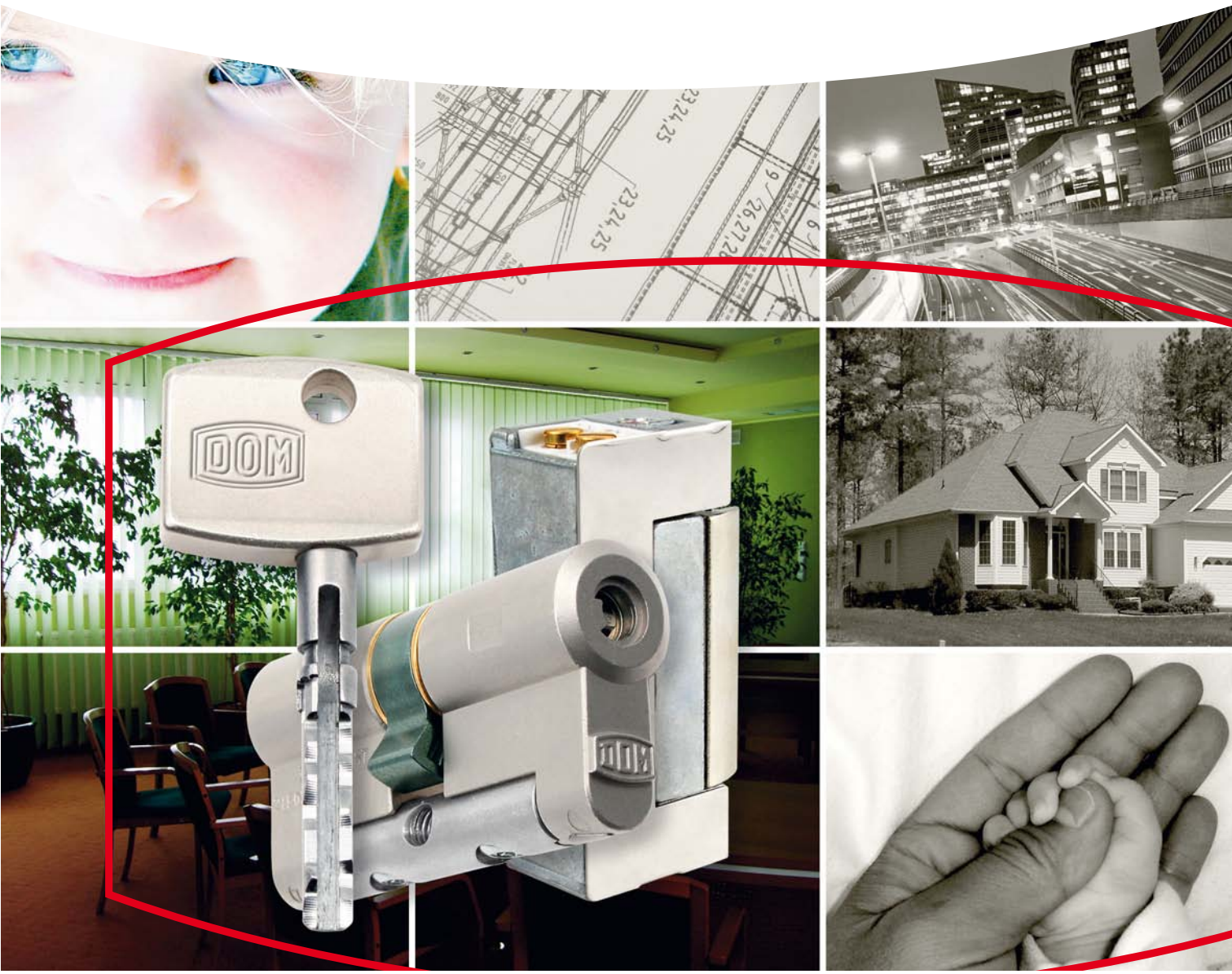
CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 3(55)/2007

ZABEZPIECZENIA

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



W NUMERZE:

System kamery modułowej AutoDome

Jedyna kamera gotowa na spotkanie z przyszłością

Przedstawiamy jedyny w branży zaawansowany system dozorowy, którego wyjątkowa konstrukcja pozwala na dostosowanie do zmieniających się potrzeb i który nigdy nie będzie przestarzały.

- Pięć wymiennych modułów zapewnia szybkie i ekonomiczne unowocześnienie lub rozbudowę funkcjonalności.
- Najnowocześniejsze funkcje pracy w sieci IP zapewniają bardziej efektywną transmisję i zapis obrazu, umożliwiając jednoczesne połączenie hybrydowe.
- Zaawansowane, inteligentne funkcje obejmujące detekcję ruchu, śledzenie, stabilizację obrazu i reguły alarmowe umożliwiają prowadzenie najbardziej precyzyjnego dozoru w całej branży.
- Innowacyjne technologie zapewniające optymalną klarowność obrazu, sterowanie położeniem kamer oraz najwyższą czułość.
- Rygorystyczna technologia testów wytrzymałościowych gwarantująca długie lata niezawodnej eksploatacji.

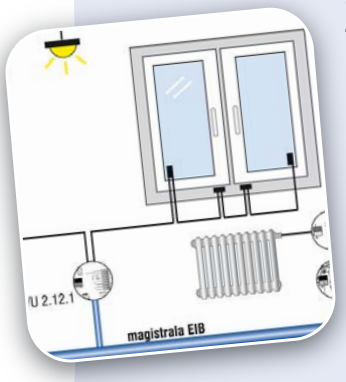
BOSCH
Technologia bliżej nas

Więcej informacji można uzyskać pod numerem telefonu 022 715 41 00 / 01
lub na stronie 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**

CZASOPISMO
ZABEZPIECZENIA
3/2007

w numerze



20
EIB – rozproszony system zarządzania budynkiem

42
Winda – ważny element bezpieczeństwa pożarowego w ewakuacji budynków

56
Teoria ochrony informacji (cz. 1.)

64
Jak się zachować w przypadku incydentu bombowego – radzi policja

PRAGOALARM 2007
PRAGOSEC 2007

W dniach 11–13 kwietnia hale targowe INCHEBA EXPO PRAGA stały się miejscem spotkania 104 wystawców branży *security* prezentujących produkty 230 firm.

Ekspozycja zajęła 2212 metrów kwadratowych, czyli więcej niż w 2005 roku. Wśród wystawców spoza Czech można było obejrzeć stanowiska firm z Hongkongu, Korei, Węgier, Niemiec, Holandii, Rosji, Słowacji, Hiszpanii, Szwajcarii, Tajwanu i Wielkiej Brytanii.

Stoiska targowe zlokalizowano w Średniej Hali Prawego Skrzydła Pałacu Przemysłu, w innych salach odbywały się liczne imprezy towarzyszące. Do najważniejszych należał cykl konferencji poświęconych między innymi systemowi certyfikacji instalatorów systemów bezpieczeństwa w Republice Czeskiej, zasadom oznaczania wyrobów europejskim symbolem CE oraz bezpieczeństwu informacyjnemu. Osobne spotkania poświęcono problematyce systemów CCTV, zarządzaniu sytuacjami kryzysowymi – dynamicznie rozwijającej się w Czechach profesji, oraz perspektywom kształcenia uniwersyteckiego w zakresie zabezpieczeń w tym kraju. Całości dopełniły pokazy tresury psów policyjnych, sztuk walki oraz pojazdów policyjnych.

Targi Pragoalarm/Pragosec stanowiły najważniejsze wydarzenie wystawiennicze dla branży *security* w Czechach w tym roku.

RED.

Więcej zdjęć na naszej stronie internetowej
http://www.zabezpieczenia.com.pl
w dziale *Fotoreportaże*

Klub ESBOC działa

12 kwietnia 2007 roku w **Pradze** (Czechy) rozpoczął oficjalną działalność **Klub Europejskich Organizacji Branży Ochrony (ESBOC)**.

Podczas spotkania podpisano Regulamin Lidera Klubu Europejskich Organizacji Branży Ochrony, ostatni dokument organizacyjny Klubu.

Członkowie Klubu ESBOC (Czechy, Polska, Słowacja, Węgry) funkcję lidera na rok przekazali przedstawicielom czeskim. Do 11 kwietnia 2008 roku będą oni przewodzić pracom Klubu.

Podczas spotkania członkowie zaakceptowali zadania do realizacji, takie jak:

– przejęcie od władz Pragi lokalu z przeznaczeniem na potrzeby klubu,
– uzgodnienie z władzami Pragi, czy można korzystać z pomieszczeń biurowych przedstawicielstwa Pragi w Brukseli,
– opracowanie projektu programu edukacyjnego obejmującego kraje członkowskie Klubu ESBOC, realizowanego dzięki dotacji z Unii Europejskiej.

Spotkanie Klubu ESBOC w Pradze odbyło się podczas Międzynarodowych Targów Wystawowych „PRAGOALARM". Klub ESBOC był ich honorowym współorganizatorem, miał swoje stoisko.

Warto wspomnieć, że prezes Polskiej Izby Ochrony Osób i Mienia Sławomir Wagner został poproszony o udział w ceremonii uroczystego otwarcia PRAGOALARMU. W ten szczególny sposób podziękowano delegacji polskiej za pracę – klub ten powstał także dzięki Polakom.

Bezp. inf. PIOOiM

Więcej zdjęć na naszej stronie internetowej
http://www.zabezpieczenia.com.pl
w dziale *Fotoreportaże*

IFSEC 2007

Tegoroczne Międzynarodowe Targi **IFSEC** – najważniejsza w Europie i jedna z większych w skali globalnej impreza, prezentująca nowości z zakresu elektronicznych systemów zabezpieczeń, w tym pożarowych, odbędzie się w dniach 21–24 maja br. w **Birmingham** (Wielka Brytania), tradycyjnie już na terenie Narodowego Centrum Wystawienniczego (NEC, ang.: *National Exhibition Centre*).

Udział zapowiedziało ponad 700 wystawców – głównie producentów i dystrybutorów z branży *security*, którzy pokażą profesjonalistom z całego świata swoje najnowsze osiągnięcia i będą zachęcać do ich stosowania.

W tym roku po raz pierwszy zostanie wydzielona specjalna powierzchnia, przeznaczona dla wystawców oferujących najnowsze technologie sieciowe (*IP & Networked Solutions*). Będzie tam można obejrzeć systemy wizualizacji, rozmaite oprogramowanie nadzorcze i dyspozytorskie, urządzenia wykorzystujące technologię DVR i NVR, kamery IP, sieciową kontrolę dostępu oraz systemy inteligentnego przetwarzania wideo. Potrzeba utworzenia takiego miejsca, w którym mogliby, z dala od tłoku i gwaru, spotkać się profesjonaliści z branży IT, integratorzy systemów oraz wszyscy zaangażowani w tworzenie rozwiązań, służących do sieciowego przesyłania głosu, obrazu, danych oraz nadzorowania systemów bezpieczeństwa i automatyki budynkowej, była zgłaszana już od pewnego czasu, zarówno przez potencjalnych wystawców, jak i ich gości.

Inne wydzielone powierzchnie będą przeznaczone dla firm, specjalizujących się w ochronie fizycznej oraz policji i służb bezpieczeństwa publicznego.

Każdego dnia równolegle będą odbywać się seminaria tematyczne. Przewiduje się wystąpienia głównie producentów i dystrybutorów systemów bezpieczeństwa, ale także takich organizacji, jak BSIA (Stowarzyszenie Brytyjskiego Przemysłu Zabezpieczeń), policji czy Banku Anglii.

Jak od lat czas poświęcony na udział w IFSEC nie będzie na pewno stracony.

RED.

Tyco Fire & Integrated Solutions, Alcatel-Lucent oraz R&G Plus wdrożą System Obszarowego Sterowania Ruchem w MPK Łódź

Miejskie Przedsiębiorstwo Komunikacyjne Łódź informuje, że wybrało konsorcjum firm Tyco Fire & Integrated Solutions, Alcatel-Lucent oraz R&G Plus do budowy i instalacji **Systemu Obszarowego Sterowania Ruchem** (SOSR), który zapewni priorytetowy przejazd przez miasto dla Łódzkiego Tramwaju Regionalnego (ŁTR) na odcinku pomiędzy pętlami Helenówek i Chocianowice.

Firma **Tyco Fire & Integrated Solutions** wykona prace inżynieryjne, instalacyjne i integracyjne systemu na ponad 60 największych skrzyżowaniach w mieście.

Zmodernizowane na nich sygnalizacje świetlne zostaną zintegrowane i podłączone do centralnego serwera SCATS, który zarządza ruchem ulicznym, dając pierwszeństwo Łódzkiemu Tramwajowi Regionalnemu. SCATS na bieżąco analizuje parametry ruchu i na tej podstawie steruje długością cykli, faz i offsetów podlegających mu sterowników sygnalizacji świetlnej. Natychmiastowa reakcja na zmieniające się warunku ruchu zapewnia optymalne parametry pracy sygnalizacji świetlnych. Pozwala to efektywnie wykorzystać istniejący układ drogowy.

System będzie także przesyłał do centrum sterowania ruchem informacje o nieprzewidzianych zdarzeniach w ruchu drogowym, np. o awarii tramwaju lub wypadku na drodze.

– *System Obszarowego Sterowania Ruchem pozwoli na skrócenie czasu przejazdu jedną z głównych tras w mieście, ponieważ tramwaj będzie miał pierwszeństwo przed innymi uczestnikami ruchu drogowego. Połączenie infrastrukturą informatyczną sąsiednich skrzyżowań w pobliżu trasy Łódzkiego Tramwaju Regionalnego polepszy przepustowość na trasie. System przyczyni się do znacznej redukcji korków oraz zwiększenia płynności ruchu. Dzięki wizualizacji trasy będziemy mogli, w miarę potrzeby, szybko i sprawnie interweniować* – powiedział Ryszard Kowalczyk, kierownik Sekcji Nadzoru Ruchu w MPK Łódź.

Tyco Fire & Integrated Solutions wykona również System Informacji Pasażerskiej, który będzie udostępniał dane o przewidywanych czasach przyjazdu tramwajów na przystanki. Obejmie on tablice informacyjne na ośmiu przystankach oraz tablice informacyjne w 110 pojazdach. Powstanie również serwis internetowy, publikujący informacje o bieżących i przewidywanych warunkach ruchu.

– *Łódź to dynamicznie rozwijające się miasto. Sprawna komunikacja odgrywa w nim coraz większą rolę. Unowocześnienie systemu sterowania ruchem sprawi, że znajdzie się w gronie stu aglomeracji na całym świecie, w których wprowadzono te innowacyjne rozwiązania* – powiedział Wojciech Szymankiewicz, dyrektor generalny Tyco Fire & Security w Polsce.

– *Jestem przekonany, że wdrożenie Systemu Obszarowego Sterowania Ruchem jest inwestycją, która poprawi bezpieczeństwo oraz komfort pasażerów i kierowców* – dodaje.

Firma **Alcatel-Lucent Polska**, członek konsorcjum, jest odpowiedzialna za wybudowanie sieci komunikacyjnej, która zapewni transmisję danych w sieci, m.in. informacji ze sterowników sygnalizacji świetlnej zainstalowanych na 60 skrzyżowaniach, a także obrazu z kamer. Ponadto firma wykona system telewizji dozorowej składający się z 15 kamer. Rozwiązanie, zainstalowane w głównych punktach miasta, wpłynie na poprawę bezpieczeństwa na trasie przejazdu Łódzkiego Tramwaju Regionalnego.

W ramach umowy Alcatel-Lucent zaadaptuje Centrum Zarządzania Ruchem, dostarczy centralę abonencką wraz z telefonami, a także wykona projekty dla tablic zmiennych treści, które będą zainstalowane w kolejnych etapach projektu.

Alcatel-Lucent wykona także system monitorowania wizyjnego zawierający zintegrowane narzędzia do pozyskiwania, transmisji, i zarządzania informacjami w postaci materiałów wideo. Projekt ten obejmuje instalację konsoli operatorskiej, monitorów i pamięci masowej.

Bezp. inf. Tyco Fire & Integrated Solutions

Kurs projektowania systemów alarmowych w klasach od SA-1 do SA-4 podsumowanie

20 kwietnia 2007 roku zakończył się kolejny, przeznaczony dla kadry technicznej, kurs **„Projektowanie systemów alarmowych w klasach od SA-1 do SA-4”**. Organizatorem była Szkoła Elektronicznych Systemów Zabezpieczeń działająca przy Zakładzie Rozwoju Technicznej Ochrony Mienia **„Techom”**.

Na dwóch 5-dniowych sesjach poruszane były zagadnienia techniczne, i prawne, normalizacyjne.

Uczestnicy szkolenia po obronie prac dyplomowych otrzymali zaświadczenia ukończenia kursu oraz autoryzację „Techomu” dla reprezentowanego przez siebie zakładu pracy. Ich firma została wpisana do Katalogu Autoryzowanych Zakładów Instalacji Alarmowych. Uzyskana autoryzacja jest honorowana przez PZU przy udzielaniu zniżek ubezpieczeniowych dla obiektów chronionych. Stanowi także, wraz ze

świadectwem ukończenia kursu, rekomendację przy uzyskaniu koncesji MSWiA i podstawę do ubiegania się o licencję I stopnia zgodnie z Ustawą o ochronie osób i mienia.

Terminy kolejnych kursów zawodowych organizowanych przez „Techom” można znaleźć na stronie internetowej *http://www.techom.com*.

Bezp. inf. Techom

Konferencja sekcji MUZ

Badania i certyfikowanie mechanicznych urządzeń zamykających

26 stycznia br. w Domu Technika w Warszawie odbyła się pierwsza w tym roku konferencja z cyklu poświęconego badaniom i certyfikowaniu mechanicznych urządzeń zamykających (MUZ).

W spotkaniu wzięli udział członkowie Sekcji MUZ i zaproszeni goście. Konferencja poświęcona była problemom, które wystąpiły po rozpoczęciu przez laboratorium akredytowane badań zamków i wkładek bębenkowych według norm: PN-EN 12209:2003 IDT (zastępuje PN-EN 12209:2004 (U), PN-91/B-94400, PN-91/B-94408 i PN-79/B-94450-02) „Zamki mechaniczne z zaczepami. Wymagania i metody badań” oraz PN-EN 1303:2005 IDT (zastępuje PN-EN 1303:2000) „Wkładki bębenkowe do zamków. Wymagania i metody badań”.

Problematykę powyższą szczegółowo przedstawił **kierownik zakładu certyfikacji MUZ Wojciech Dąbrowski** (na zdjęciu poniżej).

Normy te nie obejmują badań odporności na włamanie. Według euronormy PN-EN 12209 zamki mechaniczne należy klasyfikować zgodnie z układem klasyfikacyjnym jedenastu właściwości, a według euronormy PN-EN 1303 wkładki bębenkowe do zamków należy klasyfikować zgodnie z układem ośmiu właściwości. W przypadku badania zamków mechanicznych są one następujące: kategoria użytkowania, trwałość, masa drzwi i siła zamykająca, przydatność do zastosowania w drzwiach przeciwpożarowych/dymoszczelnych, bezpieczeństwo, odporność na korozję i temperaturę, zabezpieczenie i odporność na wiercenie, obszar stosowania do drzwi, sposób uruchamiania kluczem i ryglowania, typ działania trzpienia, wymagania dotyczące identyfikacji klucza (jedenasta właściwość).

W przypadku badania wkładek bębenkowych są to kolejno następujące właściwości: kategoria użytkowania, cykle próbnej trwałości, masa drzwi, odporność ogniowa, bezpieczeństwo, odporność na korozję, wytrzymałość, zabezpieczenie i odporność na wiercenie (ósma właściwość).

Omawiane normy nie obejmują badań odporności na włamanie. Może się zdarzyć, że zamek, który łatwo można otworzyć, manipulując przy nim, jak np. zamek do łazienki, otrzyma wysoką klasę. Warto tutaj wspomnieć choćby o tym, że konstrukcja przyrządu do badania odporności na wiercenie według tych norm narzuca ruch wiercenia tylko wzdłuż osi wiertła, a badana wkładka może zmieniać położenie względem trzech osi. Próba zwiercenia na przyrządzie kończy się niepowodzeniem, ale inaczej jest, gdy trzymamy wiertarkę w rękach.

Polski Zakład Certyfikacji MUZ prowadzi dodatkowo badania odporności na włamanie. Jest to jeden z powodów, dla których warto polecać zamki do mieszkań i sejfów posiadające certyfikaty polskiego Zakładu Certyfikacji.

Podczas konferencji Prezes Sekcji MUZ SIMP wręczył legitymacje i odznaki SIMP nowym członkom kol. kol. Janowi Bonkowskiemu i Mariuszowi Michalcowi.

Bezp. inf. – Józef Rudziński, Prezes Sekcji MUZ SIMP

Targi Zabezpieczeń i Ochrony Mienia
Prewencja 2007 – podsumowanie

Dobiegły końca organizowane po raz trzeci w naszych halach Targi Zabezpieczeń i Ochrony Mienia PREWENCJA, które stały się okazją do zdobycia i wymiany informacji oraz doświadczeń. Chcąc sprostać oczekiwaniom firm i instytucji prezentujących się podczas targów, kolejna edycja towarzyszyła Międzynarodowym Targom Budowlanym BUD-GRYF – największej i najliczniejszej ze względu na liczbę wystawców i odwiedzających imprezie targowej w regionie.

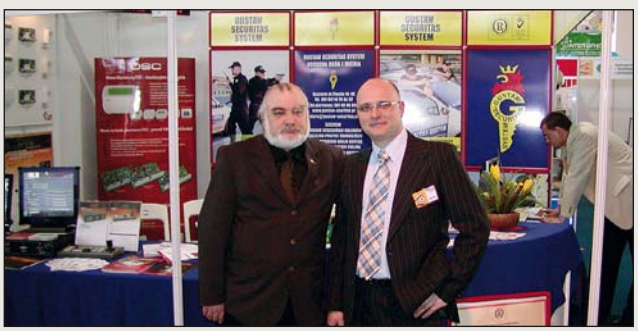
Targi zgromadziły setki wystawców i tysiące gości, głównie z branży *security* (prawie 10 000 zwiedzających).

Przez trzy dni swoje oferty prezentowali producenci, dystrybutorzy oraz instalatorzy elektronicznych systemów zabezpieczeń, alarmów, urządzeń łączności wewnętrznej, drzwi zabezpieczeniowych do pomieszczeń specjalnych i budownictwa, systemów inteligentnego sterowania instalacjami elektrycznymi w budynku, zintegrowanych systemów alarmowych oraz samochodów specjalnych do monitoringu imprez masowych. Swoje usługi zaprezentowały także firmy ochroniarskie z Zachodniopomorskiego.

Tegoroczni wystawcy byli organizatorami wielu prelekcji, wykładów i pokazów, dotyczących m.in. zastosowania systemów klucza generalnego w domach, firmach i obiektach użyteczności publicznej, możliwości systemów bezprzewodowych, możliwości zamków elektrycznych jako elementów wykonawczych w nowoczesnych systemach kontroli dostępu i inteligentnego domu.

Zapraszamy w przyszłym roku.

Bezp. inf. MTS



Podczas imprezy rozstrzygnięto następujące konkursy:

I. Produkt o najlepszych walorach użytkowych

Konkurs przygotowany przez Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem Polalarm oraz MTS.

Komisja konkursowa obradowała w składzie:
- Krzysztof Borowy – Polalarm Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem – przewodniczący,
- Marek Chromiński – Polalarm Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem,
- Marzena Piotrowska – Międzynarodowe Targi Szczecińskie.

Konkurs rozstrzygnięto w czterech kategoriach:
1. Urządzenie sygnalizacji włamania i napadu
2. Urządzenie nadzoru wizyjnego
3. Urządzenie zabezpieczenia przeciwkradzieżowego pojazdu
4. Urządzenie zabezpieczenia przeciwkradzieżowego towaru, produktu

Po zapoznaniu się ze zgłoszonymi produktami Komisja przyznała nagrody:
- w kategorii **Urządzenie nadzoru wizyjnego**: firmie **PAG za Mobilne Centrum Monitoringu**;
- w kategorii **Urządzenie sygnalizacji włamania i napadu**: firmie **Gustaw Securitas System za centralę alarmową PC 1616**;
- w kategorii **Urządzenie przeciwkradzieżowe pojazdu**: firmie **Alfa-Alarm Wesołowski Wojciech za urządzenie Trim Trac**;
- w kategorii **Zabezpieczenie przeciwkradzieżowe towaru**, produktu: **Regionalnej Agencji Rozwoju Rynku za urządzenie OV Dot**.

II. Prewencja No1

Konkurs na najlepszą stronę internetową wystawcy targów, organizowany przez portale internetowe: www.4safe.pl, www.alarmy.org, www.e-instalacje.pl, www.budnet.pl oraz MTS.

Po zapoznaniu się ze zgłoszonymi stronami Komisja przyznała:
1. W kategorii **Ochrona**:
   - pierwszą nagrodę i godło Prewencja No1: firmie **Gustaw Securitas System ze Szczecina,**
   - wyróżnienie: firmie PAG z Bogdanki .
2. W kategorii **Instalacje**:
   - pierwszą nagrodę i godło Prewencja No1: firmie **Patronic ze Szczecina**,
   - wyróżnienie: firmie **Alfa-Alarm Wesołowski Wojciech ze Szczecina**.

Konferencja naukowa w Krakowskiej Szkole Wyższej

Zarządzanie przepływem i ochroną informacji w państwie i przedsiębiorstwie

W dniach 25 i 26 marca 2007 Katedra Zarządzania Informacją Krakowskiej Szkoły Wyższej im. Andrzeja Frycza Modrzewskiego w Krakowie była organizatorem pierwszej konferencji naukowej z cyklu „Zarządzanie przepływem i ochroną informacji w państwie i przedsiębiorstwie. Problemy teorii i praktyki".

Obrady konferencji otworzył przewodniczący komitetu organizacyjnego – prof. Mirosław Kwieciński. Przywitał wszystkich uczestników, a w szczególności Kanclerza – dr. Klemensa Budzowskiego – profesora KSW.

Konferencja skierowana była przede wszystkim do przedstawicieli organizacji państwowych i prywatnych, teoretyków i praktyków oraz wszystkich zainteresowanych tą tematyką.

Celem spotkania była prezentacja poglądów na przepływ i ochronę informacji w państwie i przedsiębiorstwie.

Rada Naukowa Konferencji:

prof. dr hab. Janusz Czekaj (AE w Krakowie/KSW)

dr inż. Wiesław M. Grudzewski – prof. KSW (Instytut Organizacji i Zarządzania w Przemyśle „ORGMASZ")

prof. dr hab. Bogusław Kaczmarek (Uniwersytet Łódzki)

prof. zw. dr hab. inż. Leszek Kiełtyka (Politechnika Częstochowska)

prof. zw. dr hab. inż. Wiesław Kotarba (Politechnika Wrocławska)

prof. zw. dr hab. Wiesław Wróblewski (Uniwersytet Szczeciński)

Komitet Organizacyjny:

dr hab. Mirosław Kwieciński – prof. KSW – przewodniczący

mgr Magdalena Mielus – sekretarz

mgr Arletta Kowalik

Uczestnicy konferencji podczas swoich wystąpień podjęli próby odpowiedzi na postawione przez organizatorów pytania:

1. Jak wygląda praktyka przepływu i ochrony informacji? Czy teorie znajdują zastosowanie w praktyce?
2. Z czego wynikają różnice w ochronie informacji w państwie i przedsiębiorstwie? W jakim kierunku zmierza współczesne zarządzanie przepływem i ochroną informacji?

Skoncentrowano się na następujących zagadnieniach:

a) rola informacji w integrującej się Europie,
b) wykorzystanie i przepływ informacji w państwie i przedsiębiorstwie,
c) wywiad i kontrwywiad gospodarczy w zarządzaniu przedsiębiorstwem,
d) eliminowanie patologii zarządzania informacją w działalności gospodarczej i publicznej,
e) ochrona informacji w państwie i przedsiębiorstwie,
f) edukacja na rzecz sprawnego przepływu i ochrony informacji,
g) zarządzanie wiedzą chronioną w przedsiębiorstwie,
h) zarządzanie bezpieczeństwem.

