i komputer kieszonkowy zmodyfikują kod towaru tak, aby przy bezobsługowej kasie sklepowej np. aparat cyfrowy był rozpoznawany jako karton mleka.

Ostatnio coraz więcej uwagi poświęca się wpływowi promieniowania elektromagnetycznego na organizm człowieka. Mimo, iż badania prowadzone w tym kierunku z wiadomych przyczyn nie są popularne, a ich wyniki mogą być celowo utajniane, wielu z nas ma świadomość, że używanie np. telefonu komórkowego, bezprzewodowego dostępu do Internetu czy choćby kuchenki mikrofalowej nie jest obojętne dla naszego zdrowia.

Implanty RFID, wszczepiane ludziom w celach identyfikacyjnych (ochrona dzieci) czy usprawniających system leczenia, budzą wiele kontrowersji zarówno z przyczyn etycznych, jak i ze względu na możliwość szkodliwego oddziaływania. Według agencji Associated Press przeprowadzone w ostatnich kilku latach badania dowodzą, że wszczepienie chipów RFID zwierzętom mogło zwiększać ryzyko zachorowania na nowotwory. Chociaż wyniki badań nie są jednoznaczne, naukowcy ostrzegają, że może istnieć związek między tagiem RFID a pojawieniem się nowotworowych schorzeń u badanych szczurów i myszy. Zalecają wstrzymanie się z wszczepianiem implantów ludziom do czasu zakończenia długoterminowych testów na większych zwierzętach. Dr Robert Benezra z nowojorskiego centrum onkologicznego Memorial Sloan-Kettering Cancer Center w rozmowie z dziennikarzami agencji Associated Press powiedział, że nigdy w życiu nie zgodziłby się na instalację chipu RFID u siebie lub kogokolwiek z jego rodziny. Natomiast Scott Silverman, szef firmy VeriChip produkującej implanty RFID, odpowiada, że nic mu nie wiadomo o wynikach badań świadczących o szkodliwym wpływie implantów na organizmy żywe. Produkty VeriChip zostały zaakceptowane przez amerykańską rządową agencję ds. żywności i leków FDA (ang. *Food and Drug Administration*) w 2004 roku. Pozytywna opinia wydana przez FDA dla danego produktu spożywczego lub leku jest uznawana także poza USA za wyznacznik jakości i potwierdzenie niestwierdzenia negatywnego wpływu na zdrowie.

W raporcie Amerykańskiego Stowarzyszenia Medycznego AMA (ang. *American Medical Association*), który podsumowuje szereg testów i analiz dotyczących wszczepiania ludziom implantów RFID, czytamy, że implanty te mogą stanowić fizyczne zagrożenie z uwagi na możliwość przemieszczania się ich pod ludzką skórą. Może to sprawić, że ich usunięcie będzie bardzo trudne, a w niektórych przypadkach wręcz niemożliwe. Innym zagrożeniem, na które zwracają uwagę autorzy raportu, jest możliwość zakłócania pracy aparatury medycznej (np. rozruszników serca) przez interferencje elektromagnetyczne spowodowane implantami radiowymi.

A zatem, choć oficjalnych dowodów na szkodliwe działanie implantów RFID nie ma, to i tak, podobnie jak to jest w przypadku telefonów komórkowych, większość z nas podejrzewa ich szkodliwy wpływ i świadomie się na to zgadza. Nie sądzę jednak, aby w dniu dzisiejszym było możliwe wprowadzenie w którymkolwiek z państw prawnego obowiązku wszczepiania identyfikatorów radiowych ludziom.

Podsumowanie

Identyfikacja radiowa jest technologią, której znaczenie będzie rosło w miarę jej rozwoju. Już teraz jest ona przedmiotem

politycznego zainteresowania, gdyż bardzo szybko może stać się nowym motorem wzrostu gospodarczego i tworzenia miejsc pracy. Przewiduje się, że powszechne stosowanie RFID umożliwi osiągnięcie znacznych korzyści w procesach biznesowych zarówno w sektorze publicznym, jak i prywatnym. Identyfikacja radiowa wzbudza dziś wiele kontrowersji. Jesteśmy świadkami batalii, w której z jednej strony stają rząd, firmy i instytucje, z drugiej zaś obrońcy prywatności i praw człowieka. Jest rzeczą oczywistą, że identyfikacja radiowa musi być wykorzystywana w sposób akceptowany społecznie i politycznie, dopuszczalny etycznie i dozwolony prawem. Konieczne jest zatem stworzenie jasnych i przewidywalnych ram polityczno-prawnych, pozwalających na skrupulatną kontrolę wykorzystywania RFID. Twórcy tej technologii muszą dołożyć wszelkich starań, aby była ona bezpieczna i odporna na wszelkie próby ataków. Należy także zwrócić szczególną uwagę na to, aby końcowi użytkownicy byli świadomi zagrożeń, jakie niesie ona ze sobą, co pozwoli zminimalizować negatywne skutki jej użytkowania.

Przemysław Mierzwiak
Instytut Inżynierii Systemów Bezpieczeństwa

Literatura:

1. www.ama-assn.org
2. www.networld.pl
3. www.rfidvirus.org – *RFID Viruses and Worms*
4. www.washingtonpost.com – *Chip Implants Linked to Animal Tumors*
5. Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie identyfikacji radiowej RFID – (2007/C 256/13)

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

SERIA CZUJEK CYFROWYCH DSC

Precyzyjna cyfrowa technologia opracowana przez firmę DSC pozwala wykryć intruza, redukując tym samym ilość fałszywych alarmów do minimum.

Na terenie prywatnych posiadłości, jak i w budynkach biurowych, seria czujek LC usprawnia system alarmowy, zapewniając niezawodność działania również podczas najbardziej wymyślnych prób włamania.

Dodatkowo smukła linia obudowy, odporność na zwierzęta, prosta instalacja, różne sposoby montażu, odporność na światło białe oraz wiele innych właściwości powoduje, że nowa seria czujek jest niezwykle atrakcyjnym produktem.

Wyłączny dystrybutor w Polsce:

AAT

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

LC-100-PI Czujka PIR odporna na zwierzęta

Wymiary ..... 92 mm x 62,5 mm x 40 mm
Waga ..... 61 g
Metoda detekcji ..... czteroelementowy pasywny czujnik podczerwieni (Quad PIR)
Zasilanie ..... od 8,2 do 16 V=
Pobór prądu (czuwanie) ..... 8 mA (± 5%)
Pobór prądu (działanie) ..... 10 mA (± 5%)
Sabotaż: styk NC ..... 0,1 A @ 28 V=
Odporność na zakłócenia:
• radiowe ..... 10 V/m 80-1000 MHz
• statyczne ..... 8 kV kontakt, 15 kV powietrze
• przepięciowe..... 2,4 kV @ 1,2 J

LC-101-CAM Czujka PIR z kamerą (czarno-biała/kolorowa), odporna na zwierzęta

Wymiary ..... 116 mm x 62,5 mm x 40 mm
Waga ..... 112 g
Metoda detekcji ..... czteroelementowy pasywny czujnik podczerwieni (Quad PIR)
Zasilanie ..... od 8,2 do 16 V=
Pobór prądu (czarno-biała) ..... 115 mA
Pobór prądu (kolorowa) ..... 150 mA
Sabotaż: styk NC ..... 0,1 A @ 28 V=
Odporność na zakłócenia:
• radiowe ..... 10 V/m 80-1000 MHz
• statyczne ..... 8 kV kontakt, 15 kV powietrze
• przepięciowe..... 2,4 kV @ 1,2 J

LC-102-PIGBSS Czujka PIR oraz zbicia szyby, odporna na zwierzęta

Wymiary ..... 118 mm x 62,5 mm x 41 mm
Waga ..... 83 g
Metoda detekcji ..... czteroelementowy pasywny czujnik podczerwieni (Quad PIR)
Zasilanie ..... od 8,2 do 16 V=
Pobór prądu (czuwanie) ..... 16,5 mA
Pobór prądu (działanie) ..... 22 mA
Sabotaż: Styk NC ..... 0,1 A @ 28 V=
Odporność na zakłócenia:
• radiowe ..... 10 V/m 80-1000 MHz
• statyczne ..... 8 kV kontakt, 15 kV powietrze
• przepięciowe..... 2,4 kV @ 1,2 J

LC-103-PIMSK Czujka PIR + mikrofala z antymaskingiem, odporna na zwierzęta

Wymiary ..... 118 mm x 62,5 mm x 41 mm
Waga ..... 102 g
Metoda detekcji ..... czteroelementowy pasywny czujnik podczerwieni (Quad PIR) + mikrofala Doppler
Zasilanie ..... od 8,2 do 16 V=
Pobór prądu (czuwanie) ..... 18 mA
Pobór prądu (działanie) ..... 25,5 mA
Sabotaż: styk NC ..... 0,1 A @ 28 V=
Odporność na zakłócenia:
• radiowe ..... 10 V/m 80-1000 MHz
• statyczne ..... 8 kV kontakt, 15 kV powietrze
• przepięciowe..... 2,4 kV @ 1,2 J

LC-104-PIMW Czujka PIR + mikrofala

Wymiary ..... 118 mm x 62,5 mm x 41 mm
Waga ..... 102 g
Metoda detekcji ..... czteroelementowy pasywny czujnik podczerwieni (Quad PIR) + mikrofala Doppler
Zasilanie ..... od 8,2 do 16 V=
Pobór prądu (czuwanie) ..... 18 mA
Pobór prądu (działanie) ..... 25,5 mA
Sabotaż: styk NC ..... 0,1 A @ 28 V=
Odporność na zakłócenia:
• radiowe ..... 10 V/m 80-1000 MHz
• statyczne ..... 8 kV kontakt, 15 kV powietrze
• przepięciowe..... 2,4 kV @ 1,2 J

LC-105-DGB Czujka zbicia szyby

Wymiary ..... 79 mm x 48 mm x 21 mm
Waga ..... 40 g
Zasięg ..... 10 m max
Zasilanie ..... od 9 do 16 V=
Pobór prądu (czuwanie) ..... 15 mA @ 12 V=
Pobór prądu (działanie) ..... 40 mA @ 24 V=
Sabotaż: styk NC ..... 50 mA @ 24 V=
Odporność na zakłócenia:
• radiowe ..... 10 V/m 80-1000 MHz
• statyczne ..... 8 kV kontakt, 15 kV powietrze
• przepięciowe..... 2,4 kV @ 1,2 J

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

NOVUS®

Profesjonalne rozwiązanie dla systemów CCTV

NOWA generacja monitorów LCD

profesjonalne monitory LCD serii 400

- zaprojektowane specjalnie dla systemów CCTV
- przekątna ekranu: 23", 32"
- wysoka rozdzielczość: 580 TVL
- wbudowany 4-kanałowy multiplekser z funkcją pamięci 60 obrazów
- równoczesne wyświetlanie wielu sygnałów wizji
- złącza sygnału wideo: 4 x BNC, S-Video, VGA, RCA
- wbudowane głośniki
- blokada przycisków i dostęp do menu zabezpieczony hasłem
- menu ekranowe w języku polskim
- solidna metalowa obudowa

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

System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001

Cz. 2. Procesy zarządzania bezpieczeństwem informacji

Artykuł ten jest kontynuacją cyklu poświęconego zarządzaniu bezpieczeństwem informacji zgodnemu z normą ISO/IEC 27001. W kolejnych częściach zostaną omówione elementy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz jeden z modeli zarządzania bezpieczeństwem systemów informatycznych (PDCA)

1. Wprowadzenie

Zarządzanie bezpieczeństwem systemów informatycznych oznacza ciągły proces składający się z pewnej liczby innych procesów (subprocesów). Dla celów jednoznacznego i przejrzystego zaprezentowania w tym rozdziale zagadnień z tym związanych określono definicję terminu proces. I tak, zgodnie ze słownikami języka polskiego:
proces oznacza przebieg następujących po sobie i powiązanych przyczynowo określonych zmian, stanowiących stadia, fazy, etapy rozwoju czegoś; przebieg, rozwijanie się, przeobrażanie się czegoś.

Zgodnie z normą PN-I-13335-1:1999 do najistotniejszych procesów wchodzących w skład procesu zarządzania bezpieczeństwem systemów informatycznych można zaliczyć:
- zarządzanie konfiguracją,
- zarządzanie zmianami,
- zarządzanie ryzykiem.

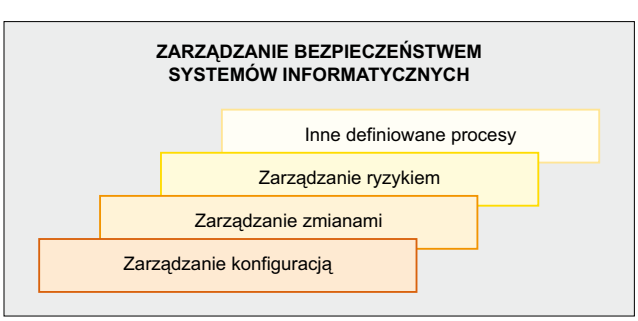
Na rysunku nr 1[1] przedstawiono proces zarządzania bezpieczeństwem systemów informatycznych z uwzględnieniem tworzących go procesów.

2. Zarządzanie konfiguracją

Zarządzanie konfiguracją jest procesem weryfikacji zmian w systemie. Podstawowym celem bezpieczeństwa w tym zakresie jest wiedza i świadomość wprowadzonych zmian. Zarządzanie konfiguracją ma gwarantować:
- wprowadzanie zmian, które nie obniżą efektywności funkcjonowania systemu, skuteczności mechanizmów zabezpieczających oraz ogólnego bezpieczeństwa organizacji,
- wprowadzanie stosownych zmian dotyczących planowania ciągłości działania i odtwarzania po awarii.

Proces zarządzania konfiguracją nie dotyczy tylko zmian konfiguracji, lecz obejmuje również:
- weryfikację legalności oprogramowania,
- sprawdzenie mechanizmów kontrolnych przechowywania oprogramowania,
- inwentaryzację zasobów organizacji.

W tym obszarze audytor powinien zweryfikować m.in.:
- istnienie procedur gwarantujących, że w rejestrze zasobów wskazane są wyłącznie istniejące i autoryzowane składniki konfiguracji,
- stosowanie procedur zapewniających rejestrowanie wszelkich zmian konfiguracji,
- aktualność, spójność i kompletność rejestru konfiguracji,
- istnienie konfiguracji wzorcowej, czyli punktu kontrolnego używanego do ewentualnego powrotu po zmianach,
- stosowanie oprogramowania antywirusowego,
- stosowanie procedur zabraniających używania własnego i nielicencjonowanego oprogramowania,



Rys. 1. Proces zarządzania bezpieczeństwem systemów informatycznych

1) na podstawie M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*.

– istnienie polityki zarządzania wersjami,
– stosowanie procedur sprawdzania legalności oprogramowania.

3. Zarządzanie zmianami

Zarządzanie zmianami polega na identyfikowaniu nowych wymagań w zakresie bezpieczeństwa, gdy wprowadzane są zmiany w systemie informatycznym.

Szybki rozwój usług i technologii, a także ciągłe pojawianie się nowych zagrożeń oraz podatności sprawia, że systemy informatyczne podlegają nieustannym zmianom. Mogą one dotyczyć:
– nowych procedur i funkcji systemu,
– aktualizacji oprogramowania, zmian sprzętowych,
– pojawienia się nowych użytkowników,
– wprowadzenia dodatkowych połączeń sieciowych i międzysieciowych.

Każda planowana zmiana w systemie informatycznym powinna być poddana analizie pod kątem jej wpływu na bezpieczeństwo, z uwzględnieniem związanych z nią rodzajów ryzyka oraz potencjalnych zysków i kosztów.

W przypadku niewielkich zmian pełna analiza ryzyka nie jest wymagana i może być przeprowadzana w trakcie spotkania roboczego. Wszelkie ustalenia powinny być jednak odpowiednio udokumentowane. Poważne zmiany w systemie wymagają dokładnej oceny ryzyka w celu określenia nowych wymagań bezpieczeństwa.

W tym obszarze audytor powinien zweryfikować m.in.:
– istnienie procedur wprowadzania zmian w infrastrukturze informatycznej,
– sposób definiowania wymagań funkcjonalnych dla nowych lub modyfikowanych komponentów,
– istnienie wymagań w zakresie mechanizmów bezpieczeństwa, które muszą posiadać nowe lub modyfikowane komponenty,
– istnienie metod sprawdzania stosowania wymaganych mechanizmów bezpieczeństwa w odniesieniu do nowych lub modyfikowanych komponentów,
– sposób analizowania zgodności nowych komponentów z pozostałymi elementami systemu informatycznego,
– istnienie szczegółowego planu wprowadzania zmian,
– sposób planowania infrastruktury informatycznej w organizacji.

Skuteczny proces zarządzania zmianami zapewnia spójność infrastruktury informatycznej, odpowiedni poziom bezpieczeństwa informacji przy projektowaniu nowych rozwiązań oraz wdrożenie komponentów o wysokiej jakości.

4. Zarządzanie ryzykiem

Zarządzanie ryzykiem to proces szacowania ryzyka mający na celu ograniczenie go do akceptowalnego poziomu. Formalny proces zarządzania ryzykiem musi być włączony w planowanie, nabywanie, rozwój, testowanie i działania służące odpowiedniemu rozmieszczeniu systemów informatycznych.

Zgodnie z PN-I-13335-1:1999 – **zarządzanie ryzykiem to całkowity proces identyfikacji, kontrolowania i eliminacji lub minimalizowania prawdopodobieństwa zaistnienia niepewnych zdarzeń, które mogą mieć wpływ na zasoby systemu informatycznego**.

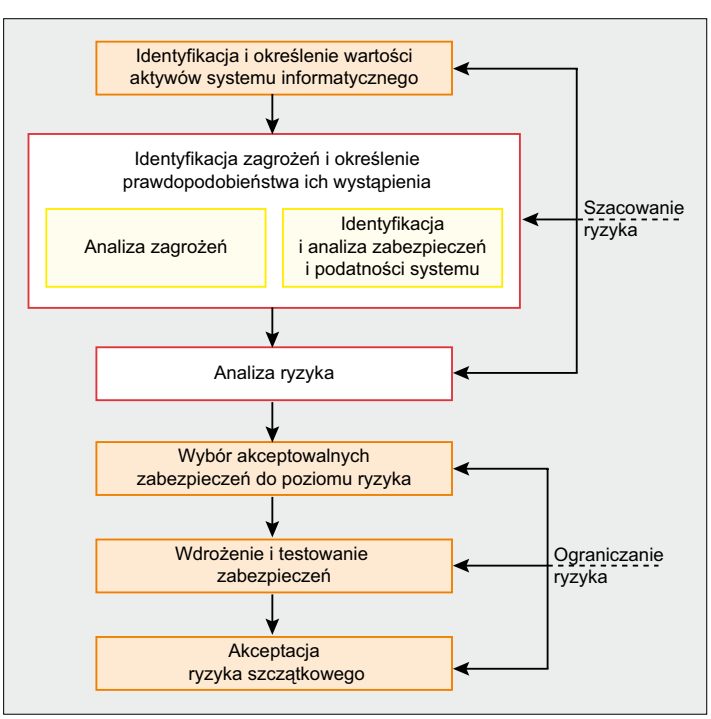
Efektywny program zarządzania ryzykiem powinien zapewniać osiągnięcie celów biznesowych organizacji przez:
– skuteczniejsze zabezpieczenie systemów informatycznych, które służą do przechowywania, przetwarzania i przesyłania informacji należących do organizacji,
– umożliwienie kierownictwu uzasadnienia swych decyzji dotyczących wydatków na zarządzanie ryzykiem zaplanowanych w budżecie.

Program zarządzania ryzykiem powinien mieć cel zdefiniowany przez dyrektora jednostki. Powinny zostać zdefiniowane także cele szczegółowe, np. ograniczenie kosztów ponoszonych na ubezpieczenie. Skuteczne opracowanie, wdrożenie, utrzymanie i doskonalenie procesu zarządzania ryzykiem wymaga powołania specjalnego komitetu oraz zespołu wykonawczego, a także wsparcia ze strony kierownictwa w zakresie identyfikacji obszarów ryzyka i rozwoju strategii postępowania z ryzykiem.

„Stary model" (wcześniejszy) zarządzania ryzykiem został przedstawiony na rys. 2.

W ramach „starego modelu" zarządzania ryzykiem można wyróżnić dwa procesy główne:
– szacowanie ryzyka,
– ograniczanie ryzyka.

Szacowanie ryzyka obejmuje:
1. zidentyfikowanie i określenie wartości aktywów organizacji – można wykorzystać tu metodę jakościową lub ilościową (patrz tab. 1),
2. zidentyfikowanie zagrożeń i określenie prawdopodobieństwa ich wystąpienia,
3. analizę ryzyka – ocenę podatności systemów lub aktywów na wystąpienie czynników ryzyka (czynniki ryzyka sprzyjające wystąpieniu strat).



Rys. 2. Wcześniejsze podejście do zarządzania ryzykiem[2]

2) na podstawie M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*.

Metoda jakościowa szacowania wartości aktywów (5-stopniowa skala wartościowania)	Metoda ilościowa szacowania wartości aktywów
Pomijana	<1 000 zł
Niska	<10 000 zł
Średnia	<100 000 zł
Wysoka	<1 000 000 zł
Katastrofalna	>1 000 000 zł

Tab. 1. Przykładowe porównanie metody jakościowej i ilościowej szacowania wartości aktywów

Poniżej przedstawione zostały dwa modele zarządzania ryzykiem, tzw. „stary model", bazujący na wcześniejszych normach, oraz „model nowy" (Rys. 3), opracowany na podstawie metodologii ISO/IEC 27001.

Na ograniczanie ryzyka składają się następujące działania:
- wybór odpowiednich mechanizmów zabezpieczeń,
- wdrożenie, testowanie i monitorowanie mechanizmów zabezpieczeń,
- akceptacja ryzyka szczątkowego.

Ryzyko szczątkowe (*residual risk*) **to ryzyko, które pozostaje po wprowadzeniu mechanizmów zabezpieczających**.

Proces szacowania ryzyka obejmuje identyfikację informacji lub aktywów informatycznych, które są podatne (wrażliwe) na naruszenie bezpieczeństwa.

Przykładowe aktywa informatyczne to:
- oprogramowanie i sprzęt komputerowy,
- zasoby informacyjne,
- usługi,
- dokumenty organizacji,
- pracownicy,
- zasoby intelektualne,
- spis inwentarza,
- środki finansowe,
- budynki, wyposażenie itp.

Kolejnym etapem procesu szacowania ryzyka jest zdefiniowanie zagrożeń związanych ze wskazanymi w poprzedniej fazie aktywami oraz określenie prawdopodobieństwa wystąpienia podatności.

Podatność oznacza słabość mechanizmów kontroli wewnętrznej, która może być wykorzystana do uzyskania nieautoryzowanego dostępu do systemu lub zakłócenia jego pracy.

Zagrożenie oznacza niebezpieczeństwo dla systemów informatycznych, podwyższające prawdopodobieństwo poniesienia strat.

Rezultatem wykorzystania podatności przez zagrożenie jest następstwo (np. strata aktywów informatycznych). Następstwo może mieć charakter ilościowy (bezpośrednia strata pieniędzy, niewykorzystanie możliwości, zakłócenie) lub jakościowy (naruszenie prawa, zniszczenie reputacji, odejście załogi) oraz może oznaczać pośrednie lub bezpośrednie straty dla organizacji.

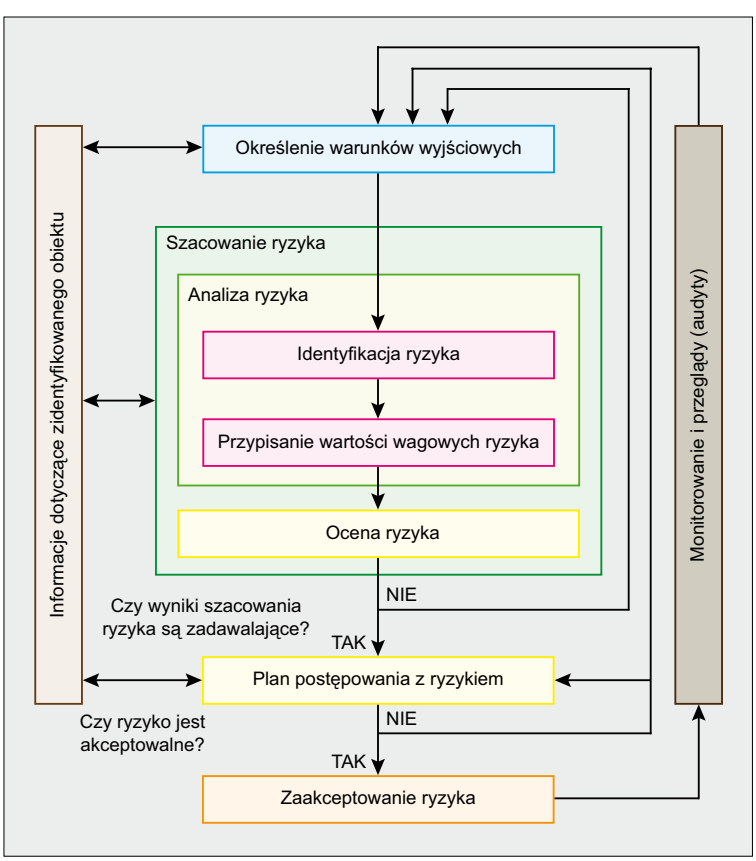
Po zidentyfikowaniu aktywów, zagrożeń i podatności organizacja musi określić akceptowalny poziom ryzyka. Dla wszystkich nieakceptowanych rodzajów ryzyka audytor powinien wskazać i ocenić istniejące mechanizmy kontrolne. Weryfikacja ta wskazuje, czy konieczne jest wdrożenie dodatkowych środków zabezpieczających w celu zredukowania ryzyka lub ograniczenia ryzyka szczątkowego.

Po wdrożeniu mechanizmów kontrolnych w jednostce zawsze pozostaje pewne ryzyko szczątkowe. Kierownictwo może wykorzystać je do określenia obszarów wymagających dodatkowych mechanizmów kontrolnych. Akceptacja ryzyka szczątkowego zależy od polityki organizacji, planu zarządzania ryzykiem oraz efektywności kosztowej wdrożenia dodatkowych mechanizmów kontrolnych.

Obecnie funkcjonuje również nowe podejście do zarządzania ryzykiem; szczegóły tego podejścia przedstawione zostały na rysunku 3[3].

W nowym modelu celem procesu zarządzania ryzykiem jest ograniczenie ryzyka do akceptowalnego poziomu przez opracowanie odpowiedniego planu postępowania z ryzykiem. W modelu tym istotną sprawą jest również to, że działania (monitoring, przeglądy) są efektywne, jeśli wykonywane są w sposób ciągły i systematyczny.

W celu lepszego wyjaśnienia zasad regulujących efektywne zarządzanie ryzykiem warto wskazać wzajemne relacje między elementami bezpieczeństwa związanymi z tym procesem (Rys. 4).



Rys. 3. Nowy model zarządzania ryzykiem

3) na podstawie M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*.

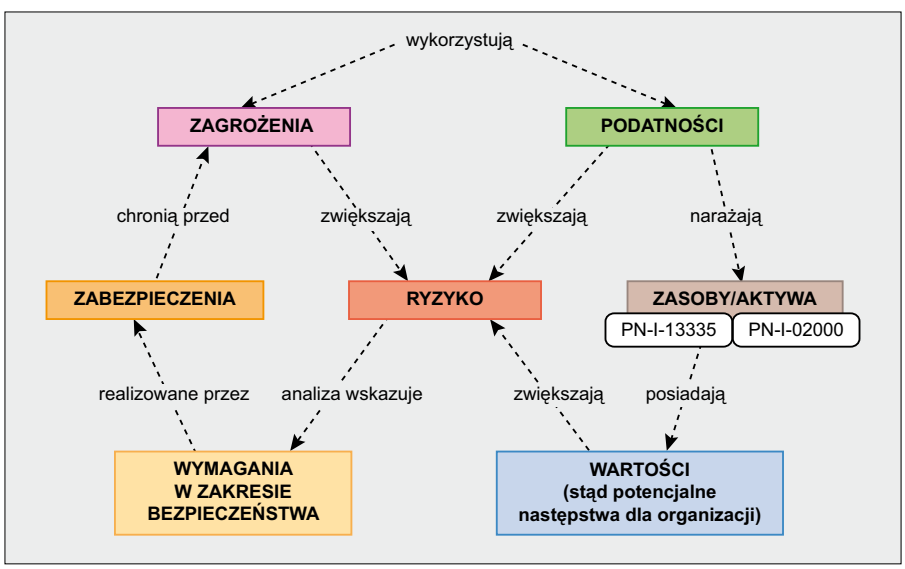
5. Identyfikacja ryzyka

Istnieje wiele metod wskazywania ryzyka. Wybór odpowiedniej techniki zależy od charakteru badanego obszaru, a także obszaru dotyczącego zarządzania ryzykiem, tj. systemu bezpieczeństwa informacji. Do istotnych narzędzi identyfikujących ryzyko można zaliczyć:

- **analizę środowiskową** – ocenę wpływu zmian środowiska zewnętrznego na procesy zarządzania i kontroli w organizacji,
- **scenariusze zagrożeń** – symulowanie awarii i słabości systemu kontroli wewnętrznej,
- **analizę potencjalnych strat** – ocenę z punktu widzenia zasobów organizacji,
- **identyfikację systemową** – ocenę wpływów wszystkich możliwych do zidentyfikowania czynników ryzyka.

Do popularnych wśród profesjonalistów narzędzi analizy ryzyka należą:

1. **CRAMM** (*CCTA Risk Analysis and Management Method*) – metoda realizująca wymagania norm poprzez analizę luk i opracowywanie programu poprawy bezpieczeństwa, tworzenie rejestru zasobów informacji, definiowanie zakresu zarządzania bezpieczeństwem informacji oraz poprzez tworzenie dokumentacji wdrożonych środków zaradczych.
2. **COBRA** (*Control Objectives for Risk Analysis*) – pełna metodyka analizy ryzyka, zaprojektowana dla zarządu i kierownictwa organizacji do całościowej oceny profilu ryzyka związanego z prowadzoną działalnością, ze szczególnym uwzględnieniem bezpieczeństwa wizerunku jednostki, zgodności z obowiązującymi regulacjami prawnymi i ustawodawczymi, oraz do wewnętrznych mechanizmów kontrolnych.
3. **MARION** (*Mission Analysis and Risk Impact on Operations Net-work-tool*).
4. **MEHARI** (*Methode Harmonisee d'Analyse de Risques*) – realizuje zalecenia norm BS 7799 i ISO/IEC 13335 przy użyciu jednolitego systemu oszacowania ryzyka, prawidłowo dobranych zabezpieczeń i lokalizacji zasobów.
5. **EBIOS** (*Expression des Besoins et Identification des Objectifs de Securite*) – to nie tylko metoda szacowania ryzyka, lecz również narzędzie wspomagające zarząd (służące do określania wymagań, definiowania zakresu badania). W powiązaniu z *Common Criteria* oraz ciągłym rozwojem w zakresie zarządzania bezpieczeństwem informacji (seria ISO 27000) EBIOS staje się techniką całościowego zarządzania ryzykiem.



Rys. 4. Zależności między elementami bezpieczeństwa w kontekście zarządzania ryzykiem[4]

4) Na podstawie PN-I-13335-1:1998, *Wytyczne do zarządzania bezpieczeństwem systemów informacyjnych*.

DR INŻ. ANDRZEJ WÓJCIK

ES INSTAL sp. z o.o.
02-743 Warszawa
ul. Batuty 1/804
tel./faks 022 847 47 52
e-mail: andrzej@acn.pl
http://www.esinstal.pl

Jesteśmy firmą, która rozwiązuje problemy z zakresu bezpieczeństwa osób, mienia i ochrony informacji

Realizujemy projekty z każdego, najbardziej wymagającego zakresu zabezpieczenia techniczno-organizacyjnego i branż pokrewnych

Audyty bezpieczeństwa
Usługi projektowe
Kosztorysowanie
Kompleksowe opracowanie Polityki Bezpieczeństwa
Usługi prawno-organizacyjne

Jesteśmy ekspertami w zakresie projektowania systemów sygnalizacji zagrożeń, okablowania strukturalnego, organizacji ochrony fizycznej, systemów ochrony informacji niejawnej, zarówno w zakresie technicznym, jak i organizacyjnym

Rozproszony system bezpieczeństwa
dla dużego rozległego obiektu w aspekcie zdalnego zarządzania

Zaprojektowanie oraz realizacja rozproszonego Systemu Sygnalizacji Włamania i Napadu (SSWiN) dla dużego i rozległego obiektu wymaga sporej wiedzy technicznej, jak również dużego doświadczenia. Istnieją obiekty, w których ze względów ekonomicznych, a także logistycznych może jedynie wchodzić w rachubę integracja mniejszych systemów. Szczególnie trudne w realizacji są obiekty, które są eksploatowane ze stochastyczną intensywnością

Można zaprojektować SSWiN złożony z kilku central, np. o pojemności 128 linii dozorowych każda, i, jeśli to możliwe, integrować je. Z analizy różnych systemów wynika, że niewiele typów central alarmowych można ze sobą łączyć, ponadto nie zawsze jest to konieczne. Ze względów logistycznych można zastosować kilka central alarmowych o sporej liczbie linii dozorowych, które będą obsługiwać np. określone fragmenty obiektu, a więc każda z central będzie miała własny manipulator, za pomocą którego będzie można realizować określone funkcje systemu.

Takie rozwiązanie przyjęto w jednym z dużych i rozległych obiektów Politechniki Warszawskiej (PW), który stał się swoistym poligonem doświadczalnym. W obiekcie zastosowano siedem central INTEGRA 128 produkcji polskiej. Do dyspozycji użytkowników producent przewidział dla jednej centrali alarmowej 32 strefy. Ze względu na charakter użytkowania tego naukowo-dydaktycznego obiektu oraz pomimo bardzo dużej złożoności SSWiN przyjęto generalną zasadę uproszczenia do minimum sposobu obsługi części systemu (podsystemu) przez użytkowników. Dokonano analizy liczby stref niezbędnych do prawidłowego funkcjonowania poszczególnych central. Przyjęto zasadę, że dany fragment SSWiN (podsystem) posiada minimum jeden własny manipulator z wyświetlaczem LCD i klawiaturą do wprowadzania kodów użytkownika. Manipulator jest wyposażony również w czytnik kart zbliżeniowych. Karcie zbliżeniowej przyporządkowano użytkownika, dokładnie określonego dla jego łatwej identyfikacji, oraz określone strefy, do których ma on dostęp. Można więc w dwojaki sposób włączać lub wyłączać dozorowanie danej strefy: poprzez wprowadzenie kodu użytkownika lub za pomocą karty zbliżeniowej.

W pomieszczeniach recepcji obiektu zostały zainstalowane tablice synoptyczne, na których pokazywana jest informacja o aktualnym stanie stref oraz stanie wybranych linii dozorowych całego SSWiN. Elementami informującymi tablic synoptycznych są dwukolorowe diody LED. Odpowiednio zaprogramowany sposób świecenia diod daje pełną informację o stanie stref oraz stanie wybranych linii dozorowych. I tak przykładowo: kolor zielony to informacja, że dana strefa jest w stanie dozoru, kolor czerwony pulsujący oznacza, że wystąpił alarm włamaniowy wynikający z naruszenia czujki danego pomieszczenia (strefy), czerwony ciągły – alarm pożarowy wynikający z naruszenia optycznej czujki dymu w danym pomieszczeniu, brak świecenia diody LED oznacza, że dana strefa jest w stanie gotowości, bez dozoru. Dodatkowo informacje o wystąpieniu alarmu w danej konkretnej centrali alarmowej (podsystemie) są przesyłane drogą radiową do wydzielonej centrali tego samego typu, oznaczonej C-7, która jest centralą odpowiedzialną za monitoring zewnętrzny oraz alarm głośny w pomieszczeniu recepcyjnym. Jest to pierwszy stopień monitorowania SSWiN. Przewidziano jeszcze drugi stopień monitorowania o wystąpieniu zagrożenia. Po godz. 22:00 centrala C-7 ma możliwość automatycznego przekazywania informacji o alarmie łączami komutowanymi (przez własną sieć telekomunikacyjną) lub drogą radiową (także przez własną sieć – radiokomunikacyjną) do Straży Akademickiej Politechniki Warszawskiej. Ta, po zweryfikowaniu alarmu z opisywanego obiektu, wysyła patrole interwencyjne. Warto również nadmienić, że ze względu na bardzo duży stopień rozbudowania SSWiN autorzy bardzo starannie dobrali rezerwowe źródła zasilania (o parametrach wynikających z bilansu energetycznego).

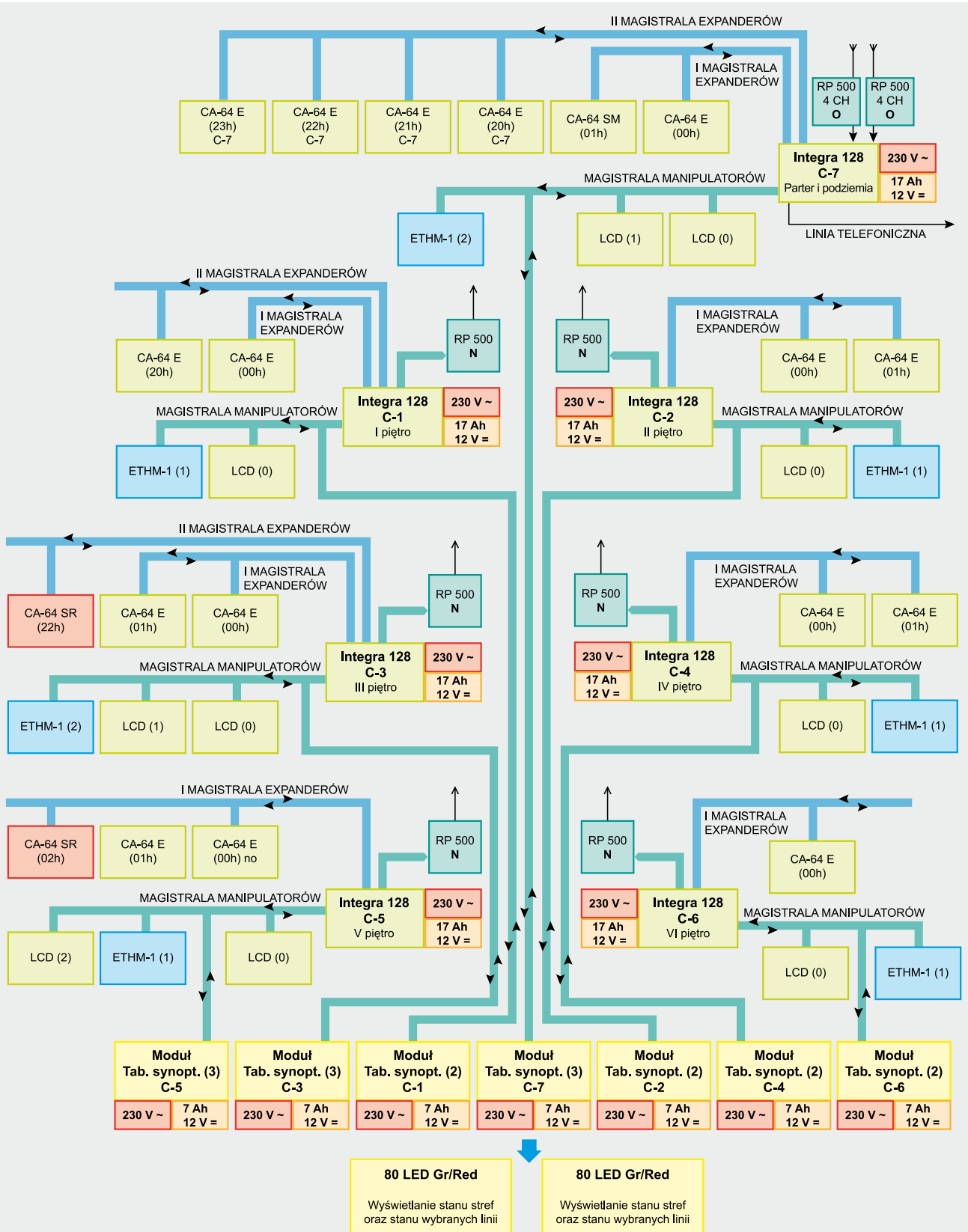
Na rys. 1 przedstawiono rozproszony SSWiN, złożony z siedmiu jednostek mikroprocesorowych (central) typu INTEGRA 128, do których za pośrednictwem magistral transmisyjnych dołączono wiele różnych modułów. Cały system SSWiN za pośrednictwem modułów ethernetowych ETHM-1 współpracuje poprzez sieć LAN z serwerem umożliwiającym administrowanie tak bardzo złożonym systemem bezpieczeństwa.