Obrady konferencji podzielono na sesje tematyczne:

1. Bezpieczeństwo współczesne implikacje i wyzwania w teorii oraz praktyce funkcjonowania państwa i przedsiębiorstwa – panel profesorski (moderatorem był dr hab. Mirosław Kwieciński – prof. KSW. Uczestnicy panelu: prof. dr hab. Andrzej Chodyński, dr hab. Stanisław Galata – prof. KSW, prof. dr hab. Bogusław Kaczmarek, prof. zw. dr hab. inż. Leszek Kiełtyka, prof. zw. dr hab. Kazimierz Perechuda, prof. dr hab. inż. Mirosław Włodarczyk, prof. zw. dr hab. Wiesław Wróblewski).
2. Przepływ, przetwarzanie i ochrona informacji we współczesnych systemach zarządzania – panel śląsko-małopolski.
3. Informacja jako determinanta tworzenia wartości dodanej oraz przewagi konkurencyjnej – panel dyskusyjny
4. Zarządzanie wiedzą w wybranych dziedzinach aktywności gospodarczej i publicznej – panel praktyków.

Referaty prezentowane w trakcie konferencji zostaną wydane w recenzowanym wydawnictwie.

RED.

Sprzęt, który może uratować życie

PULSE Barryvox, niewielkie przenośne urządzenie szwajcarskiej firmy Mammut, to niezbędny element ekwipunku dla tych, którzy od leżenia na plaży wolą chodzenie po górach, zwłaszcza zaśnieżonych.

Jego posiadanie w ekstremalnych warunkach może decydować o życiu lub śmierci. W razie zasypania przez lawinę wykorzystuje się je jako nadajnik (częstotliwość pracy – 457 kHz), co pomaga ratownikom, wyposażonym w identyczne urządzenia, w szybszym odnalezieniu i odkopaniu zasypanego. Nie trzeba nikomu tłumaczyć, jak istotną rolę odgrywa wtedy czas. Sprzęt jest wyposażony również w funkcję mierzenia oddechu. Dokonane pomiary są wykorzystywane do określenia statusu zdrowotnego poszukiwanej osoby, wysyłanego do ratowników. Dzięki temu wiedzą oni, w jakim jest stanie, oraz jaki czas upłynął od zasypania (określanym od momentu ustania ruchu człowieka wyposażonego w PULSE Barryvox). W tym celu stosuje się w Europie częstotliwość 869,8 MHz (w Ameryce Północnej – wyższą, zgodnie z przepisami odnośnie wykorzystania pasma radiowego).

PULSE Barryvox może pracować w trybie wysyłania (*SEND*) – jeśli wykorzystywany jest przez osobę narażoną na zasypanie lawiną. Może też być przełączony w tryb poszukiwania (*SEARCH*), wówczas lokalizuje zasypanych przez lawinę. Na prostym wyświetlaczu LCD urządzenie wskazuje położenie ofiary i pozostały do niej dystans. Może namierzać kilka osób jednocześnie. Ekranik LCD, mimo niepozornego wyglądu, jest czytelny pod praktycznie każdym kątem, a także w pełnym słońcu.

Zasięg wykrywania PULSE Barryvox wynosi w standardowym trybie cyfrowym maksymalnie 60 m. Możliwe jest także przełączenie urządzenia na tryb analogowy, wtedy zasięg zwiększa się do 90 m, ale kosztem ograniczenia informacji odnośnie do kierunku położenia zaginionego (możliwe jest tzw. szukanie akustyczne, jak w przypadku klasycznych analogowych detektorów tego typu). Do zasilania urządzenia wykorzystuje się trzy baterie alkaliczne typu AAA, pozwalające na pracę przez co najmniej 200 godzin.

Opracowano na podstawie materiałów firmy Mammut

HID Global przejmuje firmę Integrated Engineering

Decyzja ta umocni pozycję firmy jako lidera w technologii kart inteligentnych

Firma **HID Global**, główny producent rozwiązań kontroli dostępu oraz członek Global Technologies Division grupy ASSA ABLOY, ogłosiła przejęcie firmy **Integrated Engineering** (IE). IE to amsterdamski producent czytników bezdotykowych kart inteligentnych, znany między innymi dzięki serii MIFARE/DESFire, mającej zastosowanie w kontroli dostępu, identyfikacji oraz sprzedaży bezgotówkowej. Najlepszym dowodem potencjału rozwojowego IE jest fakt, że przedsiębiorstwo zaoferowało pierwszy czytnik zgodny ze standardem PIV.

Pozyskując platformę czytników opartych na technologii MIFARE, HID Global jest w pełni gotowy, by konkurować na rynku produktów 13,56 MHz. Coraz więcej przedsiębiorstw, uniwersytetów oraz agend rządowych pragnie wykorzystać możliwości implementacji dodatkowych aplikacji takich jak obsługa parkingu, kontrola czasu pracy i obecności pracowników lub weryfikacja biometryczna. Karty inteligentne w technologii 13,56 MHz stały się głównym źródłem takiej funkcjonalności.

Platforma MIFARE uzupełnia linię produktową iCLASS, jasno podkreślając zaangażowanie firmy HID w rozwój technologii 13,56 MHz. Obecnie w ofercie koncernu jest wiele produktów do obsługi bezdotykowych kart inteligentnych, dostępnych u ponad 40 000 przedstawicieli na całym świecie.

– *Mamy nadzieję połączyć potencjał produkcyjny HID Global z innowacyjnością Integrated Engineering, aby doskonałe produkty IE stały się dostępne dla większej liczby odbiorców na całym świecie* – stwierdził Steve Wagner z HID Global.

– *Dodając do swojego portfolio tę markę, HID Global konsekwentnie realizuje politykę umacniania pozycji lidera w technologii 13,56 MHz* – podkreślił Denis Hébert, prezes HID Global.

Bezp. inf. HID

Elektrozaczepy w ofercie firmy Dom Polska

Z przyjemnością informujemy Państwa że firma **Dom Polska** wprowadziła do swojej oferty nowy produkt – elektrozaczepy (na wszystkie modele dajemy pięć lat gwarancji).

W naszej ofercie znajdą Państwo zarówno modele standardowe, jak również niskoprądowe, z pamięcią, odblokowaniem czy sygnalizacją. Wszystkie oferowane elektrozaczepy są symetryczne, z regulacją ustawienia zapadki.

Nasze elektrozaczepy mogą współpracować z domofonami, szyfratorami, czytnikami kart oraz systemami kontroli dostępu. Konstrukcja elektrozaczepów DES firmy Dom Polska pozwala na zastosowanie ich zarówno w drzwiach metalowych czy drewnianych, jak i aluminiowych i PVC. Elektrozaczepy przystosowane są do montażu zarówno w drzwiach zewnętrznych, jak i wewnętrznych.

Pełną ofertę znajdą Państwo na stronie *http://www.dom-polska.pl*.

Bezp. inf. Dom Polska

Przedłużona 3-letnia gwarancja na urządzenia Axis

Axis Communications, wieloletni partner **Softex Data**, pionier rozwiązań cyfrowych na rynku systemów monitoringu i dozoru wizyjnego, przedłuża okres gwarancyjny na sieciowe produkty wideo.

Oferowany do tej pory okres gwarancyjny został przedłużony do 3 lat.

Oferta dotyczy wszystkich sieciowych produktów Axis, zakupionych od 1 stycznia 2007, z wyjątkiem kamer AXIS 206 i AXIS 207.

W ramach wydłużonego okresu gwarancyjnego Axis zapewnia wymianę wadliwego produktu. Klient nie poniesie przy tym dodatkowych kosztów.

Bezp. inf. Softex Data

AXIS obserwuje Sztokholm

Władze Sztokholmu zainwestowały 25 milionów funtów w **system bezpieczeństwa wizyjnego**. Projekt zakłada zainstalowanie ponad 15 000 kamer w środkach transportu publicznego, zarówno na stacjach kolejowych, stacjach metra, jak również w autobusach i pociągach podmiejskich. Sieć będzie strzegła około 65 000 pasażerów każdego dnia korzystających ze sztokholmskiego transportu.

Ponadto projekt zakłada otwarcie w lipcu **centrum bezpieczeństwa** – punktu, w którym będzie sprawowana kontrola nad wszystkimi kamerami, alarmami i systemami ostrzegania zainstalowanymi w środkach publicznego transportu.

Axis Communication, światowy lider i jednocześnie producent najlepszych urządzeń służących zapewnieniu bezpieczeństwa, został wybrany na dostawcę kamer dla miasta. Firma dostarczy różne typy urządzeń, m.in. kamer ogólnego nadzoru (*general surveillance*), kamer identyfikujących (*identification*) oraz inteligentnych kamer służących bezpieczeństwu w tunelach. Co ciekawe, kamery instalowane w autobusach współpracują z programem automatycznej lokalizacji autobusów, a te z kolei z systemem GPS, co w znacznym stopniu ułatwi współpracę Centrum Bezpieczeństwa z władzami odpowiedzialnymi za reakcję na ewentualne niewłaściwe zachowania w pojazdach.

Na stacjach metra i kolejek zostanie zainstalowana kombinacja kamer Axis 225FD zapewniających profesjonalny nadzór nawet w trudnych warunkach oraz Axis 212PTZ, które gwarantują zoom bez uszczerbku dla rozdzielczości, a tym samym jakości rejestrowanego obrazu. W autobusach zdecydowano się na kamery Axis 209FD-R, które jako pierwsze na świecie zostały specjalnie zaprojektowane do użycia w tego typu środkach transportu. Ich wymiary, zabezpieczenie w postaci odpornej na zniszczenie obudowy oraz specjalna konstrukcja pozwolą na pewne umieszczenie urządzeń nawet na tzw. trudnych powierzchniach o nieregularnych kształtach.

Wicedyrektor Axis Johan Lembre jest przekonany o najwyższej jakości dostarczanego do Sztokholmu sprzętu. Podkreśla także opłacalność inwestycji oraz wskazuje na nowatorskie rozwiązania zastosowane w urządzeniach:

– Axis 209FD-R to pierwsza kamera na rynku, która naprawdę zwraca uwagę na to, co dzieje się w publicznych środkach transportu.

Lembre zaznacza także, że została ona wyposażona w system wysyłający sygnał do Centrum Bezpieczeństwa, gdy tylko zostanie naruszona.

Rozbudowa sieci kamer to nie jedyna inwestycja sztokholmskich władz. Kolejnym krokiem, jeśli chodzi o usprawnienie sieci bezpieczeństwa, jest także wymiana przestarzałych kamer analogowych na cyfrowe, lub przynajmniej włączenie ich do sieci, by system był kompletny. Martin Gren, współzałożyciel Axis, podkreśla przewagę cyfrowej technologii, która nie tylko zapewnia wyższą jakość przekazu czy pozwala na używanie większej liczby funkcji, lecz także znacznie ułatwia zarządzanie siecią. Jedną z takich nowoczesnych funkcji jest bez wątpienia zdolność kamer cyfrowych do powiadamia o ich zakryciu lub innym naruszeniu. Pozwala to znacznie zminimalizować ryzyko, że oglądający jednocześnie obrazy z kilkunastu kamer pominie podejrzane zachowanie. Inteligentne kamery pomagają więc nie tyle łapać sprawców naruszeń, ile w dużej mierze po prostu tym naruszeniom zapobiegają.

Kolejnym przedsięwzięciem wpisującym się w nurt zasady „Lepiej zapobiegać, niż leczyć" jest wspólny projekt Checkpoint i Axis dotyczący systemów bezpieczeństwa w sklepach detalicznych. Simon Edgar z Checkpoint podkreśla, że dzięki współpracy z Axis zamierzają powstrzymać ogromną falę kradzieży sklepowych dokonywanych nie tylko przez klientów, lecz także samych pracowników sklepów. Skala problemu jest ogromna – tylko w Europie straty z powodu kradzieży sklepowych wynoszą rocznie ponad 32 miliardy euro!

Przykład sztokholmski pokazuje, jak systemy bezpieczeństwa wkraczają w nasze codzienne życie. Axis Communications nie zamierza więc spoczywać na laurach i już planuje kolejne inwestycje. Zgodnie z zasadą „5x5" firma zakłada 5-krotne zwiększenie skali swojej działalności w kolejnym pięcioleciu. Ambitna wizja nie jest jednak przesadna, jeśli weźmiemy pod uwagę wysoką jakość oferowanych urządzeń i fakt, że władze innych miast z zazdrością patrzą na transport miejski w Sztokholmie.

Autoryzowanym dystrybutorem kamer Axis w Polsce jest **Softex Data**.

Bezp. inf. Softex Data

Nowe spojrzenie na obudowy kopułkowe

Medusa to nowy standard obudów kopułkowych do kamer szybkoobrotowych i sieciowych o sterowanym zdalnie położeniu. Zbudowane z trwałego stopu aluminium obudowy z oknem poliwęglanowym gwarantują wyśmienite zabezpieczenie przed czynnikami zewnętrznymi (IP66) oraz wstrząsami.

Opatentowany sposób montażu jest innowacyjny i niezwykle przyjazny dla użytkownika, zarówno przy pierwszej instalacji, jak i podczas późniejszych prac serwisowych. Dzięki temu, że obudowa jest otwierana od góry, kamera jest przy montażu wsuwana w prowadnicę, co pozwala uniknąć trudnego i złożonego jej mocowania.

Bogaty zestaw dopasowanych do obudowy akcesoriów sprawia, że często jest ona idealnym rozwiązaniem i ma wiele zastosowań. Dostępne są: przełącznik antysabotażowy, grzejniki z wentylatorami do pracy w niskich temperaturach, system chłodzenia, przydatny przy dużej temperaturze otoczenia, różne modele zasilaczy.

Medusa będzie prezentowana, wraz z innymi nowościami firmy **Videotec**, podczas targów IFSEC 2007.

Bezp. inf. Videotec

Międzynarodowa Wystawa Zabezpieczeń i Metod Otwierania Drzwi, Sejfów oraz Samochodów

ZIEH-FIX Warszawa 2007

W dniach od 18 do 21 kwietnia 2007 roku w siedzibie firmy **Freiberger** w Warszawie po raz pierwszy w Polsce odbyła się Międzynarodowa Wystawa Zabezpieczeń i Metod Otwierania Drzwi, Sejfów oraz Samochodów „ZIEH-FIX Warszawa 2007".

Wystawa zainaugurowała wprowadzenie do oferty firmy Freiberger specjalistycznych narzędzi i urządzeń przeznaczonych do awaryjnego otwierania.

Tematem wystawy były nowoczesne techniki awaryjnych otwarć.

Gośćmi specjalnymi byli:
- Adalbert Wendt – szef WENDT GmbH,
- Theo Schürmann – szkoleniowiec firmy WENDT GmbH,
- Frederic Versteeg (VERSEC Technics/Holandia) – uznany specjalista od awaryjnych otwarć sejfów,
- Józef Matyjas – Systemy Zabezpieczeń.

Główną atrakcją wystawy były pokazy awaryjnych otwarć zamków mieszkaniowych, samochodowych, a także sejfów mechanicznych i elektronicznych. Odwiedzający mogli wypróbować w praktyce prezentowane narzędzia.

Więcej informacji na temat prezentowanych urządzeń znajdą Państwo na *http://www.zieh-fix.pl*.

Bezp. inf. Freiberger

Fotoreportaż na http://www.zabezpieczenia.com.pl

Megapikselowa kamera sieciowa IP7138/IP7139 Vivotek

Wszyscy już przywykli do dynamicznego rozwoju produktów stosowanych w systemach monitoringu sieciowego. Większość producentów kamer ulepsza je, stosując prosty trik – dodanie ciekawszej obudowy. Jest to całkiem zrozumiałe. Jakość obrazu, jaką obecnie oferują systemy sieciowe, bardzo często wykracza poza standardy znane z systemów analogowych, a niewielu producentów postanowiło już dzisiaj przekroczyć barierę rozdzielczości PAL. Do tego małego grona można od teraz zaliczyć także firmę **Vivotek**.

Producent zaprezentował dwie kamery megapikselowe, które otrzymały nazwy handlowe IP7138 i IP7139.

Kamery **VIVOTEK IP7138/39** wyposażone są w przetwornik CMOS o rozdzielczości 1,3 megapiksela zapewniający wysokiej jakości obraz; idealny do zdalnego monitoringu miejsc, w których niezbędne są wysoka rozdzielczość oraz duży poziom szczegółowości obrazu. Zastosowanie nowego procesora VVTK-1000 pozwala na symultaniczny obraz w kompresji MPEG-4 oraz MJPEG (Dual Codec). Zaletami są też:
- dwukierunkowa transmisja audio,
- możliwość podglądu obrazu na telefonach komórkowych obsługujących 3 G,
- zasilanie kamery przez sieć (PoE – Power over Ethernet), zgodnie ze standardem 802.3af (IP7138),
- możliwość podłączenia poprzez Wi-Fi, zgodnie ze standardem 802.11b/g (IP7139),
- wymienne obiektywy,
- gniazdo kart Compact Flash pozwalające na lokalne przechowywanie obrazu w razie braku połączenia z siecią,
- wejście i wyjście alarmowe,
- strefy prywatności,
- dołączone oprogramowanie 16-kamerowe.

Bezp. inf. Suma

HID Global poszerza serię FlexSmart

HID Global, główny producent urządzeń kontroli dostępu, ogłosił, że poszerza serię produktów **FlexSmart**, bezstykowych czytników typu MIFARE DESFire. Wśród nowych urządzeń znajdują się bardzo wytrzymałe czytniki wyposażone w klawiaturę i przeznaczone do częstego użytku.

Rodzina bezstykowych kart ISO 14443A spełnia wymagania klienta. Znajdziemy tutaj zarówno proste czytniki HID Format MIFARE, jak i czytniki MIFARE i DESFire, w których można dowolnie ustawiać parametry.

W skład elastycznych, wysoce bezpiecznych i eleganckich bezstykowych czytników wyposażonych w klawiaturę wchodzą: FlexSmart MIFARE (model 6071), FlexSmart MIFARE (model 6072) i FlexSmart DESFire (model 6073).

Bezp. inf. HID

Firma GE Security zainstalowała na międzynarodowym lotnisku w Sharm El Sheikh w Egipcie zaawansowany system wykrywania materiałów wybuchowych

GE Security Inc., firma należąca do General Electric Co., poinformowała o sprzedaży i instalacji dwóch zaawansowanych systemów wykrywania materiałów wybuchowych na międzynarodowym lotnisku w Sharm El Sheikh w Egipcie.

Instalacja systemu **GE CTX 9000 DSi** to pierwszy przypadek wykorzystania tak zaawansowanych technologii wykrywania materiałów wybuchowych na egipskim lotnisku. Decyzja o zakupie jednego z najnowszych rozwiązań przez lotnisko w Skarm El Sheikh jest związana z troską o podniesienie bezpieczeństwa na Bliskim Wschodzie.

Wysoce zautomatyzowane systemy skanowania bagażu CTX firmy GE, oparte na technologii tomografii komputerowej, są o wiele bardziej skuteczne niż standardowe systemy prześwietlania promieniami Roentgena. Bagaż pasażera, przesuwając się po pasie transportowym, przechodzi przez maszynę, która w pierwszej kolejności tworzy rentgenowski obraz projekcyjny. Następnie wbudowane w system GE CTX 9000 DSi algorytmy komputerowe analizują obrazy oraz porównują właściwości wykryte przez tomograf komputerowy z parametrami znanych materiałów wybuchowych. Jeżeli dane do siebie pasują, system automatycznie uruchamia alarm i wyświetla obiekt na ekranie. Operator ogląda obraz, sprawdzając, czy istnieje faktyczne zagrożenie, a następnie postępuje zgodnie z ustalonymi procedurami. GE CTX 9000 DSi gwarantuje szybką odprawę bagażu i ma najwyższą przepustowość spośród systemów wykrywania materiałów wybuchowych, także tych, które zaprojektowano w sposób umożliwiający integrację z systemami zarządzania bagażem. Pas transportowy szerokości 1 m i obszerny tunel sprawiają, że rozwiązanie GE Security może skanować zarówno bagaż standardowych rozmiarów, jak i bagaż niewymiarowy.

Dzięki łatwości obsługi i konserwacji oraz niskiemu współczynnikowi fałszywych alarmów system CTX 9000 DSi jest znakomitą inwestycją dla portów lotniczych o dużym natężeniu ruchu. Architektura systemu obejmuje modularne komponenty, które ułatwiają rozbudowę i serwis skanera.

– *Sharm El Sheikh to jedno z najpopularniejszych miejsc na Bliskim Wschodzie. Dlatego też jednym z naszych celów jest wyposażenie tego lotniska w najnowsze i najlepsze technologie bezpieczeństwa. Dzięki instalacji dwóch najnowocześniejszych systemów GE CTX 9000 zapewniamy pasażerom najlepszą dostępną technologię skanowania bagażu* – powiedział inż. Tarek H Zaher, szef działu inżynierii mechanicznej i przemysłu w firmie konsultingowej Dar Al-Handasah Consultant (Shair and Partners).

– *GE Security bardzo cieszy, że lotnisko w Sharm el Sheikh wybrało CTX 9000 DSi jako system wykrywania materiałów wybuchowych – jest to pierwsza tego rodzaju instalacja na lotnisku w Egipcie* – powiedział Dennis Cooke, prezes działu Homeland Protection w GE Security. – *Sharm el Sheikh wpisuje się w coraz powszechniejszy na Bliskim Wschodzie i na świecie trend korzystania z zaawansowanych technologii skanowania bagażu. Wszystko dzięki systemowi CTX 9000 DSi. Umożliwia on poprawę skuteczności i wydajności skanowania bagażu, a pasażerowie pozostają usatysfakcjonowani.*

GE CTX 9000 DSi wykorzystuje przeszło dziesięcioletnie doświadczenie firmy GE Security w konstruowaniu podobnych urządzeń. System jest wyposażony w praktyczne i innowacyjne funkcje, dzięki którym spełnia rygorystyczne wymogi lotniskowe. System jest zbudowany z modularnych komponentów, które ułatwiają rozbudowę i serwis skanera. Urządzenie zyskało certyfikat amerykańskiej Administracji Bezpieczeństwa Transportu (TSA) i jest znakomicie dostosowane do szybkiego tempa pracy, właściwego dla portów lotniczych.

Bezp. inf. GE Security

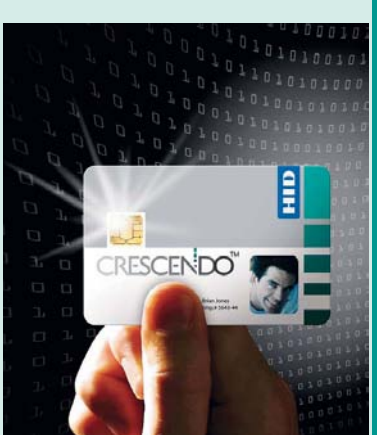
Crescendo

najnowsza seria kart inteligentnych z HID

Seria wielofunkcyjnych kart smart **Crescendo** została wprowadzona do oferty w lutym br. i obejmuje gotowe rozwiązania o wysokim stopniu bezpieczeństwa, przeznaczone dla różnych wariantów kontroli dostępu. Produkty te gwarantują najniższe na rynku koszty użytkowania zintegrowanego systemu logicznej i fizycznej kontroli dostępu. Łącząc w sobie standardową technologię zbliżeniową firmy HID – Indala, oraz iCLASS i inne technologie, w tym wykorzystujące częstotliwość 13,56 MHz (MIFARE, DESFire), Crescendo umożliwia wiele różnych zastosowań pojedynczej karty.

Standardowe karty Crescendo są dostępne w trzech wersjach, wspierających następujące standardy:

1. iCLASS i technologię zbliżeniową HID (fizyczna kontrola dostępu), połączoną z chipem kontaktowym (logiczna kontrola dostępu),
2. iCLASS i technologię zbliżeniową HID (fizyczna kontrola dostępu) z paskiem magnetycznym (inne zastosowania), połączoną z chipem kontaktowym (logiczna kontrola dostępu),
3. MIFARE (fizyczna kontrola dostępu) w połączeniu z chipem kontaktowym (logiczna kontrola dostępu).



– *Klienci firmy HID już dawno zgłaszali zapotrzebowanie na produkt charakteryzujący się łatwością implementacji, użytecznością dla logicznej i fizycznej kontroli dostępu oraz walorami ekonomicznymi* – stwierdził Troy S. Dunson, nowo mianowany starszy inżynier sprzedaży w HID Global.

– *HID łączy innowacyjne technologie, przemyślane usługi, nasze doświadczenie oraz zrozumienie potrzeb klientów, tworząc zabezpieczenia, którym można zaufać* – podkreśla Debra Spitler, wiceprezes HID Connect.

Bezp. inf. HID

Dyskretna ochrona danych

Firma **3M** stworzyła filtr na monitor komputera, dzięki któremu dane wyświetlane na ekranie widzi tylko użytkownik siedzący na wprost monitora, nie zaś osoby postronne. Dzięki systemowi mikrożaluzji siedzący z boku nie mogą podejrzeć, co znajduje się na ekranie – widzą jedynie czarny ekran, bo filtr ogranicza pole widzenia do 60 stopni. Innowacyjne i proste w działaniu rozwiązanie pozwala zachować poufność informacji w trakcie służbowej podróży, negocjacji biznesowych lub w punktach obsługi klienta. Jak wynika z badań, niezabezpieczony laptop to dla firm i instytucji duże ryzyko. Ponad połowa przypadków kradzieży danych dotyczy ich utraty z laptopa. Utrata danych wprost z laptopa była też przyczyną trzech z pięciu największych katastrof informacyjnych w 2006 roku. W sumie dane straciło 13,7 milionów klientów, a firmy, którym skradziono dane, straciły reputację. Nic dziwnego, że organizacje gorączkowo szukają zabezpieczeń dla swoich danych.

Filtr prywatyzujący 3M chroni je przed wyciekiem wprost z ekranu służbowych komputerów.

Bezp. inf. 3M Poland

Routery CISCO bezpieczne

dzięki nowemu portowi komunikacyjnemu w UPS-ach Lieberta

Nowe rozwiązania w UPS-ach Lieberta otrzymały prestiżowy certyfikat bezpieczeństwa Cisco Systems. Bezprzerwowe zasilacze Emerson Network Power to najwyższa jakość i unikatowa technologia, dzięki której routery powiadamiane są o minimalnym poziomie baterii w UPS-ie. Umożliwia to wydzielony port komunikacyjny, który posiada separację galwaniczną, a tym samym zabezpieczony jest przed awariami na skutek usterki elektrycznej.

Podstawowe zabezpieczenia systemów IT, które muszą istnieć, by można było mówić o bezpieczeństwie fizycznym sieci, obejmują ochronę na wypadek przerwy w dostawie prądu i ewentualnych wahań napięcia. Implikuje to wymóg efektywnej komunikacji pomiędzy gwarantującymi ciągłość przepływu prądu zasilaczami bezprzerwowymi (UPS-ami) oraz infrastrukturą IT. Może się zdarzyć, że przerwa w dostawie prądu jest dłuższa niż okres działania baterii w chroniącym router UPS-ie, wówczas podłączone urządzenia muszą być zasilane w prąd, aż do momentu gdy zmagazynowane dane zostaną zapisane, a wszystkie aplikacje zamknięte. Router skonfigurowany jest tak, aby po odebraniu sygnału wysłać na port pomocniczy polecenie zamknięcia wszystkich otwartych aplikacji, ale dopiero po uprzednim zachowaniu w pamięci danych. W efekcie wyłączenie zasilania nie powoduje uszkodzeń ani utraty informacji.

Rozwiązanie Lieberta jest unikatowe, ponieważ wspomniany sygnał wysyłany jest przez specjalnie zaprojektowane połączenie z separacją galwaniczną od sekcji elektrycznej UPS-a. Zapobiega to ryzyku transmisji przeciążeń bądź innych elektrycznych anomalii pochodzących z UPS-a, a mogących wpłynąć na pracę routera. Z tego względu nowatorskie rozwiązanie zastosowane w UPS-ach Lieberta uzyskało certyfikat Cisco. Inżynierowie firmy będącej światowym liderem rozwiązań sieciowych przetestowali interfejs łączący Liebert UPS z routerami Cisco i zaaprobowali go.

U konkurencji to port szeregowy przekazuje sygnał do kabla komunikacyjnego, tym samym wystawiając podłączony sprzęt na ryzyko przepięć lub wahań napięcia. W UPS-ach Lieberta zarówno na porcie, jak i kablu komunikacyjnym nie występują przepięcia. Przepięcie pojawia się tylko na interfejsie routera, który jest podłączony do zasilacza UPS. Urządzenie Lieberta jest zaopatrzone jedynie w napięcie z portu routera, a nie na odwrót, jak u konkurencji.

– Dzięki zastosowaniu separacji galwanicznej na porcie komunikacyjnym UPS-a wykluczyliśmy możliwość uszkodzenia urządzenia komunikującego się z zasilaczem awaryjnym, w tym przypadku routerów firmy Cisco. Zyskało to szczególne uznanie inżynierów tej firmy. Zastosowane rozwiązania mają zapewniać ciągłość i niezawodność pracy połączeń sieciowych – powiedział Cezary Gutowski, kierownik sprzedaży produktów DPG z Emerson Network Power.

Bezp. inf. Emerson Network Power

Metal Mickey w służbie ratowniczej

Kamera firmy **Forward Vision** o oznaczeniu **Mic1-400**, pieszczotliwie nazywana Metal Mickey, stosowana jest w mobilnych systemach CCTV biorących udział w działaniach ratunkowych w Wielkiej Brytanii.

Systemy te zostały zaprojektowane przez partnera Forward Vision – przedsiębiorstwo Excelerate Technology z Cardiff – i działają dzięki przenośnej antenie satelitarnej zapewniającej szerokopasmowe połączenie z siecią VPN. Innowacyjna technologia umożliwia władzom ustanowienie niezawodnego kanału komunikacji między miejscem wypadku a siedzibami organizacji koordynujących ratunek. Dwukierunkowe przekaźniki danych wysyłają informację wygenerowaną przez Mic 1-400 PTZ w formie wiadomości e-mail, przekazu wideo i za pośrednictwem telefonii głosowej. Bezpieczne szerokopasmowe łącze satelitarne pozwala na niezawodny dostęp do baz danych i aplikacji centrali – wszystko po to, aby w czasie akcji i w obliczu kataklizmów, wypadków przemysłowych, ataków terrorystycznych i awarii prądu móc nieść jak najskuteczniejszą pomoc.

Szerszy opis produktu znajdą Państwo w numerze 2/2007 czasopisma *Zabezpieczenia*, na stronie 9.

Bezp. inf. Forward Vision

Wandaloodporne oświetlenie CCTV Rayteca

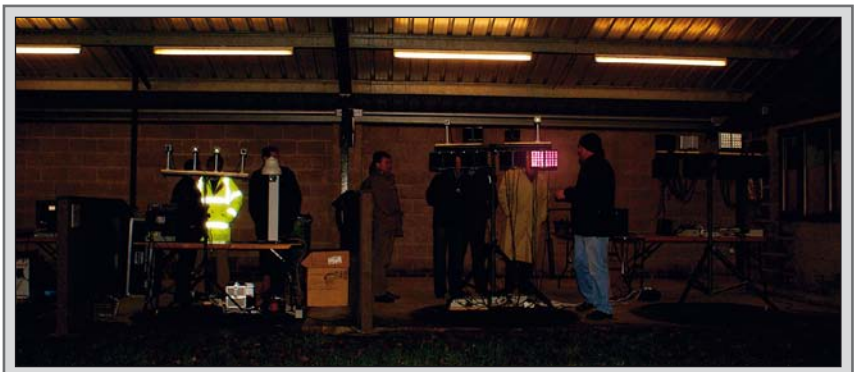
Firma **Raytec** ogłosiła, że wszystkie oświetlacze RAYMAX Infra-Red i RAYLUX White-Light są od teraz dostępne w wersji wandaloodpornej. Każdy oświetlacz wyposażony jest w poliwęglanową soczewkę, który ma za zadanie chronić go przed uderzeniami łomów, kijów bejsbolowych i kamieni, a nawet przed strzałami z wiatrówek.

Nowa poliwęglanowa soczewka standardowo jest montowana we wszystkich oświetlaczach Raytec. Soczewka ta pozwala też na zwiększenie zasięgu iluminacji i w konsekwencji zapewnia Raytecowi pozycję lidera w branży.

– *Wprowadzenie modeli wandaloodpornych jest odpowiedzią na oczekiwania klientów. Nasze urządzenia są często eksploatowane w trudnych warunkach. Nasi klienci uważali, że niezniszczalność to najważniejsza cecha tego typu produktów. Zawsze stawiamy sobie za cel stworzenie bardziej efektywnego oświetlenia dla systemów CCTV. Powstają nowe produkty, dzięki temu się rozwijamy* – mówi Shaun Cutler, dyrektor zarządzający Rayteca.

Produkty oświetleniowe firmy Raytec są wykorzystywane w ponad 35 krajach na pięciu kontynentach. Dzięki nim kamery telewizji dozorowej generują obrazy wysokiej jakości w zupełnej ciemności.

Bezp. inf. Raytec



Testowanie urządzeń CCTV w ciemnościach

Przeprowadzone niedawno nocne testy urządzeń CCTV zorganizowane przez firmę **Raytec** okazały się dużym sukcesem. Uczestnicy poznali oświetlacze ze światłem podczerwonym o zasięgu do 350 m oraz ze światłem białym o zasięgu do 200 m, wyposażone w najnowsze elementy oświetleniowe w technologii SMT LED.

Próby przeprowadzono w ciągu dwóch wieczorów w centrum testowym Rayteca, w angielskim regionie Northumberland. Wykorzystano do tego celu spowite w całkowitych ciemnościach pole golfowe o długości 350 m. Oświetlacze ze światłem podczerwonym oraz białym zainstalowano w jednej budce, w innych zamontowano kamery firm Baxall, Covi, Dallmeier, Ganz, Ikegami, Samsung, Sanyo i Vista. Goście byli zaskoczeni, widząc, jak światło podczerwone oświetla dystans do 350 m. Ponadto wielu z nich po raz pierwszy zetknęło się z profesjonalnymi oświetlaczami wykorzystującymi światło białe, pozwalającymi uzyskać doskonałe kolory w nocy.

Shaun Cutler z Rayteca podkreśla satysfakcję z wyniku przeprowadzonych testów. Jak twierdzi: „Uczestników zadziwiła odległość, na jaką nasze urządzenia działające w podczerwieni potrafią oświetlać przestrzeń, oraz jakość nagrań przy użyciu nowoczesnych systemów kamerowych. Prezentacja oświetlaczy w technologii LED ze światłem białym również stanowiła ważny punkt programu".

Aby zarezerwować sobie miejsce podczas następnych nocnych testów oraz w celu zamówienia publikacji Raytec Product Guide 07, prosimy wysłać e-mail na adres sales@rayteccctv.com.

Bezp. inf. Raytec

laserem na lotniskach

Od czasu zamachu z 11 września 2001 roku zintensyfikowano działania mające na celu poprawienie bezpieczeństwa lotów – przede wszystkim te związane z odprawą pasażerów. Pozwalają one na sprawdzenie, czy pasażerowie nie mają przy sobie broni.

Firma **Terahertz Microelectronics** stworzyła pierwsze na świecie **terahercowe urządzenie nadawczo-odbiorcze** wielkości monety. Może ono być wykorzystywane **do wykrywania niebezpiecznych materiałów**, nawet tych ukrytych pod ubraniem. Technologia oparta jest na promieniowaniu terahercowym, które mieści się między mikrofalami a falami podczerwonymi. Promieniowanie to wykorzystywane jest głównie przez radioastronomów i naukowców zajmujących się badaniem atmosfery. Pozwala ono na identyfikację związków chemicznych w mgławicach i atmosferze.

Sandia National Laboratories we współpracy z **Massachusetts of Technology** opracowuje terahercowy kwantowy laser kaskadowy. Takie urządzenia są bardzo małe i mogą generować promień lasera o mocy wyjściowej przekraczającej 100 mW. Wykorzystując tę technologię, można stworzyć przenośny skaner do prześwietlania podejrzanych pakunków.

Technologia może być wykorzystywana do wykrywania broni (także broni masowego rażenia) i materiałów wybuchowych. Obecnie brakuje jednak niezbędnej infrastruktury, koniecznej do tego, by technologię terahercową można było stosować nie tylko w laboratorium, lecz też w praktyce.

Źródło: Softpedia

Jak **nie zgubić** dzieci w supermarkecie

Dzięki systemowi **ionKids** można nie martwić się już, że zgubi się dzieci w supermarkecie albo w parku.

System składa się z jednostki bazowej (lokalizatora) z ekranem LCD oraz z bransoletek zawierających nadajniki. Bransoletki nakłada się tym, których miejsce przebywania podlega monitorowaniu. Z jednym lokalizatorem, zbliżonym wymiarami do typowych pilotów telewizyjnych, może działać do czterech nadajników. System ionKids ma zasięg ok. 60 m wewnątrz budynków i ok. 90 m na zewnątrz.

Pozwala na zdefiniowanie różnej wielkości stref dozwolonych wokół lokalizatora, co umożliwia osobie go obsługującej kontrolowanie, czy np. bawiące się dzieci, wyposażone w bransoletki z nadajnikami, nie odeszły za daleko. W takim przypadku słychać dźwięk ostrzegawczy i pojawia się dodatkowo sygnalizacja wibracyjna, a lokalizator podświetla ekran na czerwono.

Zagubionych można szybko odnaleźć, wykorzystując funkcję Search. Na ekranie lokalizatora jest widoczne koło, podzielone promieniowo na osiem równych segmentów. Jeden z nich jest wyróżniony i wskazuje kierunek, w którym należy szukać zagubionych. Pokazywana jest także odległość, w jakiej się znajdują – co prawda nie w jednostkach długości, ale w zrozumiały i wystarczająco precyzyjny sposób graficzny (znacznik w polu działania urządzenia).

Co kilka sekund zmienia się częstotliwość, na jakiej działają urządzenia systemu. Znacznie zmniejsza to możliwość nieautoryzowanego monitorowania nadajników systemu albo symulacji ich działania.

Fot. 2. Urządzenie może być również wykorzystywane do lokalizacji zwierząt

Rys. 1. Lokalizator i bransoletka z nadajnikiem

Urządzenia produkowane na rynek amerykański działają na częstotliwościach ok. 900 MHz, a wersja przeznaczona na rynek europejski – w zakresie od 868 do 869,5 MHz.

Wodoodporna bransoletka jest urządzeniem bezobsługowym. Pasek do mocowania na przegubie ręki ma regulowaną długość. Jest wyposażony w zamek zabezpieczający przed jej zdjęciem bez specjalnego klucza. W takim przypadku (a także w razie sabotażu) w jednostce bazowej włącza się alarm, który można wyłączyć.

Urządzenia ionKids są zasilane przez akumulatory litowo-jonowe, których żywotność wynosi 10 lat. Jest zapewniona sygnalizacja niskiego poziomu naładowania akumulatora – zarówno dla stacji bazowej, jak i dla bransoletki.

Dostępna jest także wersja nadajnika w postaci breloka. System ionKids z brelokiem można wykorzystać do kontroli przebywania w ustalonym miejscu np. osób w podeszłym wieku, a także do lokalizacji zwierząt.

RED.

Źródło: www.ion-kids.com

Obudowa zwiększająca bezpieczeństwo danych

Drobo firmy **Data Robotics** jest rodzajem zewnętrznej obudowy na pamięć masową. Urządzenie to pozwala na zintegrowane zarządzanie danymi na wszystkich dyskach twardych w nim umieszczonych (można zamontować do czterech).

Drobo nie wykorzystuje macierzy RAID, zamiast tego używa wirtualizacji pamięci masowej. W przeciwieństwie do RAID 5, który wymaga minimum trzech dysków twardych o takiej samej pojemności, w przypadku Drobo użytkownik może łączyć dyski o różnych rozmiarach. Ubytek pamięci masowej, związany z wirtualizacją, zależy od pojemności największego dysku. Jeśli wynosi ona 500 GB, to właśnie taka będzie maksymalna przestrzeń utracona w celu zapewnienia bezpieczeństwa danych. Przy czterech dyskach o pojemności 1 TB adresowalna przestrzeń dyskowa wynosi 3 TB (po sformatowaniu ok. 2,7 TB).

Drobo może zarządzać dowolną ilością danych, ograniczoną tyko przez system plików i pojemność dysków.

Urządzenie nie obsługuje FireWire 400/800 ani eSATA dlatego, że jest to zbędne. Wewnętrzny transfer danych nie jest wystarczająco szybki, aby mieć z tych interfejsów jakiekolwiek korzyści. Drobo może formatować dyski tylko w systemach NTFS oraz HFS (PC i Mac). Jednakże urządzenie to będzie można uaktualnić, aby wspierało inne systemy plików.

Urządzenie jest wyposażone w NVRAM (pamięć, która nie traci przechowywanych informacji po zaniku zasilania) oraz baterie, dzięki którym dane są chronione w przypadku braku prądu.

Data Robotics planuje wypuszczenie na rynek urządzeń o większej pojemności, z większą liczbą zatok na dyski twarde. Urządzenie będzie sprzedawane, bez dołączonych dysków, latem tego roku.

Źródło: Engadget

Z Czesławem Półtorakiem, regionalnym menedżerem sprzedaży firmy HID, rozmawia Teresa Karczmarzyk

Czesław Półtorak dołączył do firmy HID jako regionalny menedżer sprzedaży na Polskę, ale po roku stał się również odpowiedzialny za działania na Litwie, Łotwie, Węgrzech i w Estonii.

Wcześniej Czesław Półtorak pracował dla ADT Poland (jedna z firm koncernu TYCO). Ma więc olbrzymie doświadczenie w zaawansowanych systemach kontroli dostępu.

Firma HID dostarcza produkty wysokiej jakości, daje dożywotnią gwarancję na większość z nich. Co więcej, dzięki sieci naszych partnerów i programowi HID Connect, możemy zaoferować klientom dodatkowe aplikacje, które sprawiają, że nasze produkty znajdują nowe zastosowania.

Które produkty z oferty firmy HID udało się wprowadzić na polski rynek od czasu, gdy pracuje Pan dla tej firmy?

Moim głównym celem było spopularyzowanie nowej technologii iCLASS, a ostatnio również wprowadzenie – za pomocą programu HID Connect – produktów z serii VertX.

Jakie produkty zadebiutowały w ostatnim czasie?

Bezdotykowe czytniki kart inteligentnych FlexSmart serii MIFARE oraz DESFire.

Produkty te stanowią gotowe rozwiązania dla klientów poszukujących czytników z możliwością dopasowania do konkretnych zastosowań. Nowa, otwarta architektura czytników uzupełnia uznaną linię produktową HID o nazwie iCLASS, jasno podkreślając dążenie firmy do promowania technologii 13,56 MHz. Biorąc pod uwagę wszystkie produkty, mamy do czynienia z najszerszą w branży ofertą komponentów do obsługi kart działających w otwartym standardzie, dostępnych u przeszło 40 000 dilerów na całym świecie.

Jakie korzyści dla klientów niesie wykorzystanie produktów HID?

Firma HID dostarcza produkty wysokiej jakości, daje dożywotnią gwarancję na większość z nich. Co więcej, dzięki sieci naszych partnerów i programowi HID Connect, możemy zaoferować klientom dodatkowe aplikacje, które sprawiają, że nasze produkty znajdują nowe zastosowania.

Jakie główne cechy wyróżniają technologię iCLASS?

Proponowana przez HID technologia odczytu/zapisu kart bezdotykowych iCLASS 13.56, wraz z produktami firm partnerskich, pozwala zbudować różnorodne systemy zapewniające między innymi identyfikację biometryczną, sprzedaż bezgotówkową czy bezpieczny dostęp do sieci teleinformatycznych.

Jak iCLASS wpisuje się w cele polskiego oddziału firmy?

Urządzenia iCLASS dzięki swojej zaawansowanej technologii są odpowiednie do budowy wielu różnorodnych rozwiązań. Polskie firmy wykazują duże zainteresowanie wykorzystywaniem produktów iCLASS nie tylko w standardowych systemach kontroli dostępu, lecz także do identyfikacji biometrycznej, sprzedaży bezgotówkowej, programów lojalnościowych i wielu innych zastosowań.

Co to jest HID Connect?

HID Connect ma sprawić, że użytkownicy naszych produktów będą mogli robić z nimi dużo więcej, niż tylko otwierać nimi drzwi. Aplikacje rozwijanie obecnie obejmują kontrolę obecności pracownika i czasu pracy, bezpieczne logowanie do sieci teleinformatycznych, sprzedaż bezgotówkową, identyfikację biometryczną, kontrolę parkowania, uzbrajanie/rozbrajanie paneli alarmowych oraz systemy komunikacyjne.

Jakie projekty zostały już zrealizowane za pomocą HID Connect?

Na dziś zrealizowano jeden duży projekt, kontrolowany w pełni przez jednego z naszych partnerów biznesowych.

Jaka firma jest oficjalnym partnerem programu HID Connect w Polsce?

HID kooperuje z firmą VEMCO – naszym oficjalnym partnerem. Przedsiębiorstwo to rozwija nowe aplikacje, wspierając między innymi urządzenia serii VertX.

Jakie korzyści dla partnerów niesie program HID Connect?

W zależności od poziomu współpracy partnerzy odnoszą korzyści z udziału w programie HID Connect przez liczne promocje korporacyjne – obecność na stoiskach targowych HID, udział w seminariach tematycznych, reklamie korporacyjnej i w innych formach wsparcia marketingowego oraz rozwojowego.

Jak HID zamierza wychodzić naprzeciw wymaganiom klientów w roku 2007?

Budując jeszcze silniejsze więzy z nabywcami produktów i partnerami biznesowymi oraz odwiedzając klientów tak często, jak to tylko możliwe, aby zapewnić im stałą, pełną satysfakcję.

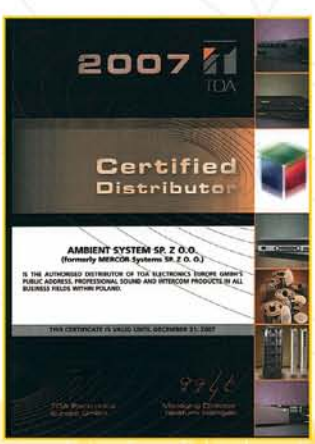
Dziękuję za rozmowę.

ambient SYSTEM
DAWNIEJ MERCOR SYSTEM

Precyzyjne wykonanie
Wszechstronne zastosowanie
Niezawodne funkcjonowanie

TOA

Ambient System Sp. z o.o. (dawniej Mercor System Sp. z o.o.) oferujący na rynku polskim dźwiękowy system ostrzegawczy MCR-Venas oraz głośniki pożarowe serii MCR-S przedstawia na bazie partnerskiej współpracy z japońską firmą TOA system Public Address Venas - seria VM-2000.



- Zintegrowany System Wielostrefowy;
- Opcjonalnie jednostki wzmacniaczy VM-2120 (moc 120 W) lub VM-2240 (moc 240 W);
- W każdej jednostce 5 przełączanych wysoko impedancyjnych linii głośnikowych z indywidualną regulacją wzmocnienia;
- Możliwość łączenia 9 jednostek w celu zwiększenia mocy wyjściowej i ilości linii (do 45 linii);
- 4 kanały wejściowe z regulacją wzmocnienia i korekcją tonów basu/sopranu na panelu frontowym;
- 2 wejścia BGM z regulacją poziomu;
- 3 wejścia mikrofonowe/liniowe oraz wejście telefoniczne;
- Możliwość podłączania do 4 mikrofonów zdalnych;
- Całkowita odległość między mikrofonami do 800 metrów;
- Opcjonalnie funkcje monitorowania m.in. linii głośnikowych (przerw, doziemień), wzmacniacza mocy, z wizualną sygnalizacją awarii oraz możliwością podania informacji o awarii na wyjścia sterujące systemu;
- 2 wiadomości ostrzegawcze, 5 komercyjnych oraz 1 gong (wszystkie wcześniej nagrane);

AUTORYZOWANY DYSTRYBUTOR TOA:

AMBIENT SYSTEM Sp. z o.o, ul. Sucha 25, 80-531 Gdańsk, tel./fax +48 58 345 51 95, 344 45 95,
sekretariat@ambientsystem.pl, www.ambientsystem.pl

EIB

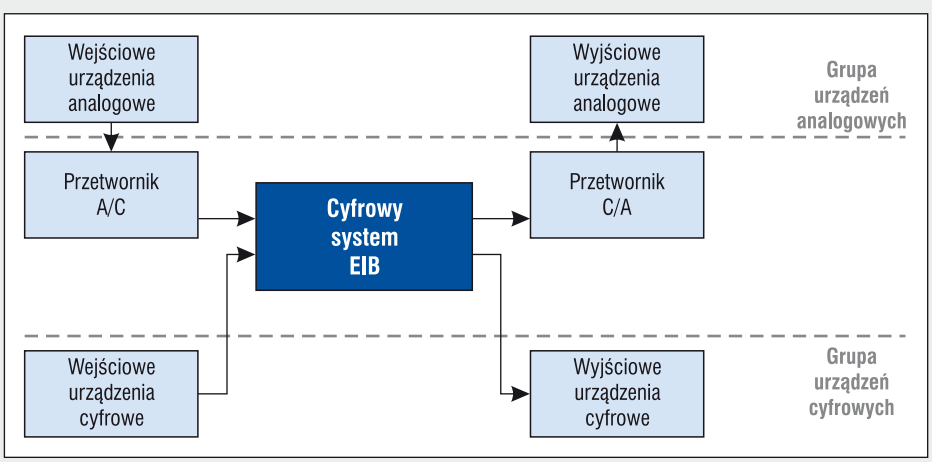
rozproszony system zarządzania budynkiem

Rozpoczynamy cykl artykułów na temat Europejskiej Magistrali Instalacyjnej (ang.: *European Installation Bus*, EIB). Jest to technologia wykorzystywana najczęściej w zastosowaniach innych niż elektroniczne systemy bezpieczeństwa, głównie ze względu na jej otwarty charakter. Choć w wielu przypadkach nie gwarantuje to wystarczającego stopnia zabezpieczenia przed nieautoryzowaną ingerencją, to jednak umożliwia zarządzanie systemami, związanymi z ochroną życia i mienia w budynkach.
Część pierwsza artykułu pozwoli PT Czytelnikowi na usystematyzowanie wiadomości o systemie EIB i zasygnalizuje możliwości zastosowań tego wygodnego i mającego wiele zalet rozwiązania. W części drugiej zostaną omówione stosowane w tym systemie urządzenia, a w kolejnej – zagadnienia, związane z wzajemną komunikacją pomiędzy nimi. Część ostatnia będzie poświęcona zastosowaniom EIB w praktyce

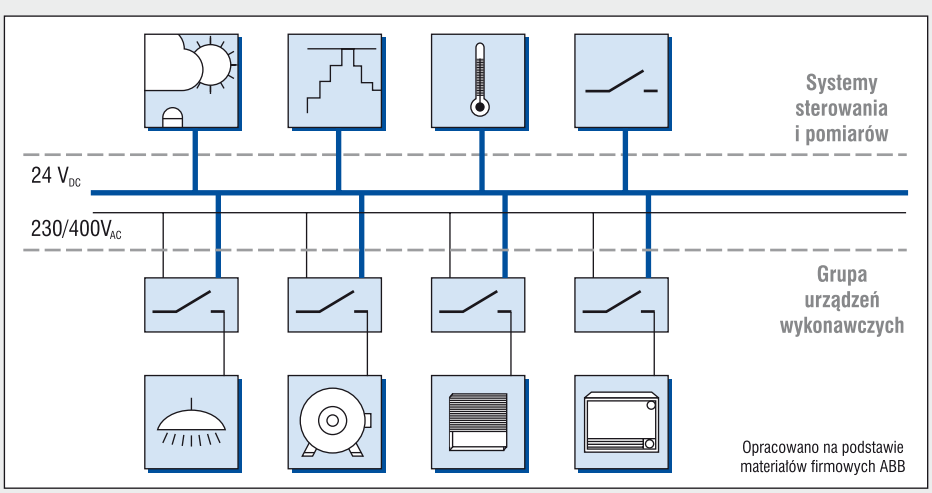
CZĘŚĆ 1. Topologia i obszary zastosowań systemów EIB

Wprowadzenie

Tradycyjny system EIB jest cyfrową rozproszoną technologią czasu rzeczywistego, w której stan procesu jest próbkowany w dyskretnych przedziałach czasu, a sam proces jest sterowany w określonych chwilach. Technologia ta obsługuje zarówno sygnały analogowe, czyli ciągłe, jak i cyfrowe. Sposób wykorzystywania sygnałów w systemie EIB pokazano schematycznie na rys. 1. Sygnały analogowe występują głównie po stronie czujników, czyli urządzeń przetwarzających wielkość mierzoną, np. temperaturę lub natężenie światła, na inną, a w systemie EIB na sygnał elektryczny. Dodatkowo występują po stronie sterownia urządzeniami wykonawczymi, np. silnikami lub siłownikami elektrycznymi. Urządzenia wykorzystujące sygnały analogowe wyposażone są w przetworniki A/C lub C/A w zależności od kierunku wykorzystania sygnału. Na to, jakie rodzaje sygnałów dominują w systemie, ma wpływ konkretne rozwiązanie techniczne.



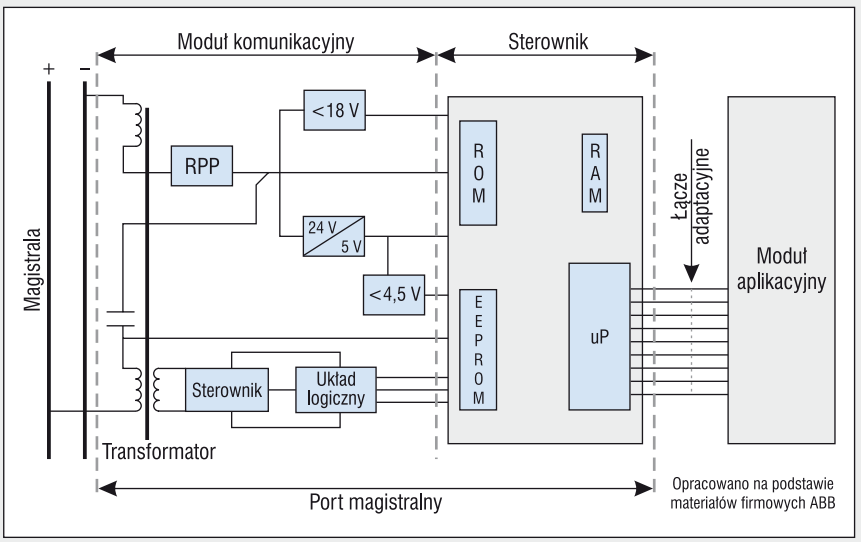
Rys. 1. Sposób wykorzystywania sygnałów fizycznych w systemie EIB



Rys. 2. Idea rozdziału w technologii EIB systemu zasilania elektroenergetycznego urządzeń wykonawczych (dolna warstwa) od systemów sterowania i pomiarów (górna warstwa)

Biorąc pod uwagę współczesne sieciowe systemy komputerowe typu serwer–klient, system EIB można uznać za złożony z samych klientów. Klient w systemie EIB nie tylko oczekuje na usługi ze strony sieci, ale sam dostarcza określone usługi. Nie ma nigdzie ani jednego komputera lub sterownika pełniącego rolę serwera z zamówionymi usługami.

System EIB wykorzystuje do wymiany informacji między urządzeniami własny, znany powszechnie protokół komunikacji EIB. System EIB został opracowany i wprowadzony głównie do automatycznego sterowania różnymi urządzeniami



Rys. 3. Schemat blokowy portu magistralnego EIB

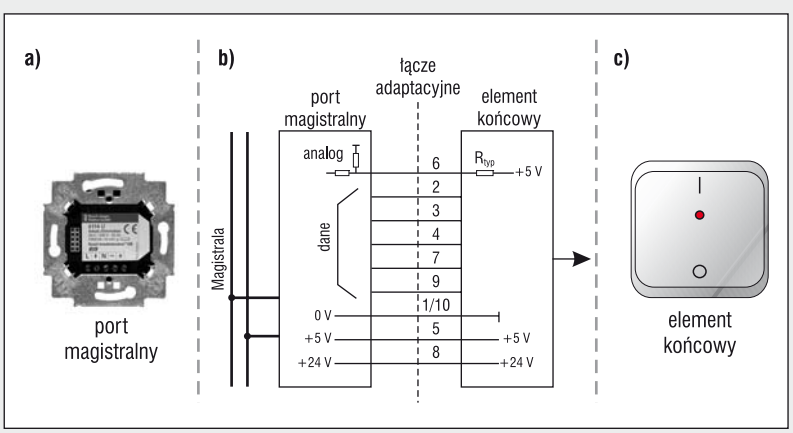
w budynkach. Podstawowym założeniem było oddzielenie obwodów zasilania elektroenergetycznego urządzeń od ich obwodów pomiarowych, kontrolnych, regulacyjnych i sterowania. Idee tego rozdziału pokazano na rys. 2., gdzie linia gruba 24 V_{DC} pokazuje magistralę systemu sterowania, a linia cienka 230/400 V_{AC} linię zasilania elektroenergetycznego.