Założenia oraz konfiguracja rozproszonego SSWiN dla dużego obiektu

W trakcie projektowania oraz późniejszej realizacji rozproszonego systemu bezpieczeństwa autorzy przyjęli następujące założenia:

a) obiekt, w którym ma być realizowany SSWiN, jest obiektem rozległym, o kilku piętrach,
b) konfiguracja SSWiN ma charakter rozproszony i ma być wielocentralowa,
c) maksymalna liczba linii dozorowych (perspektywiczna) wynosi 896 (w pierwszym etapie –240),
d) maksymalna liczba central typu INTEGRA 128, zlokalizowanych na różnych piętrach obiektu, wynosi 7 (od C-1 do C-7),
e) liczba stref w jednym systemie bezpieczeństwa nie przekracza 32,
f) system bezpieczeństwa musi mieć możliwość realizacji lokalnej kontroli dostępu,
g) system pracuje przez 24 godziny na dobę, przy czym przedział pomiędzy godz. 7:00 a 22:00 wyznacza godziny pracy użytkowników obiektu,
h) kategoria zagrożeń – Z3,
i) klasa SSWiN – III (dawniej SA3),
j) kategoria sprzętowa – C,
k) system bezpieczeństwa (zaprojektowany i zrealizowany) musi być monitorowany co najmniej jedną drogą do godz. 22:00 i dwiema drogami po godz. 22:00,
l) system bezpieczeństwa musi zawierać minimum 7 klawiatur z 7 czytnikami kart zbliżeniowych (zintegrowane klawiatury),
m) system bezpieczeństwa musi posiadać lokalną kontrolę dostępu z czytnikami kart zbliżeniowych,

n) system bezpieczeństwa musi być wyposażony w tablice synoptyczne z awaryjnym źródłem zasilania, zlokalizowane w pomieszczeniach recepcyjnych,
o) każda z central INTEGRA 128 powinna być wyposażona w moduł ETHM-1 do współpracy z serwerem przez sieć LAN dla administrowania i zarządzania SSWiN,
p) zaprojektowany i zrealizowany system bezpieczeństwa wyposażono w rezerwowe źródła zasilania, tak aby w razie zaniku zasilania zasadniczego (230V) mógł pracować przez okres ok. 40 godzin,
r) system bezpieczeństwa jest wspomagany przez 32 kamery telewizyjne (zewnętrzne i wewnętrzne) z zapisem



Rys. 1. Uproszczony schemat blokowy elektronicznego rozproszonego systemu bezpieczeństwa dla dużego obiektu

zdarzeń na twardym dysku i z możliwością podglądu z wykorzystaniem sieci teleinformatycznych, zarówno lokalnych jak i rozległych.

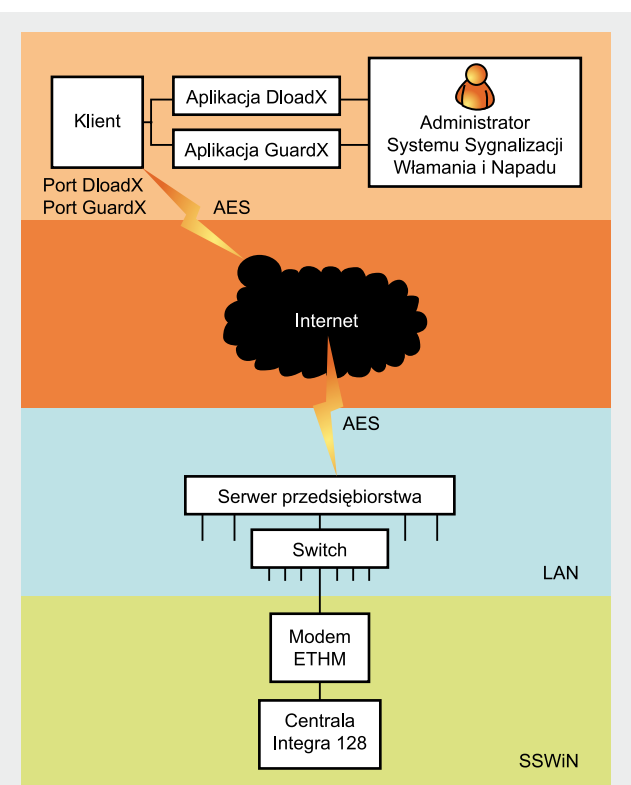
Syntetyczny opis budowy rozproszonego systemu bezpieczeństwa dla dużego obiektu

Na rys. 1 przedstawiono uproszczony schemat blokowy rozproszonego elektronicznego systemu bezpieczeństwa dla dużego obiektu. SSWiN został zaprojektowany na bazie jednostki mikroprocesorowej typu INTEGRA 128. Wprost do wejść linii dozorowych płyt głównych zostały dołączone czujki usytuowane blisko central alarmowych (np. na określonym piętrze i korytarzu). Pomieszczenia dalsze są obsługiwane za pośrednictwem modułów typu CA-64 E (ekspanderów wejść).

Każda z central alarmowych została wyposażona w co najmniej jeden manipulator (klawiaturę z wyświetlaczem LCD oraz wbudowanym czytnikiem kart zbliżeniowych). Manipulatory zostały zlokalizowane w widocznych miejscach na korytarzach kolejnych pięter obiektu i zabezpieczone mechanicznie (ich obudowy metalowe zamykane są na zamek patentowy).

Lokalizacja tych manipulatorów została starannie dobrana tak, aby w możliwie prosty sposób upoważniony użytkownik danego piętra mógł włączać lub wyłączać dozorowanie określonych stref – pomieszczeń, do których posiada uprawnienia. Użytkownik może wykonywać tę czynność w dwojaki sposób: używając przydzielonego kodu lub używając przypisanej mu karty zbliżeniowej. Oba sposoby przynoszą ten sam skutek.

Centrala C-7 pełni dodatkową, w pewnym sensie integracyjną rolę w rozproszonym SSWiN. Każda z pozostałych central (od CA-1 do CA-6) została wyposażona w wielokanałowy nadajnik typu RP-500N, który drogą radiową transmituje sygnał alarmowy właśnie do centrali C-7. Jest ona wyposażona w dwa czterokanałowe odbiorniki sygnalizujące alarm z poszczególnych podsystemów. Do centrali C-7 został dołączony moduł CA-64 SM (ekspander syntezerów mowy umożliwiający nagranie do 16 komunikatów słownych). Moduł CA-64 SM umożliwia wysyłanie 15-sekundowych komunikatów słownych, wykorzystywanych do powiadamiania telefonicznego o zdarzeniach, które wystąpiły w systemie bezpieczeństwa, np. o alarmach, napadach, sabotażach, awariach itp. Tylko centrala C-7 jest połączona przez wbudowany dialer z siecią telefoniczną. Centrala C-7 obsługuje również system ochrony obwodowej. Obejmuje on bariery aktywne podczerwieni oraz czujki zewnętrzne podczerwieni. Manipulatory centrali alarmowej C-7 znajdują się w pomieszczeniach recepcyjnych.



Rys. 2. Przykład połączenia „Administratora Systemu" z jedną centralą INTEGRA 128 przez niezabezpieczoną sieć Internet

Pewnym wyjątkiem są także centrale alarmowe C-3 i C-5, do których dołączono po dwa manipulatory wraz z czytnikami kart zbliżeniowych. W obu przypadkach za pośrednictwem magistral transmisyjnych poza klasycznymi modułami rozszerzającymi typu CA-64 E zostały dołączone do central moduły CA-64 SR (ekspandery czytników kart zbliżeniowych), które współpracują z lokalną kontrolą dostępu. Drzwi wejściowe do części chronionej przez centrale C-3 i C-5 współpracują z ryglami elektromagnetycznymi, które są sterowane przez moduły CA-64 SR. Z modułami CA-64 SR współpracują czytniki kart zbliżeniowych typu CZ-EMM (są zamontowane obok drzwi wejściowych). Moduł taki może współpracować z jednym lub z dwoma czytnikami kart zbliżeniowych. Pomieszczenia chronione przez centrale C-3 i C-5 to pomieszczenia o specjalnym przeznaczeniu. Są one również nadzorowane za pośrednictwem kamer telewizyjnych.

Centrale alarmowe typu INTEGRA 128 zostały zainstalowane w obiekcie w miejscach trudnodostępnych dla osób postronnych. Każda z central poza zasilaniem głównym (230 V) została wyposażona w źródło rezerwowe w postaci akumulatora żelowego o pojemności 17 Ah.

Sygnały z central alarmowych docierają drogą kablową (magistralą transmisyjną) do modułów tablic synoptycznych CA-64 PTSA, które sterują dwukolorowymi diodami LED. Moduły CA-64 PTSA oraz tablice z diodami LED są umieszczone w pomieszczeniu recepcji na parterze budynku. Na tablicy synoptycznej zaświeca się czerwona dioda LED, sygnalizując alarm w określonej strefie. Jak już wspomniano, tablice synoptyczne (2 szt.), zawierające po 80 dwukolorowych diod LED, mogą wyświetlić stan 160 stref dozorowych całego SSWiN oraz aktualny stan specjalnie wybranych linii dozorowych (takich jak linie pożarowe, zewnętrzne, napadowe, 24-godzinne). Moduły tablic synoptycznych CA-64 PTSA poza własnym zasilaniem zasadniczym (230 V) zostały wyposażone w akumulatory rezerwowe o pojemności 7 Ah.

Zdalna obsługa serwisowa oraz nadzór i administracja rozproszonego SSWiN

Ze względu na to, że opisywany w tym artykule rozproszony SSWiN obejmuje wiele autonomicznych podsystemów (central od C-1 do C-7) o dużej złożoności, musi on być poddawany okresowym przeglądom i obsłudze serwisowej dla zapewnienia wysokiego poziomu gotowości. Obsługa

BEZPRZEWODOWY SYSTEM ALARMOWY Z KOMUNIKACJĄ DWUKIERUNKOWĄ

WL 31

2 dodatkowe wejścia
w każdym czujniku magnetycznym

32 czujki bezprzewodowe
4 strefy
8 pilotów
4 sygnalizatory zew. w pełni bezprzewodowe
18 kodów użytkowników
wbudowany sygnalizator wewnętrzny
dialer GSM

opatentowana przez ELKRON technologia REPLAY dwukierunkowej komunikacji

system całkowicie bezprzewodowy, nie wymaga zasilania zewnętrznego i może być stosowany tam gdzie sieć elektryczna nie jest dostępna

8 kanałów komunikacji w paśmie 433,050 Mhz - 434,790 Mhz
system działa jednocześnie na 2 kanałach (automatycznie wybranych)

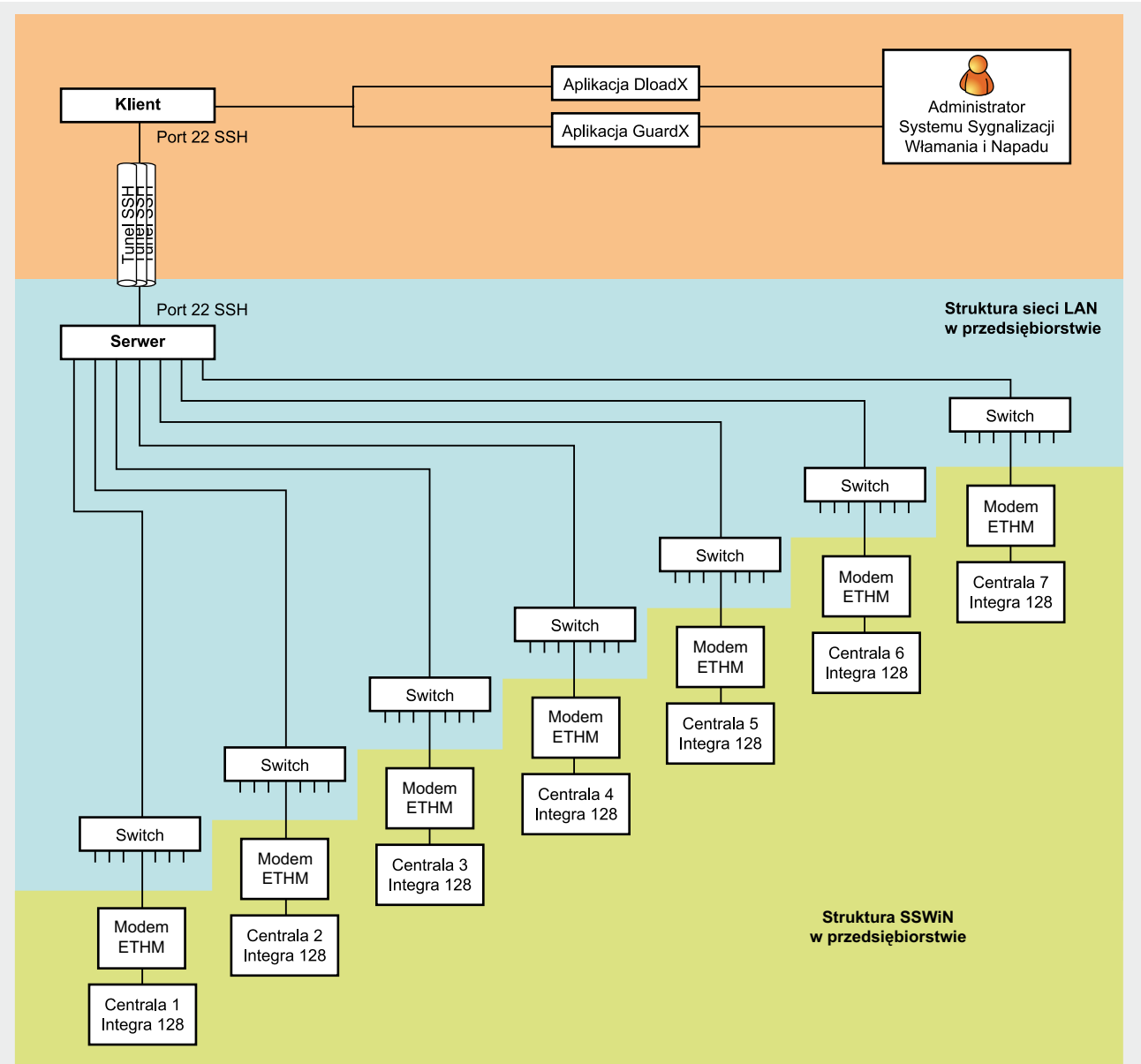
ciągłe nadzorowanie urządzeń i wykrywanie prób zagłuszania sygnału radiowego

zasięg w otwartej przestrzeni do 500m dla czujek, klawiatur i sygnalizatorów, do 200m dla pilotów

ELKRON

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



Rys. 3. Przykład połączenia „Administratora Systemu" z centralami INTEGRA 128 przez sieć LAN z wykorzystaniem protokołu SSH (Secure Shell)

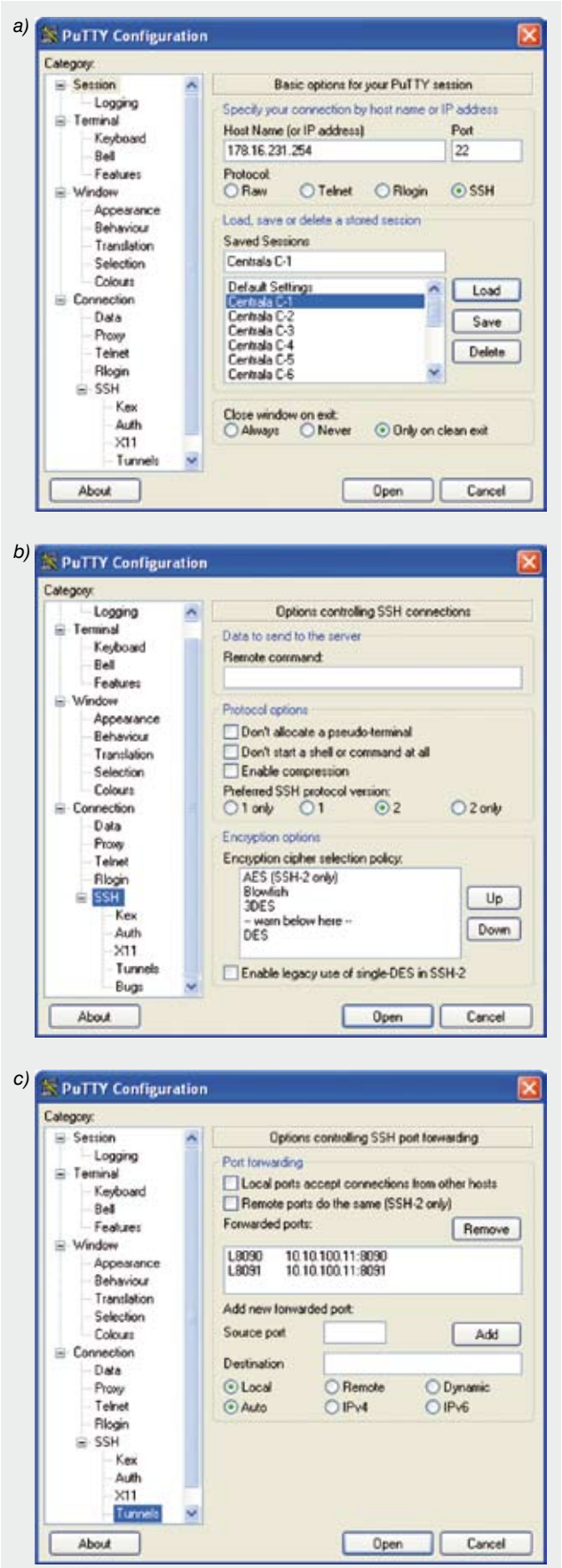
serwisowa takiego systemu wymaga od serwisantów sporo wysiłku i czasu. Serwisant musi podłączyć komputer do każdego podsystemu w celu dokonania podstawowego przeglądu serwisowego.

Dlatego też SSWiN składający się z siedmiu podsystemów wykorzystujących jednostki centralne INTEGRA 128 wyposażono w moduły ETHM-1, które umożliwiają obsługę serwisową oraz nadzór i administrację przez LAN lub przez Internet.

W celu nawiązania połączenia z wykorzystaniem algorytmu AES (Rijndael) informacje są przesyłane przez niezabezpieczoną sieć Internet do modułu ETHM-1. Na rys. 2 przedstawiono przykład połączenia „Administratora Systemu" z centralą alarmową INTEGRA 128 przez taką sieć.

Chcąc wprowadzić alternatywne zabezpieczenia przed dostępem osób nieuprawnionych do nadzorowanego i zarządzanego zdalnie SSWiN poprzez sieć LAN przedsiębiorstwa, zastosowano dodatkowe środki bezpieczeństwa na poziomie połączenia administratora systemu (klienta) z poszczególnymi podsystemami rozproszonego SSWiN.