W systemie tym odstąpiono od wymagań typowych dla systemów czasu rzeczywistego na korzyść niezawodności i dostępności urządzeń do medium komunikacyjnego, jakim jest magistrala. Magistrala jest tu rozwiązaniem topologicznym umożliwiającym komunikowanie się elementów między sobą. System EIB nie jest szybki, przetwarza w procesie komunikacji około 10 kb/s. Wybrany został sposób asynchronicznej transmisji informacji w systemie z metodą dostępu do magistrali typu CSMA/CA (ang.: *Carrier Sense Multiple Access with Collision Avoidance*), czyli z unikaniem kolizji. Każdy uczestnik w procesie komunikacji z magistralą ma przydzielony priorytet ważności. W momencie równoczesnej próby nadawania do magistrali przez dwóch użytkowników ten z niższym priorytetem musi poczekać na zwolnienie sieci. W sytuacji gdy dwóch użytkowników o tym samym priorytecie próbuje nawiązać łączność z magistralą, z pomocą przychodzi niepowtarzalny tzw. adres fizyczny użytkownika lub urządzenia. Adres fizyczny określa rzeczywiste położenie elementu w systemie podłączeń do magistrali. Użytkownik z wyższym adresem fizycznym musi udostępnić magistralę. Magistrala w systemie EIB pełni podwójną rolę; zasila urządzenia napięciem bezpiecznym 24 V_{DC} typu SELV (ang.: *Safety Extra Low Voltage*) oraz zapewnia komunikację cyfrową urządzeń.

EIB jest systemem otwartym z rozproszoną inteligencją, wykorzystującym zdecentralizowany sieciowy system operacyjny. Strukturę zdecentralizowaną uzyskano przez wyposażenie wszystkich elementów realizujących komunikację w mikroprocesory. Każde urządzenie systemu jest małym komputerem mającym własną aplikację i łączność z siecią systemu EIB. Głównym elementem urządzenia EIB jest tzw. port magistralny, który można uważać za jednostkę inteligentną. Port jest wyposażony w jednostkę procesorową CPU, pamięci: ROM, RAM, EEPROM, interfejsy: użytkownika i komunikacji z siecią. Schemat blokowy portu magistralnego pokazano na rys. 3. i 4. Pamięć ROM jest przeznaczona tylko do odczytu i zawiera oprogramowanie systemowe wpisane tam przez producenta. Pamięć RAM wykorzystuje się do przechowywania przetwarzanych chwilowych wartości systemu i aplikacji. W przypadku zaniku zasilania wartości te są tracone. Pamięć EEPROM, która jest elektrycznie zapisywalną i kasowalną pamięcią, służy do przechowywania aplikacji elementu, jego adresu fizycznego i grupowego, co zostanie dalej szczegółowo omówione.

Port magistralny EIB pod względem funkcjonalnym można podzielić na dwa moduły: moduł komunikacji z magistralą i moduł sterownika (rys. 3.). Moduł komunikacji jest zarządzany przez sterownik z jednym procesorem, dlatego też prędkość transmisji danych w systemie EIB jest raczej mała. Moduł komunikacji w porcie magistralnym wykonuje następujące funkcje:

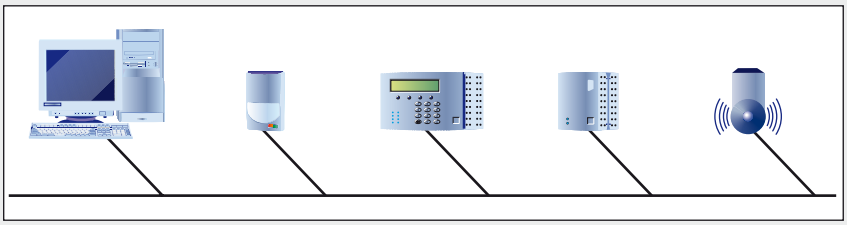
a) steruje procesem wysyłania i odbioru danych z magistrali,
b) oddziela stałe napięcie zasilania magistrali od cyfrowych strumieni danych,
c) wytwarza napięcia stabilizowane 5 V_{DC} i 24 V_{DC} do zasilania obwodów portu magistralnego,
d) chroni port magistralny przed omyłkową zmianą polaryzacji napięcia zasilania na magistrali,
e) rozpoczyna zabezpieczania danych aplikacyjnych, jeżeli napięcie na magistrali spadnie poniżej 18 V_{DC},
f) uruchamia reset procesora, jeżeli napięcie w module komunikacji spadnie poniżej stabilizowanego napięcia 4,5 V_{DC},



Rys. 4. Rzeczywiste połączenie portu magistralnego z magistralą EIB i z elementem końcowym, gdzie:
a) port magistralny w wykonaniu podtynkowym;
b) port magistralny z elementem końcowym połączonym poprzez łącze adaptacyjne (interfejs użytkownika);
c) element końcowy, tutaj przycisk jednokanałowy

g) sprawdza poprawność przesyłanych telegramów, czyli wydzielonych porcji danych.

Znajdujący się w module komunikacyjnym transformator pełni rolę filtru oddzielającego napięcie przemienne niosące informację od napięcia stałego zasilającego magistralę. Port magistralny rozróżnia dołączany moduł aplikacyjny po charakterystycznym dla rozwiązania technicznego spadku napięcia na rezystancji R_{typ} (rys. 4.).



Rys. 5. Rozwiązanie magistrali w systemie EIB

Każdy element systemu EIB może komunikować się z dowolnym innym bezpośrednio, bez udziału jednostki centralnej nadzorującej. To jest cecha podstawowa systemu zdecentralizowanego. System EIB nazywany jest też inteligentnym, ponieważ może manipulować informacją znajdującą się w jego układach elektronicznych. Można ten rodzaj inteligencji nazwać techniczną.

Ogólnie system EIB zaliczany jest do tzw. otwartych systemów sterowania. O tym, czy dany system automatycznego sterowania można zaliczyć do otwartego, można się przekonać, analizując urządzenia, protokoły komunikacyjne, oprogramowanie systemowe, narzędziowe i użytkowe zastosowane w tym systemie.

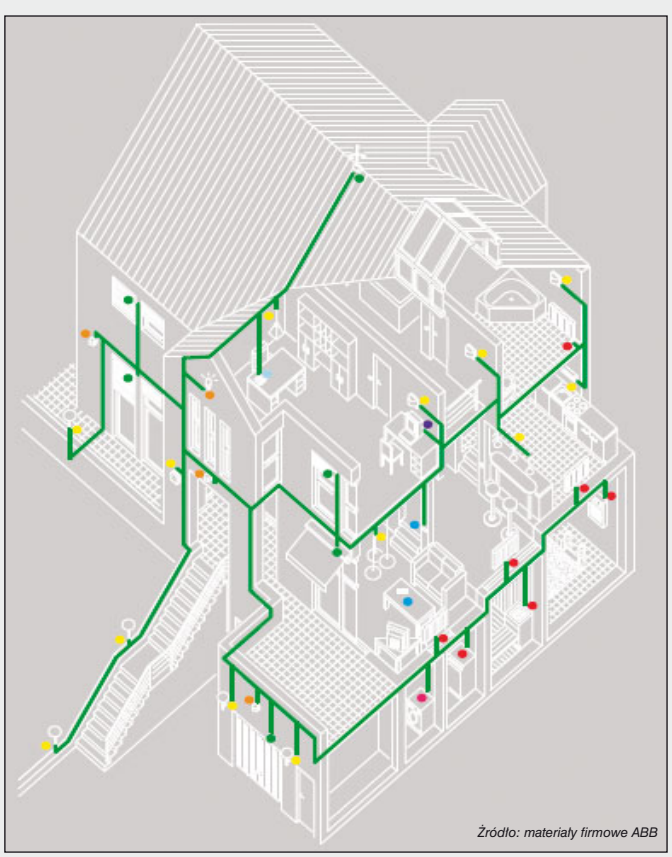
Według powyższych wskazówek system EIB jest systemem otwartym, ponieważ ma wymienione poniżej cechy charakterystyczne.

– Urządzenia wykorzystywane w systemie EIB pochodzą od różnych producentów, ale mogą ze sobą współpracować, a to dzięki przyjęciu pewnych standardów urządzeń i funkcji oraz istnieniu wielu producentów podobnych funkcjonalnie urządzeń spełniających ustalone założenia. Przez standard rozumie się pewien zestaw parametrów urządzenia, które zapewniają jego prawidłowe działanie, poziom jakości i niezawodności i co najważniejsze, prawidłową współpracę urządzeń przez stosowanie tego samego protokołu komunikacji. Urządzenia z logo EIB są kompatybilne. Aby urządzenie uzyskało logo EIB, musi zostać poddane procesowi certyfikacji pod patronatem organizacji i certyfikowanych laboratoriów EIBA. Producenci urządzeń, których jest ponad stu, skupieni są w organizacji EIBA (ang.: *European Installation Bus Association*).
– Urządzenia komunikują się za pomocą jawnego, powszechnie dostępnego standardowego protokołu. Wykorzystywane są też standardowe media komunikacyjne, jak np. TP – skrętka miedziana, światłowód, sieci elektroenergetyczne lub fale radiowe.
– Stosowane oprogramowanie narzędziowe i systemowe jest powszechnie dostępne, często pochodzi od wielu niezależnych producentów. Natomiast oprogramowanie użytkowe może być tworzone przez firmy niezależne od producenta lub dostawcy systemu. Możliwe są zmiany i edycja oprogramowania aplikacyjnego bez konieczności zatrzymywania pracy systemu.
– Urządzenia wykonawcze (siłowniki lub silniki) i czujniki z podstawowej warstwy zarządzania obiektem mogą pochodzić od różnych producentów. Charakterystyki pracy czujników mogą być konfigurowane przez użytkownika systemu.

Topologia Systemu EIB

Topologia w systemach technicznych oznacza połączenie urządzeń w celu umożliwienia przesyłania sygnałów między nimi. Sygnały mogą być analogowe lub cyfrowe. Sygnałami analogowymi są np. prądy przepływające między połączonymi przewodami elementami w sieciach elektrotechnicznych. Jednak techniczne określenie topologii najbardziej związane jest z sieciami cyfrowymi. W systemach cyfrowych można nawet wydzielić zagadnienia topologii fizycznej i logicznej. Topologia fizyczna dotyczyć będzie realnych „fizycznych" połączeń między urządzeniami za pomocą różnych mediów komunikacyjnych. Do najbardziej popularnych rozwiązań topologii fizycznej należą połączenia w gwiazdę, pierścień, magistralę i drzewo. Najczęściej stosowane są połączenia kablowe wykonane przewodami miedzianymi o wymaganej kategorii lub (coraz częściej) przewodami światłowodowymi. Jako media komunikacyjne można także wykorzystać kanały transmisji radiowej, podczerwień lub przewody elektroenergetyczne.

Topologia logiczna opisuje procedury komunikowania się wybranych logicznie urządzeń w systemie już skonfigurowanym w określonej topologii fizycznej. W topologii logicznej urządzenia udostępniają sobie nawzajem informację. Topologia



Rys. 6. Rozchodząca się po budynku magistrala przypomina z wyglądu drzewo

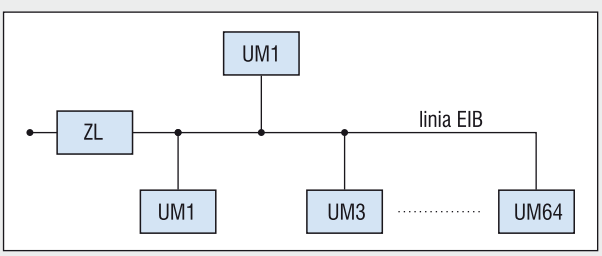
logiczna tworzy grupy urządzeń współpracujących nawzajem w jakimś konkretnym celu, np. w systemie EIB w celu regulacji oświetlenia typu załącz/wyłącz.

W systemie EIB topologię fizyczną zapewnia magistrala komunikacyjna – w postaci przewodu miedzianego typu skrętka ekranowana, np. 2 x 0,8 m^2. Do magistrali podłączone jest każde urządzenie (klient) EIB, przez co magistrala pełni rolę fizycznego łącza, tak jak to widać na rys. 5.

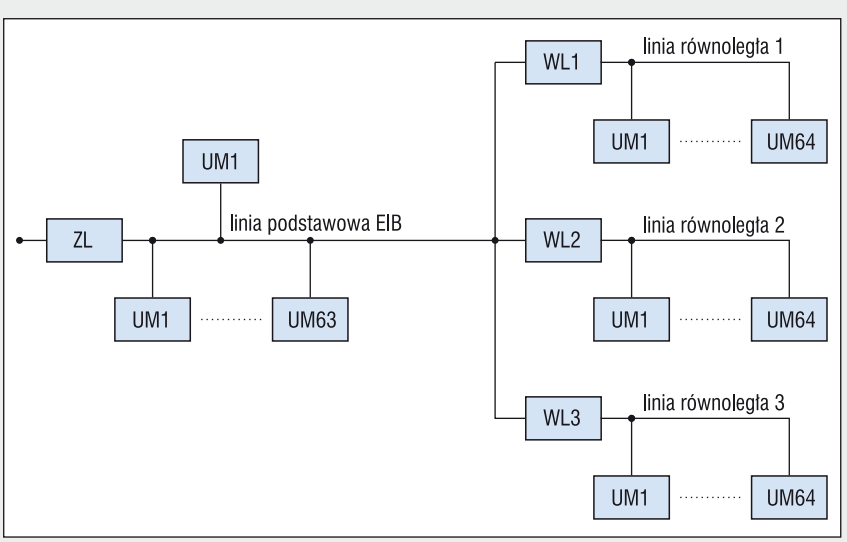
Magistrala jest łatwa do instalowania w budynkach i tworzy topologicznie strukturę rozgałęzionego drzewa, pnąc się kolejno przez pomieszczenia i piętra, co pokazano na rys. 6. Jest przeważnie przewodem miedzianym, dlatego musi mieć ograniczoną długość, głównie ze względu na tłumienie sygnałów elektrycznych przesyłanych między najodleglejszymi urządzeniami.

W początkowym okresie istnienia system EIB był przeznaczony do sterowania, w najbardziej ogólnym podejściu, całościowo oświetleniem budynków, włączając w to również sterowanie żaluzjami. Z tego powodu jego topologia przypomina rozwiązania konstrukcyjne budynku. Jak wiadomo, budynek ma w swoim wnętrzu piętra, na piętrach pomieszczenia o różnym przeznaczeniu. Dlatego w topologii EIB występuje element podstawowy, czyli linia z podłączonymi do niej urządzeniami, odpowiadająca podłączeniom wszystkich urządzeń, np. w pokoju, do magistrali. Każda linia musi być wyposażona we własny zasilacz o mocy odpowiadającej zapotrzebowaniu energetycznemu urządzeń w niej.

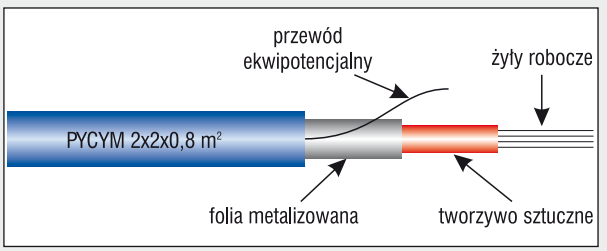
Najmniejsza linia składać się będzie z zasilacza, urządzenia sterującego wysyłającego polecenia do magistrali oraz z urządzenia wykonawczego, które te polecenia wykona. Budowę linii EIB pokazano na rys. 7.



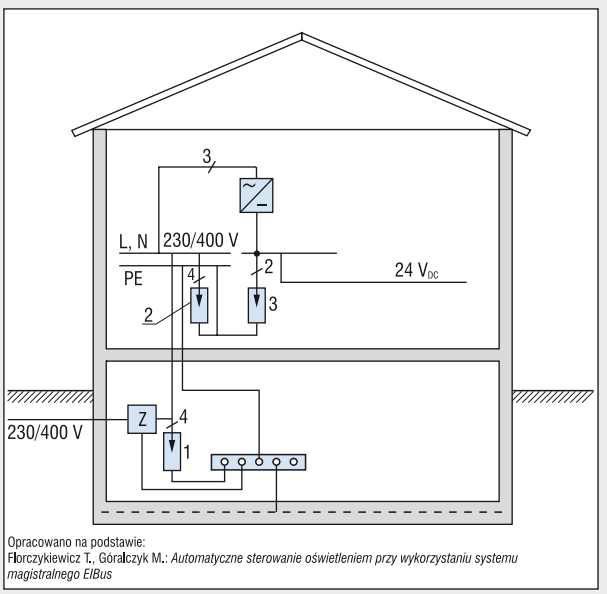
Rys. 7. Budowa linii EIB jako elementu podstawowego systemu, gdzie:
ZL – zasilacz linii,
UMx – urządzenie magistralne o numerze x



Rys. 8. Możliwość zwiększenia liczby elementów magistralnych w linii przez dodanie linii równoległych, gdzie WLx – wzmacniacz linii o numerze x



Rys. 9. Kabel magistrali systemu EIB

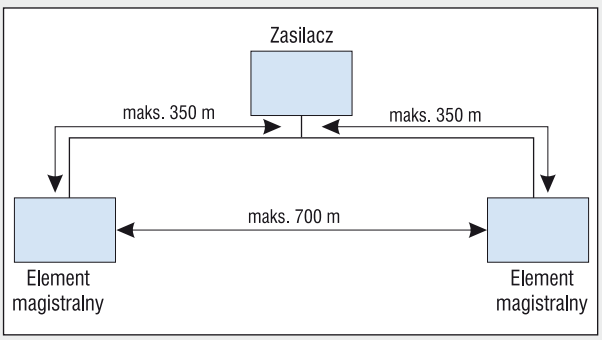


Opracowano na podstawie:
Florczykiewicz T., Góralczyk M.: *Automatyczne sterowanie oświetleniem przy wykorzystaniu systemu magistralnego EIBus*

Rys. 10. Ochrona przeciwprzepięciowa instalacji systemu EIB, gdzie:
Z – złącze,
1 – ograniczniki przepięć klasy B,
2 – ograniczniki przepięć klasy C,
3 – ograniczniki przepięć klasy D o poziomie ochrony niższym niż 350 V,
4 – iskiernik

Z punktu widzenia łatwości i szybkości dostępu do magistrali istnieje ograniczona liczba urządzeń pracujących na jednej linii. W systemie EIB można podłączyć w ten sposób 64 urządzenia. Jeżeli jednak istnieje konieczność dołączenia większej liczby elementów do linii, można na jej końcu dodać maksymalnie trzy linie równoległe, jak to pokazano na rys. 8. W linii podstawowej można wtedy umieścić tylko 63 elementy magistralne, a 64. (ostatnim) elementem staje się umieszczony na początku każdej linii równoległej tzw. wzmacniacz liniowy. Wzmacnia on i powtarza sygnał cyfrowy, nie powodując filtracji.

Stosowany przewód magistralny linii ma rezystancje 72 Ω/km i pojemność 0,12 μF/km. Fabrycznie podwójnie izolowany przewód wyposażany jest w cztery żyły, dwie robocze, a dwie zapasowe, jak widać na rys. 9.



Rys. 11. Zalecany sposób umieszczania zasilacza w linii magistrali

Przewód magistralny powinien być chroniony od przepięć za pomocą ochronników podłączonych do przewodów ochronnych, tak jak to pokazano na rys. 10. Kabel magistralny jest również przewodem zasilającym system EIB. Jest to sieć niskiego napięcia typu SELV, zasilana z transformatora bezpieczeństwa, mająca podwójną izolację i charakteryzująca się brakiem połączeń z przewodami ochronnymi.

Rozproszona rezystancja przewodu linii powoduje przy jej znacznych długościach tłumienie przesyłanego sygnału. Teoretycznie sygnały informacji krążące po magistrali systemu EIB powinny mieć kształty prostokątów. Jednak ze względu na tłumiące oddziaływanie rezystancji przewodu zostają one odkształcone. Pojemność elektryczna linii wprowadza dodatkowo opóźnienia w przesyłanych sygnałach, co ma istotnie wpływa na szybkość działania systemu. Parametry RC linii magistrali ograniczają jej parametry instalacyjne. Pojemność linii ogranicza jej długość maksymalnie do 1000 m, a rezystancja maksymalną odległość między elementami magistralnymi do 700 m. W przypadku odległości do 700 m możliwe jest jeszcze wykrycie kolizji pomiędzy uczestnikami (niska wartość sygnału). Większa odległość wprowadza dodatkowo opóźnienie w przesyłaniu sygnału pomiędzy elementami magistralnymi.

Zaleca się umieszczenie zasilacza pośrodku linii, jak na rys. 11., aby przewody magistralne rozchodziły się od niego promieniście. Elementy magistralne oddalone są wtedy od zasilacza maksymalnie o 350 m, a odległość pomiędzy najdalszymi elementami wynosi nie więcej niż wymagane 700 m.

Urządzenia magistralne mogą pracować przy napięciu minimalnym 21 V, a ich pobór mocy jest rzędu 150–200 mW. W przypadku większego poboru możliwa jest praca równoległa zasilaczy. W sytuacji gdy przewód jednej linii jest długi i konieczne jest zastosowanie dwóch zasilaczy dla jednej linii, minimalna odległość pomiędzy dwoma zasilaczami to 200 m.

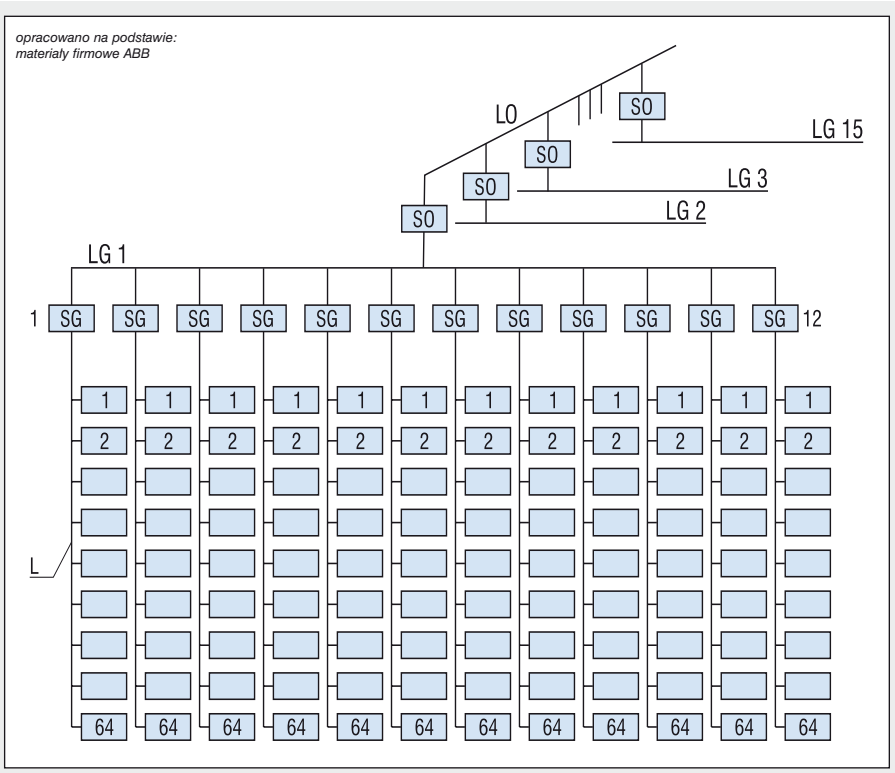
Jedna linia nie wystarczy oczywiście do zbudowania instalacji w dużym budynku, dlatego należy je łączyć, tworząc obszary odpowiadające np. połączeniom urządzeń EIB na piętrze. Obszar jest następnym pojęciem topologicznym w systemie EIB. Może teoretycznie obejmować 15 linii połączonych linią główną LGx, jak na rys. 12. Praktycznie łączy się 12 linii, tworząc jeden obszar. Każda linia, w tym główna, musi być wyposażona w zasilacz.

Zbudowane obszary łączy się ze sobą linią obszarową LO wyposażoną we własny zasilacz. Teoretycznie można zbudować 15 obszarów.

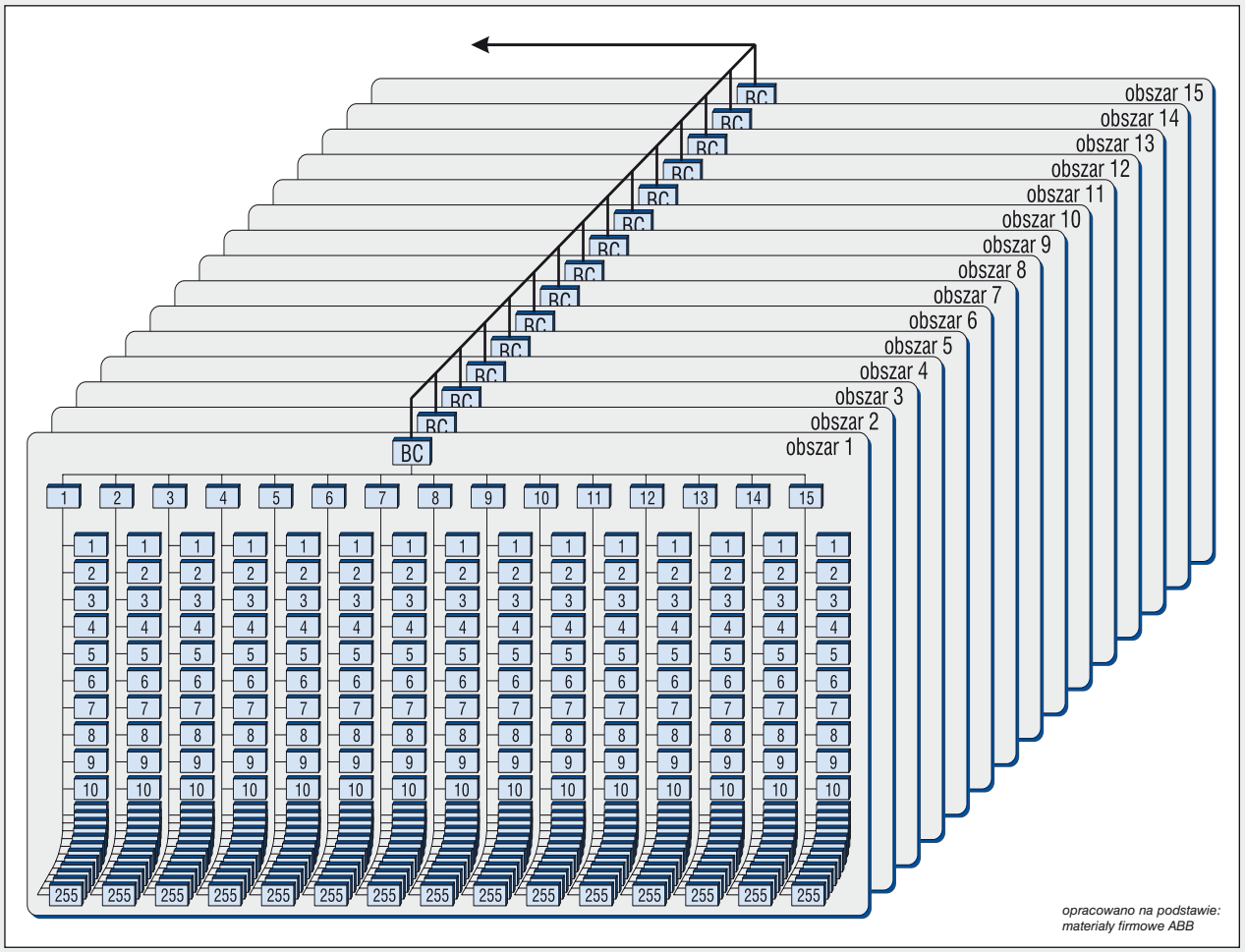
Podstawowym problemem w dużej instalacji EIB jest ograniczenie rozchodzenia się informacji po systemie, co może powodować dodatkowe opóźnienia w działaniu. Telegram, czyli informacja wysłana z urządzenia nadającego, powinna dotrzeć do konkretnego urządzenia odbiorczego jak najkrótszą drogą. Aby uporządkować ruch na magistralach w rozbudowanych systemach EIB, wprowadzono tzw. sprzęgła. Sprzęgło pełni rolę filtru, który przepuszcza tylko uprawnioną informację w żądanym kierunku.

W systemie EIB występują sprzęgła liniowe oraz obszarowe. Sprzęgła liniowe wpuszczają lub wypuszczają informację nadawaną przez urządzenia w linii do innych linii tego samego obszaru, natomiast sprzęgła obszarowe kierują ruchem pakietów informacji między obszarami.

Sprzęgła oddzielają między sobą linie lub obszary. Biorąc pod uwagę ograniczenia dotyczące elementów w liniach oraz liczbę linii i obszarów, można określić teoretyczną liczbę urządzeń, które może obsłużyć największy możliwy do realizacji system EIB. Liczba urządzeń w systemie EIB bez rozszerzania linii podstawowych wyniesie:



Rys. 12. Topologia fizyczna sytemu EIB, gdzie:
L – linia jako element podstawowy systemu,
LGx – linia główna łącząca ze sobą linie Lx,
LO – linia obszarowa łącząca obszary, np. piętra budynku,
SG – sprzęgła w liniach,
SO – sprzęgła obszarowe



Rys. 13. Pełna topologia systemu EIB; 15 linii w obszarze i 15 obszarów (area)

$$M_1 = 64 \text{ (urządzenia w linii) x } 15 \text{ (liczba linii w obszarze) x } 15 \text{ (liczba obszarów) } = 14\,400,$$

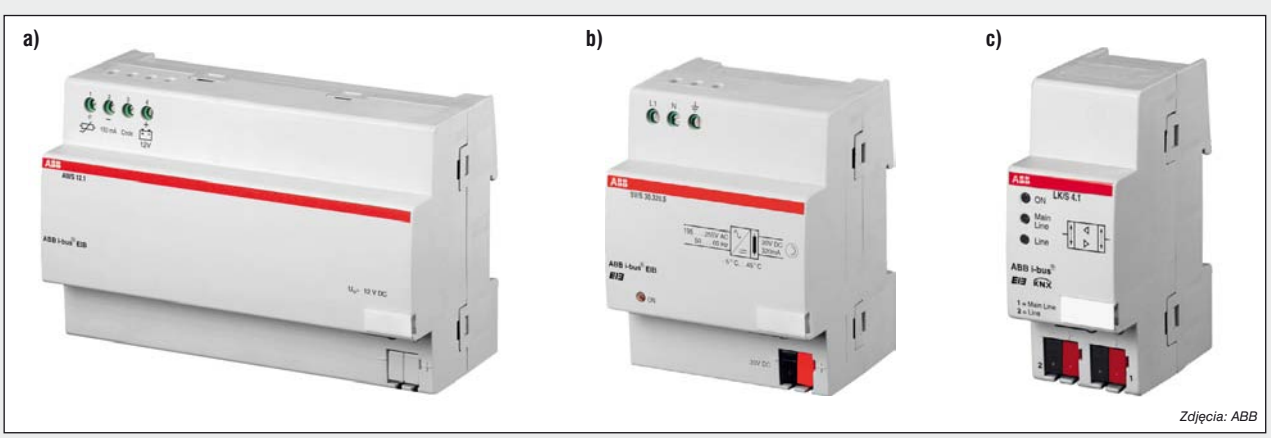
a z dodatkowymi trzema liniami równoległymi po 64 urządzenia w każdej, zgodnie z rys. 8.:

$$M_2 = (63 + 3 \text{ x } 64) \text{ (urządzenia w linii plus trzy linie równoległe) x } 15 \text{ x } 15 = 57\,375$$

W praktycznych rozwiązaniach systemów przyjmuje się mniejsze liczby urządzeń w liniach i w obszarach, głównie ze względu na umożliwienie wprowadzania przyszłych zmian, wtedy optymalna liczba urządzeń wyniesie odpowiednio:

$$N = 60 \text{ (urządzeń w linii) x } 12 \text{ (linii w obszarze) x } 15 \text{ (liczba obszarów) } = 10\,800$$

Jak widać, system EIB nie jest przeznaczony do zarządzania wielkimi budynkami, głównie ze względu na małą prędkość działania i ograniczoną liczbę urządzeń do sterowania. Jednak dzięki przyjaznemu oprogramowaniu wspomagającemu projektowanie i uruchamianie systemu jest on obecnie bardzo popularny w zarządzaniu energią elektryczną i warunkami komfortu w domach jednorodzinnych, rezydencjach i średnich budynkach.

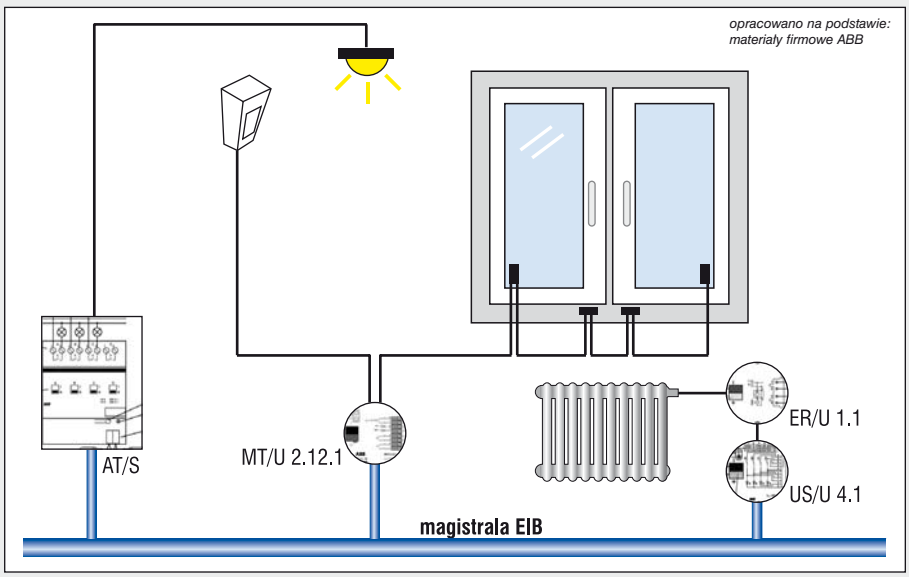


Rys. 14. Moduł baterii awaryjnej (a), zasilacz linii magistrali (b) oraz sprzęgło (c)

Możliwości zastosowania systemu EIB

Obszary możliwych zastosowań sytemu EIB wykraczają poza tradycyjne instalacje elektryczne. Dzięki rozdzieleniu obwodów zasilania w energię elektryczną od obwodów sterowania uzyskano bezpieczny, niezawodny i bogaty w funkcje zarządzające system automatycznego sterowania wieloma podsystemami i urządzeniami. Obecnie system EIB jest w stanie zarządzać następującymi podsystemami:

– oświetlenie żarowe i jarzeniowe, wewnątrz i na zewnątrz budynku (rys. 15),
– żaluzje pionowe i poziome, wewnątrz i na zewnątrz budynku,
– bezpieczeństwo użytkowania budynku,
– bezpieczeństwo i ochrona mienia w budynku,
– ogrzewanie, klimatyzacja i wentylacji,
– zarządzanie energią elektryczną,
– zdalny serwis i monitorowanie obiektu.



Rys. 15. Sterowanie oświetleniem w systemie EIB

System EIB jest chętnie stosowany w domach jednorodzinnych typu rezydencje, jak również w budownictwie użyteczności publicznej, jak np. hotele, biurowce, obiekty sportowe czy nawet obiekty sakralne. Dzieje się tak głównie ze względu na zalety, jakie ten system ma. Poniżej zestawiono podstawowe zalety systemu EIB:

– możliwość uzyskania dużych oszczędności w eksploatacji budynku przez wspólne zarządzania różnymi urządzeniami, np. oświetleniem, ogrzewaniem i żaluzjami;
– stosowany jest tylko jeden kabel magistrali, do którego podłączone są wszystkie urządzenia;
– większe bezpieczeństwo eksploatacji (np. pożarowe) przez oddzielenie obwodów energetycznych od obwodów sterowania. Obwody sterowania są zasilane napięciem bezpiecznym SELV;
– istnieje łatwość realizowania nawet złożonych wymagań wymyślonych przez przyszłego użytkownika;
– duża elastyczność systemu poprzez łatwość dokonywania późniejszych zmian, np. konieczność dołożenia dodatkowych przycisków sterujących;
– dzięki zastosowaniu topologii magistrali istnieje możliwość wspólnego sterowania różnymi systemami, np. ogrzewaniem i oświetleniem;
– niektóre urządzenia sterujące, jak np. czujki ruchu, czujniki elektromagnetyczne, mogą być wykorzystywane równocześnie podsystemie bezpieczeństwa i podsystemie ogrzewania lub oświetlenia. Wykrycie ruchu powoduje złączenie oświetlenia i ogrzewania;
– zarządzanie optymalnym zużyciem energii elektrycznej, przez odpowiednie wyłączanie lub załączanie odbiorników w otoczeniu szczytowych poborów mocy. System EIB ma dostęp wszystkich urządzeń pracujących na jednej magistrali;
– możliwość sterowania globalnego całym obiektem, np. wyłączenie oświetlenia w całym budynku jednym przyciskiem, załączenie sytemu bezpieczeństwa po przekręceniu klucza w drzwiach wyjściowych;
– możliwość wprowadzania późniejszych zmian w systemie sterowania bez konieczności wykonywania prac budowlanych;
– system sterowania jest jeden i jedna tylko będzie firma wykonująca serwis;
– zintegrowane funkcje urządzeń sterujących zmniejszają liczbę łączników w porównaniu z tradycyjnym systemem;
– system EIB łączy w jedną całość różne funkcje, jak: sterowanie, kontrola, pomiary i działania centralne;
– możliwa jest współpraca urządzeń EIB pochodzących od wielu producentów, co daje końcowemu użytkownikowi duże możliwości wyboru wykonawcy i wzoru użytkowego wyrobu.

Instalacje elektryczne systemu EIB mogą obecnie sprostać wysokim wymaganiom technicznym dzięki ich efektywności, elastyczności oraz bezpieczeństwu. System EIB jest zorientowany na przyszłość. Polecenia do systemu mogą być wysyłane lokalnie w budynku oraz zdalnie przez telefon stacjonarny lub komórkowy, albo przez Internet. Istnieją możliwości monitorowania stanów aktualnych urządzeń i zakłóceń w pracy instalacji EIB w budynku.

DR HAB. INŻ JERZY MIKULIK – PROF. AGH

Literatura:

1. Kastner D.: *EIB Installation Bus System,* Huethig GmbH, KG, Heidelberg, 2000.
2. *Handbuch Gebäudesystemtechnik.* t. 1. *Grundlagen,* t. 2. *Anwendungen,* Frankfurt a. Main, Zvei-Zveh, 1997.
3. Florczykiewicz T., Góralczyk M.: *Automatyczne sterowanie oświetleniem przy wykorzystaniu systemu magistralnego EIBus*, praca dyplomowa mgr, Politechnika Krakowska, 2004.
4. Petykiewicz P.: *Technika systemowa budynku instabus EIB. Podstawy projektowania,* WZ Graf, Warszawa, 1999.
5. Petykiewicz P.: *Nowoczesna instalacja elektryczna w inteligentnym budynku,* COSiW SEP, Warszawa, 2001.
6. Mikulik J., Jakubas W.: *Badania sygnałów w magistrali systemu EIB*, 2nd International Congress on Intelligent Building Systems, Politechnika Krakowska, Kraków, 2002.
7. Materiały firmowe ABB.
8. Materiały firmowe Busch Jaeger.

Sprawdź nasze ceny!!!

RADFORD

- niezawodne bramki wejściowe obrotowe i uchylne
- szeroki wybór rozwiązań

IDESCO

SECURE IDENTIFICATION

- czytniki zbliżeniowe do każdego systemu i formatu
- czytniki biometryczne
- różne obudowy (europuszka, drewno, kamień)
- indywidualne wykonanie dla klienta (logo, kolor)

TIMELOX®

Intelligent Security.

- autonomiczne lub systemowe zamki bezprzewodowe dla biurowców i hoteli
- obsługa kartami magnetycznymi, mikroprocesorowymi i zbliżeniowymi oraz kodem PIN

Wyłączny dystrybutor:

DYSKRET

DYSKRET Sp. z o.o.

30-023 Kraków, ul. Mazowiecka 131
Tel. 012 423 3100, Faks 012 / 423 4461
e-mail: office@dyskret.com.pl

www.dyskret.com.pl

artykuł sponsorowany

Urządzenia do kontroli dostępu

istotne z punktu widzenia aranżacji wnętrz

Firmy instalacyjne zajmujące się techniczną ochroną obiektów, mienia i osób, a szczególnie integratorzy systemów bezpieczeństwa, działają w czasach dynamicznego rozwoju technologii informatycznych. Do dyspozycji mają obecnie dziesiątki coraz to nowocześniejszych urządzeń i dedykowanego oprogramowania w swojej branży. Ponadto, dzięki gwałtownemu postępowi w telekomunikacji – w tym stale bezpieczniejszemu i szybszemu przesyłaniu dużych ilości informacji przez sieci lokalne (LAN) i rozległe (WAN), coraz częściej wykorzystujące łącza światłowodowe – rośnie liczba systemów zarządzania bezpieczeństwem (SMS) w stosunku do klasycznie rozumianych systemów bezpieczeństwa. W zdecydowanej większości systemy SMS powstały na skutek modyfikacji dostępnych na rynku systemów kontroli dostępu. Dlatego niezależnie od integracji poszczególnych komponentów, np. telewizji dozorowej CCTV czy sygnalizacji włamania i napadu, najważniejsza w takiej instalacji pozostaje nadal kontrola dostępu

Jak w każdym łańcuchu, także w przypadku systemu bezpieczeństwa jakość poszczególnych jego ogniw stanowi o niezawodności całego rozwiązania. Skuteczna kontrola ruchu osób w danym obiekcie realizowana jest ostatecznie na poziomie oprogramowania zarządzającego oraz monitorującego jednostki centralnej systemu, ale zależy w znacznej mierze od sprawności poszczególnych urządzeń. Oferta producentów jest bardzo zróżnicowana technologicznie, jakościowo i cenowo, ale dla każdej dbającej o swój wizerunek firmy instalującej system bezpieczeństwa najważniejszym kryterium pozostaje niezawodność i funkcjonalność stosowanych urządzeń.

Trzema ważnymi elementami w obrębie systemu kontroli dostępu, istotnymi z punktu widzenia aranżacji wnętrz, są: bramki, czytniki zbliżeniowe oraz urządzenia do kontroli porządkowej, tj. stosowane w pojedynczych wejściach do pomieszczeń.

Bramki

Bramka to podstawowe urządzenie wspomagające selekcję wszystkich użytkowników systemu kontroli dostępu, a także osób wchodzących do danego obiektu i wychodzących z niego.

Przydatność tych urządzeń zależy oczywiście od rodzaju i wielkości chronionego obiektu oraz stopnia wymaganego bezpieczeństwa. Ich instalacja nie wszędzie jest możliwa czy też konieczna, ale są obecnie coraz powszechniejsze. Jest to ważny element systemu bezpieczeństwa, ale też narzędzie porządkujące ruch osób. Stosuje się je w takich miejscach jak: biurowce, kompleksy handlowe, budynki użyteczności publicznej, dworce, urzędy, lotniska, obiekty sportowe i rekreacyjne etc. Wybierając dostawcę bramek, należy uwzględnić wiele kryteriów, w tym: jakość i różnorodność oferowanych przez danego producenta rozwiązań, ich niezawodność, stosowane materiały, cena, dostosowanie do warunków atmosferycznych (temperatura i wilgotność otoczenia, możliwość pracy w terenie otwartym), estetyka i referencje wynikające z doświadczenia w tej branży.

Mając na uwadze powyższe, z pewnością polecić można produkty brytyjskiej firmy Radford. Należy ona do międzynarodowego holdingu ITABmk Ltd. (*http://www.itabmk.com*) i od wielu lat umacnia swoją pozycję na rynku międzynarodowym. Radford oferuje duży wybór niezbędnych urządzeń, które pozwalają na funkcjonalne, estetyczne oraz ekonomiczne zaplanowanie bezpiecznej przestrzeni wejściowej i wyjściowej w każdym obiekcie. Produkty tej firmy obejmują wszystkie cztery główne grupy urządzeń, a mianowicie: bramki uchylne, klasyczne bramki obrotowe, wysokie bramki do kontroli specjalnej oraz wyposażenie uzupełniające.

W tej pierwszej kategorii Radford oferuje wiele mechanicznych i automatycznych (sterowanych) bramek uchylnych, jedno- i dwukierunkowych, w tym dwa główne ich typy: Eurogate i Rotogate. Oba występują w kilku estetycznie zaprojektowanych odmianach, a ich ramiona mogą być standardowe – tj. wykonane z wygiętych rur stalowych, lub pełne – ze szkła hartowanego. Trwałe bramki uchylne firmy Radford można stosować jako element główny albo porządkujący kontroli dostępu, a także jako wyjścia ewakuacyjne albo uzupełniające inne bramki systemu.

Grupa druga omawianych tu urządzeń obejmuje najpowszechniej stosowane, półpełne bramki obrotowe. Dlatego w bogatej ofercie firmy Radford znajdziemy zarówno urządzenia mechaniczne, jak i automatyczne oraz napędzane siłownikami elektrycznymi (z regulacją szybkości ruchu), jedno- i dwukierunkowe, z opcjami ewakuacyjnymi (dwa lub trzy opadające albo łamane ramiona). Te ładne i niezawodne bramki zaprojektowano jako wolnostojące (pojedyncze i przyścienne) oraz do instalacji grupowej, np. w szeregach. Główne ich typy to: TriFlo – w odmianach Sentry, Console

i Concept, urządzenia Elite – w tym Elite Ultra, a także bramki Radstar i Premier. Na szczególną uwagę zasługują unikatowe, eleganckie bramki obrotowe typu Opus, o nietypowej, ergonomicznej konstrukcji kołowej wykorzystującej gięte ramiona ze stali i przegrody z hartowanego szkła. Najnowszym produktem z tej grupy jest dwustronna, automatyczna bramka typu Fast-Trak, w której przegrodę fizyczną – tj. klasyczne ramiona lub przeszklenia – zastąpiono wiązką podczerwieni, co znacznie przyspiesza i ułatwia przechodzenie. Jak sama nazwa wskazuje, urządzenie to przeznaczone jest do szybkiej kontroli ruchu osób, zwłaszcza przemieszczających się w znacznej liczbie. Bramka Fast-Trak umożliwia również dokładną analizę statystyczną ruchu osobowego, co pozwala na zastosowanie skuteczniejszych metod rozładowania tłoku na wejściach i wyjściach w godzinach szczytu.

Bramka to podstawowe urządzenie wspomagające selekcję wszystkich użytkowników systemu kontroli dostępu, a także osób wchodzących do danego obiektu i wychodzących z niego.

Z kolei do bramek specjalnych Radford zalicza się ich trzy typy: Astral, Ecco i Forum. Te wysokie bramki, o specjalnie wzmocnionej konstrukcji, przeznaczone są do skutecznej, ścisłej ochrony zewnętrznej i wewnętrznej danego obiektu lub terenu przed osobami niepożądanymi. Konstrukcja bramek wymusza ruch pojedynczy i pozwala na zablokowanie w nich intruza stwarzającego potencjalne zagrożenie. Również i te bramki występują w wersjach jedno- i dwukierunkowych, z napędem i czujnikami ruchu regulującymi szybkość pracy. Mimo spełniania surowych wymogów bezpieczeństwa, bramki specjalne Radford są jak zawsze estetyczne i dobrze komponują się z każdym rodzajem otoczenia.

Wreszcie czwarta z omawianych tu grup: urządzenia i osprzęt komplementarny. Przykładowo, planując kontrolę dostępu do jakiegoś obiektu zamkniętego, np. biurowca, musimy często uzupełnić otoczenie bramek elementami dodatkowymi. Powinny one być z jednej strony funkcjonalne (jako przegrody) – a z drugiej, pod względem estetycznym pasować do przyjętych rozwiązań urządzeń głównych. Dlatego też firma Radford oferuje standardowe i nietypowe urządzenia przeznaczone do tego celu: od modularnych, dostosowanych wymiarami do potrzeb danego miejsca barierek oraz poręczy ze stali lub hartowanego szkła, przez specjalne postumenty do montażu czytników kart, do przenośnych lub stałych słupków i separatorów taśmowych (ustawianie i porządkowanie kolejek osób). Wszystkie te elementy wyposażenia pozwalają na skuteczne i ergonomiczne zagospodarowanie każdego miejsca na potrzeby systemu kontroli dostępu.

Warto podkreślić, że wszystkie bramki oraz urządzenia uzupełniające Radford projektowane są przez specjalistów tej firmy i są produkowane z najwyższej jakości materiałów oraz komponentów. Dominuje charakterystyczna dla takich produktów stal nierdzewna, ale dostępne są również urządzenia z trwałymi powłokami lakierniczymi lub estetyczne tworzywa sztuczne w różnych kolorach. Umożliwia to architektom i plastykom harmonijne oraz przyjazne dla użytkownika skomponowanie wystroju każdego chronionego wnętrza lub otoczenia.

Czytniki

Stanowią one kolejny z trzech głównych komponentów, istotnych dla sprawnego rozwiązania kontroli dostępu, w tym obsługi opisanych wyżej bramek wejściowych. Najczęściej są to czytniki zbliżeniowe, współpracujące z kartami pasywnymi (coraz rzadziej aktywnymi lub magnetycznymi) oraz, w niektórych aplikacjach, z różnego rodzaju innymi transponderami – np. w formie breloków czy żetonów.

Tworząc system kontroli dostępu od podstaw, można oczywiście wykorzystać właściwie każdy istniejący na rynku produkt danego rodzaju. Wybór jest tu jednak często celowo i świadomie ograniczany przez producentów oprogramowania zarządzającego oraz sterowników (kontrolerów) do konkretnego typu urządzeń lub producenta. Ale nawet wtedy, a zwłaszcza w sytuacji rozbudowy albo podwyższania standardu istniejącego systemu, możliwe jest dobranie funkcjonalnych czytników, łatwych do adaptacji. Te cechy gwarantują produkty firmy Idesco Oy z Finlandii (*http://www.idesco.fi*).

Już na początku lat dziewięćdziesiątych ubiegłego wieku młodzi, utalentowani inżynierowie tej spółki – powstałej w roku 1989, a czerpiącej z doświadczeń tego samego parku technologicznego co telekomunikacyjny gigant Nokia – dali się poznać jako doskonali projektanci, innowatorzy, a wkrótce także producenci zaawansowanych technologicznie czytników, modułów, transponderów i kart do nowej wtedy dziedziny RFID (ang.: *Radio Frequency Identification*) – tj. identyfikacji zbliżeniowej drogą radiową. Firma Idesco Oy jest zatem jednym z pionierów tej branży na świecie. Nic dziwnego, że już w roku 1990 – jako pierwsza – zastosowała praktycznie w nowej technologii rozwiązanie tzw. R/W

Czytniki Idesco z klawiaturą (po lewej) i bez klawiatury

(ang.: *Read/Write*), tj. bezstykowego odczytu informacji z nośnika (karty) i równoczesnego zapisu na nim.

Obecnie Idesco oferuje, między innymi, bardzo duży wybór czytników do aplikacji przemysłowych (w zakresie 24 – 125 kHz), np. typ Microlog – stosowany w logistyce, magazynach, służbie zdrowia, systemach płatniczych etc., specjalistyczne czytniki EX – jako jedyne w tej klasie dopuszczone do pracy w środowiskach

niebezpiecznych (zakłady chemiczne, magazyny paliw, rafinerie, petrochemia) oraz czytniki IR (4110 B, 6070 B, 4060, 4000, 4030 B i moduły IM 4000) – wszystkie stosowane w przemyśle motoryzacyjnym, systemach automatyki przemysłowej, kontroli czasu pracy, magazynach, do rozwiązań logistycznych (transport) itp.

Jednak z punktu widzenia typowych systemów kontroli dostępu dla osób, co stanowi przedmiot niniejszego tekstu, najbardziej interesujące są niewielkie gabarytowo, nowoczesne, trwałe i atrakcyjne cenowo czytniki typu Access, na karty zbliżeniowe i (lub) klawiaturę kodującą. Firma Idesco stworzyła je w roku 2001. Początkowo występowały głównie w technologii 125 kHz, ale obecnie wykorzystują raczej technologię 13,56 MHz, wprowadzoną przez Idesco Oy już w 1997 roku, a coraz powszechniej stosowaną przez głównych producentów systemów kontroli dostępu.

Estetycznie zaprojektowane czytniki doskonale sprawdzają się np. w hotelach

Najważniejszą zaletą czytników Idesco Access jest ich wielofunkcyjność, osiągnięta dzięki połączeniu wielu technologii w jednym czytniku. Te wysokiej jakości, estetycznie zaprojektowane i niezawodne urządzenia odczytują kody identyfikacyjne standardów Philips Mifare, I-Code, Inside PicoTag oraz większości już stosowanych lub planowanych do wprowadzenia transponderów, zgodnych z normą ISO 15693, takich jak ST, Tag-i, Infineon itd. Interfejsy do standardów Clock and Data, Wiegand (26, 32, 64, 66 b) i RS (232/485/422) umożliwiają stosowanie czytników w większości rozwiązań kontroli dostępu. Warto w tym miejscu podkreślić, że czytniki Idesco Access dostępne są również w uznanych powszechnie technologiach HID oraz Legic, umożliwiając współpracę z kartami zbliżeniowymi tych producentów. Najnowszym produktem firmy Idesco Oy jest biometryczny czytnik Access MFinger. Może on występować jako terminal autonomiczny albo komponent zwiększający poziom bezpieczeństwa większego systemu kontroli dostępu. MFinger wykorzystuje trzy typy identyfikacji: linie papilarne (od dwóch do sześciu wzorców odcisku palca na jednego użytkownika), kartę zbliżeniową (w technologii Mifare) oraz kod PIN (od trzech do dziesięciu cyfr).


Zamek TimeLox

Trwałość układów elektronicznych i odporność obudowy, wykonanej ze specjalnych żywic, gwarantuje ich funkcjonowanie nawet w trudnych warunkach otoczenia (w temperaturach od –40° do +55°). Czytniki można instalować bez izolacji bezpośrednio na powierzchniach metalowych. Równie trwałe oraz innowacyjne są czytniki z klawiaturą, której opatentowane rozwiązanie opiera się na braku części ruchomych, dzięki czemu jest ona odporna na wandalizm i nie wymaga konserwacji. Oprócz czytników dostępne są również same moduły zbliżeniowe, co ułatwia instalację w trudniejszych (brak miejsca) lub nietypowych warunkach (np. ukrywanie ich pod panelami sterującymi wind).

Do wszystkich zalet tych wielofunkcyjnych czytników należy dodać niespotykaną w branży elastyczność w podejściu do potrzeb klienta oraz szybkość działania ich producenta. Idesco Oy stawia sobie za punkt honoru sprostanie wszelkim wymaganiom potencjalnych użytkowników. Oferta tej firmy obejmuje dostawy obudów w określonych kolorach palety RAL, opracowanie dla konkretnej aplikacji czytników dwusystemowych (np. Legic i Mifare w jednym), a także wiele obudów specjalnych – w drewnie (Exclusive Woody – w tym z wygrawerowanym logo czy nazwą klienta), w kamieniu (wersja Rock) oraz czytniki specjalne typu Quattro – do szybkiego montażu w standardowej europuszce instalacji elektrycznej.

Autonomiczna kontrola porządkowa

Firma Timelox (*http://www.timelox.com*) to szwedzki producent należący do grupy Solid, funkcjonującej w ramach znanego, międzynarodowego holdingu Assa Abloy, światowego lidera w dziedzinie mechanicznych i elektronicznych urządzeń oraz systemów do kontroli dostępu, zamknięć i bezpieczeństwa technicznego. Od połowy lat osiemdziesiątych ubiegłego wieku buduje swoją pozycję przodującego dostawcy autonomicznych zamków elektronicznych i systemów bezprzewodowej kontroli dostępu, obsługiwanych kartami magnetycznymi oraz mikroprocesorowymi (tzw. chipowymi) – a obecnie także kartami zbliżeniowymi – jak również klawiaturą. Znajdują one coraz powszechniejsze zastosowanie nie tylko w branży hotelarskiej – dla której zresztą zostały stworzone i gdzie zdecydowanie dominują nad systemami przewodowymi – ale także w obiektach biurowych, urzędach, zakładach przemysłowych, a nawet w bankach.