Dodatkowym w stosunku do oryginalnych zabezpieczeniem w kwestii zagrożenia podsłuchem (*sniffing*) jest zastosowanie tunelu (*tunelling*) z wykorzystaniem programu SSH (*Secure Shell*). Na rys. 3 przedstawiono przykład połączenia „Administratora Systemu" z centralami alarmowymi INTEGRA 128 przez sieć LAN z wykorzystaniem SSH. Jest to dość proste, a zarazem skuteczne rozwiązanie. Cała operacja polega na utworzeniu szyfrowanego połączenia tam, gdzie sieć jest najbardziej narażona na atak, czyli wtedy, gdy dane są przesyłane przez sieć (np. Internet), której nie można kontrolować. Programy służące do nadzoru, serwisu i administracji, zamiast połączyć się ze zdalnym serwerem, np. przez Internet (przez port 80), łączą się z lokalnym komputerem (klientem), wykorzystując port (najczęściej 22), na którym czuwa SSH. Na tym odcinku połączenia dane są przesyłane w sposób jawny, lecz nie może być tutaj mowy o podsłuchiwaniu. Natomiast połączenie



Rys. 4. Okna konfiguracyjne programu PuTTY

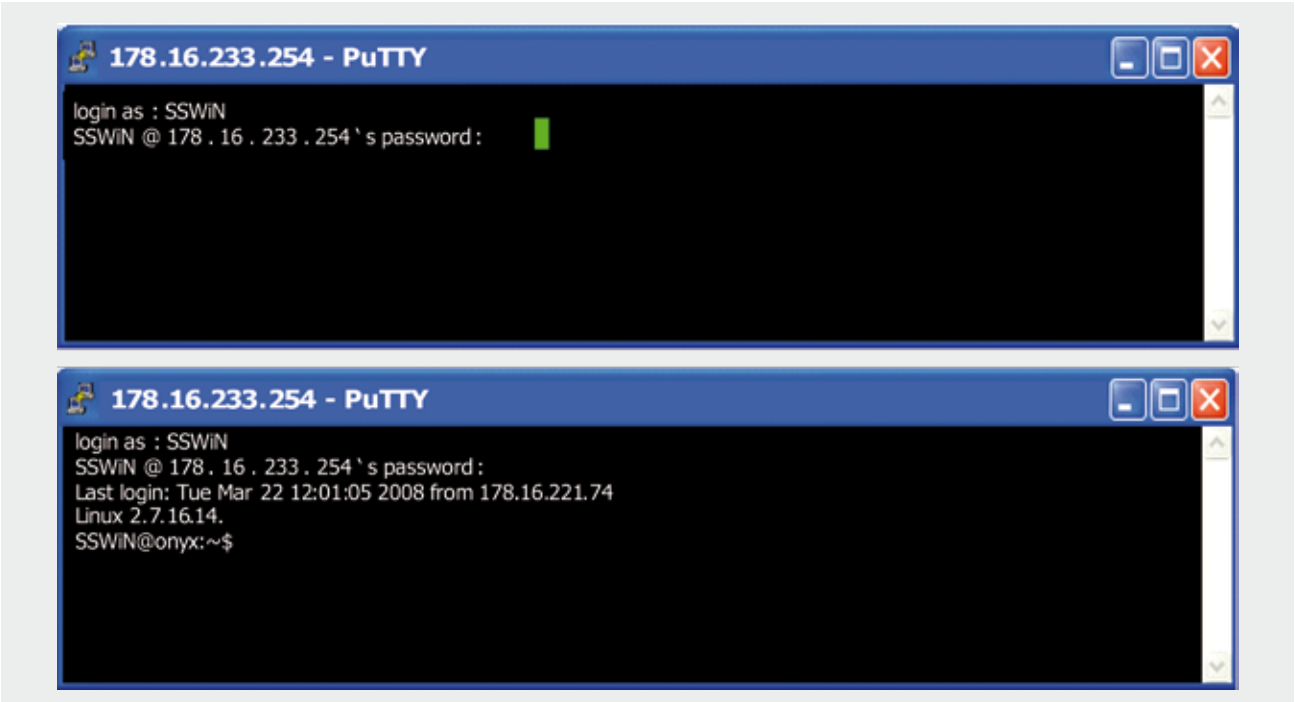
klient – serwer jest już szyfrowane. SSH na serwerze, z którym jesteśmy połączeni, przekazuje dane do właściwego portu na tym właśnie serwerze, dalej przez ściśle określone porty elementów sieci LAN przedsiębiorstwa do modułów ethernetowych podsystemów SSWiN. Na tym odcinku dane nie są kodowane, lecz jeśli korzystamy z danej usługi na serwerze, z którym łączymy się właśnie poprzez tunel z wykorzystaniem SSH, możemy czuć się bezpieczni.

Zasada działania protokołu SSH opiera się na kryptograficznej technologii RSA (nazwa RSA jest akronimem utworzonym z pierwszych liter nazwisk jego twórców). Każdy z komputerów, na których zainstalowane jest oprogramowanie SSH, posiada parę kluczy: tzw. klucz prywatny, dostępny tylko dla administratora komputera (i oczywiście oprogramowania systemowego obsługującego protokół SSH), oraz klucz publiczny, dostępny dla wszystkich użytkowników sieci. Klucze te są tak zbudowane, że informację zaszyfrowaną kluczem prywatnym można rozszyfrować tylko przy pomocy klucza publicznego i odwrotnie – informację zaszyfrowaną kluczem publicznym można rozszyfrować wyłącznie przy pomocy klucza prywatnego. Klucze są więc ze sobą powiązane, ale żadnego z nich nie można odtworzyć na podstawie znajomości drugiego. Połączenie SSH inicjowane jest po stronie programu – klienta SSH. Klient łączy się z serwerem i otrzymuje od niego jego klucz publiczny. Klucz ten porównywany jest z zachowanym w wewnętrznej bazie danych klienta, z poprzednich połączeń. Następnie klient przekazuje serwerowi swój klucz publiczny, generuje losową 256-bitową liczbę, szyfruje ją przy pomocy swojego klucza prywatnego oraz klucza publicznego serwera. Serwer po otrzymaniu tak zakodowanej liczby rozszyfrowuje ją przy pomocy swojego klucza prywatnego i klucza publicznego klienta. Tak otrzymana liczba jest losowa, a ponadto znana tylko klientowi i serwerowi. Jest ona używana jako klucz do kodowania podczas dalszej komunikacji.

W opisywanym przypadku do szyfrowanego połączenia wykorzystano program PuTTY, który jest darmowym emulatorem terminala dla systemów MS Windows, obsługującym protokoły TELNET oraz SSH w wersji 1 oraz 2. Program nie wymaga instalacji, wystarczy umieścić go w wybranym katalogu i utworzyć do niego skrót w Menu Start lub na pulpicie systemu Windows.

W celu konfiguracji sesji SSH wybiera się pozycję menu „*Session*”, następnie wprowadza adres serwera, np. 178.16.231.254. Automatycznie zostanie wybrany port 22. Przedstawiono ten stan na rys. 4a, na którym odbierane są przez serwer żądania otwarcia sesji SSH. Następnie zaznacza się protokół „SSH”. Ten stan interpretuje rys. 4b. Następnie tworzy się tunel (*tunnels*). Ten stan interpretuje rys. 4c. W małym okienku umieszczonym pod napisem „*Saved Sessions*” wprowadza się i zapisuje nazwę sesji, np. „Centrala C-1”. Ten stan przedstawiono na rys. 4a. Ponieważ opisywany SSWiN składa się z siedmiu autonomicznych podsystemów (centrale od C-1 do C-7), dla każdego podsystemu tworzy się odrębną sesję.

Po otwarciu odpowiedniej sesji i wpisaniu hasła (co zostało przedstawione na rys. 5) zostaje uruchomiony kanał SSH, przez który można bezpiecznie używać aplikacji do nadzoru, administracji i zarządzania centralami INTEGRA (GuardX i DloadX).



Rys. 5. Okna terminala PuTTY (zrzut z ekranu)

Zakończenie i wnioski

Zaproponowany i zrealizowany przez autorów SSWiN dla potrzeb rozległego obiektu wraz z jego systemem zarządzania i administrowania to dosyć trudne wyzwanie, szczególnie z punktu widzenia eksploatacyjno-niezawodnościowego. Problematyka dotycząca rozproszonych systemów bezpieczeństwa wraz z matematyczną analizą eksploatacyjno-niezawodnościową była przez autorów (dra inż. Waldemara Szulca i dra inż. Adama Rosińskiego) poruszana w *Zabezpieczeniach* Nr 1(47) w 2006 r.

Jest to problem skomplikowany i wymagający długofalowych badań. Brak jest aktualnie danych dotyczących powyższego SSWiN w aspekcie eksploatacyjno-niezawodnościowym, a to ze względu na to, że system został oddany do eksploatacji w styczniu 2008 roku. Dane są zbierane cały czas i z całą pewnością zostanie obliczony tzw. wskaźnik gotowości K_G, ale po co najmniej 12 miesiącach użytkowania. Trwają prace nad budową modelu eksploatacyjno-niezawodnościowego tego bardzo skomplikowanego systemu bezpieczeństwa. Dodatkowym utrudnieniem jest zaproponowany system nadzoru i administrowania SSWiN poprzez lokalne sieci ethernetowe. Nasuwają się także bardzo ostrożne wnioski:

- konfigurację tak skomplikowanych systemów bezpieczeństwa należy ustalać po bardzo szczegółowej analizie rozległego obiektu, z uwzględnieniem wymogów logistycznych oraz niezawodnościowych i eksploatacyjnych,
- zaproponowany SSWiN wymagał bardzo starannej instalacji z uwzględnieniem konieczności zachowania kompatybilności elektromagnetycznej oraz przemyślanej lokalizacji central oraz modułów,
- niezmiernie istotną sprawą przy tak dużym i rozproszonym SSWiN jest dobór zasilania, zarówno zasadniczego, jak i rezerwowego (wynikającego z bilansu energetycznego),
- nowatorski system nadzoru i administrowania rozproszonego systemu bezpieczeństwa wraz z zabezpieczeniem danych (podany powyżej) należy do bardzo trudnych i skomplikowanych procedur informatycznych,
- powinna być wykonana staranna dokumentacja do przyszłych procedur serwisowych, zarówno opisowa, jak i rysunkowa.

Bibliografia

1. Cole E., Krutz R. L., Conley J., *Bezpieczeństwo sieci. Biblia*, Helion, Gliwice 2005.
2. Dostálek L., *Bezpieczeństwo protokołu TCP/IP*, seria: *(Nie) bezpieczeństwo*, Wydawnictwo Naukowe PWN 2006.
3. Haykin S., *Systemy telekomunikacyjne*, t. 1 i 2. Wydawnictwa Komunikacji i Łączności
4. Instrukcje i materiały firmy Satel.
5. Kaeo M., *Tworzenie bezpiecznych sieci*, Mikom, Warszawa 2000.
6. Karbowski M., *Podstawy kryptografii*, wydanie II, Helion, Gliwice 2007.
7. Szulc W., Szmigiel A., prace własne, *Elektroniczne Systemy Bezpieczeństwa*, PW, Wydz. Transportu, Warszawa 2008.
8. www.bezpieczenstwo-sieci.pl, 2008.
9. www.satel.pl, 2008.

doc. dr inż. Waldemar Szulc
WSM Wydz. Informatyki Stosowanej,
Zakład Bezpieczeństwa Obiektów i Informacji,
współpracownik PW – Wydział Transportu,
Zakład Telekomunikacji w Transporcie,
współpracownik WAT – Wydział Elektroniki
inż. Andrzej Szmigiel
PW, Wydział Transportu,
Zakład Telekomunikacji w Transporcie

SZKOŁA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ
TECHOM w WARSZAWIE
inż. Bogdana Tatarowskiego

Zezwolenie Kuratorium Oświaty
i Wychowania w Warszawie nr 663/K/95

zaprasza na

KURSY ZAWODOWE

w zakresie

- **Instalowania, konserwacji i eksploatacji systemów alarmowych**
  Dla przyszłych wykonawców prac instalatorskich i konserwacyjnych oraz dla użytkowników systemów, inwestorów i administratorów obiektów chronionych
- **Projektowania systemów alarmowych w klasach od SA-1 do SA-4**
  Dla obiektów cywilnych i wojskowych oraz obiektów z tzw. „listy wojewody"
- **Zarządzania bezpieczeństwem obiektu**
  Bezpieczeństwo teleinformatyczne
  Wymogi Prawne i normatywne
- **Rzeczoznawstwa**
  – Systemy Technicznego Zabezpieczenia Osób i Mienia
  – Zarządzania Bezpieczeństwem Obiektu

Autoryzacja absolwentów kursów
Dla potrzeb inwestorów
i towarzystw ubezpieczeniowych

Informacja oraz przyjmowanie zgłoszeń:

TECHOM

ul. Marszałkowska 60/27
00-545 Warszawa
tel. 022 625 34 00, 022 625 32 96
tel./faks 022 625 26 75
e-mail: techom@techom.pl
www.techom.com

Nowoczesne technologie w detektorach firmy RISCO Group

Podczas instalacji systemu sygnalizacji włamania użytkownik zwraca zwykle uwagę na centralę alarmową (lub jej klawiaturę), utożsamiając skuteczność systemu z jej możliwościami. Jest to podejście słuszne, ponieważ właśnie klawiatura stanowi interfejs pomiędzy użytkownikiem a systemem ochrony. Niestety dość często rozbudowana funkcjonalność centrali alarmowej nie jest wystarczającym czynnikiem, aby uznać cały system za skuteczny. Nie należy zapominać, że system jest tak skuteczny, jak skuteczne są użyte w nim technologie detekcji. Poniżej przedstawiamy zbiór nowoczesnych technologii, które w ostatnich latach wprowadzone zostały do produktów firmy RISCO Group

Rys. 1. Detektor iWise z opcją Zielona Linia i technologią Anti-Cloak

Rys. 2. Bezprzewodowy detektor iWise odporny na ruch zwierząt

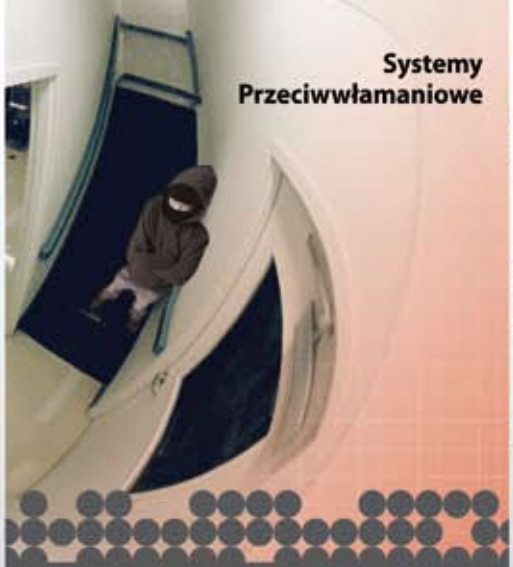
Technologia Rozpoznawania Kołysania (*Sway Recognition Technology*) rozpoznaje i odrzuca (ignoruje) obiekty, które poruszają się powtarzalnym ruchem wahadłowym na tej samej drodze. Dotyczy to np. kołyszących się gałęzi drzew lub ruchomych części maszyn. Dwa kanały mikrofalowe są w stanie rozróżnić ruch do przodu i do tyłu, a odejmując uzyskane współczynniki zmierzyć przebyty przez obiekt dystans. Elementy poruszające się w sposób powtarzalny na zdefiniowanym dystansie nie są traktowane jako wtargnięcie intruza.
Zastosowanie: detekcja mikrofalowa w WatchOUT (detektorze zewnętrznym) oraz WatchIN (detektorze przemysłowym)

Technologia Cyfrowej Korelacji (*Digital Correlation Technology*) zapewnia, że tylko te obiekty, które wywołają podobny i skorelowany sygnał z dwóch kanałów PIR są brane pod uwagę jako potencjalne zagrożenie. Dwa niezależne kanały PIR z oddzielnymi soczewkami tworzą w płaszczyźnie pionowej odpowiednią strefę detekcji, która jest odporna na ruch zwierząt. Małe zwierzęta, z uwagi na swoje rozmiary, nie mogą być w obu strefach detekcji jednocześnie. W nieprzewidywalnym środowisku zewnętrznym różne zdarzenia, takie jak ruch gałęzi w jednym kanale PIR oraz ruch zwierzęcia w drugim, stworzą sygnał nieskorelowany, który zostanie właściwie zinterpretowany, a następnie zignorowany.
Zastosowanie: detekcja PIR w WatchOUT (detektorze zewnętrznym)

Technologia Detekcji Intruza Pod Przykryciem (*Anti-Cloak Technology – ACT*) wykorzystuje zalety technologii dualnej przy jednoczesnym uniknięciu jej niedociągnięć. Kanał PIR w detektorach dualnych posiada dwie główne słabości:

- intruz może ukryć się za osłoną z materiału, która blokuje promieniowanie IR i detektor nie jest w stanie tego intruza zauważyć,
- czułość detektora ulega znacznej redukcji, gdy temperatura otoczenia jest zbliżona do temperatury ciała intruza.

ACT zapewnia wysoką skuteczność detekcji poprzez przełączenie się czujki w tryb pracy jedynie z kanałem mikrofalowym w przypadku wzrostu poziomu temperatury otoczenia do wartości bliskiej temperaturze ciała intruza lub gdy wykryto intruza pod przykryciem.
Zastosowanie: detekcja mikrofalowa w WatchIN (detektorze przemysłowym), Industrial LuNAR, LuNAR DT, iWISE DT



MaxiTalk

Obsługuje do 22000 użytkowników i 4000 drzwi

Maxi.Net

Zarządzanie Systemem Kontroli poprzez internet

MaxiMate

Łatwy, szybki i przyjazny System Kontroli Dostępu do 8700 użytkowników i 16 drzwi

ProSYS™

Zintegrowane Systemy Bezpieczeństwa

Agility™

Elastyczne rozwiązanie bezprzewodowe z komunikacją dwustronną

WisDom™

Bezprzewodowe Systemy Bezpieczeństwa

WatchOUT™

niezawodny Detektor Zewnętrzny

WatchIN™

Przemysłowy Detektor Grade 3

SynopSYS™

System Zarządzania Bezpieczeństwem i Automatyką budynków rozproszonych

- to oprogramowanie do zdalnego zarządzania automatyką budynków rozproszonych
- łączy bezpieczeństwo i automatykę budynków w jedno rozwiązanie
- elastyczny w implementacji indywidualnych projektów

RISCO GROUP

Creating Security Solutions. With Care

riscogroup.com

RISCO Group Poland Tel: +48 22 500 28 40, Fax +48 22 500 28 41, email: Poland@riscogroup.com

Cyfrowa Obróbka Sygnału (*Intelligent Digital Signal Processing*). Największym wyzwaniem dla producentów detektorów PIR jest wybór progu działania urządzeń. Jeżeli próg jest ustawiony za nisko, detektor będzie podatny na fałszywe alarmy. Wysoki próg może oznaczać zbyt małą czułość. Technologia DSP zapewnia dynamiczną adaptację progu działania, w czasie rzeczywistym, do prędkości przemieszczania się intruza.
Zastosowanie: detekcja PIR w WatchOUT, WatchIN, Industrial LuNAR, LuNAR DT, iWISE, Digi-Sense oraz w detektorach PIR systemu bezprzewodowego

Dynamiczny próg przy ruchu zwierząt (*Variable Pet Treshold – VPT*) VPT to unikatowy algorytm, który w połączeniu z odpowiednią soczewką pozwala detektorowi na łatwe rozróżnianie pomiędzy intruzem a ruchem zwierząt przy zachowaniu maksymalnej skuteczności działania detektora.

Poziom sygnału na wyjściu piroelementu zależy między innymi od szybkości przemieszczania się obiektu w polu detekcji. Intruz poruszający się z dużą prędkością spowoduje w efekcie niski poziom sygnału, natomiast zwierzę poruszające się wolno wygeneruje wyższy poziom sygnału. Jeżeli próg działania detektora byłby stały, to alarm spowodowałoby zwierzę, natomiast intruz zostałby zignorowany.