Systemy liniowe kontroli dostępu – zwłaszcza rozbudowywane w istniejących już i zagospodarowanych obiektach – mają dwie cechy, które bywają uciążliwe dla ich właścicieli oraz użytkowników: kłopotliwe wykonanie okablowania i montażu oraz koszty dodatkowe, np. oprogramowania, sterowników, czytników i urządzeń wykonawczych (rygli elektrycznych etc.). Zdecydowanie tańsze i właściwie bezproblemowe w instalacji porządkowej kontroli dostępu – tj. na pojedynczych drzwiach do poszczególnych pomieszczeń zlokalizowanych wewnątrz chronionych liniowo stref – jest zastosowanie zamków autonomicznych (bezprzewodowych).

Niezawodne, ergonomiczne, niedrogie i estetyczne zamki Timelox – wyposażone w mikroprocesor, obwód kontrolny sygnalizujący niski poziom napięcia, moduł pamięci oraz zegar kwarcowy – zasilane są jedną baterią o napięciu 9 V co zależnie od przeznaczenia zamka wystarcza na rok, a nawet na kilka lat. Oprócz wersji tradycyjnej, tj. z klamką, zamki elektroniczne występują również jako czytniki naścienne Wallox przeznaczone do montażu wewnątrz budynku – np. obok drzwi lub na ich ościeżnicy, oraz Wallox E, skonstruowane

specjalnie do pracy na zewnętrz obiektu (wyposażone w grzejnik do zabezpieczenia przed wilgocią oraz mrozem). Czytniki Wallox mogą sterować każdym rodzajem zamknięcia (elektrozaczep, bramka obrotowa, zwora, szlaban itp.). Wszystkie wymienione typy zamków rodziny Timelox oferowane są standardowo w kilku atrakcyjnych wersjach obudowy (mosiądz, chrom, lakiery kolorowe), dzięki czemu można zharmonizować je z każdym wystrojem wnętrza.

Potencjalni użytkownicy systemów Timelox mają do wyboru wiele zróżnicowanych funkcjonalnie rozwiązań bezprzewodowej kontroli dostępu, z których każde oferuje kilka opcji sprzętowych i konfiguracyjnych. Jeżeli planowane jest objęcie kontrolą niewielkiej liczby drzwi (od jednych do np. kilkorga), z powodzeniem można zbudować system stosujący najprostsze zamki: Timelox Access (TLA) – na same karty magnetyczne, działające jak klucze, oraz TL Office (TLO) – na karty oraz klawiaturę PIN. Ich moduły pamięci zapisują informacje o 100 ostatnich wejściach, w tym dane użytkownika (numer karty lub kod), datę oraz godzinę. Informacje te można odczytać za pomocą prostego w obsłudze komunikatora i przenieść do bazy danych w komputerze.

Jeżeli zamków jest więcej lub wymagany jest zapis większej liczby zdarzeń, można sięgnąć po system TL Company (TLC), wyposażony we własne oprogramowanie (na platformie MS Windows) i koder kart magnetycznych (ręczny lub automatyczny). Za pomocą przenośnego komunikatora HCU – służącego do różnorodnych celów programujących, diagnostycznych i kontrolnych – można również zapisywać bezpośrednio do jego własnej pamięci dane dotyczące 1000 ostatnich wejść. System TLC może obsłużyć właściwie nieograniczoną liczbę drzwi. Natomiast dla swoich najbardziej wymagających klientów, szczególnie dbających o bezpieczeństwo, firma Timelox wprowadziła również z wielkim powodzeniem jedno z najnowocześniejszych i najciekawszych rozwiązań w tej klasie: dualny system Timelox Commercial (TC) oparty na elektronicznych zamkach obsługiwanych kartami mikroprocesorowymi (stykowymi) oraz magnetycznymi, pozwalający na zarządzanie oprogramowaniem systemowym za pomocą sieci komputerowej (LAN/WAN). Istotną cechą TC jest gromadzenie danych kontroli dostępu w zamkach oraz na kartach mikroprocesorowych, ponieważ każdy zamek systemowy działa nie tylko jako czytnik, ale również jako urządzenie zapisujące. Wszelkie zebrane w ten sposób informacje, obejmujące około 2000 zdarzeń, mogą być odczytywane wprost z karty lub za pomocą ręcznego komunikatora HCU, a następnie – dzięki oprogramowaniu z systemem filtrów – dowolnie przetwarzane w systemowej bazie danych. Obecnie firma Timelox wprowadziła też na rynek z powodzeniem rozwiązania autonomiczne bazujące na technologiach zbliżeniowych 13,56 MHz, co czyni tę ofertę jeszcze bardziej atrakcyjną ze względu na kompatybilność z systemami przewodowymi kontroli dostępu już na poziomie karty lub transpondera.

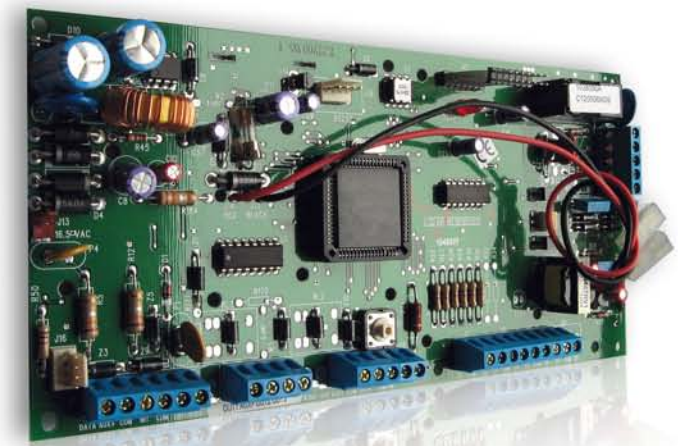
Podsumowanie

Można stwierdzić, że funkcjonalność, przystępna cena, niezawodność oraz walory estetyczne urządzeń Radford, Idesco i Timelox to jedynie część zalet, które sprawiają, że to idealna propozycja dla każdego rodzaju (i każdej wielkości) instytucji, zakładu, firmy, urzędu lub banku.

Jacek C. Ożarowski
Dyskret

GE Security

D-max



CS375

CS375

twoje centrum zarządzania inteligentnym budynkiem

www.systemcomfort.eu

Dualna Kamera Szerokodynamiczna Wysokiej Rozdzielczości

DCC-540F

- WDR - zakres dynamiki 120dB
- 540 TV lines
- PIXIM DPS ORCA - przetwornik
- DAY/NIGHT - kamera dualna
- DNR - perfekcyjny system redukcji szumów
- OSD - menu ekranowe

www.d-max.e-alpol.com.pl

ZAPRASZAMY
do nowo otwartego oddziału:

ALPOL Sp. z o.o. dystrybutor urządzeń D-MAX i Comfort na terenie całego kraju.

HURTOWNIA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ

GE Security

D-max

tel: 0 801 77 77 90

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

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

C & C

TH GROUP

Obserwuj przyrodę...
budzi się do życia!

SID 50

1/3" Kamera kolorowa
kopułkowa
o wysokiej rozdzielczości

SDC-415

1/3" Kamera kolorowa
o wysokiej rozdzielczości
z funkcją Dzień i Noc

SAMSUNG TECHWIN

Autoryzowany dystrybutor Samsung Techwin w Polsce:
C&C Partners - Leszno

www.samsungcctv.ccpartners.pl

artykuł sponsorowany

Smartlink na parkingu

W numerze 4 z 2005 roku opublikowany został artykuł zatytułowany *Smartlink to jest to* przedstawiający jedno z zastosowań aplikacji Smartlink. Przypomnę, że aplikacja Smartlink jest częścią pakietu programu EntraPass firmy Kantech w wersjach Corporate i Global. Wykorzystując funkcjonalność tej aplikacji, użytkownik we współpracy z programistą może realizować własne niestandardowe funkcje

Kontrola wjazdu i wyjazdu z parkingu

Sytuacja przedstawiona w poniższym artykule jest typowa. Biurowiec, w którym funkcjonuje wiele firm, a na dolnych kondygnacjach lub obok, na wydzielonym terenie – parking. Parking przeznaczony jest dla pracowników poszczególnych firm. Każda firma ma najczęściej wykupioną określoną liczbę miejsc parkingowych. Ze względu na:

– pojemność parkingu,
– koszt wynajęcia miejsc parkingowych,
– fakt, że część pojazdów jest zwykle poza terenem firmy

liczba miejsc parkingowych przydzielonych firmie jest mniejsza od liczby pojazdów. Należy jednak kontrolować wjeżdżające oraz wyjeżdżające pojazdy i rejestrować je. Najprostsza metoda to dodatkowe czytniki przed wjazdem i wyjazdem oraz wykorzystanie tych samych kart zbliżeniowych, które używane są w systemie kontroli dostępu wewnątrz biurowca. Do poprawnego funkcjonowania wymagane jest, oprócz czytników, oprogramowanie, które umożliwi:

– przypisanie każdej z firm wynajętych miejsc parkingowych,
– rejestrację wjazdów i wyjazdów pojazdów oddzielnie dla każdej firmy,
– udzielenie zgody na wjazd pojazdu w przypadku, gdy są jeszcze wolne miejsca dla danej firmy.

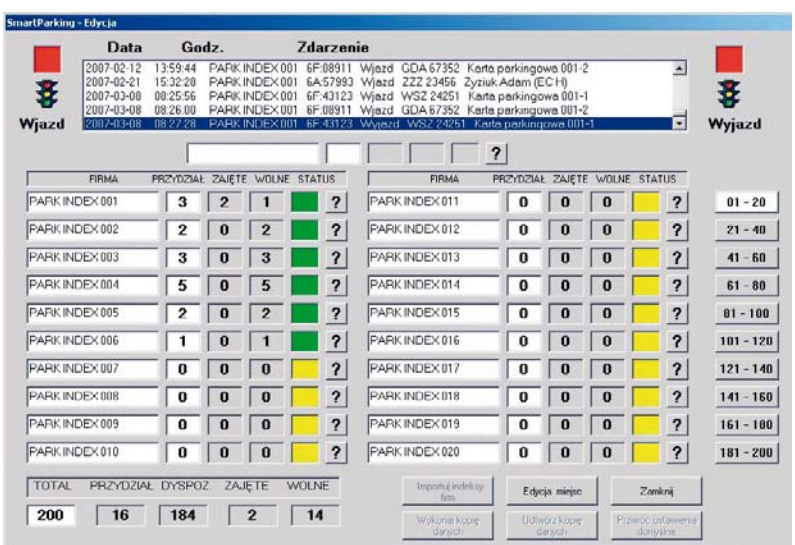
Programy do kontroli dostępu nie mają tak rozbudowanej funkcjonalności. Najczęściej standardowe funkcje pozwalają jedynie na kontrolę zajętości całego parkingu i blokadę wjazdu po zajęciu wszystkich miejsc. W przypadku, gdy mamy kilkanaście lub kilkadziesiąt firm, niezależna kontrola każdej grupy wymaga dodatkowego programu.

Oczywiście dostępne są specjalizowane systemy do kontroli parkingów, w tym również bezobsługowe, ale są to rozwiązania kosztowne i wymagające oddzielnego administrowania.

Jeżeli w obiekcie funkcjonuje już system kontroli dostępu (SKD), a tym samym użytkownicy mają karty dostępu, najtańszym i najwygodniejszym rozwiązaniem jest rozszerzenie funkcjonalności przez zainstalowanie dodatkowego programu Smart Parking.

Co to jest Smartlink?

Przypomnijmy podstawowe informacje o aplikacji Smartlink. Smartlink jest to program komunikacyjny, który po zainstalowaniu na wybranym komputerze i uruchomieniu łączy się z głównym serwerem systemu EntraPass. Po odpowiednim skonfigurowaniu udostępnia on dwukierunkowy kanał komunikacyjny pomiędzy serwerem a aplikacją zewnętrzną klienta. Kanał ten może być udostępniony przez sieć Ethernet pod określonym adresem IP lub jako port COM w komputerze, na którym jest on zainstalowany. Smartlink działa zgodnie ze szczegółową specyfikacją zawartą w załączonej do niego dokumentacji. Jest to aplikacja bezpłatna, w cenie pakietu podstawowego obu wymienionych programów.



Rys. 1. Smart Parking – okno stanu

Podstawowe tryby pracy programu Smartlink są następujące:

– jednokierunkowy – polega na przesyłaniu do aplikacji klienta wybranych zdarzeń z SKD w trybie *online* lub buforowaniu ich w trybie *offline* i przesyłaniu ich po nawiązaniu komunikacji;
– dwukierunkowy – polega na przesyłaniu poleceń od

aplikacji klienta przez Smartlinka do SKD, przy czym serwer SKD wysyła z kolei tą samą drogą potwierdzenie do aplikacji klienta o wykonaniu bądź niewykonaniu otrzymanego polecenia.

Możliwe jest działanie w obu trybach równocześnie, tym samym lub oddzielnymi kanałami. Typowym przykładem może być następująca sekwencja działań:
- przesłanie informacji o zdarzeniu alarmowym do aplikacji klienta (np. alarm pożarowy),
- wysłanie polecenia do SKD (np. odryglowanie na stałe drzwi ewakuacyjnych),
- wysłanie potwierdzenia wykonania polecenia z serwera SKD do aplikacji klienta.

Głównym zastosowaniem programu Smartlink jest możliwość integracji SKD z innymi systemami zabezpieczeń elektronicznych, działającymi w obiekcie pod kontrolą wspólnego programu nadzorczego BMS.

Funkcje programu Smartlink

Klient, który chce skorzystać z aplikacji Smartlink, może:
- kupić jedną z gotowych, dostępnych na rynku aplikacji,
- zlecić programiście napisanie aplikacji dostosowanej do własnych potrzeb.

Jedynym ograniczeniem funkcjonalnym jest w drugim przypadku szczegółowa specyfikacja Smartlink, która określa, jakie polecenia mogą być zainicjowane przez aplikację klienta i zrealizowane przez SKD. Najważniejsze grupy poleceń, które mogą być tą drogą realizowane to operacje na:
- kartach (dodawanie, modyfikacja, kasowanie, zmiana statusu),
- wyjściach przekaźnikowych,
- wejściach linii dozorowych,
- drzwiach i czytnikach,
- podsystemach alarmowych.

Można tworzyć dowolne połączenia zdarzeń i poleceń pod warunkiem zachowania logiki w działaniu systemu. Możliwe jest sekwencyjne realizowanie całego ciągu różnych akcji jako reakcji na wybrane zdarzenie. Warunkiem efektywnej realizacji takiego ciągu zdarzeń jest oczywiście pełna komunikacja w systemie: od kontrolera począwszy, przez program bramki GSI, serwer, Smartlink, na aplikacji klienta kończąc. Dołączona do programu specyfikacja umożliwia programiście napisanie odpowiedniego programu komunikacyjnego w języku C++ albo Visual Basic.

Na uwagę zasługuje również to, że Smartlink umożliwia realizację wybranych funkcji globalnych i sterujących w programie CORPORATE, który sam takich funkcji nie posiada. W przypadku programu GLOBAL jego możliwości zostają rozszerzone o funkcje, które nie są wbudowane w program, jak np. opisana poniżej kontrola parkingu.

Program Smart Parking

Program Smart Parking przeznaczony jest do kontroli wjazdu samochodów na parking i wyjazdu z niego. System umożliwia przydział dowolnej liczby miejsc każdej z 200 grup, może obsłużyć dowolną liczbę miejsc parkingowych. Jest przeznaczony do obsługi parkingów firmowych lub osiedlowych z określoną liczbą miejsc. W praktyce oznacza to, że każda grupa osób (np. firma) może mieć przydzieloną pewną liczbę miejsc, ale posiadać więcej pojazdów. Jeżeli wszystkie miejsca przydzielone danej grupie są zajęte, wjazd następnego pojazdu jest możliwy dopiero po wyjeździe przez bramkę wyjazdową co najmniej jednego pojazdu z danej grupy. Parking może posiadać do czterech wjazdów i wyjazdów. System nie kontroluje obecności pojazdu na konkretnym stanowisku. W momencie próby wjazdu sprawdza jedynie, czy są wolne miejsca dla danej grupy.

W przypadku mniejszej liczby grup (do 12) możliwa jest również sygnalizacja optyczna zajętości miejsc dla każdej z grup.

Kontrola odbywa się przez system czytników zbliżeniowych i kart lub czytników radiowych i pilotów z numerami identyfikacyjnymi zainstalowany przy wjazdach. Czytniki dołączone są do kontrolerów systemu kontroli dostępu, które sterują również bramkami lub szlabanami wjazdowymi. Kontrola parkingu może być częścią systemu kontroli dostępu na obiekcie lub działać samodzielnie.

Program Smart Parking przeznaczony jest do współpracy z programami nadzorczymi firmy Kantech typu EntraPass CORPORATE lub GLOBAL, z którymi komunikuje się przez aplikację Smartlink, dostępną w pakiecie instalacyjnym każdego z tych programów.

Operator może kontrolować stan zajętości całego parkingu lub miejsc dla poszczególnych grup, a nawet godziny wjazdu/wyjazdu samochodu o określonym numerze rejestracyjnym. Oprócz tego wskaźniki w głównym oknie programu informują o stanie komunikacji w całym systemie. Wyświetlane na bieżąco komunikaty informują o zdarzeniach. Operator może również aktualizować stan parkingu w programie, przez dodawanie lub usuwanie pojazdów z ewidencji, co umożliwia łatwe doprowadzenie do zgodności stanów w programie ze stanem faktycznym (np. w momencie uruchamiania systemu).

Rys. 2. Smart Parking – główne okno programu

Główne funkcje programu Smart Parking:
- do 200 grup użytkowników,
- dowolna liczba użytkowników w każdej grupie,
- kontrola nieograniczonej liczby miejsc parkingowych,
- do czterech wjazdów/wyjazdów na parking i z niego,
- wizualizacja stanów zajętości miejsc parkingowych dla poszczególnych grup,
- aktualizacja stanu parkingu przez operatora (dodawanie i usuwanie pojazdów),
- współpraca z programami nadzorczymi EntraPass Corporate lub Global firmy Kantech,
- możliwość używania tych samych kart do SKD i parkingu lub pilotów radiowych.

Poniżej omówiono poszczególne okna programu Smart Parking.

Główne okno programu

Okno to umożliwia:
- podgląd stanu komunikacji z aplikacjami systemu EntraPass i kontrolerami,

– wyświetlanie komunikatów związanych z odbieranymi zdarzeniami oraz realizacją akcji,
– logowanie operatora,
– przejście do okna konfiguracji wjazdów i wyjazdów,
– przejście do okna kontroli stanu parkingu.

W prawej, górnej części okna znajdują się wskaźniki stanu programu i stanu komunikacji:

Odczyt – prawy wskaźnik: sprawdzanie bufora zdarzeń serwera Smartlink, lewy wskaźnik: odczyt informacji,
LOG – stan zalogowania do serwera SmartLink,
SML – stan komunikacji z serwerem SmartLink,
SRV – stan komunikacji z serwerem EntraPass,
GSI – stan komunikacji z bramką GSI,
KT1-KT4 – stan komunikacji z kontrolerami,
przy czym znaczenie kolorów jest następujące:
– kolor zielony: komunikacja OK,
– kolor czerwony: brak komunikacji,
– kolor żółty: element niezaprogramowany.

Okno zdarzeń – wyświetlane w głównym oknie

W oknie tym wyświetlane są na bieżąco komunikaty dotyczące zdarzeń w programie. Każdy komunikat zawiera datę, godzinę, opis zdarzenia i nazwisko użytkownika oraz numer rejestracyjny pojazdu. Niezależnie od wyświetlania zdarzeń w powyższym oknie, zdarzenia te zapisywane są w plikach tekstowych, zlokalizowanych w katalogu: C:\Program Files\ \Kantech\SmartDll_CE\Generaldata\SML_P\Zdarzenia\ i mają rozszerzenia typu: SML_ZD_Data.txt. Można je przeglądać w dowolnym edytorze tekstu (np. w Notatniku) i drukować.

Okno konfiguracji – wejście przez przycisk >Konfiguracja<

Dostępne w tym oknie pola umożliwiają:
– definiowanie czytników wjazdu i wyjazdu,
– definiowanie przekaźników sterujących szlabanami,
– definiowanie przekaźników sterujących sygnalizatorami.

Okno stanu

W oknie tym wyświetlane są tylko komunikaty dotyczące wjazdu i wyjazdu oraz stany zajętości miejsc dla poszczególnych firm. Operator może sprawdzić, jakie pojazdy z danej grupy znajdują się na parkingu. W razie potrzeby może również ręcznie w programie usunąć lub dodać pojazd w celu aktualizacji stanu parkingu.

Podsumowanie

Powyższy opis nie obejmuje oczywiście wszystkich funkcji i szczegółów. Zainteresowanych czytelników odsyłam do materiałów źródłowych, czyli dokumentacji dostępnej na CD i na stronie *http://www.aat.pl* w zakładce *Oprogramowanie*. Najlepszym rozwiązaniem jest zainstalowanie na własnym komputerze w pełni funkcjonalnej wersji demonstracyjnej programu EntraPass CORPORATE, którą można otrzymać wraz z dokumentacją bezpłatnie w naszej firmie. Wersja demo zawiera również programy Smartlink i Smartlink Interface, które są niezbędne do testowania aplikacji klienta. W najbliższym czasie na stronie internetowej firmy AAT dostępna będzie również wersja demo programu Smart Parking.

W miarę powstawania kolejnych aplikacji klienta do programu Smartlink będziemy je prezentować na łamach *Zabezpieczeń*.

Ryszard Sobierski
AAT-T

PRT 12

zewnętrzny czytnik RFID/PIN

Czytniki serii PRT

- Identyfikacja zbliżeniowa oraz PIN
- Technologia EM 125 kHz oraz Mifare
- Praca autonomiczna lub jako czytnik podległy kontrolerowi
- Interfejsy Wiegand oraz Magstripe (Clock & Data)
- Praca w warunkach zewnętrznych (IP65)
- Obudowa jasnoszara lub ciemna

RACS

ROGER ACCESS CONTROL SYSTEM

RACS

roger®

www.roger.pl

artykuł sponsorowany

KRONOS

GRATIS od NEXT!

Otworzywszy dziś skrzynkę na listy, dowiedziałem się, że mogę stać się posiadaczem tostera, wystarczy, że kupię pralkę marki X. Nic mnie to nie będzie kosztować, wszystko gratis. Zacząłem się zastanawiać, cóż znaczy słowo „gratis". Absolutnie nic. Przyzwyczailiśmy się do szukania gwiazdki przy każdym napisie „Promocja", wiedząc, że nie ma nic za darmo.

Mimo to my w firmie Next!, dzięki uprzejmości redakcji *Zabezpieczeń*, postanowiliśmy przy okazji wydania nowych wersji oprogramowania, rozdać je za darmo. Wszystkim, którzy są zainteresowani, proponujemy lekturę niniejszego artykułu i zainstalowanie oprogramowania z dołączonej płyty CD.

Historia

Dla większości z Was jesteśmy producentem Kronosa – oprogramowania integrującego dla stacji monitoringu. To tylko część prawdy. Zadomowieni w branży ochrony jesteśmy twórcami także innych aplikacji kierowanych na ten rynek. Trzon firmy stanowią osoby, które w drugiej połowie lat 90. ubiegłego wieku i na początku obecnego pracowały w średniej wielkości agencji ochrony na południu Polski. Dwudziesty pierwszy wiek postawił przed nami zadanie dostosowania przestarzałych rozwiązań technicznych i informatycznych do szybko zmieniających się potrzeb klientów. Zaczęliśmy szukać różnych rozwiązań, pytać o nie i wreszcie je testować. Przez rok szukaliśmy rozwiązania stworzonego przez ludzi znających zagadnienie monitoringu, jak i będących ekspertami do spraw programowania. Efektem rocznych poszukiwań była decyzja: zróbmy to sami. Odeszliśmy z firmy i najpierw we dwójkę, potem w trzy osoby, powołaliśmy do życia firmę „Next!". Był rok 2002.

Teraz, po pięciu latach, jest nas ośmioro. Grupa składa się z ludzi zafascynowanych nowymi technologiami i chcących tworzyć nowatorskie rozwiązania. Jednym z efektów jest Kronos. System, który przoduje w innowacyjności, oferując to, co w konkurencyjnych systemach wprowadzane jest dopiero po kilku latach.

Fakty

Oprócz tego, że wszystko jest gratis, przyzwyczailiśmy się do tego, że wszystko jest naj. Tymczasem rzeczywistości nie budują reklamy, tylko fakty. Stąd garść faktów.

O użyteczności oprogramowania Kronos świadczy liczba jego użytkowników i tempo ich przybywania. Naszych rozwiązań używa dziś około 100 firm. Dokładnej liczby nie znamy, gdyż nasze programy są rozdawane w znacznej części za darmo i często dopiero po czasie dowiadujemy się, kto z nich korzysta. Stąd liczba faktycznych użytkowników może znacznie przekraczać podaną na początku wartość.

Są z nami zarówno duże, jak i średnie agencje ochrony, takie jak: Impel, G4S Litwa, Sezam, Ajax, Ascopol, Argos Kielce, Komes, Era Chorzów, Nordserwis, Alkon Szczecin, są też mniejsze, ale prężnie się rozwijające, jak: Ad Ochrona czy Arma Krosno. Nie mamy tyle miejsca na łamach, by wymienić wszystkich użytkowników oprogramowania Kronos. Wiele osób poznaliśmy osobiście w trakcie wdrożeń. Zawsze najważniejsze są dla nas partnerskie i bliskie relacje z naszymi klientami, niezależnie od ich wielkości, co pozwoliło nam zbudować z nimi partnerskie i bliskie relacje. To dla nas najważniejsze, bo tylko tą drogą możemy budować rzeczywiście użyteczne aplikacje.

Jesteśmy obecni także za granicą: w Czechach, na Ukrainie, na Litwie, w Gruzji, Mołdawii, Austrii, a ostatnio nawet w RPA i Chinach.

Naszym udziałem są również wdrożenia nietypowe, dla takich klientów jak:

- Grupa Żywiec – chyba pierwszy w naszej branży monitoring środowiska wykorzystujący urządzenia eCoder przesyłające sygnały przez sieci Ethernet,
- Rafineria Lotos,
- Największy port Marynarki Wojennej RP,
- Port Lotniczy Okęcie w Warszawie.

Wszędzie tam wybrano Kronosa jako platformę dla nowoczesnego centrum monitorowania.

I na koniec przedmiot szczególnej dumy i znak jakości naszych produktów – współpraca z innymi twórcami urządzeń i programów do monitoringu. Jesteśmy partnerami m.in. Jablotronu, Messera, Gorke Electronic czy EBS. Firmy te w dużej mierze zaprzestały rozwoju własnego oprogramowania na rzecz naszych produktów. Warto podkreślić, że w większości przypadków było to skutkiem wnikliwych testów rozwiązań naszych i konkurencji, co wskazuje wyraźnie na jakość, możliwości i elastyczność naszej oferty.