VPT rozwiązuje ten problem poprzez pomiar prędkości i wybór właściwego progu działania. Próg ten jest ustawiony powyżej poziomu sygnału uzyskanego przy ruchu zwierząt oraz poniżej poziomu sygnału uzyskanego przy ruchu intruza w całym zakresie prędkości.
Zastosowanie: detekcja PIR w WatchOUT, iWISE Pet, iWISE DT Pet oraz w detektorach PIR (wersja Pet) systemu bezprzewodowego, Zodiac DT Pet, Zodiac Digital Pet

Podsumowanie

Producenci nie ograniczają się do pojedynczej technologii. Zaczęto implementować w jednym produkcie po kilka z nich, aby zwiększyć skuteczność działania detektora. Nie zapomniano o ochronie detektora przed próbami maskowania. Wiele wspomnianych wyżej detektorów wyposażono w systemy **antymaskingu**, wykorzystujące aktywne kanały podczerwieni. Dodatkowo wprowadzono funkcję „Zanieczyszczona soczewka" (np. w WatchOUT), informującą użytkownika o takim stanie.

Ochrona środowiska także zaznacza swój wpływ na konstruowane urządzenia. Przejawem tego są produkty z serii **Zielona Linia** (*Green Line*), będące odpowiedzią na wzrost zagrożeń dla ludzi ze względu na środowisko. Technologia ta ma zapobiegać dodatkowej emisji promieniowania w obiektach, w których przebywają ludzie. Detektory wyposażone w to rozwiązanie dezaktywują promienniki mikrofalowe w momencie, gdy system alarmowy jest wyłączony (rozbrojony).

Należy stale mieć na uwadze, że wymagania użytkowników, warunki środowiskowe itp. ciągle się zmieniają. Dostosowanie możliwości detektorów do tych wymagań to główny cel RISCO Group. Aby go osiągnąć, a przy tym zachować parametry dozorowe, takie jak szybkie i pewne wykrycie intruza, lista stosowanych technologii stale się rozszerza.

Aby być bliżej klientów, firma RISCO Group otworzyła biuro w Polsce.

Rys. 3. Detektor LuNAR z opcją Zielona Linia i technologią Anti-Cloak

Rys. 4. Detektor WatchOUT z kamerą

Więcej informacji można znaleźć na stronie: *www.risco-group.com*.

Biuro w Warszawie
ul. 17 Stycznia 56, 02–146 Warszawa
tel.: (22) 500 28 40
faks: (22) 500 28 41

...znajdziesz nas również w sieci
www.zabezpieczenia.com.pl

Nowa seria czujek OPTiMAL

Spośród nowości produktowych zaprezentowanych na targach IFSEC 2008 wyróżniła się oferta firmy Optex. Jak przystało na wiodącą firmę produkującą urządzenia do wykrywania obecności intruza, Optex zaprezentował nowe produkty w szerokim spektrum zastosowań – dwie linie czujek zewnętrznych oraz linię czujek wewnętrznych OPTiMAL

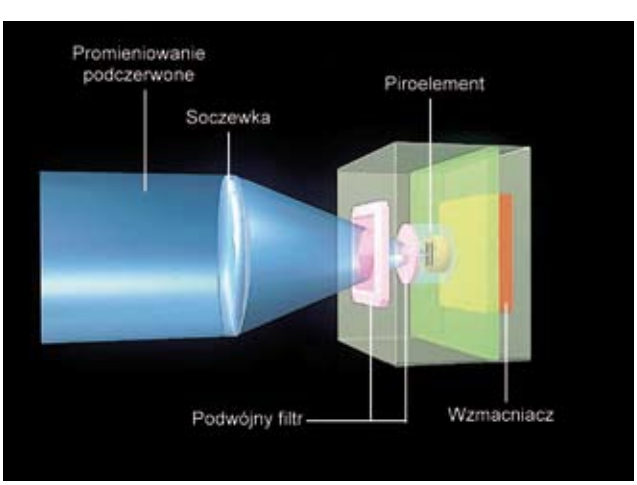
Czujki OPTiMAL to urządzenia adresowane do klientów o wysokich wymaganiach estetycznych. Wszystkie czujki serii, pomimo różnic funkcjonalnych, wyglądają jednakowo. Taka unifikacja jest niezwykle istotna dla wyglądu wnętrz, niezależnie bowiem od wymaganej funkcjonalności czujek, wynikającej np. ze stopnia ochrony instalacji alarmowej, zastosowane czujki będą wyglądały jednakowo. Jednocześnie, projektowane zgodnie z wymaganiami normy EN50131, spełniają wysokie standardy ochrony na poziomie klas 2 i 3 (odpowiedniki polskich klas C i S).

Seria czujek ruchu składa się z następujących produktów:
OML-ST – pasywna czujka podczerwieni (PCP) klasy C (EN: klasa 2)
OML-AM – PCP klasy S z funkcją antymaskingu (EN: klasa 3)
OML-DT – PCP i czujka mikrofalowa klasy C (EN: klasa 2)
OML-DAM – PCP i czujka mikrofalowa klasy S z funkcją antymaskingu (EN: klasa 3)

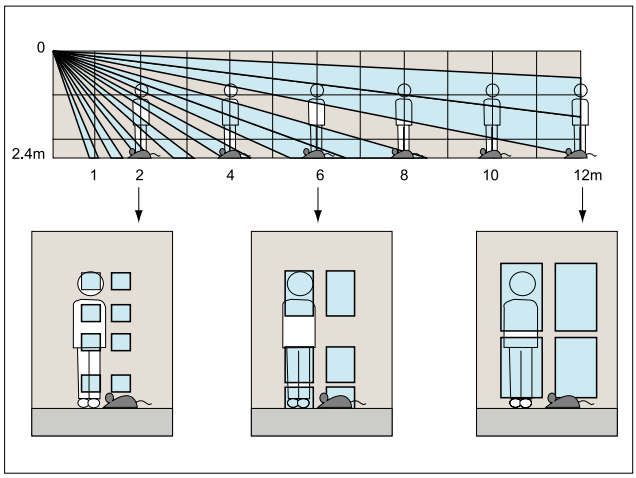
Seria czujek OPTiMAL bazuje na wieloletnim doświadczeniu rynkowym związanym z produktami serii CX i DX. Światowy sukces tych urządzeń został potwierdzony sprzedażą tysięcy sztuk oraz faktem uznania tych produktów za standard zabezpieczeń przez organizacje finansowe o światowym zasięgu. Siłą rzeczy nowe urządzenia posiadają wiele cech charakterystycznych dla swoich poprzedników, w tym sprawdzone technologie poprawiające skuteczność detekcji i zapobiegające powstawaniu fałszywych alarmów. Uzupełnione o zdobycze nowych rozwiązań, czujki OPTiMAL oferują wysoki standard detekcji w najtrudniejszych nawet warunkach pracy. Poza tym nowe czujki zaprojektowane zostały zgodnie z wymaganiami norm europejskich, które znajdują coraz szersze rzesze zwolenników w wielu krajach Europy, w tym w Polsce. Rozszerzeniem gamy urządzeń firmy Optex przeznaczonym do instalacji o wysokich wymaganiach ochronności jest czujka dualna (PCP zintegrowana z czujką mikrofalową) z funkcją antymaskingu. Wypełnia ona swego rodzaju lukę w dotychczasowej ofercie firmy dla instalacji wysokiego ryzyka. Dotychczasowa oferta firmy Optex nie zawierała czujek dualnych PCP i mikrofalowych, które byłyby wyposażone w funkcję antymaskingu realizowaną przy użyciu technologii podczerwieni. Dotychczas w ofercie Optex w tym segmencie występowały wyłącznie czujki dualne PCP i mikrofalowe, realizujące funkcję ochrony przed sabotażem z wykorzystaniem technologii mikrofalowych (seria urządzeń DX).

Zastosowane technologie

Jak wszystkie czujki wewnętrzne firmy Optex, urządzenia serii OML są wyposażone w podwójne pyroelementy oraz posiadają wysokiej jakości wzmacniacze analogowe. W zakresie detekcji PCP są wzorowane na najlepszych rozwiązaniach, znanych z czujek serii CX. Tor optyczny został wyposażony w filtry światła białego (*Double Conductive Shielding*). Filtry wykonane w tej technologii skutecznie oddzielają promieniowanie podczerwone od innych źródeł promieniowania oraz pełnią rolę ekranu chroniącego przed zakłóceniami elektromagnetycznymi. Najważniejszym elementem toru optycznego jest soczewka. Precyzja wykonania, powtarzalność parametrów oraz dokładność pozycjonowania względem pyroelementu w gotowej czujce to kluczowe czynniki decydujące o jakości PCP. Detektory OML nie są wyjątkiem od reguły, według której czujki Optex to przykład pedantycznej wręcz dbałości o najdrobniejsze szczegóły układów optycznych. Soczewka zastosowana w czujkach OML to rozwiązanie znane z czujek serii CX-502, łączące w sobie zalety soczewki sferycznej (będąc wycinkiem kuli, zapewnia optymalny kąt przejścia promieniowania podczerwonego) i płaskiej (niewielkie rozmiary czujek). Projekt każdego



Rys. 1. Opatentowany filtr światła białego Double Conductive Shielding



Rys. 2. Technologia detekcji Quad-Zone Logic

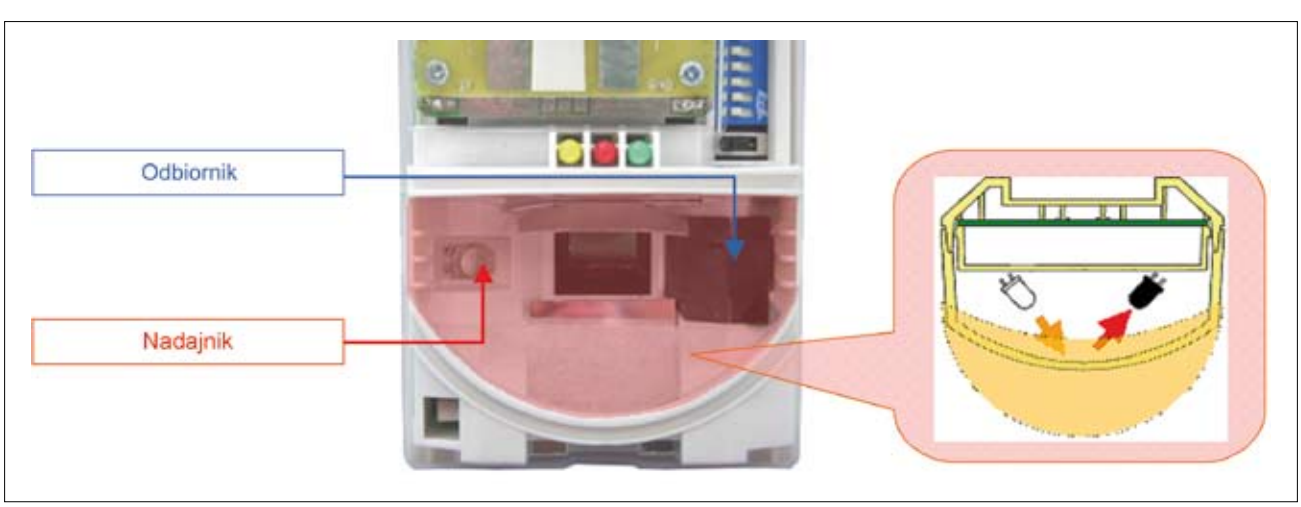
elementu soczewki jako osobnego wycinka i złożenie zaprojektowanych w ten sposób wycinków w jednolitą wypukłą powierzchnię (*Offset Spherical Lens*) powoduje, że uzyskana w ten sposób spłaszczona soczewka umożliwia konstrukcję czujek o niewielkich rozmiarach.

Zastosowanie technologii segmentacji pola widzenia czujki (*Quad Zone Logic*) pozwala wykorzystać efekt zwielokrotnienia sygnału docierającego do pyroelementu. Dzięki tej technologii obiekty duże (wielkości człowieka) generują kilkukrotnie większy sygnał użyteczny niż obiekty małe (zwierzęta domowe). Niezwykle istotne jest to, że zwielokrotnienie sygnału realizowane jest w torze optycznym, więc nie ma wpływu na poziom szumów pochodzących ze wzmacniaczy. Rozwiązania znane ze swojej skuteczności w poprzednich modelach uzupełnione zostały o nowe rozwiązania, zwiększające szansę wykrycia intruza. Należy do nich strefa czułości chroniąca przestrzeń tuż pod czujką (*Look Down Zone*), stanowiąca dopełnienie ochrony przed przeczołganiem i funkcji antymaskingu w systemie detekcji intruza w przypadku czujek o wysokim poziomie ochrony.

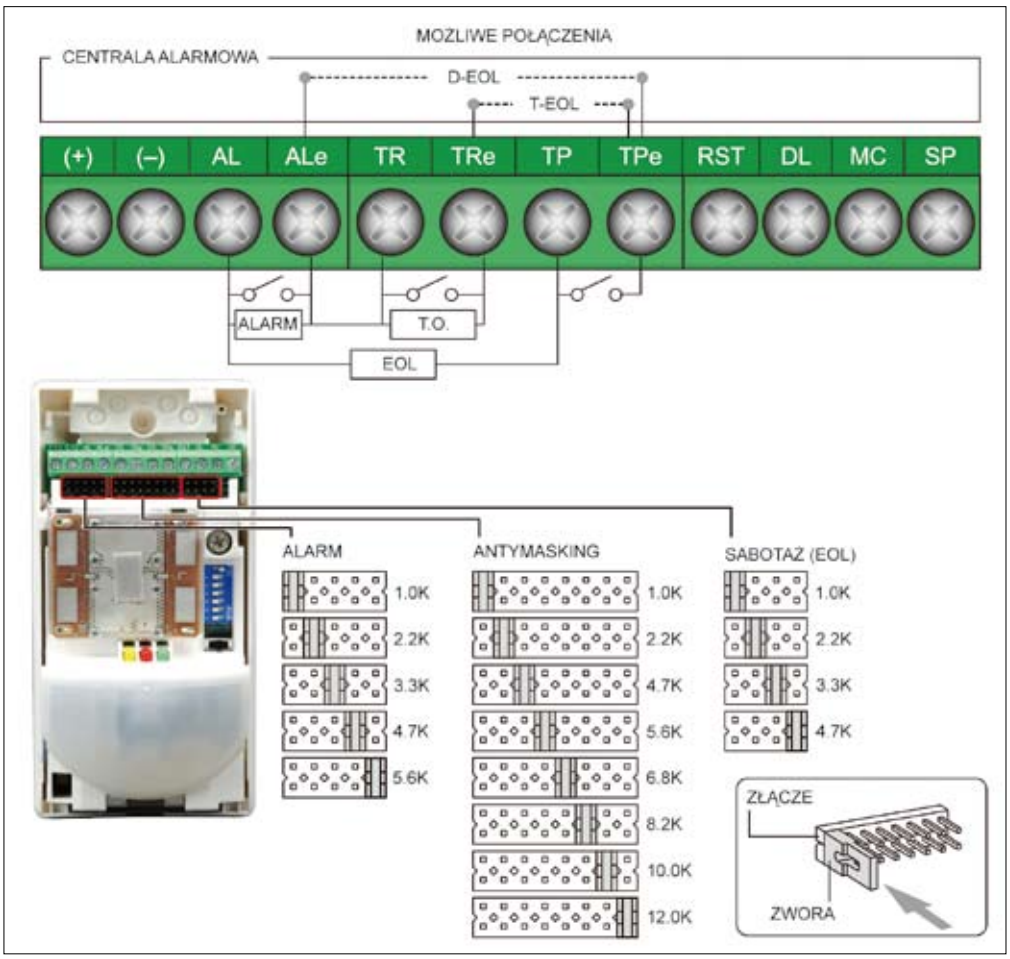
Tor mikrofalowy czujek OML wzorowany jest na rozwiązaniach czujek serii DX. Te mało znane na polskim rynku czujki są elitą rozwiązań w tym segmencie urządzeń alarmowych. Ze względu na istotną różnicę pomiędzy falami nanometrowymi a mikrometrowymi wykorzystanie ich w jednym urządzeniu nie jest zagadnieniem trywialnym. Promieniowanie podczerwone blokowane jest przez każdą napotkaną przeszkodę, natomiast mikrofalowe przechodzi przez niemal wszystkie materiały o niskiej gęstości. W typowym otoczeniu biurowym mamy więc często do czynienia z wykrywaniem ruchu obiektów lub materii poza chronionym pomieszczeniem, co może skutkować niestabilną pracą czujek, a więc fałszywymi alarmami. Zbytnie ograniczenie czułości toru mikrofalowego prowadzi do sytuacji, w której intruz nie zostanie wykryty ze względu na nadmierne ograniczenie pola działania mikrofal. Dlatego niezwykle istotna z punktu widzenia instalatora i użytkownika końcowego jest możliwość precyzyjnego dostrojenia pola detekcji czujki dualnej tak, aby pola detekcji obu torów pokrywały się. Czujki OML wyposażono w znaną z czujek DX technologię, pozwalającą na niezwykle precyzyjne dostrojenie czułości toru mikrofalowego (*Microwave Area Shaping Technology*). Trzy poziomy czułości zostały uzupełnione o możliwość płynnego dostrajania czułości urządzenia, tak aby nawet najbardziej skomplikowany wariant regulacji mógł zostać zrealizowany.

Z uwagi na fakt, że fale mikrofalowe nie są obojętne dla zdrowia, uzupełniono funkcjonalność czujek OML o możliwość wyłączania toru mikrofalowego na czas rozbrojenia systemu (*Microwave Control Switch*). Czujnik został wyposażony w odpowiednie wejście informacyjne, sterujące działaniem toru mikrofalowego. Po aktywacji funkcji odpowiednim przełącznikiem czujka wyłącza tor mikrofalowy i działa wykorzystując wyłącznie tor PCP. Nie ma więc ryzyka zupełnego wyłączenia czujki przez nieodpowiednie wysterowanie tej funkcji.

Czujki klasy S (EN: klasa 3) to przede wszystkim zdolność detektora do wykrycia próby wyłączenia lub ograniczenia zdolności detekcji intruza. W tym zakresie najważniejsze znaczenie ma funkcja antymaskingu, która ma umożliwić sygnalizację przypadkowego zasłonięcia czujki, np. w wyniku zmian konfiguracji umeblowania pomieszczenia, lub – co bardziej istotne – sygnalizować próbę celowego jej zasłonięcia (np. zaklejenia lub zamalowania soczewki). Realizacja tej funkcji w czujnikach OML jest wzorowana na rozwiązaniach znanych z czujki CX-502AMplus, w której funkcja antymaskingu realizowana jest przez wykorzystanie promieniowania podczerwonego. Unikatowy układ antymaskingu (*Spherical Lens Protection*) składa się z elementu emitującego promienie podczerwone oraz z elementu światłoczułego (obydwa



Rys. 3. Elementy układu realizującego funkcję antymaskingu (Spherical Lens Protection)



Rys. 4. Sposób doboru rezystorów parametryzujących

elementy umieszczone są za soczewką). Funkcjonowanie tego układu bazuje na odbiciu promieniowania podczerwonego od ewentualnych przeszkód znajdujących się przed czujką. Osiągnięcie pewnego poziomu promieniowania na elemencie światłoczułym powoduje aktywację wyjścia T.O. (wyjście usterki – *Trouble Output*). Dzięki odpowiedniemu skalibrowaniu układu jest on w stanie wykrywać wszelkie próby maskowania, łącznie z przezroczystymi substancjami nanoszonymi na powierzchnię soczewki w formie sprayu, a także czarną zasłoną z papieru, umieszczoną w pewnej odległości od czujki. Zastosowanie najnowszych zdobyczy w dziedzinie algorytmów samonastrajalnych (*Digital Anti-Masking Technology*) umożliwiło adaptowanie się funkcji antymaskingu do zmiennych warunków otoczenia – poziomu promieniowania tła, zakresu temperatur pomieszczenia itd.

Jak przystało na serię czujek wysokiej klasy, zostały one wyposażone w rozwiązania wykluczające sabotaż styków wynikający z działania zewnętrznych pól magnetycznych (tzw. *Silent Relay*). Zastosowanie technologii optoelektronicznych i unipolarnych pozwoliło na uzyskanie izolacji elektromagnetycznej układów elektronicznych czujki od obwodów systemu alarmowego. Również obwody zasilania wyposażono w odpowiednie filtry i środki ochrony przeciwprzepięciowej. To nie wszystko. Wychodząc naprzeciw zapotrzebowaniu instalatorów pracujących z różnymi centralami alarmowymi, czujki OML zaopatrzono w zestaw rezystorów parametryzujących. Wielkości rezystancji włączanych w obwód alarmowy, sabotażowy i wyjścia antymaskingu zostały dobrane na podstawie wartości charakterystycznych dla najpopularniejszych central alarmowych i zapewniają współpracę z każdym typem centrali dostępnej na rynku w niemal każdej znanej konfiguracji. To znaczne ułatwienie pracy instalatora, który niejednokrotnie musiał dokonywać cudów zręczności, łącząc obwody w czujkach. W ramach uzupełnienia należy dodać, iż konstrukcja czujki umożliwia łatwe odłączenie bloku detektora wraz z zaciskami od obudowy, która stanowi jednocześnie podstawę montażową czujki. W ściance tylnej obudowy zintegrowano styk antysabotażowy, który aktywowany jest przy próbie oderwania czujki od podłoża. Nie bez znaczenia jest fakt, iż wszystkie czujki serii OML wyglądają jednakowo. Jest to nie tylko odpowiedź na rosnące wymagania estetyczne klientów, ale również na zagadnienie identyfikacji czujek alarmowych i oferowanych przez nie funkcji. Stosując czujki OML sprawimy, że potencjalny intruz nie będzie w stanie określić, z jakimi urządzeniami ma do czynienia: czy z czujkami PCP klasy C, czy z czujkami dualnymi z funkcją antymaskingu klasy S.

Podsumowanie

Kolejny raz firma Optex udowadnia, że jej pozycja lidera technologii detekcji intruza nie jest przypadkowa. Czujki OPTiMAL to optymalne rozwiązanie dla profesjonalnych instalacji w szerokim zakresie zastosowań. To również materialny dowód na ciągłe ulepszanie technologii detekcji oraz na szczególną uwagę projektantów firmy, jaką poświęcają oni walorom użytkowym i estetycznym swoich produktów. Komfort pracy instalatora oraz gusta estetyczne klienta końcowego będą miały w przyszłości rosnące znaczenie przy wyborze urządzeń alarmowych. Projektanci firmy Optex biorą to pod uwagę już dziś. Najpierw jednak oferowane rozwiązania detekcji intruza muszą osiągnąć właściwy poziom perfekcji. Firma Optex serią produktów OPTiMAL określa bardzo wysokie standardy w tym zakresie. To tylko jedna z nowości zaprezentowanych na targach IFSEC 2008. W następnym numerze ciąg dalszy.

Jarosław Gibas
Optex Security

Uniwersalny komunikator alarmowy GSM/GPRS GS3055

DSC

Przedstawiamy Państwu uniwersalny komunikator alarmowy GSM/GPRS, który może pracować jako podstawowy lub pomocniczy nadajnik alarmowy. Głównym zadaniem urządzenia jest wysyłanie wiadomości tekstowych SMS na zaprogramowane numery telefonów komórkowych, informując o zaistniałych alarmach w systemie. GS3055 ma także możliwość sterowania systemem alarmowym, poprzez wysyłanie odpowiednio zaprogramowanych wiadomości tekstowych na numer telefoniczny karty SIM umieszczonej w urządzeniu. Dzięki wyżej wymienionym funkcjom, nadajnik GS3055 idealnie nadaje się do montażu w domach jednorodzinnych, biurach, jak i mieszkaniach.

GS3055 kompatybilny jest z każdą centralą alarmową obsługującą format Contact ID. Nadajnik łączy dialer centrali alarmowej z siecią GSM i wysyła kody raportujące bezpośrednio do stacji monitorowania wyposażonej w odbiorniki Sur-Gard SYSTEM II/III.
Urządzenie GS3055 pracując jako pomocniczy komunikator alarmowy, wysyła wszystkie informacje za pośrednictwem linii naziemnej PSTN, a w przypadku usterki przełącza się automatycznie na sieć GSM, powiadamiając stację monitorowania.
Dla użytkowników, którzy nie posiadają na swoich obiektach linii naziemnej PSTN, nadajnik GS3055 może zostać użyty jako podstawowy komunikator.

Cechy urządzenia

- możliwość wysyłania wiadomości tekstowych SMS informujących o zdarzeniach w systemie na zaprogramowane numery telefonów komórkowych;
- 4 wyjścia OC na płycie;
- 4 wejścia na płycie;
- kompatybilny z każdą centralą alarmową obsługującą format Contact ID;
- raportowanie wszystkich zdarzeń zaistniałych w systemie;
- tania, szybka oraz skuteczna transmisja alarmu poprzez GPRS do odbiornika IP;
- kompatybilny z odbiornikami Sur-Gard SYSTEM II/III.

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

PROJEKTANT A WYKONAWCA

Wobecnie realizowanych inwestycjach projekty przetargowe (wykonawcze) dla poszczególnych branż występują jako części projektu budowlanego, złożonego w celu uzyskania pozwolenia na budowę. Opisują one w dużej mierze zarysy poszczególnych systemów. Po uzyskaniu pozwolenia na budowę, w trakcie przygotowania prac sporządzane są szczegółowe techniczne projekty wykonawcze. Przyjęte są dwa sposoby działania: projekt wykonawczy przygotowywany jest przez zewnętrzną firmę nie wykonującą instalacji albo przygotowuje go wykonawca instalacji.

W wielu przypadkach wykonawca, przyjmując do wykonania instalację, otrzymuje już gotowy techniczny projekt wykonawczy systemu. Najlepsza jest sytuacja, w której istnieje stały kontakt z projektantem. W takim przypadku można na bieżąco uzyskać informacje uzupełniające, czy też uzgodnić i wprowadzić ewentualne zmiany do projektu.

Przy stałej współpracy projektanta z wykonawcą wszelkie nieprzewidziane zmiany – przykładowo: zmiany tras kablowych z uwagi na brak możliwości instalacyjnych, czy też zmiany urządzeń – można wprowadzić bardzo szybko, ograniczając znacznie koszty wykonania i uzgadniania. Należy pamiętać, że w przypadku realizacji dużych inwestycji, gdy tempo zmian aranżacyjnych wprowadzanych przez architektów lub projektantów branżowych wymusza zmiany, wszelkie opóźnienia mogą skutkować poważnymi konsekwencjami finansowymi dla wykonawcy.

W większości przypadków etap projektowania rozpoczyna się, zanim zostanie wbita przysłowiowa pierwsza łopata w ziemię na terenie budowy inwestycji. Z rysunków architektonicznych nie wszystko da się odczytać. Rysunki powiązanych branż są na etapie bardzo ogólnych koncepcji. Na tym etapie informacje w nich zawarte mogą być obarczone błędnymi danymi, a wtedy wykonanie instalacji może być niemożliwe. Czasami projekt jest na tym etapie zamykany i przekazywany do wykonania. Wykonawca, otrzymawszy niepełną dokumentację, pozostawiony samemu sobie, bez kontaktu z projektantem, będzie miał duże trudności z realizacją swojego zakresu prac. W wielu systemach takie rozwiązania mogą być wystarczające, np. w systemach kontroli dostępu, gdzie można łatwo wytypować przejścia, które należy objąć ochroną, a zwiększenie ich liczby nie pociąga za sobą, przy obecnie stosowanych rozwiązaniach, większych trudności. Inaczej jest w przypadku systemów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia, np. systemów sygnalizacji pożaru (SSP) wraz z automatyką pożarową oraz dźwiękowych systemów ostrzegawczych (DSO). W tych systemach dowolność interpretacji zapisów projektu może skutkować poważnymi konsekwencjami. Instalacja kablowa praktycznie przechodzi przez wszystkie obszary obiektu i wymaga dokładnego oraz przemyślanego prowadzenia. Zmiany trasy przewodów lub dokładanie przewodów do istniejących tras w korytach kablowych może powodować wadliwą pracę urządzeń lub nadmierne nagrzewanie się przewodów poza zakresami dopuszczanymi przez normy. Takie czynności powinny być uzgadniane na bieżąco z projektantem, dlatego dobrze jest, gdy projekt i wykonawstwo są wykonywane równolegle. Podobnie jest z rozmieszczaniem urządzeń. W przypadku czujników systemu sygnalizacji pożaru przesunięcie czujek w niewielkim zakresie nie zakłóci pracy systemu, natomiast zmiana typu głośników lub miejsca ich instalacji w systemie DSO może bardzo poważnie wpłynąć na uzyskanie poprawnych wartości współczynnika zrozumiałości przekazów słownych RASTI/STI.

Na podstawie mojego doświadczenia w realizacjach dużych inwestycji, w których miałem możliwość uczestniczyć jako projektant lub jako osoba nadzorująca prawidłowe wykonanie instalacji, mogę powiedzieć, że współpraca projektanta z wykonawcą jest wręcz niezbędna. Podczas wykonywania instalacji kablowych, gdy w projekcie zawarte są dokładne i precyzyjne informacje o miejscu ułożenia, sposobie mocowania oraz elementach, których należy użyć, wykonawca posiadający doświadczenie poradzi sobie bez większych problemów. Jeśli jednak instalacja jest wykonywana przez zespół bez doświadczenia, w przypadku wystąpienia nieprzewidzianych przez projektanta okoliczności może powstać poważny problem, który w konsekwencji może doprowadzić do opóźnienia w wykonaniu prac, a tym samym do przekroczenia planowanego terminu zakończenia budowy.

Konieczność wprowadzenia zmian trasy, ułożenia dodatkowych przewodów, czy też zmiana lokalizacji urządzeń lub ich zamiana na inne typy wymaga już akceptacji projektanta, a w niektórych systemach, np. SSP czy DSO, również aprobaty rzeczoznawcy ds. zabezpieczeń ochrony przeciwpożarowej. Wszelkie uwagi, pomysły lub propozycje, które może przekazać instalatorowi projektant, albo projektantowi instalator, mogą wpłynąć pozytywnie na wynik końcowy dokumentacji wykonawczej. W wielu miejscach to instalator ma możliwość oceny, jaki będzie najlepszy sposób wykonania mocowania trasy, czy też prowadzenia okablowania i montażu urządzeń.

W sytuacji, gdy montaż instalacji nie został jeszcze rozpoczęty lub wykonywane są początkowe prace, wszelkie zmiany w instalacji nie powinny powodować większego kłopotu. W przypadku zaawansowanych prac zmiany, które wprowadzi projektant, mogą spowodować bardzo poważne konsekwencje. Zamknięte sufity, zakończone prace przy wykończeniach ścian, czy też powiązanych systemach mogą powodować, że zmiany nie będą możliwe do wykonania albo koszt ich wykonania będzie ogromny. W przypadku, gdy projektant jest w stałym kontakcie z wykonawcą, takie zmiany można przed wprowadzeniem skonsultować, znaleźć sposób nie powodujący kolizji z innymi instalacjami czy powstania dodatkowych kosztów (zmiany w projektach/instalacjach mogą być spowodowane np. zmianami koncepcji inwestora, błędami projektowymi, instalacyjnymi, brakiem możliwości zastosowania rozwiązań montażowych, instalacyjnych itp.).

Wiadomo, iż architekci dążą do uzyskania jak najbardziej estetycznego wyniku końcowego i najlepszego wykorzystania powierzchni na potrzeby najmu. Efektem tego jest przeznaczanie coraz mniejszych pomieszczeń na potrzeby instalacji elektrycznych/teletechnicznych. Na początku, gdy trwają jeszcze prace projektowe, a wykonywanie dopiero się zaczyna, można uwzględnić i przewidzieć, ile miejsca będą potrzebować poszczególne branże. Jeśli jednak prace instalacyjne są już bardzo zaawansowane, w szachtach pojawiają się kolejne rozdzielnie, niekiedy pojawiające się „znikąd", jedynie wykonawca może w szybki sposób poinformować o takim fakcie projektanta. W powyższej sytuacji niestandardowe rozwiązania sprawdziłyby się najlepiej. Każdy obiekt to nowe doświadczenia i rozwiązania techniczne.

Powyższe zagadnienie doskonale ilustrują niżej opisane rzeczywiste sytuacje. W jednym z ostatnio realizowanych obiektów zastosowanie standardowych obudów do modułów wykonawczych wymagałoby zajęcia w szachcie praktycznie całej powierzchni ścian. Zaproponowane rozwiązanie alternatywne ograniczyło zajętą powierzchnię do minimum. Więcej miejsca niż moduły wykonawcze zajmują zasilacze. Zabudowanie w zbiorczych obudowach i zastosowanie złącz kablowych dla wszystkich przewodów połączeniowych pomiędzy modułami pozwoliło na minimalną ingerencję instalatorów w połączenia samych modułów. Zadaniem instalatorów było zainstalowanie skrzynki z modułami, wprowadzenie do niej okablowania oraz podłączenie według dokumentacji przewodów do złącz,

jednakże wraz z zaawansowaniem budowy i wprowadzaniem zmian w systemach wentylacji wymagana była przebudowa skrzynek. Przyjęte rozwiązanie umożliwiło w większości przypadków bezproblemową zmianę urządzeń. Dużo miejsca w części kablowej oraz na szynach z modułami pozwoliło na modernizacje wnętrza skrzynki.

Charakterystyczną cechą systemów sygnalizacji pożaru jest konieczność objęcia sterowaniem oraz nadzorem stanu położenia klap pożarowych wentylacji bytowej, jak i nawiewu/wyciągu pożarowego. Aby bezproblemowo dokonać podłączeń przewodów z klap, zaprojektowano dedykowane obudowy, w których zamontowane zostały moduły wraz z zestawem złącz kablowych. Wszelkie połączenia pomiędzy modułem a złączami zostały wykonane na etapie prefabrykacji obudowy, w zakresie prac instalatorów było wprowadzenie przewodów do obudowy i podłączenie ich do odpowiednich złącz. Rozwiązanie to, mimo potencjalnie wyższego kosztu początkowego, pozwoliło zaoszczędzić na czasie montażu i uruchomienia systemu. Do zrealizowania sterowań innych urządzeń z systemu SSP, np. zatrzymywania pracy schodów ruchomych, zjazdu dźwigów osobowych, czy też zamykania wydzieleń pożarowych, zastosowana została podobna metoda. W obudowach zostały umieszczone moduły wykonawcze wraz z zestawem złącz. Zastosowanie takiego rozwiązania pozwoliło na bezkonfliktowe sprawdzenie pracy całego systemu na etapie budowy. Po zakończeniu testów poszczególnych sterowań, aby nie zakłócać pracy innych branż, można było czasowo rozłączyć przewody w obudowach.

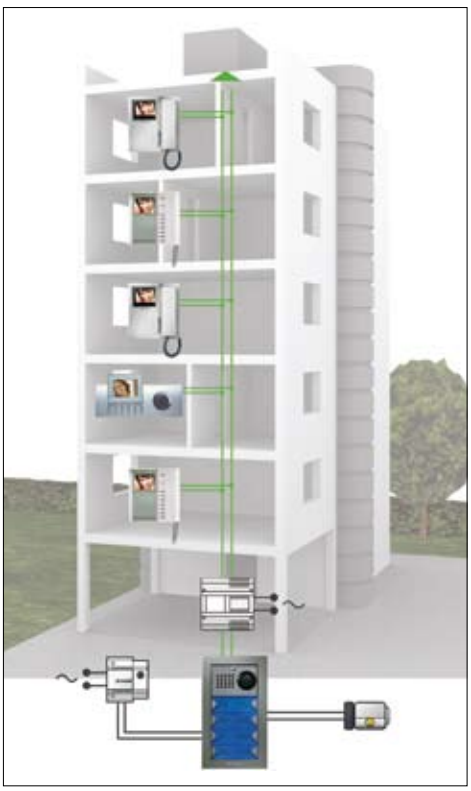
Podobne rozwiązanie przyjęto w systemie wykrywania wycieku gazu ziemnego. Główne magistrale na poszczególnych piętrach mają możliwość wykonania obejścia instalacji na poszczególnych piętrach z zachowaniem ciągłości pracy reszty urządzeń podłączonych do magistrali. Podczas instalacji systemu pojawiały się różnego rodzaju problemy, włącznie z koniecznością zmiany trasy ułożenia rurociągu tranzytu gazu. Zastosowanie przy podłączeniach puszek z listwami dystrybucyjnymi pozwoliło na obniżenie kosztów przerabiania już wykonanych odcinków instalacji kablowej. Wystarczyło przenieść czujnik w nowe miejsce i doprowadzić przewód od czujnika do najbliższej puszki dystrybucyjnej. W wielu przypadkach instalatorzy jako pierwsi mieli informacje o zmianach w branżach powiązanych. Szybkie przekazanie informacji projektantowi umożliwiło ograniczenie kosztów zmian w instalacji. Wykorzystanie dedykowanych dla poszczególnych magistral zasilaczy pozwoliło na zastosowanie urządzeń o mniejszych gabarytach i ograniczyło emisję ciepła z urządzeń. Przyspieszyło również uruchomienie systemu. Podczas gdy instalatorzy wykonywali kolejne magistrale, część już zainstalowana mogła być sprawdzana i testowana.

Przedstawiona na powyższych przykładach metodologia współpracy między projektantem a wykonawcą pozwala na sprawne i prawidłowe wykonanie instalacji i tym samym zakończenie inwestycji z sukcesem. Dlatego, aby uniknąć ewentualnych problemów związanych z kwestią kompetencji i odpowiedzialności za projektowanie lub wykonanie instalacji, proponuję, by w każdych umowach wykonawczych/podwykonawczych zawierać dodatkową klauzulę ustalającą nadzór autorski projektanta nad wykonywaniem instalacji przez wykonawcę.

Piotr Murawski
Projektant Systemów Bezpieczeństwa
GEO-KAT

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 Simplebus2 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

GOLD-IBT

inteligentny tester akumulatorów

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

Jak zmierzyć jego pojemność?

Inteligentny Tester Akumulatorów GOLD-IBT w kilka sekund dokonuje symulacji pełnego rozładowania akumulatora. Automatycznie wyświetla temperaturę otoczenia, napięcie akumulatora i aktualną pojemność.

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

Dane techniczne:

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

alarmnet®

ALARMNET Sp. j.
ul. Karola Miarki 20C
01-496 Warszawa

tel.: 022 663 40 85
faks 022 833 87 95
www.alarmnet.com.pl

Rejestratory cyfrowe 9 i 16 - kamerowe firmy Falcon

Model		DD09200DV	DD16200DV
Wideo	**Format**	**PAL/CCIR**	
	Wejścia wideo	9-CH, BNC	16-CH, BNC
	Monitor główny	BNC x 2, S-wideo x 1, XGA x 1	
	Monitor pomocniczy	BNC x 2	
	Wyjścia wideo	9-CH, BNC	16-CH, BNC
Audio	Wejście / Wyjście	4 / 2, RCA-jack	
Nagrywanie	Kompresja	H.264	
	Prędkość zapisu / Rozdzielczość	PAL - 50 / 720 x 576, 100 / 720 x 288, 200 / 352 x 288	
	Znak wodny	tak	
	Opcje nagrywania	ręczne / według kalendarza /alarmowe / z detekcji ruchu	
	Pre-record	0 - 60 s	
	Post-record	0 - 60 min	
Wyświetlanie	Rozdzielczość	PAL - 720 x 576	
	Podział ekranu	1 / 4 / 7 / 9	1 / 4 / 7 / 9 / 10 / 13 / 16
Odtwarzanie	Prędkość / Rozdzielczość	PAL - 50 / 720 x 576, 100 / 720 x 288, 200 / 352 x 288	
	Wyszukiwanie	data/czas, kamera, alarm, ruch	
Zapis	Dyski twarde	1 gdy zainstalowany DVD/ 2 bez DVD/ 3 z HDD kit	
	Macierz dyskowa	opcjonalnie podłączenie 2 x MDD004 (dodatkowo 8 dysków)	
	Archiwizacja	1 x DVD, 2 x USB 2.0 dla podłączenia zewnętrznych dysków USB	
Alarm	Wejścia / Wyjścia	16 / 4	
	Naruszenie	czujnik, utrata sygnału, detekcja ruchu	
Sieć LAN	Ethernet	1 RJ-45 10 / 100BaseT	
	WWW	zdalne programowanie, monitoring, przegląd alarmów	
	E-mail	informacja o zdarzeniach alarmowych	
	FTP	zapis plików alarmowych	
	Dostęp	8 użytkowników jednocześnie	
Sterowanie	I/R	1 x pilot IR, steruje do 4 rejestratorów	
	RS-232	1 D-type, sterowanie kamerami ruchomymi	
	RS-485/422	1 RJ-45, do podłączenia klawiatury sterującej	
Programowanie	Lokalne	przez panel przedni, pilota IR lub klawiaturę sterującą	
	Zdalne	przez sieć LAN za pomocą dołączonego oprogramowania	
Zabezpieczenia	System	automatyczne uruchomienie po utracie zasilania	
	Filtr przeciwpyłowy	tak	
	Hasła	wielopoziomowy system haseł (18 kont użytkownika)	
Wymiary / Masa	Wymiary	430 (szer.) x 330 (gł.) x 88 (wys.) mm	
	Masa	5 kg (bez HDD)	
Zasilanie	Źródło	90 ~ 264 V AC, 47 ~ 63 Hz	
	Pobór mocy	65 W maks.	65 W maks.