KRONOS LT

Program jest jednostanowiskowy i pozwala zintegrować do czterech odbiorników stacji bazowych takich producentów jak:

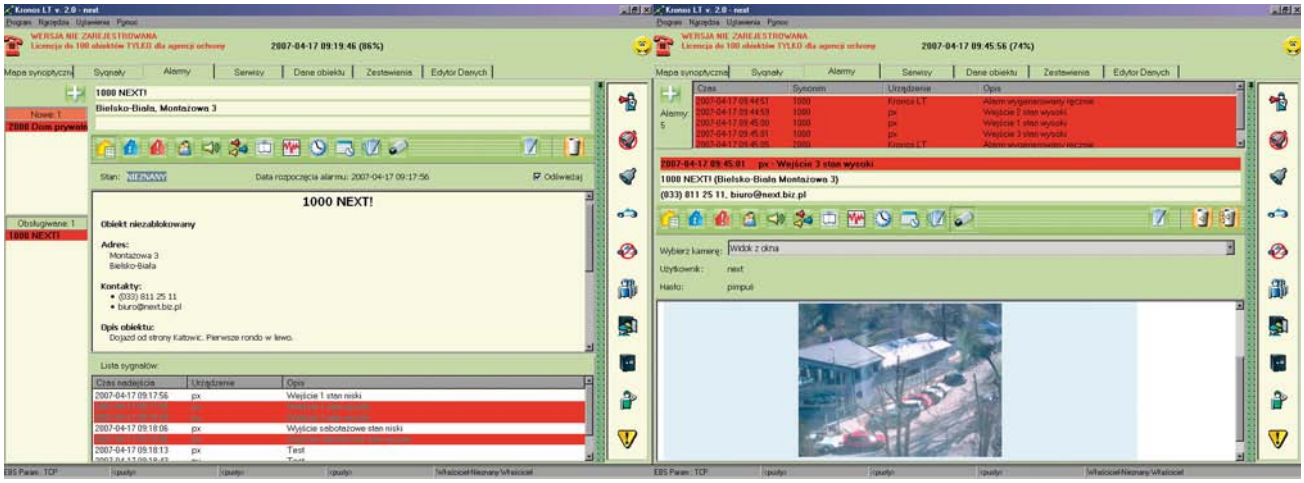
- **Radio:** Dyskam, Gorke, Messer, Nokton (w sieciach zarówno bez inteligentnych retransmiterów, jak i z nimi), Esom, Visonic, KP, Link, Stekop
- **Telefon:** Dyskam, Nokton, Satel, Esom, Visonic, SurGard, Stekop, Security, Optoscan
- **GSM/GPRS:** Pronal, EBS, Keratronik, Jablotron, Esom, Dyskam, Ambra, Informer, Optoscan oraz praktycznie każdy typ modułu przesyłający SMS/CLIP
- **Internet:** EBS, eCoder

Kronos LT

Wracając jednak do oferty gratisowej. Po długim, prawie dwuletnim oczekiwaniu zasadniczo przebudowaliśmy ofertę dla mniejszych agencji ochrony (do 500 obiektów chronionych). Przedstawiamy nasze najmłodsze dziecko: Kronosa LT 2.0. Nowa wersja jest jeszcze prostsza w obsłudze i ma jeszcze większe możliwości. Najważniejsze jednak jest to, że nadal nie zmieniła się polityka dotycząca tego produktu, pozostał on darmowy dla agencji ochrony do zabezpieczania 100 obiektów.

Dzięki niemu można bez kosztów rozpocząć monitoring w sieci GSM SMS/GPRS, gdyż odbiorniki stacji bazowych są zastępowane w takich przypadkach przez nasze sterowniki.

Program ten jest jednostanowiskowy i pozwala zintegrować do czterech odbiorników stacji bazowych takich producentów jak:



▲ *Dwie metody obsługi alarmów w Kronos LT*

- Radio: Dyskam, Gorke, Messer, Nokton (w sieciach zarówno bez inteligentnych retransmiterów, jak i z nimi), Esom, Visonic, KP, Link, Stekop.
- Telefon: Dyskam, Nokton, Satel, Esom, Visonic, SurGard, Stekop, Security, Optoscan.
- GSM/GPRS: Pronal, EBS, Keratronik, Jablotron, Esom, Dyskam, Ambra, Informer, Optoscan oraz praktycznie każdy typ modułu przesyłający SMS/CLIP.
- Internet: EBS, eCoder.

Jak tylko pojawiają się nowe urządzenia, uzupełniamy listę sterowników. Istotne jest, że wszystkie sterowniki są wypróbowane i działają w wielu agencjach ochrony.

W zakresie nowych funkcjonalności dodaliśmy wiele mechanizmów znanych z dużych i płatnych systemów, czyli: monitoring środowiska, podgląd z kamer, rozsyłanie maili i SMS-ów, generowanie alarmów zadaniowych, nawiązywanie i odbieranie połączeń głosowych. Wprowadziliśmy też modyfikacje czyniące wersję LT bardziej dopasowaną do potrzeb małych i samodzielnych centrów monitoringu, które nie korzystają z usług wykwalifikowanej kadry informatycznej. Pojawiły się m.in. gotowe szablony urządzeń, tworzenie kopii zapasowych bezpośrednio z programu, a także import i eksport części danych. Wprowadziliśmy ikony wykonanych czynności (komiks), jest już tablica synoptyczna, okno informujące o nowym alarmie, nowa pula zestawień, hurtownia danych osobowych i generowanie alarmów zleconych. Zmieniliśmy obsługę trybu serwisowego i dodaliśmy dwa interfejsy obsługi alarmów. Zasadniczych zmian jest ponad 30. Wszystkie te zmiany zostały jednak dokonane z uwzględnieniem zachowania maksymalnej prostoty obsługi. Produkt nadal pozostał, jak to ktoś określił: „do opanowania w ciągu godziny i to bez instrukcji obsługi".

Kronos NET

To nasz okręt flagowy i zarazem starszy brat wersji LT. Nie należy jednak mylić tych produktów i traktować Kronosa LT jako okrojonego Kronosa NET, ponieważ są to dwa niezależne programy. Ich cechą wspólną jest podobny interfejs użytkownika, ułatwiający przejście z wersji okrojonej na pełną, bez konieczności ponownego szkolenia operatorów, oraz pewna grupa funkcjonalności.

Reszta to już same różnice. Przede wszystkim Kronos NET przeznaczony jest dla dużych i średnich agencji ochrony. Odzwierciedla to wydajność programu. Tysiąc alarmów obsługiwanych na jednym stanowisku oraz kilka tysięcy obiektów chronionych w bazie, nie jest niczym szczególnym.

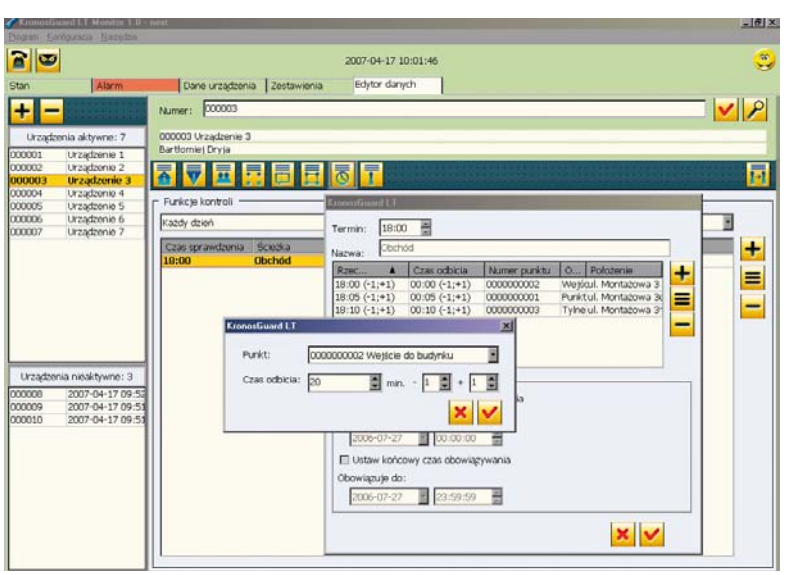
Program cechuje duże bezpieczeństwo i stabilność. Wydaje się to oczywiste, ale niestety, jak pokazuje praktyka, element ten na etapie doboru platformy do monitoringu jest często ignorowany. W przypadku Kronosa NET podejście autorów programu do tych aspektów skutkowało powstaniem unikatowej technologii buforów, możliwościami zdalnej kontroli i diagnozowania systemu oraz architekturą opartą o zarządzanie rezerwowymi niezależnymi elementami systemu. Efektem tego jest świadectwo kwalifikacyjne Techom klasa 4. Dodatkowo produkt nasz objęty jest polisą ubezpieczeniową w zakresie OC przez firmę Allianz, co jest ewenementem na rynku.

Ponadto Kronos NET to mnóstwo funkcjonalności pozwalających na oferowanie nowych usług i redukcję kosztów. Z jednej strony, mamy możliwość daleko idącej integracji, i to nie tylko urządzeń, ale także monitoringu obiektów stałych, ruchomych, środowiska, telewizji i strażników. Z drugiej to łączenie oddziałów i firm, wyniesione stanowiska, retransmisje zdarzeń do podwykonawców

KRONOS GUARD LT

Program ten to pierwsze na świecie komercyjnie oferowane narzędzie do obsługi urządzeń ActiveGuard, na bieżąco kontrolujące pracę strażników. Z naszych informacji wynika, że jest to obecnie najbardziej popularny i rozpowszechniony wśród klientów program dla tych urządzeń.

▼ *Intuicyjne definiowanie ścieżek w KronosGuard LT*



i na straże, dostęp klientów przez Internet (oczywiście nie przez zachęcające do włamań serwery www), usługi SMS, końcówki na palmtopach oraz wiele innych. Platforma ta wspiera także procesy zarządzania agencją ochrony. Miesięcznie wprowadzanych jest ponad 20 nowych funkcjonalności i modyfikacji. Trudno omówić tak obszerny system w kilku zdaniach. Jeśli są Państwo nim zainteresowani, prosimy o kontakt w celu umówienia bezpłatnej prezentacji i testów.

Kronos Guard LT

Prostota i możliwości. Te dwa słowa idealnie oddają ideę Kronosa Guard LT. Program ten to pierwsze na świecie komercyjnie oferowane narzędzie do obsługi urządzeń Active-Guard, na bieżąco kontrolujące pracę strażników.

Z naszych informacji wynika, że jest to obecnie najbardziej popularny i rozpowszechniony wśród klientów program dla tych urządzeń. Aplikacja powstała na zlecenie i jest wynikiem wyboru firmy Next! jako dostarczyciela platformy programowej. Tak jak w przypadku Kronosa LT, zdecydowaliśmy się rozdać program za darmo z otwartym limitem na 100 urządzeń. Wyczerpuje to potrzeby większości firm na rynku polskim, nie ponoszą one kosztów zakupu oprogramowania.

Oczywiście program oferuje pełne wsparcie dla funkcjonalności ukrytych w urządzeniu. Znajdziemy tu wygodne definiowanie ścieżek obchodów, które polega tylko na określeniu godziny ich rozpoczęcia i typu zastosowanego kalendarza, a także możliwość retransmisji do innych systemów, jak np.: SIMS. Program wraz z instrukcją obsługi znajduje się na dołączonej płycie.

Kronos Guard NET

Jest tym dla Kronosa Guard LT, czym Kronos NET dla Kronosa LT. To pełna i wielostanowiskowa wersja programu do monitoringu strażników. To program, który silnie ewoluuje w kierunku dużej platformy dla ochrony fizycznej i będzie alternatywą dla firm, które nie są zainteresowane pełną integracją wszystkich systemów, wykorzystującą Kronosa NET.

Urządzenia i programy specjalistyczne

Dążąc do kompleksowej obsługi naszych klientów, służymy pomocą w doborze rozwiązań sprzętowych i ich zakupie zarówno w zakresie infrastruktury informatycznej, jak i urządzeń do transmisji. Dzięki naszym kontaktom z producentami i wiedzy na temat parametrów urządzeń potrafimy wskazać urządzenia najlepiej dopasowane do przedstawionych potrzeb, niezależnie od tego, czy potrzebne są moduły do monitoringu przez GPRS i Ethernet, systemy radiowe, urządzenia do kontroli strażników, monitoringu środowiska, czy też moduły do śledzenia pojazdów.

Wykonujemy także specjalistyczne oprogramowanie na zlecenie. Są to zarówno aplikacje do obiegu dokumentów, jak i zaawansowane systemy monitoringu. Wszystko zależy od inwencji i zleceniodawców. Zapewniamy profesjonalizm, doświadczenie, zespół ludzi, serwis i stały rozwój zleconego oprogramowania.

Spotkajmy się

Trudno w kilku słowach przedstawić ofertę firmy Next!, wszystkie produkty, doświadczenie i nas samych. Zapraszamy do bezpośredniego kontaktu. Z chęcią przyjedziemy do Państwa lub zaprosimy Was do naszej siedziby.

MGR INŻ. BARTŁOMIEJ DRYJA
WSPÓŁWŁAŚCICIEL NEXT!

next!

KRONOS
GRATIS od NEXT!

Tu powinna być płyta z programami:
- **KRONOS LT,**
- **KRONOS Guard LT.**

Firma Next! dołożyła wszelkich starań, aby płyta CD-ROM działała poprawnie i nie powodowała błędów, nie ponosi jednak odpowiedzialności za ewentualne szkody powstałe w wyniku jej używania. W przypadku płyty CD posiadającej wady fizyczne, prosimy o jej odesłanie na adres producenta: Next! s.c. Sławomir Piela, Bartłomiej Dryja, ul. Montażowa 3, 43-300 Bielsko-Biała. Prosimy o podanie w przesyłce dokładnych danych teleadresowych, na które zostanie przesłana sprawna płyta.

http://www.next.biz.pl

PROTECTOR
CENTRUM TV IP

VIDEOSERWERY

SERIA M

2300zł netto

- Rozdzielczość przesyłu obrazu: PAL(704x576), CIF(352x288)
- Wejścia/wyjścia audio (VoiceIP)
- Wejścia/wyjścia alarmowe
- Sterowanie PTZ (RS-485)
- Kompresja MPEG-4
- Videodetekcja, nagrywanie
- Funkcja dekodera z sygnału LAN na Video
- Sterowanie poprzez przeglądarkę WEB lub za pomocą dołączonego oprogramowania

SERIA D

999zł netto

REJESTRATORY CYFROWE HYBRYDOWE

SERIA M 4/8/16 KANAŁOWE

NOWOŚĆ

- Jednoczesny podgląd i rejestracja z kamer dołączonych do wejść analogowych rejestratora lub rejestracja kamer IP
- Rozdzielczość - PAL(704x576), HD1(704x288),
- CIF(352x288)
- Prędkość nagrywania do 400kl/s
- LAN - do 99 użytkowników
- Maskowanie kamer
- Do 16 wejść / 8 wyjść alarmowych
- Do 16 kanałów audio
- Sterowanie PTZ
- Pełne starowanie po sieci LAN z przeglądarki WEB lub dołączonego oprogramowania
- Kompresja MPEG4

REJESTRATORY CYFROWE

SERIA D 4/8/16 KANAŁOWE

- Podgląd i rejestracja do 400kl/s
- Rozdzielczość - PAL(704x576), HD1(704x288), CIF(352x288)
- LAN - do 10 użytkowników jednocześnie
- Maskowanie kamer, USB, mysz, pilot
- Videodetekcja
- Kompresja MPEG-4/H.264
- Do 16 wejść / 6 wyjść alarmowych
- Do 16 kanałów audio
- Opcja krosownicy wizyjnej 16x4
- Sterowanie PTZ (60 protokołów)

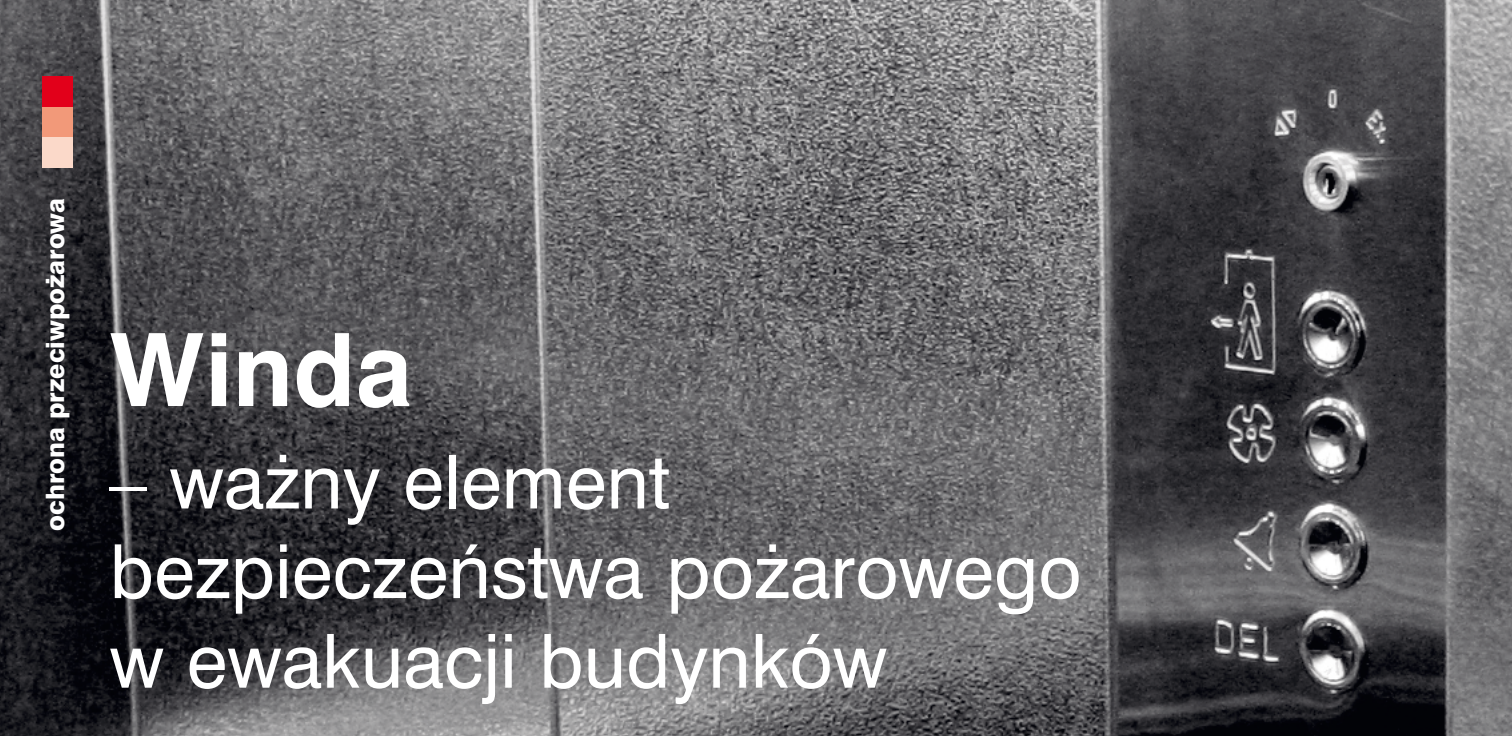
KAMERY KOPUŁOWE SZYBKOOBROTOWE

- Zoom optyczny: 18/23/26/35x
- Zoom cyfrowy: 12x
- Kamera dzień/noc 0.01 lx
- 540TVL
- Strefy prywatności
- Presety
- W komplecie: obudowa zew., uchwyt, zasilacz

www.protector-polska.pl

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

biuro@protector-polska.pl



Winda – ważny element bezpieczeństwa pożarowego w ewakuacji budynków

Europejskie Stowarzyszenie Dźwigowe (ELA – ang.: *European Lift Association*) w październiku 2006 roku zorganizowało Międzynarodową Konferencję „Pożar i zarządzanie ryzykiem" (ang.: *Fire & Risk Management*). Podsumowywała ona doświadczenia zdobyte zarówno przez grupy specjalistów badających przyczyny tragedii World Trade Center 11 września 2001 roku, jak i osoby z innych krajów zajmujące się zabezpieczaniem bardzo wysokich budynków

Specjaliści ze Stanów Zjednoczonych, z Wielkiej Brytanii, Szwajcarii, Holandii i Belgii w swoich referatach omówili najnowsze kierunki związane z:
- zabezpieczeniem przeciwpożarowym najwyższych budynków, ze szczególnym uwzględnieniem funkcjonujących w nich dźwigów,
- wykorzystaniem dźwigów przez ekipy ratownicze i ewakuacją ludności,
- procedurami ewakuacyjnymi,
- metodami i wynikami badań odporności ogniowej drzwi przystankowych.

Tragedia z 11 września 2001 roku zmieniła pogląd Europejczyków na ochronę przeciwpożarową wysokich budynków oraz na kwestię ewakuacji z nich ludzi. W skład WTC wchodziły dwie wieże: pierwsza o wysokości 415,22 m i druga, wysoka na 525 m (wraz z anteną). Budynki liczyły 110 pięter, a w każdej z wież było zainstalowane 99 wind.

W przypadku WTC potwierdziła się stara prawda, że nie ma wieżowców odpornych na ogień. Prawdziwym zagrożeniem okazało się zapadanie budynku (w przypadku pożarów innych wysokich budynków najwięcej ofiar było z powodu zatrucia toksycznym gazem).

Również użytkownicy wysokich budynków nie wiedzą, jak zachowywać się w przypadku pożaru, by ujść z niego z życiem. Schody nie umożliwiają im opuszczenia na czas palącego się budynku wysokościowego.

Ewakuacja osób niepełnosprawnych lub poszkodowanych przy użyciu dźwigów – obecne uregulowania unijne

Wykorzystanie dźwigów w czasie pożaru regulowane jest normą EN 81-72 (polski odpowiednik PN-EN 81-72:2005 *Przepisy bezpieczeństwa dotyczące budowy i instalowania dźwigów – Szczególne zastosowanie dźwigów osobowych i towarowych – Część 72: Dźwigi dla straży pożarnej*).

Z wyjątkiem specyficznych przypadków (definiowanych lokalnymi normami, np. BS 5588 w Wielkiej Brytanii lub AS4 we Francji), windy nie są wykorzystywane do ewakuacji w czasie pożaru. Są wyłączane z użycia w przypadkach zagrożeń (norma EN 81-73, polski odpowiednik PN-EN 81-73:2006 *Przepisy bezpieczeństwa dotyczące budowy i instalowania dźwigów – Szczególne zastosowanie dźwigów osobowych i towarowych – Część 73: Funkcjonowanie dźwigów w przypadku pożarów*) lub zabraniają tego instrukcje ewakuacji. Dla niektórych użytkowników budynków wysokościowych brzmi to jak wyrok śmierci.

W wysokim budynku pracują często niepełnosprawni poruszający się na elektrycznych wózkach. Trudno wyobrazić sobie ich ewakuację po schodach.

Kto jeszcze, poza osobami na wózkach, może potrzebować dźwigu do ewakuacji?

Kobiety w ciąży, ranni, osoby z ograniczeniem ruchowym – to może być do pięciu procent populacji.

Prowadzone są prace studialne Grupy Roboczej 6 (CEN/TC/WG6). Zakończą się dokumentem roboczym, który przy utrzymaniu generalnej zasady, że dźwig nie jest drogą ewakuacji, powinien odpowiedzieć na pytania:
- jakie warunki musi spełnić dźwig, aby umożliwić ewakuację niepełnosprawnych?
- jakie wymagania muszą spełnić nieskomplikowane dźwigi ewakuacyjne, aby można je było wprowadzić w niskich i średniowysokich budynkach użyteczności publicznej i zamieszkania zbiorowego?

Główne wymagania dla dźwigów określono w sposób następujący:

1. Dźwig musi spełniać określone poniżej wymagania norm:
   - EN 81-70 (polski odpowiednik PN-EN 81-70:2005 *Przepisy bezpieczeństwa dotyczące budowy i instalowania dźwigów – Szczególne zastosowania dźwigów osobowych i towarowych – Część 70: Dostępność dźwigów dla osób, w tym osób niepełnosprawnych,* ze zmianą PN-EN 81-70: 2005/A1:2006) – wymiary, poziom wyposażenia;

– EN 81-72 – wymiary, prędkość, zasilanie elektroenergetyczne, zabezpieczenie przed zalaniem wodą
– EN 81-73 – powrót automatyczny przeważnie na parter budynku.

2. Dźwig musi spełniać dodatkowe wymagania:
– specjalne sterowanie z automatycznym powrotem na wyznaczoną kondygnację, na której są zlokalizowane drzwi wyjściowe ewakuacyjne z budynku,
– specjalna sygnalizacja w kabinie i na przystankach.

Powyższe wymagania powinny być połączone z odpowiednimi wymaganiami dotyczącymi budynków w zakresie:
– systemu sygnalizacji pożarowej,
– zapewnienia niepełnosprawnym wydzielonej przed wystąpieniem pożaru przestrzeni (wielkość, dodatkowa sygnalizacja obecności),
– zabezpieczenia szybu dźwigowego i miejsc oczekiwania na ewakuację przed dymem (urządzenia do usuwania dymu i zabezpieczające przed zadymieniem),
– oświetlenia ewakuacyjnego w miejscach oczekiwania na ewakuację,
– łączności dźwiękowej pomiędzy miejscem oczekiwania na ewakuację a poziomem wyjścia ewakuacyjnego z budynku i kabiną dźwigu,
– informacji o dźwigu, przeznaczonym do ewakuacji w budynku,
– instrukcji wyświetlanej w budynku z uwzględnieniem, że dźwig do ewakuacji przeznaczony jest jedynie dla niepełnosprawnych ruchowo,
– wszystkich wymagań budowlanych zdefiniowanych już w EN 81-72 (drugie źródło zasilania elektroenergetycznego, ochrona przed zalewaniem dźwigu i szybu dźwigowego wodą gaśniczą).

Sformułowano również wymagania dla obsługujących dźwigi przeznaczone do ewakuacji, tzn. wyznaczonych na każdym piętrze tzw. opiekunów pożarowych. Do ich obowiązków należałoby:
– sprawdzanie wszystkich pokoi na danej kondygnacji i pomoc niepełnosprawnym,
– odbywanie regularnych ćwiczeń ewakuacyjnych oraz posiadanie odpowiedniego wyposażenia.

Zdefiniowano dwa rodzaje ewakuacji:
– ewakuacja z opiekunem, który porusza się dźwigiem wraz z ewakuowanymi, sterując nim specjalnym kluczem tak, że przywołania z przystanków nie działają,
– ewakuacja bez opiekuna w kabinie, ale z jego pomocą na każdej z kondygnacji (w takim przypadku funkcjonują przywołania przystankowe).

Dla tego typu budynków musi być opracowana strategia ewakuacji, która traktuje o:
– liczbie dźwigów ewakuacyjnych,
– sposobie ewakuacji – automatycznej czy z operatorem,
– liczbie osób niepełnosprawnych do ewakuacji,
– czasie całkowitej ewakuacji,
– kolejności ewakuowanych kondygnacji,
– zasadach kierowania ewakuacją przez zarządzającego budynkiem.

Niewątpliwie powyższe zasady oraz nowe rozwiązania konstrukcyjne producentów dźwigów powinny umożliwić spełnienie Deklaracji 95/357/WE Europejskiego Parlamentu, Rady i Komisji (Dziennik Urzędowy Wspólnot Europejskich L213 z 7 września 1995 roku, str. 32), zachęcającej państwa członkowskie do uczynienia niezbędnych kroków, na poziomie krajowym, aby zapewnić niepełnosprawnym dostęp do wszystkich kondygnacji w istniejących i budowanych budynkach. Deklaracja zaleca przepis mówiący, że we wszystkich nowych budynkach co najmniej jeden dźwig powinien być dostępny dla osób na wózkach. Państwom członkowskim zostawia się swobodę wyboru bardziej rygorystycznych środków, jeżeli uznają je za stosowne.

Sprawę dostępu wysokich budynków dla niepełnosprawnych omawia również Raport Grupy Ekspertów Komisji Europejskiej z października 2003 roku 2010: *A Europe Accessible for all*.

Unia Europejska przygotowała również wytyczne: *Build for all*, promujące dostępność do budynków dla wszystkich. Powinny one znaleźć zastosowanie przy tworzeniu szczególnych istotnych warunków zamówienia w przetargach publicznych na budowę budynków publicznych. Dotyczą tego również dyrektywy UE nr 2004/17/EC i 2004/18/EC z 24 marca 2004 roku.

Dostępność powinna również uwzględniać możliwość ewakuacji.

Ograniczenie rozwoju pożaru – podziały budynków na strefy pożarowe

W ubiegłym roku nastąpiła nowelizacja brytyjskich przepisów techniczno-budowlanych w zakresie:
– wymagań dotyczących wentylacji,
– konserwacji urządzeń związanych z zasilaniem budynków w energię,
– bezpieczeństwa urządzeń elektroenergetycznych.