Factor Security Sp. z o.o.
ul. Garbary 14B
61-867 Poznań

tel. (61) 850 08 00, fax (61) 850 08 04
e-mail: factor@factor.pl
www.factor.pl

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).

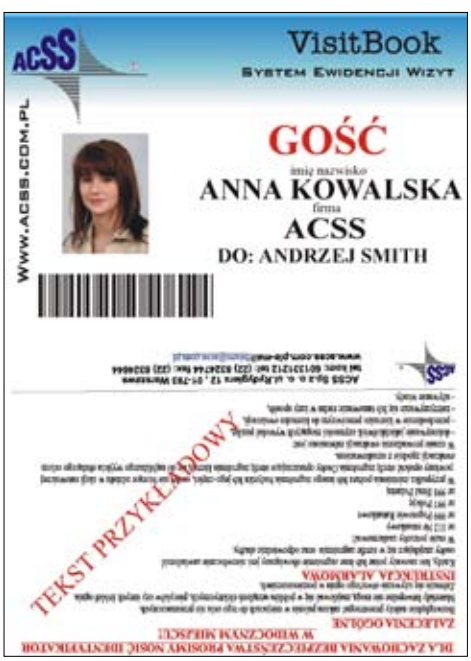
Specyfikacja techniczna
Prędkość nadruku
Wydruk karty w kolorze od krawędzi do krawędzi w 35 sekund
Monochromatyczny wydruk karty w 6 sekund
Cykl działania
Ciągły
Wbudowane zabezpieczenia
HoloKote™ anty-coping – znak wodny na całej powierzchni karty
Typ taśmy
AV1: YMCKO nadruk 250 kart
LC1: YMCKO nadruk 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
Masa
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

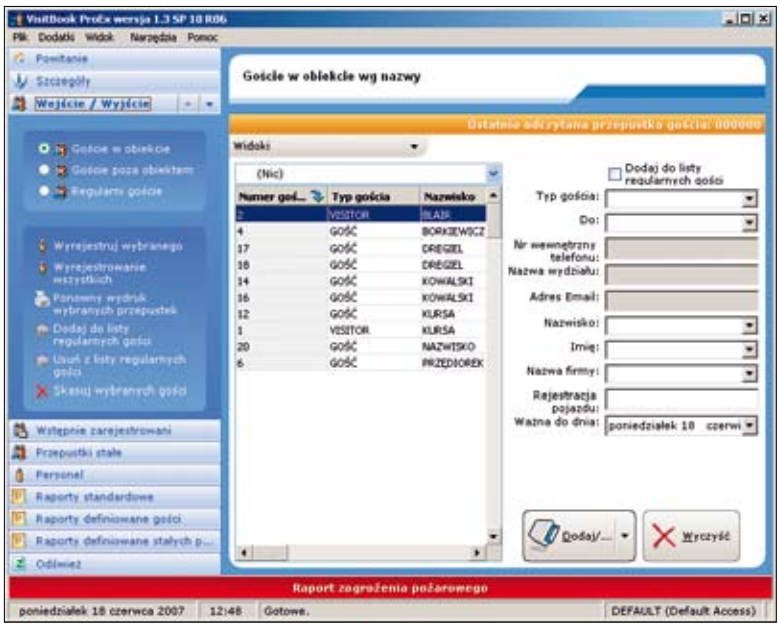
Dystrybutor w Polsce:

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

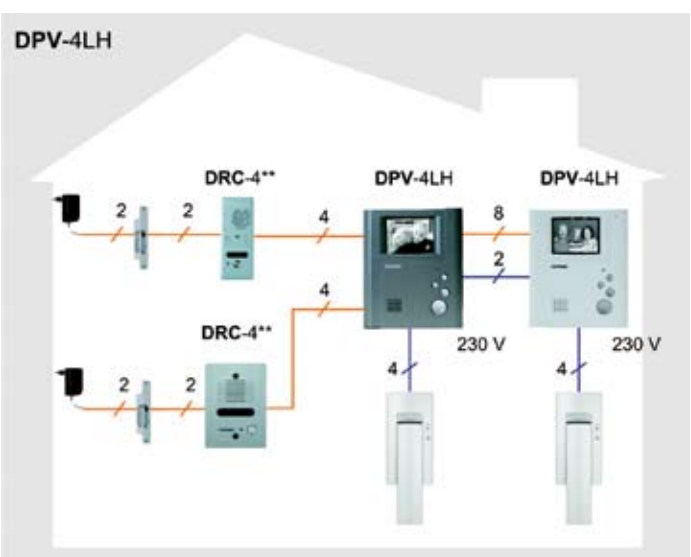
tel. (22) 832 47 44, fax (22) 832 46 44
e-mail: biuro@acss.com.pl
http://www.acss.com.pl

Monitor DPV-4LH

System wideodomofonowy COMMAX zbudowany w oparciu o monitor DPV-4LH jest ciekawą alternatywą dla prostych domofonów umożliwiających tylko łączność głosową z wejściem. Monitor DPV-4LH pozwala na rozmowę z osobą przy wejściu bez potrzeby podnoszenia słuchawki (system głośnomówiący) oraz umożliwia kontakt wzrokowy wyświetlając obraz z kamery wbudowanej w panel rozmówny lub dowolnej kamery podłączonej do wejścia wideo tego monitora. Monitor ma możliwość obsługi dwóch wejść (poprzez rozbudowę o dodatkowy panel rozmówny), podłączenia dodatkowych monitorów i unifonów (realizacja funkcji interkomu).

Dane techniczne:

Zasilanie	AC 100 ÷ 240 V; 50 / 60 Hz
Pobór mocy	maks. 16 W
Ekran monitora	czarno-biały – 4" płaski
Czas wyświetlania obrazu	60 s ±10 %
Okablowanie	28m (ø 0,5) / 50m (ø 0,65) / 70m (ø 0,8)
Temperatura pracy	0°C do + 40°C
Masa	1,2 kg
Wymiary	190 x 226 x 48 mm (szer. / wys. / gł.)



Schemat połączenia DPV-4LH

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

Monitor CDV-50P i kamera DRC-40CK

GDE POLSKA wprowadza na rynek polski nowy wideodomofon koreańskiego koncernu COMMAX. Urządzenie wyposażone jest w 5-calowy monitor, a wygląd zewnętrzny odróżnia się zdecydowanie od sprzętu innych firm. Wraz z kamerą DRC-40CK tworzy ciekawą propozycję dla osób, które chcą wyposażyć swój dom w niezawodny, a przy tym niedrogi wideodomofon. Monitor ma możliwość podłączenia drugiego panelu z kamerą, co umożliwia obsługę dwóch wejść na posesję. Wewnątrz budynku system wideodomofonowy może być rozbudowany o dodatkowe monitory lub same unifony, umożliwiające kontakt głosowy z wejściami (funkcja domofonu). Po rozbudowie systemu istnieje możliwość nawiązania łączności pomiędzy monitorami lub unifonami (funkcja interkomu).

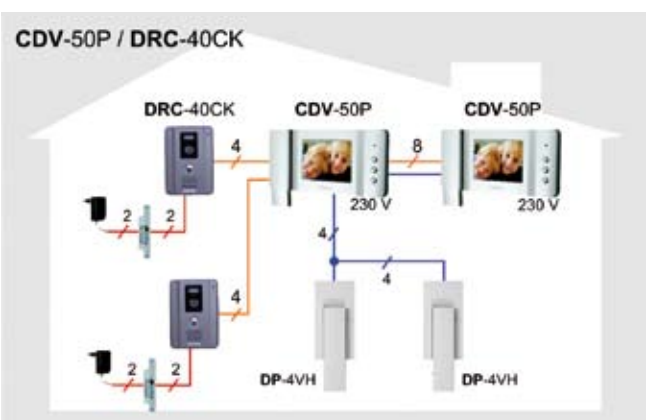
Dane techniczne:

Monitor CDV-50P

Zasilanie	AC 100 V ~ 240 V 50 / 60 Hz
Pobór mocy	maks. 16 W
Monitor	5" Color TFT LCD
System kodowania obrazu	NTSC
Okablowanie	4 przewody do kamery
Podgląd obrazu	90 s (przy rozmowie) / 60 s (przy wywołaniu)
Temperatura pracy	0°C ~ + 40°C
Wymiary	258 x 159 x 51 mm (szer. / wys. / gł.)
Masa	0,85 kg

Kamera DRC-40CK

Zasilanie	DC 12 V (z monitora)
Przetwornik	CMOS
System kodowania obrazu	NTSC
Okablowanie	4 przewody monitor – kamery + zasilanie elektrozamka
Kąt widzenia	poziomy: 75°; pionowy: 55°
Czułość	0,1 lx (30 cm od soczewki)
Temperatura pracy	- 10°C ~ + 40°C
Wymiary	101 x 142 x 32 mm (szer. / wys. / gł.)
Masa	0,30 kg



Schemat połączenia CDV-50P/DRC-40CK

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

Seria kamer megapikselowych firmy Sony

Megapikselowe kamery sieciowe minikopułkowe i stałopozycyjne, cechuje wysoka rozdzielczość obrazu oraz zaawansowane cyfrowe przetwarzanie obrazu. Rozwój przetworników firmy Sony umożliwia tworzenie wyjątkowych rozwiązań dla profesjonalistów w dziedzinie bezpieczeństwa.

SNC-DM160
Zewnętrzna minikopułkowa kamera
o wzmocnionej konstrukcji do pracy w dzień i w nocy

Sieciowa kamera minikopułkowa posiada opatentowany przez firmę Sony mechanizm mocowania obiektywu na przegubach kulowych (*Ball-Joint Lens Mount*), co umożliwia ustawienie pracy w wielu kierunkach oraz szybkie precyzyjne ustawienia ostrości. Kamera umieszczona jest w solidnej obudowie wykonanej z odlewu kokilowego, z kopułką z poliwęglanu, które są odporne na urazy mechaniczne. Możliwe jest mocowanie kamery na ścianie albo pod sufitem. Kamera posiada stopień ochrony przed wodą i kurzem IP66*. Wbudowana grzałka pozwala na eksploatację w niskich temperaturach – nawet do -30°C. Kamera SNC-DM160 może przełączać się z trybu dziennego (barwny) na tryb nocny (czarno-biały) automatycznie (reagując na panujące warunki oświetlenia), ale można też definiować przełączanie ręcznie.

Technologia ExwavePRO z zaawansowanym przetwornikiem obrazu Progressive Scan

Kamery megapikselowe wykorzystują technologię ExwavePRO łączącą przetwornik Progressive Scan CCD z filtrem barw uzupełniających w celu uzyskania wysokiej czułości oraz ostrych, nasyconych obrazów, nawet w najtrudniejszych warunkach oświetlenia. Filtry barw uzupełniających wpuszczają więcej światła do przetwornika CCD, dając lepszy obraz widzianego obszaru.
Tryb dzień/noc w połączeniu z technologią ExwavePRO zdecydowanie poprawia czułość obrazów nocnych i tym samym jakość zarejestrowanych materiałów.

Funkcja lejka świetlnego (Light Funnel Function) pozwala na uzyskanie wysokiej czułości bez zniekształceń obrazu.

Funkcja *Light Funnel* pozwala na poziome i pionowe łączenie każdej pary pikseli obrazu w celu osiągnięcia 3-krotnego zwiększenia czułości przy zwykłych czasach naświetlania. Funkcja lejka świetlnego poprawia jasność bez wywoływania zniekształceń, dając wyjątkowo jasne obrazy nawet przy monitorowaniu ruchomego obiektu o zmierzchu.

Dane techniczne:

KAMERA SNC-DM160	
Przetwornik obrazu	1/3" Progressive Scan CCD z technologią ExwavePRO
Łączna liczba pikseli	około 1.320.000
Liczba efektywnych pikseli	1.250.000 (1296 x 966)
Migawka automatyczna	1 do 1/10.000 s
Regulacja wzmocnienia	(0 dB do +35 dB)
Regulacja ekspozycji	automatyczna / kompensacja światła z tyłu / ustawienia Gamma
Balans bieli	ATW, ATW Pro
Typ obiektywu	obiektyw zmiennoogniskowy
Zoom	3,6 x zoom optyczny (7,2 z zoomem cyfrowym)
Kąt widzenia w poziomie	100,8° do 27°
Zakres zmian ogniskowej	f=2,8 do 10,0 mm
Jasność	F1,3 (szerokokątny), F3,0 (teleobiektyw)
Minimalna odległość od obiektu	300 mm
OBRAZ	
Rozdzielczość obrazu (poziom x pion)	JPEG: 1280 x 960, 960 x 720, 768 x 576, 640 x 480, 384 x 288, 320 x 240 MPEG-4: 640 x 480, 384 x 288, 320 x 240
Maksymalna liczba klatek	30 klatek/s (640 x 480) 15 klatek/s (1280 x 960, 768 x 576)
DŹWIĘK	
Kompresja dźwięku	G.711 / G.726 (40, 32, 24, 16 Kb/s)
SIEĆ	
Protokoły	TCP/IP, HTTP, ARP, ICMP, FTP, SMTP, DHCP, SNMP, DNS, NTP, RTP/RTCP, UDP
Liczba użytkowników	10
Uwierzytelnienie	IEEE802.1X
ZŁĄCZA	
Ethernet	10Base-T / 100Base-TX (RJ-45)
Analogowe wyjście sygnału	BNC x 1, 1.0 Vp-p, 75 Ω, RCA x 1
Port Wejść/Wyjść	czujnik wejście x 2, Alarm wyjście x 2
Wejście mikrofonu zewn.	mini-gniazdko (monofoniczne, 2,2k Ω 2,5 V wtyczka zasilająca)
Wejście/Wejście sygnałowe audio	wejście sygnału audio: mono
Wyjście głośnikowe	mini-gniazdko (monofoniczne) maksymalny poziom wyjściowy: 1 Vrms
WYJŚCIE ANALOGOWE SYGNAŁU WIZJI	
Rozdzielczość pozioma	600 linii TV
Stosunek sygnał/szum	więcej niż 50 dB
Minimalne oświetlenie	kolor: 0,8 lx (50IRE, F1,3, AGC 30 dB) czarno-biały: 0,15 lx (50IRE, F1,3, AGC 30 dB)
OGÓLNE	
Masa	ok. 1,4 kg
Wymiary	ok. 166 x 119 mm
Zasilanie	PoE (IEEE-802.3af) AC 24 V / DC 12 V
Pobór mocy	maks. 15 W
Temperatura robocza	-30 do 50°C

SONY

Sony Poland Sp. z o.o.
ul. Ogrodowa 58
00-876 Warszawa

tel. (22) 520 25 17
faks (22) 520 25 77

Seria kamer SNC-RX (530/550/570) firmy Sony

Wysokiej klasy kamery sieciowe mogą bez ograniczeń obracać się w płaszczyźnie horyzontalnej pozwalając użytkownikowi na nieprzerwane monitorowanie obszaru otaczającego kamerę zapewniając niezawodny i ciągły monitoring obiektów.
Kamery serii SNC-RX wyróżniają wysokie parametry elementów optycznych zapewniając wysokiej jakości obrazy z zachowaniem ostrości podczas przybliżenia. Kamera RX-570 posiada 36-krotny zoom optyczny, sumaryczne powiększenie optyczne i cyfrowe wynosi 432! Kamery pracuja w trybie Dzień/Noc zapewniając klarowny obraz nawet przy natężeniu oświetlenia 0,15 lx.
Dzięki zaawansowanej cyfrowej technologii przetwarzania obrazu kamery te umożliwiają zapis obrazu w trzech formatach kompresji: JPEG, MPEG-4 oraz H.264, tak aby użytkownicy mogli dobrać format kompresji do swoich możliwości sieciowych i sposobu monitorowania.
Dodatkowo kamery z serii SNC-RX posiadają możliwość podwójnego kodowania (*Dual Encoding*) tzn. równoczesnego wysyłania obrazu w formacie JPEG oraz MPEG-4, co pozwala na optymalizację wykorzystania zasobów sieciowych.
Kamery wyposażone są dodatkowo w inne funkcje „inteligentne", takie jak wykrywanie obiektu (*Intelligent Object Detection*) oraz wykrywanie ruchu (*Intelligent Motion Detection*). Kamery wyróżniają się stylowym wzornictwem.

Dane techniczne:

KAMERA SNC-RX570	
Przetwornik obrazu	typu 1/4" CCD w technologii Exwave HAD
Liczba efektywnych pikseli	440.000 (752 x 582)
Prędkość migawki	od 1 do 1 / 10000 s
Regulacja wzmocnienia	automatyczna / ręczna (od -3 do +28 dB)
Regulacja ekspozycji	automatyczna / w pełni automatyczna / priorytet migawki / priorytet przysłony / ręczna / kompensacja ekspozycji / kompensacja światła z tyłu
Balans bieli	auto / wnętrze / plener / jednoprzyciskowy balans bieli / ATW / ręczny
Obiektyw	zmienna ogniskowa z automatycznym ustawianiem ostrości
Zoom	zoom optyczny 36 x (z zoomem cyfrowym 432 x)
Kąt widzenia w poziomie	od 1,7 do 57,8°
Zakres zmiany ogniskowej	f=3,4 do 122,4 mm
Jasność	F1,6 (szerokokątny), F4,5 (teleobiektyw)
Minimalna odległość od obiektywu	320 mm (szerokokątny) 1500 mm (teleobiektyw)
Kąt obrotu	360° ciągły obrót
Prędkość panoramowania	300° / s (maks.)
Kąt uchyłu	-90 do 0°
Prędkość pochylania	300° / s (maks.)
OBRAZ	
Rozdzielczość obrazu (poziom x pion)	640 x 480, 320 x 240, 160 x 120 (JPEG, MPEG-4, H.264)
Format kompresji	JPEG, MPEG-4, H.264
Maksymalna liczba klatek JPEG/MPEG-4, H.264	25 kl. / s (640 x 480) 8 kl. / s (640 x 480)
DŹWIĘK	
Kompresja dźwięku	G.711 / G.726 (40, 32, 24, 16 Kb / s)
SIEĆ	
Protokoły	TCP / IP, HTTP, SSL (https)*, ARP, ICMP, FTP, SMTP, DHCP, DNS, NTP, SNMP (MIB-2), RTP / RTCP *SSL jest spełniany tylko przez kamerę SNC-RZ50P.
Liczba użytkowników	20
WYJŚCIE ANALOGOWE SYGNAŁU WIZJI	
Standard telewizji	PAL (zespolony)
Rozdzielczość pozioma	530 linii TV
Stosunek sygnał / szum	większy niż 50 dB
Minimalne oświetlenie	obraz kolorowy: 1,4 lx (50IRE, F1,6, AGC ON) obraz czarno-biały: 0,15 lx (50IRE, F1,6, AGC ON)

SONY

Sony Poland Sp. z o.o.
ul. Ogrodowa 58
00-876 Warszawa

tel. (22) 520 25 17
faks (22) 520 25 77

Kamery z serii C10DN firmy PELCO

Cechy charakterystyczne

- Kamera dzień/noc ze sterowaniem automatycznym lub manualnym
- Obudowa kompaktowa
- Format przetwornika 1/3"
- Cyfrowe przetwarzanie sygnału
- Ultra wysoka rozdzielczość 540 TVL
- Menu ekranowe konfigurowane za pomocą mini dżojstika
- Cztery zdefiniowane profile aplikacji; jeden profil definiowalny przez użytkownika
- Funkcje automatycznego balansu bieli, automatycznej regulacji wzmocnienia, sterowania elektroniczną migawką oraz kompensacji jasnego tła
- Tryb redukcji migotania
- Auto wykrywanie typu sterowania DC/wideo automatyką przysłony
- Mocowanie obiektywów CS (obiektywy z mocowaniem C wymagają opcjonalnego adaptera
- Automatycznie wykrywany typ zasilania 24 V AC/12 V DC (synchronizacja z sieci zasilającej lub wewnętrznego generatora)
- Kompensacja długiego kabla
- Montaż z góry lub z dołu
- Funkcja Eklipser

Kamery z serii **C10DN** są najmniejszymi pełnofunkcyjnymi cyfrowymi kamerami dzień/noc w ofercie Pelco. Technologia dzień/noc umożliwia osiągniecie znakomitych parametrów w szerokim zakresie warunków oświetlenia. Kamera posiada mechaniczny filtr podczerwieni do przełączania pomiędzy trybem kolorowym i czarno białym w zależności od zmian warunków oświetlenia. Ponadto filtr realizuje wymagania odnośnie czułości w zakresie podczerwieni.

Zostały zaprojektowane w celu dostarczenia wysokiej jakości obrazów w szerokim zakresie warunków pracy. Kompaktowy rozmiar w połączeniu z wieloma interesującymi funkcjami czyni kamerę idealnym rozwiązaniem dla wielu aplikacji.

Kamery cyfrowe z serii **C10DN** posiadają ultra wysoką rozdzielczość 540 TVL, a minimalne oświetlenie wynosi 0.3 luksa w trybie kolorowym oraz 0.07 luksa w trybie czarnobiałym. Funkcjonalność kamery zawiera automatycznie wykrywany typ zasilania (24VAC z synchronizacją z sieci zasilającej lub 12VDC z synchronizacją z wewnętrznego generatora), automatyczna regulacja wzmocnienia (AGC), sterowanie migawką elektroniczną (ESC) oraz tryb redukcji migotania. Kamery z serii **C10DN** posiadają także funkcję automatycznego balansu bieli (AWB) dla trudnych sytuacji oświetleniowych oraz funkcję analogowego eklipsera umożliwiającą kreowanie czytelnych obrazów dla ciemnych obszarów sceny przy silnie oświetlonym tle oraz funkcję kompensacji jasnego tła (BLC) uwypuklającą obiekty pierwszego planu przy silnie oświetlonym tle. Wszystkie te funkcje posiadają możliwość łatwego programowania z poziomu menu ekranowego.

Kamera C10DN-6X z opcjonalnym obiektywem

Kamera C10DN-7X z opcjonalnym obiektywem

Kamery z serii C10DN mogą współpracować z obiektywami o przysłonie stałej, ręcznej lub automatycznej (ze sterowaniem DC lub wideo) posiadającymi standard mocowania CS. Automatyka przysłony obiektywu jest sterowana za pośrednictwem czterostykowego czworokątnego złącza, w które są wyposażone wszystkie obiektywy Pelco. Kamera posiada na tylnej ściance złącze do zewnętrznego sterowania trybem dzień/noc, np. oświetlacza podczerwieni, fotokomórki, itp.

Wygodne menu ekranowe umożliwia programowanie funkcji, które typowo nie sa dostępne w kamerach kompaktowych, czyli ustawienia obszarów zastrzeżonych (masek), opisów tekstowych, korygowania pikseli oraz profili oświetleń. Menu pozwala także na ustawienia trybów pracy kolor/cz-b.

Instalacja kamer z serii **C10DN** jest szybka i łatwa. Kamera C10DN -6X jest idealna do montażu w obudowach kopułowych DF5, DF8A lub obudowach standardowych EH100, EH3508 i EH2508. Kompaktowe wymiary sprawiają, że jest idealnym rozwiązaniem dla pakietów DomePak® (zestaw w obudowie kopułowej) oraz ImagePak® (zestaw w obudowie standardowej).

Opcjonalny zestaw montażowy C10-UM (montaż na ścianie/suficie/ szynie) oferuje łatwą instalację w wielu aplikacjach, gdzie dodatkowa obudowa ochronna nie jest wymagana.

t.a.c by Schneider Electric

TAC Sp. z o.o.
ul. Rzymowskiego 53
02-697 Warszawa

tel. (22) 313 24 10, fax (22) 313 24 11
e-mail: tac_pol@tac.com
www.tac.com/pl

DOSTĘPNE MODELE

C10DN-6X	Kamera dzień/noc, CCD 1/3", ultra wysoka rozdzielczość, 24 V AC lub 12 V DC, PAL
C10DN-7X	Kamera dzień/noc, CCD 1/3", ultra wysoka rozdzielczość, 230 V AC, PAL

PARAMETRY OGÓLNE

Praca dzień/noc	Dzień: Filtr podczerwieni (IR)
	Noc: Filtr szklany BK-7, mechaniczny
Analizator obrazu	1/3" CCD z transferem międzyliniowym
Rozdzielczość obrazu	752 x 528 (PAL)
Obszar analizy	4.7 x 3.5 mm
System skanowania	625 linii (PAL), przeplot 2:1
Synchronizacja	z sieci AC / wewnętrzna
Rozdzielczość pozioma	540 linii TV
Przysłona automatyczna	sterowanie DC / wideo (auto-wykrywanie)
Czułość	kolor: 0.4 lx, F1.2, 50 IRE, ARW wł., reflektancja sceny 89 %
	cz-b: 0.08 lx, F1.2, 50 IRE, ARW wł., reflektancja sceny 89 %
Minimalne oświetlenie	kolor: 0.3 lx, F1.2, 40 IRE, ARW wł., reflektancja sceny 75%
	cz-b: 0.07 lx, F1.2, 40 IRE, ARW wł., reflektancja sceny 75%
Stosunek sygnał/szum	> 48 dB
Faza odchylania pion.	regulowana ± 90°
ARW	wybór
Migawka elektroniczna	wybór
Kompensacja jasnego tła (BLC)	wybór
Eklipser	wybór
Automat. balans bieli (AWB)	wybór
Synchronizacja wew.	wybór
Korekcja gamma	wybór
Redukcja migotania	wybór
Przetwarzanie sygnału	cyfrowe (DSP]
Wyjście sygnału wideo	1 Vp-p, 75 Ω
Zakres balansu bieli	2500° do 9500°K

PARAMETRY ELEKTRYCZNE

Zasilanie	C10DN-6X: 12 V DC + 15 % lub 24 V AC + 15 %, 50 Hz
	C10DN-7X: 230 V AC + 15 %, 50 Hz
Pobór mocy	3 W
Złącze zasilania	terminal z 2 zaciskami śrubowymi
Złącze wideo	BNC
Złącze sterowania przysłoną	4 stykowe (mini czworokąt)
Sterowanie	przycisk 5-pozycyjny

PARAMETRY MECHANICZNE

Mocowanie obiektywu	CS
Mocowanie kamery	śruba 1/4" x 20, montaż z góry lub z dołu

WARUNKI OTOCZENIA

Temperatura pracy	- 10° do + 50° C
Temperatura przechowywania	- 40° do + 60° C
Wilgotność pracy	20 % do 80 %, bez kondensacji
Wilgotność przechowywania	20 % do 90 %, bez kondensacji

PARAMETRY FIZYCZNE

	C10DN-6X	**C10DN-7X**
Wymiary (razem z BNC)	7.5 (dł.) x 5.5 (szer.) x 5.0 (wys.) cm	13.97 (dł.) x 5.5 (szer.) x 5.0 (wys.) cm
Waga (bez obiektywu)	0.20 kg	0.45 kg
Waga paczki	0.45 kg	0.90 kg

CERTYFIKATY

1. CE, klasa B
2. Lista UL
3. Lista UL, kanadyjskie standardy bezpieczeństwa
4. FCC, klasa B

ZALECANE MOCOWANIA

C10-UM – uniwersalny zestaw montażowy: ściana / sufit / szyna, do kamer z serii C10

ZALECANE ZASILACZE

TF 2000	zasilacz dla jednej kamery, 24 V AC, 20 V AC
Seria MCS	zasilacz dla wielu kamer, 24 V AC, aplikacje wewnętrzne
Seria VCS	zasilacz dla jednej / wielu kamer, 24 V AC, aplikacje zewnętrzne

ZALECANE OBIEKTYWY

Serie 13FA, 13FD	obiektywy o stałej ogniskowej, 1/3", przysłona: FA – ręczna, FD – automatyczna DD
Serie 13VA, 13VD	obiektywy o zmiennej ogniskowej, 1/3", przysłona: VA – ręczna, VD – automatyczna DD

AKCESORIA DO OBIEKTYWÓW

LDC100	konwerter do obiektywów z przysłoną automatyczną; umożliwia podłączenie obiektywu ze sterowaniem DC do kamery ze sterowaniem wideo
PCMA40	adapter C/CS; umożliwia podłączenie obiektywu z mocowaniem C do kamery z mocowaniem CS

***UWAGA**: W przypadku instalacji zewnętrznych zalecane jest stosowanie obudów Pelco.*

t.a.c by Schneider Electric

TAC Sp. z o.o.
ul. Rzymowskiego 53
02-697 Warszawa

tel. (22) 313 24 10, fax (22) 313 24 11
e-mail: tac_pol@tac.com
www.tac.com/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
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. Łęczycka 55, 85-737 **Bydgoszcz**
tel. (32) 720 39 65
faks (32) 790 76 85
e-mail: bydgoszcz@e-alpol.com.pl

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

Al. Solidarności 15b, 25-211 **Kielce**
tel. (32) 720 39 81
faks (32) 790 76 94
e-mail: kielce@e-alpol.com.pl

ul. Pachońskiego 2a, 31-223 **Kraków**
tel. (32) 790 76 51
faks (32) 790 76 73
e-mail: krakow@e-alpol.com.pl

ul. Ochotnicza 10, 20-012 **Lublin**
tel. (32) 790 76 50
faks (32) 790 76 74
e-mail: lublin@e-alpol.com.pl

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

ul. 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.
ul. Poleczki 3
02-822 Warszawa
tel. (22) 715 41 00/01
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

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.
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
Biuro SAP: (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. Płochocińska 19 lok. 44-45, 03-191 **Warszawa**
tel. (22) 614 39 52
faks (22) 614 39 64

ul. Kielnieńska 134 A, 80-299 **Gdańsk**
tel. (58) 554 47 46
faks (58) 552 45 24

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

Biuro Handlowe:
ul. J. Bema 5A, 73-110 **Stargard Szczeciński**
tel. (91) 561 32 02
faks (91) 561 32 29

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
faks (22) 644 35 66
e-mail: jacek.urbanowicz@edps.com.pl
katarzyna.osiecka@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
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

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

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

Plac Jana Pawła II 82i, 66-400 **Gorzów Wielkopolski**
tel. (95) 722 12 12
tel./faks (95) 722 12 14
e-mail: factor.go@factor.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. Obrońców Westerplatte 31
80-317 Gdańsk
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

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. (22) 676 77 37
faks (22) 676 82 87
e-mail: ramar@ramar.com.pl
www.ramar.com.pl

ROPAM Elektronik s.c.
os. 1000-lecia 6A/1
32-400 Myślenice
tel./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 POLSKA Sp. z o.o.
ul. Rokicińska 162
92-412 Łódź
tel. (42) 677 58 00
faks (42) 677 58 01
e-mail: centrala@solar.pl
www.solar.pl
www.weblink.solar.pl

Oddziały:
ul. Radzikowskiego 35, 31-315 **Kraków**
tel. (12) 638 91 00
faks (12) 638 91 22
e-mail: krakow@solar.pl

ul. Witosa 3, 20-330 **Lublin**
tel. (81) 745 59 00
faks (81) 745 59 05
e-mail: lublin@solar.pl

ul. Smoluchowskiego 7, 60-179 **Poznań**
tel. (61) 863 02 04
faks (61) 863 02 70
e-mail: poznan@solar.pl

ul. Heyki 3, 70-631 **Szczecin**
tel. (91) 485 44 00
faks (91) 485 44 01
e-mail: szczecin@solar.pl

ul. Krakowska 141-155, 50-428 **Wrocław**
tel. (71) 377 19 00
faks (71) 377 19 16
e-mail: wroclaw@solar.pl

ul. Łużycka 3B, 81-537 **Gdynia**
tel. (58) 662 00 00
faks (58) 664 04 00
e-mail: gdynia@solar.pl

ul. Armii Krajowej 1, 58-302 **Wałbrzych**
tel. (74) 880 01 17/14
faks (74) 847 00 69
e-mail: walbrzych@solar.pl

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) 485 50 00
faks (91) 485 50 12
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
www.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

ul. 1 Maja 11/2, 10-117 **Olsztyn**
tel. (89) 527 92 72
faks (89) 527 92 30
e-mail: olsztyn@spstrading.com.pl

CENTRUM SYSTEMÓW ZABEZPIECZEŃ

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

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
Sprzedaż: (22) 516 97 97
faks (22) 516 97 87
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl

TELCOMP-SERVICE Sp. z o.o.
ul. Annopol 4
03-236 Warszawa
tel. (22) 811 02 59
tel. kom. (0) 662 008 600
e-mail: biuro@telcompservice.pl
www.centrum-ts.pl

TP TELTECH Sp. z o.o.
ul. Tuwima 36
90-941 Łódź
tel. (42) 639 83 60
faks (42) 639 89 85
e-mail: teltechinfo@tpteltech.pl
www.tpteltech.pl

Oddziały:
al. Wyzwolenia 70, 71-510 **Szczecin**
tel./faks: (91) 423 70 55
e-mail: witold.brzozowski@telekomunikacja.pl

ul. Rzeczypospolitej 5, 59-220 **Legnica**
tel. (76) 856 60 71
faks (76) 856 60 71
e-mail: marian.sitko@telekomunikacja.pl

ul. Nasypowa 12, 40-551 **Katowice**
tel. (32) 202 30 50
faks (32) 201 13 17
e-mail: dariusz.gawor@telekomunikacja.pl

ul. Rakowicka 51, 31-510 **Kraków**
tel. (12) 431 59 01
faks (12) 423 97 65
e-mail: marek.zembaty@telekomunikacja.pl

ul. Kosmonautów 82, 20-358 **Lublin**
tel. (81) 745 39 83
faks (81) 745 39 78
e-mail: zbigniew.chodkiewicz@telekomunikacja.pl

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
tel./faks (52) 584 01 92
e-mail: lukasz.cellari@w2.com.pl
www.w2.com.pl

VISION POLSKA Sp. z o.o.
ul. Unii Lubelskiej 1
61-249 Poznań
tel. (61) 623 23 05
faks (61) 623 23 17
e-mail: biuro@visionpolska.pl
www.visionpolska.pl

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

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	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	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	-
Factor Polska	-	-	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	TAK
STRATUS	-	TAK	TAK	-	TAK
SYSTEM 7 SECURITY	TAK	TAK	TAK	-	TAK
TAC	TAK	TAK	TAK	TAK	TAK
Talcomp	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	-	-	TAK	-	TAK
Tayama	TAK	TAK	TAK	TAK	TAK
Techom	-	-	-	-	TAK
Technokabel	TAK	-	-	-	-
Telcomp-Service	-	-	-	-	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	-	-
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	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	-
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	-
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 bezobsługowe do zasilania awaryjnego urządzeń alarmowych								
Eureka	TAK	TAK	TAK	-	TAK	TAK	TAK	-	-
Factor Polska	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	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	-	-	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	-
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	TAK	TAK
S.P.S. Trading	TAK	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	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
Telcomp-Service	szkolenia								
TP TELTECH	TAK	TAK	TAK	TAK	TAK	-	TAK	-	-
Trikon	-	-	TAK	-	-	-	-	TAK	-
TYCO	TAK	TAK	TAK	TAK	-	TAK	-	-	TAK
UNICARD S.A.	-	-	TAK	-	-	TAK	-	TAK	-
W2	TAK	-	-	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 Meledyn
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

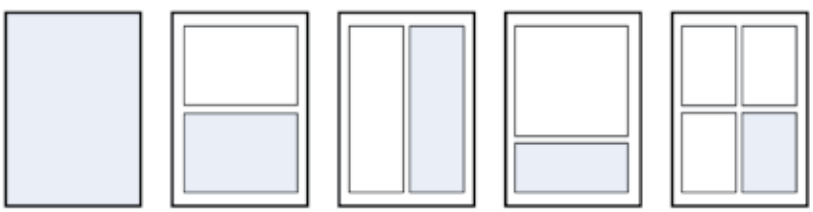
jednorazowy wpis	– 60 zł

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

3D	62
AAT-T	70, 73, 93
ACSS	68
ADD	85
Alarmnet	54
Alarmtech	41
Altram	59
ATline	39
Bosch	119
C&C Partners Telecom	51
CBC Poland	55
ES Instal	77
Gunnebo	89
HID	120
Info-Cam	65
Kabe	72
Laskomex	96
Miwi-Urmet	40, 81
MTK	36
PAG	40
Panasonic	2
Polon-Alfa	36
RISCO Group	87
Roger	69
Satel	35
Softex Data	1
Techom	85
Unicard	64
Zabezpieczenia	89

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

Professional Series

Czujki ruchu, które potrafią odróżnić prawdziwe zagrożenie od źródeł fałszywych alarmów

Rewolucyjna technologia przetwarzania danych z kilku detektorów to prawdziwy przełom w inteligentnym wykrywaniu zagrożeń.

BOSCH
Technologia bliżej nas

- Wyjątkowa skuteczność wykrywania i eliminacja fałszywych alarmów
- Dostępna jedynie w rozwiązaniach firmy Bosch technologia wspólnego przetwarzania sygnałów z pięciu detektorów
- Najwyższa skuteczność detekcji dzięki ciągłemu dostosowywaniu czułości detektorów
- Funkcja aktywnej redukcji białego światła oraz trójogniskowy układ optyczny eliminują fałszywe alarmy, zapewniając najlepszą skuteczność wykrywania we wszystkich zasięgach
- Teraz z technologią wielopunktowego antymaskingu i zintegrowanym wykrywaniem zablokowania soczewki sprayem
- Możliwość dostosowania wszystkich modeli do każdego zastosowania

Aby uzyskac więcej informacji, zapraszamy do odwiedzenia naszej strony internetowej www.boschsecurity.pl

Robert Bosch Sp. z o.o.
Security Systems
ul. Poleczki 3, 02-822 Warszawa
tel.: +48 22 715 41 00 / 01, fax: +48 22 715 41 05 / 06
securitysystems@pl.bosch.com **www.boschsecurity.pl**

Myślisz, że nie możesz uzyskać wysokiej jakości wydruku?

hidglobal.com

FARGO®

Niezawodna drukarka Fargo HDP5000 gwarantuje wysoką jakość wydruku kosztowo porównywalnego do jakości wydruku ze standardowych drukarek.

Firma HID Global, światowy lider w dziedzinie zbliżeniowych systemów identyfikacji, przedstawia nowość pośród drukarek wysokiej wydajności - Fargo HDP5000. Wykorzystanie technologii retransferowej pozwala uzyskać niezwykłą ostrość obrazu i zabezpiecza przed uszkodzeniem przy przenoszeniu go na kartę. HDP5000 idealnie radzi sobie z kartami wyposażonymi w moduł chipowy, ponieważ drukarka nie ma bezpośredniego kontaktu z kartą. To chroni zarówno drukarkę jak i kartę przed ewentualnym uszkodzeniem i eliminuje ewentualne koszty wymiany.

Pomyśl o drukarce HDP5000, jeżeli chcesz uzyskać wysoką i trwałą jakość wydruku za bezprecedensową cenę.

HID

ACCESS quality.

www.hidglobal.com/hdp

Więcej informacji uzyskasz pod numerem 1-800-459-5636 lub pisząc na adres sales@fargo.com