Brytyjskie wymagania dotyczące bezpieczeństwa pożarowego budynków określają:
– warunki ewakuacji (liczbę, wymiary, lokalizację dróg ewakuacyjnych, ich zabezpieczenie przed pożarem, oznaczenie znakami bezpieczeństwa, urządzenia chroniące drogi ewakuacyjne przed dymem),
– drogi pożarowe i urządzenia dostępu do budynku dla jednostek straży pożarnej,
– zabezpieczenie przed rozprzestrzenianiem się pożaru z zewnątrz (konstrukcja ścian budynku uniemożliwiająca rozprzestrzenianie się pożaru, liczba niechronionych obszarów ograniczana w zależności od określonego promieniowania cieplnego, dachy konstruowane w sposób zabezpieczający przed rozprzestrzenianiem się pożaru i jego penetracją do wnętrza),
– zabezpieczenie przed rozprzestrzenianiem się pożaru wewnątrz budynku (rodzaje zastosowanych materiałów wykończeniowych z uwzględnieniem właściwości wykładzin, ścian, stropów i posadzek w zakresie powierzchniowego rozprzestrzeniania się ognia oraz ciepła wydzielanego podczas spalania, konstrukcja o wymaganej klasie odporności pożarowej i ogniowej elementów budowlanych, podział na strefy pożarowe oraz zamknięcie wszystkich otworów w elementach oddzieleń przeciwpożarowych).

Warunki ewakuacji uwzględniają: funkcję budynku, liczbę osób w nim przebywających, klasyfikacje ryzyka, długość drogi ewakuacyjnej, wydzielenie części budynków jako miejsc bezpiecznych.

Autor referatu [1] uważa, że wydzielenie przeciwpożarowych dróg ewakuacyjnych to najbezpieczniejsze rozwiązanie dla prowadzenia sprawnej ewakuacji ludzi z budynku.

Brytyjskie rozwiązania projektowe stosowane w wysokich budynkach polegają na umożliwieniu wykorzystania przez straż pożarną klatki schodowej, oddzielonej od powierzchni użytkowej każdej kondygnacji przedsionkiem przeciwpożarowym, będącym jednocześnie spocznikiem wydzielonego dźwigu przeznaczonego dla straży pożarnej. W przedsionku tym lokalizuje się także suchy pion z zaworami hydrantowymi. Pożarowe wydzielenie części kondygnacji, w której znajduje się pionowa droga komunikacyjna (będąca jednocześnie drogą ewakuacyjną) oraz dźwig wykorzystywany przez straż pożarną ze spocznikiem przed drzwiami przystankowymi i fragmentem korytarza, zapewniają bezpieczne miejsce dla ewakuowanych, w tym przede wszystkim dla niepełnosprawnych.

Zastosowanie dźwigów w przypadku pożaru – perspektywy w Stanach Zjednoczonych

Autor referatu [3] przedstawił niektóre z 30 zaleceń Narodowego Instytutu Standardów i Technologii w odniesieniu do najwyższych budynków. Zalecenia te dotyczyły:

– podniesienia klasy odporności pożarowej,

– zastosowania nowych metod zapewnienia odporności ogniowej ich elementów,

– poprawy warunków ewakuacji i skuteczności reagowania w przypadku zagrożenia.

Nie sposób omówić wszystkich tych zaleceń. Założenie jest takie, że wysokie budynki powinny być tak projektowane, aby można było przeprowadzić sprawną ewakuację w przypadku:

– zaniku zasilania energetycznego,
– trzęsienia ziemi,
– pożaru,
– huraganu,
– wybuchu,
– ataku terrorystycznego.

Technologie ewakuacyjne należy zmieniać tak, aby w przyszłości można było korzystać z:

a) dobrze zabezpieczonych dźwigów:
   – chronionych przed ogniem, dymem i wodą,
   – wykorzystywanych przez ekipy ratownicze do ewakuacji niepełnosprawnych i poszkodowanych w pożarach
b) zewnętrznych urządzeń ratowniczych,
c) klatek schodowych ewakuacyjnych.

Autor przedstawił także propozycje zabezpieczeń przeciwpożarowych w budynkach wysokościowych Międzynarodowej Rady Przepisów (ang.: *International Code Council* – ICC), mające zapewnić użytkownikom budynku odpowiednie warunki ewakuacji i prowadzenia działań ratowniczych przez wydzielony pożarowo trzon komunikacyjny. W budynku takim przewidziano korytarz/pomieszczenie dla ewakuowanych osób, o powierzchni określonej w zależności od liczby użytkowników, przyjmując trzy stopy kwadratowe na jedną osobę i miejsce dla 1/4 liczby osób znajdujących się na kondygnacji.

W trzonie ewakuacyjnym zaleca się przewidzieć dwie klatki schodowe ewakuacyjne oraz dwa specjalne dźwigi przeznaczone dla ewakuacji.

Proponuje się specjalny dźwig do celów ratowniczych, wydzielony oddzieleniem przeciwpożarowym, wraz z klatką schodową i przedsionkiem dźwigu, od pozostałych części trzonu komunikacyjnego. Wydzielony spocznik dźwigu pożarowego z nadciśnieniem powinien być połączony ze spocznikiem klatki schodowej (również z nadciśnieniem), przy czym oprócz tego, że jedne drzwi dźwigu otwierają się na jego spocznik, drugie zapewniają połączenie z usytuowanym obok holem dźwigowym.

Zabezpieczenie szybów dźwigowych przez zapewnienie w nich nadciśnienia na wypadek ewakuacji

Ludzi zabija przede wszystkim toksyczny gaz, a nie ogień. Dlatego najważniejszą sprawą jest zapewnienie nadciśnienia w szybach dźwigowych dźwigów dla straży pożarnej oraz ewakuacji niepełnosprawnych. Skutecznie zabezpiecza to szyb przed jego zadymianiem, zapewnia bezpieczeństwo przebywającym w nim w czasie pożaru ludziom.

W szybach dźwigowych i zlokalizowanych przy nich klatkach schodowych powinno być nadciśnienie rzędu 50 Pa w stosunku do pomieszczeń na kondygnacji (zakłada się niższe o 5 Pa przy drzwiach łączących się z innymi pomieszczeniami).

System ochrony szybu dźwigowego przed dymem polega na:

a) wykryciu dymu czujką dymową systemu sygnalizacji pożaru,
b) aktywacji systemu kontroli rozprzestrzeniania się dymu przez:
   – włączenie wentylatora nadciśnieniowego, zlokalizowanego w najniższej lub najwyższej części szybu dźwigowego,
   – wytworzenie nadciśnienia w szybie dźwigowym, a także w przedsionku dźwigu przez przepływ przez nieszczelne drzwi przystankowe,
   – zapewnienie przepływu powietrza do palącego się pomieszczenia przez zawory nadciśnieniowe,
   – powstrzymanie wypływu dymu z palącego się pomieszczenia.

Odpowiednio zaprogramowany system sygnalizacji pożaru uniemożliwia zatrzymanie się dźwigu na kondygnacji, na której wybuchł pożar.

Ograniczenie rozprzestrzeniania się pożaru przez szyby dźwigowe – EN 81-58

W celu skutecznego zapobiegania pożarowi w dźwigu ewakuacyjnym zaleca się konstruować dźwigi z materiałów niepalnych oraz badać w szczególności odporność ogniową drzwi przystankowych. Określa to polska norma PN-EN 81-58:2005 *Przepisy bezpieczeństwa dotyczące budowy i instalowania dźwigów – Badania i próby – Część 58: Próba odporności ogniowej drzwi przystankowych*.

Autor [2] omówił genezę powstania normy EN 81-58.

Założenia normy:

– drzwi przystankowe – uniemożliwiają wejście pożaru do szybu i przemieszczenie się nim na wyższą kondygnację,
– pożar musi pokonać dwoje drzwi przed ponownym zetknięciem się z materiałem palnym,
– występuje efekt kominowy w szybach dźwigowych przez otwory wentylacyjne,
– bardzo mało pożarów powstaje w szybie dźwigowym,
– mało pożarów powstaje w skrzydłach drzwi przystankowych,
– różnica ciśnień mierzona w drzwiach przystankowych jest większa niż pomiędzy sąsiednimi pomieszczeniami na tej samej kondygnacji,
– występuje większa prędkość przepływu gazów przez drzwi przystankowe niż pomiędzy pomieszczeniami na tej samej kondygnacji.

Kryteria badań wg EN 81-58:
– warunki temperaturowe od badanej strony drzwi wg krzywej: $T=345\cdot\log_{10}(8t+1)$, gdzie T to temperatura, a t–czas,
– ciśnienie od badanej strony drzwi przystankowych: ok. 20 Pa,
– czas oceny badania: 15, 20, 30, 45, 60, 90 i 120 minut.

Kryteria oceny:
– szczelność ogniowa (E),
– izolacyjność cieplna (I),
– odporność na działanie promieniowania cieplnego (W).

Według autora metoda badań opisana w EN 81-58 najlepiej odzwierciedla warunki odpowiadające możliwości przeniesienia się pożaru przez drzwi przystankowe do dźwigu do szybu dźwigowego i zasadne jest wprowadzenie wniosku o uregulowanie jej w ocenie zgodności z wymaganiami podstawowymi dyrektywy dźwigowej (inne metody mogą być stosowane do czasu ustalenia procedur oceny zgodności w dyrektywie dźwigowej).

Nowe spojrzenie na możliwość ewakuacji przy zastosowaniu dźwigów

Ewakuacja z budynków wysokich schodami:
– odbywa się zbyt wolno (1 kondygnacja w ciągu minuty) – zejście z 100. piętra powinno trwać 100 min, a wieże WTC zawaliły się po 102 i po 56 minutach,
– nagromadzenie ludzi grozi paniką,
– strumienie ludzi schodzących napotykają wchodzących ratowników,
– podział budynków na kondygnację robocze/mieszkalne i ewakuacyjne,
– potrzeba zastosowania dźwigów do ewakuacji osób z najwyższych kondygnacji,
– BURJ DUBAJ – najwyższy apartamentowiec na świecie – 700 m wysokości, kondygnacje ewakuacyjne 42, 75, 111 i 138, dziesięć dźwigów ewakuacyjnych.

Operacja „łódź życia" jako nowe podejście do ewakuacji budynków wysokościowych:
– na każde 15–20 pięter kondygnacja ewakuacyjna lub jedna strefa dźwigowa, na której mogą zbierać się ludzie i oczekiwać na ewakuację,
– dźwigi sprawdzone pod względem operacyjnym i zasilania elektrycznego,
– dźwigi powinny poruszać się po przeciążeniu (Europa: 100% obciążenia, Stany Zjednoczone: 125% obciążenia),
– ruch dźwigu po sprawdzeniu, czy droga nie jest zadymiona,
– budynek powinien być ewakuowany w czasie 20 minut i krótszym.

Podsumowanie

Zastosowanie dźwigów do prowadzenia ewakuacji w budynkach jest objęte programem prac studialnych i normalizacyjnych.

W przyszłości dźwigi mogą stanowić równorzędną z klatkami schodowymi drogę ewakuacji.

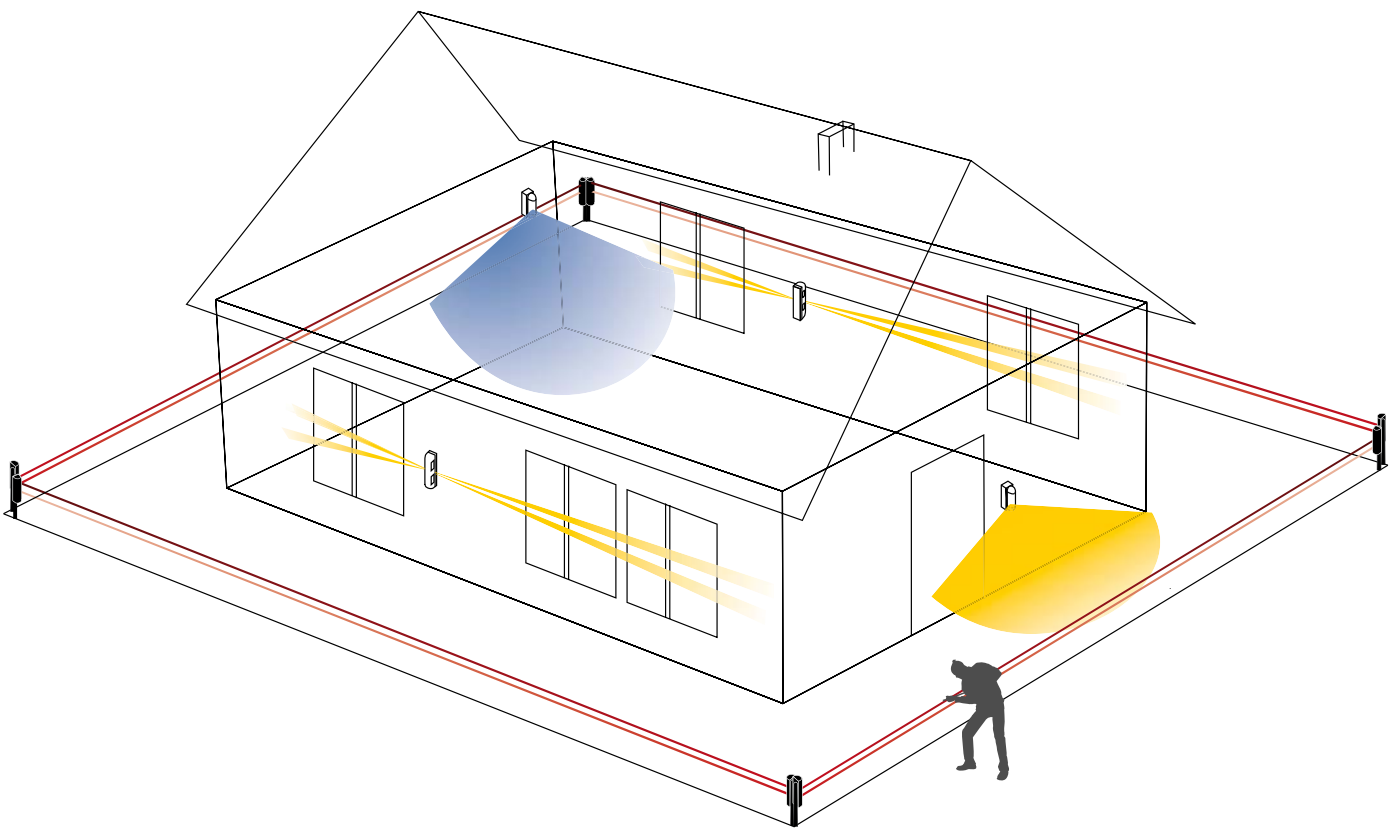
Projektowane w Polsce budynki wysokościowe powinny uwzględniać wyniki najnowszych prac koncepcyjnych i obowiązujące procedury związane z możliwością wykorzystania dźwigów do ewakuacji w czasie zagrożeń

Tadeusz Popielas
Sekretarz generalny
Polskiego Stowarzyszenia Producentów Dźwigów

Bibliografia:

Referaty wygłoszone na Konferencji „Fire & Risk Management", Bruksela, 4 października 2006 roku:
1. Robert Greet: *Ograniczanie rozwoju pożaru – Podziały budynku na strefy pożarowe.*
2. Pierre Bianchini: *Ograniczenie rozprzestrzeniania się pożaru przez szyby dźwigowe – nowa norma europejska EN 81-58.*
3. Eugene Doherty: *Lekcja 9.11* [11 września - przyp. red.] *– Zastosowanie dźwigów w przypadku pożaru – perspektywy w Stanach Zjednoczonych, Końcowy raport ze zniszczenia WTC Narodowego Instytutu Standardów i Technologii USA.*
4. Derek Smith: *Wykorzystanie dźwigów do ewakuacji w przypadku zagrożenia.*
5. Jean Paul Vestri: *Ewakuacja osób poszkodowanych i niepełnosprawnych przy użyciu dźwigów – sytuacja na poziomie normalizacyjnym Europejskiego Komitetu Normalizacyjnego (CEN).*
6. H. A. Ermer, prof. dr.: *Zabezpieczenie szybów dźwigowych przez zapewnienie w nich nadciśnienia na wypadek prowadzenia ewakuacji.*
7. James Fortune: *Nowe spojrzenie na możliwość ewakuacji przy zastosowaniu dźwigów po zniszczeniu WTC.*

TRÓJSTREFOWA ochrona



Firma Optex stworzyła niezawodny, kompleksowy system urządzeń, wykrywających wtargnięcie intruza na teren obiektu chronionego, jak i na jego obrzeża. System składa się z trzech stref ochrony obiektu:

• STREFA OCHRONY WEWNĘTRZNEJ

Chroni pomieszczenia obiektu.

W tej strefie zastosowanie znajdują pasywne czujki podczerwieni, czujki dualne (PIR + mikrofala) oraz bariery podczerwieni.

- RX-40QZ/40PT
- MX-40QZ/50QZ
- CX-502AM
- CX-702
- FX-360
- SX-360Z
- AX-100S/100SR

• STREFA OCHRONY ZEWNĘTRZNEJ

Chroni elewację budynku oraz obszar pomiędzy ogrodzeniem a obiektem.

W tej strefie zastosowanie znajdują pasywne czujki podczerwieni oraz bariery podczerwieni.

- LX-402
- LX-802N
- VX-402/402REC
- BX-80N
- BX-100PLUS

• STREFA OCHRONY OBWODOWEJ

Chroni obwód terenu wokół budynku.

W tej strefie zastosowanie znajdują cyfrowe i analogowe bariery podczerwieni krótkiego i dalekiego zasięgu.

- AX-70TN/130TN/200TN
- AX-100TF/200TF
- AX-250PLUS/500PLUS
- AX-350TF/650TF
- AX-350/650DH MK III

Te trzy poziomy bezpieczeństwa zapewniają pewną ochronę obiektu i polepszają działania prewencyjne.

Specyfikacja techniczna

OCHRONA WEWNĘTRZNA

	RX-40QZ/40PT	MX-40QZ	MX-50QZ	CX-502AM	CX-702	FX-360	SX-360Z	AX-100S/100SR
								
W domach	✓	✓	✓	–	–	✓	–	✓
W małych biurach	✓	✓	✓	–	–	✓	✓	✓
W dużych biurach	–	–	✓	✓	✓	–	✓	–
W pomieszczeniach przemysłowych	–	–	–	✓	✓	–	–	–
Zasięg detekcji	12x12m	12x12m	15x15m	15x 5m	21x21m 45x2,4m	Ø18-20m	Ø18m	30m
Zasilanie	9,5 - 16V=	9,5 - 16V=	9,5 - 16V=	9 - 18V=	9,5 - 16V=	9,5 - 18V=	6 - 18V=	8 - 18V=
Pobór prądu (odbiornik + nadajnik)	17mA maks.	18mA maks.	20mA maks.	19mA maks.	11mA	18mA maks.	18mA maks.	52mA maks. odbiornik+nadajnik
Temperatura pracy	-20°C - +50°C	-10°C - +55°C	-10°C - +55°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C

OCHRONA ZEWNĘTRZNA

	LX-402	LX-802N	VX-402	VX-402REC	BX-80N	BX-100PLUS
						
W domach	✓	✓	✓	✓	✓	✓
W małych biurach	✓	✓	✓	✓	✓	✓
W dużych biurach	–	✓	✓	✓	✓	–
W pomieszczeniach przemysłowych	–	–	✓	✓	✓	–
Współpraca z CCTV	✓	✓	✓	✓	✓	–
Zasięg detekcji	12 x 15m	24 x 2m	12m 90°	12m 90°	24m (12m na każdą stronę)	30m
Zasilanie	10,8 - 13.2V =	10,8 - 13,2V =	9,5 - 18V =	9,5 - 18V =	10 - 28V =	10,5 -30V =
Pobór prądu	25mA maks.	25mA maks.	NC : 28mA maks. NO : 35mA maks.	NC : 180mA maks. NO : 200mA maks.	38mA maks.	75mA maks.
Klasa ochrony IP	IP54	IP54	IP54	IP54	IP55	IP54
Temperatura pracy	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-35°C - +55°C

OCHRONA OBWODOWA

	AX-70TN/AX-130TN	AX-200TN	AX-100TF/AX-200TF	AX-250PLUS/AX-500PLUS	AX-350TF/AX-650TF	AX-350DH MKIII/AX-650DH
						
W domach	✓	✓	–	–	–	–
W małych biurach	✓	✓	✓	–	–	–
W dużych biurach	–	–	✓	✓	✓	✓
W pomieszczeniach przemysłowych	–	–	✓	✓	✓	✓
Zasięg detekcji	20m/40m	60m	30m/60m	75m/150m	100m/200m	100m/200m
Zasilanie	10,5 - 28V =	10,5 - 28V =	10,5 - 28V =	10,5 - 30V =	10,5 - 30V =	10,5 - 30V =
Pobór prądu (odbiornik + nadajnik)	38mA maks./41mA maks.	45mA maks.	44mA maks./48mA maks.	50mA maks.	78mA maks./80mA maks.	105mA maks./110mA maks.
Klasa ochrony IP	IP65	IP65	IP65	IP54	IP54	IP65
Temperatura pracy	-35°C - +60°C	-35°C - +60°C	-35°C - +60°C	-25°C - +55°C	-35°C - +60°C	-35°C - +60°C

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; e-mail: aat.warszawa@aat.pl

artykuł sponsorowany

Przegląd systemów sygnalizacji pożarowej firmy GE Security

Firma GE Security posiada bogatą ofertę systemów sygnalizacji pożarowej. W ciągu lat pojawiało się w niej wiele modeli o różnych symbolach. Artykuł ma na celu zaprezentowanie aktualnej oferty central pożarowych. Zostaną przedstawione zarówno analogowe adresowalne centrale pożarowe, jak i centrale konwencjonalne

Analogowe adresowalne centrale pożarowe

System adresowalny gwarantuje, że każdy element na pętli ma przypisany unikatowy adres. Dzięki temu centrala identyfikuje podłączone do niej urządzenie. Z kolei system analogowy mówi nam, że każda czujka i moduł przekazują do centrali informację o swoim stanie. Centrala na podstawie otrzymanych danych odpowiednio reaguje. Pozwala to na znaczne poszerzenie funkcjonalności systemu m.in. dzięki informowaniu o alarmie wstępnym, możliwości indywidualnego ustalania czułości elementów, kompensacji zanieczyszczeń czujek optycznych lub zmianie czułości systemu w zależności od pory dnia.

W ofercie firmy GE Security znajdą Państwo dwie serie analogowych adresowalnych central. Pierwsza to FP2000 – dla dużych obiektów i do wyrafinowanych zastosowań. Druga to seria FP1500 – system wprowadzony w zeszłym roku, cieszący się dużą popularnością, a instalowany w mniejszych obiektach.

Rodzina FP2000 – stabilność od wielu lat

Seria central FP2000 jest na rynku od wielu lat. To sprawdzona linia produktów, ciesząca się zaufaniem klientów. FP2000 jest cały czas rozwijana i udoskonalana. Obecnie występujące modele to FP1216N18 (do mniejszych instalacji) oraz FP286418 (do dużych obiektów). Różnią się konstrukcją oraz możliwością rozbudowy o dodatkowe moduły. Warto jednak pamiętać, że czujki oraz urządzenia pętlowe dla obu tych central są identyczne. Dotyczy to również funkcji, w jakie wyposażona jest centrala. Centrala FP1216N18 ma prawie wszystkie funkcje poprzednika, FP2864N18. Oba modele mają fabrycznie zapewnioną obsługę dwóch pętli. Ich liczbę oczywiście można zwiększyć, w przypadku centrali FP1216N18 do czterech pętli, a w przypadku FP2864N18 do ośmiu.

Najważniejszymi zaletami central z serii FP2000 są:

– **Zaawansowany algorytm weryfikacji fałszywych alarmów**. W celu eliminacji fałszywych alarmów po wykryciu zadymienia czujka optyczna wysyła w odstępie dwóch sekund dodatkowe dwa impulsy świetlne. W przypadku gdy dodatkowy pomiar potwierdzi stan zadymienia przekraczający próg alarmu, czujka sygnalizuje pożar. Ponadto czujki optyczne, jak i termiczne mają mechanizm automatycznej kompensacji zanieczyszczenia, uwzględniający w obliczeniach warunki środowiskowe oraz postępujące zanieczyszczenie czujki.
– **Elastyczny przydział pamięci**. W obiekcie, w którym potrzebna jest duża liczba wejść i wyjść, można powiększyć pamięć przewidzianą na tablice logiczne (ustawienia fabryczne przewidują 130 logicznych wejść i tyle samo wyjść). W tym przypadku centrala skorzysta z pamięci przeznaczonej na opisy tekstowe czujek i/lub stref.
– **Inne ustawienia pracy czujek w dzień i w nocy**. W trybie nocnym próg alarmu jest niższy o jeden poziom; czujka jest bardziej czuła.
– **Rozbudowane programowanie wejść/wyjść**. Centrale serii FP2000 cechują się bardzo dużymi możliwościami definiowania wejść/wyjść. Instalator może stworzyć do 999 logicznych wejść i tyle samo wyjść. Do dyspozycji są też zegary oraz znaczniki ułatwiające oraz upraszczające zapis w tablicy logicznej.
– **Szybka autokonfiguracja systemu.** Tryb autokonfiguracji zapewnia szybkie i łatwe programowanie centrali. Wystarczy, że po instalacji wszystkich urządzeń pętlowych instalator wejdzie do menu System\Ustawienia fabryczne\Urządzenia\ i wybierze albo konkretną pętlę, albo (przez cyfrę „0") wszystkie. Wtedy centrala „skanuje" pętlę i zapisuje wszystkie wykryte urządzenia. Po autokonfiguracji należy przypisać urządzenia do odpowiedniej strefy (po autokonfiguracji przypisane są do strefy 0) i dodać ich opis.

Adresowalna, analogowa centrala FP1216N18 – sprawdzona i pewna technologia od wielu lat

Rodzina FP1500 – rozwiązanie dla mniejszych obiektów

Jeśli potrzebujemy systemu sygnalizacji pożarowej do obiektu małej lub średniej wielkości, warto zwrócić uwagę na serię central FP1500. Instalator ma do wyboru dwa modele: FP1501 lub FP1502. Różnią się one jedynie tym, że pierwszy obsługuje jedną pętlę, a drugi dwie. Obu nie można rozbudować w tym zakresie. Centrale są niezawodne, wytrzymałe, mają też atrakcyjną cenę. Co więcej, wyróżniają się estetycznym wyglądem oraz łatwością konfiguracji i obsługi.

Instalator ma do zagospodarowania 250 adresów na każdej pętli. Przestrzeń adresowa od 1 do 125 przeznaczona jest na czujki. Jedna czujka zajmuje jeden adres. Do programowania czujek potrzebne jest urządzenie PG700 – programator czujek, umożliwiający również odczytanie bieżącej wartości czujki oraz skalibrowanie czujki po wymianie komory optycznej. Druga przestrzeń adresowa zaczyna się

Łatwa w obsłudze, szybka w instalacji, posiadająca estetyczny wygląd – centrala serii FP1500

od wartości 128, a kończy na 252. Jest przeznaczona na pozostałe moduły, tzn. na moduły wejściowe, wyjściowe oraz ROP-y (ręczne ostrzegacze pożarowe). Istotne dla instalatora jest to, że każdy moduł wejściowy lub wyjściowy zajmuje cztery adresy. ROP, tak jak czujka, zajmuje jeden adres.

Centrale z serii FP1500, podobnie jak centrale FP2000, mają tryb autokonfiguracji, inne ustawienia dla pracy czujek w dzień i w nocy oraz mechanizm kompensacji zanieczyszczenia. Oferują również programowanie wejść i wyjść przez tablice logiczne.

Konwencjonalne centrale pożarowe

W przypadku małych obiektów, gdzie potrzebne jest tylko zamontowanie kilku lub kilkudziesięciu czujek, nieekonomiczne jest decydowanie się na centralę adresowalną i analogową. Zdecydowanie bardziej opłacalne jest wybranie jednego z modeli central konwencjonalnych. Do wyboru jest centrala FP604 lub któraś z central z rodziny FP400.

FP604 – niezawodność działania przy małych obiektach

Model FP604 jest dostępny w ofercie GE już od dawna. Niezawodna konstrukcja gwarantuje długotrwałą i bezawaryjną pracę całego systemu. Centrala posiada cztery linie, jednak po zastosowaniu modułu ZI602 ich liczba zwiększa się do sześciu. Moduł ten zwiększa także liczbę wyjść. Stosując miniaturowe przekaźniki, można wykorzystać sześć dodatkowych wyjść typu NC do sygnalizacji stanów poszczególnych linii.

Regularny przegląd systemu jest prosty i dzięki wbudowanym funkcjom testowym może być przeprowadzony przez jedną osobę. Wszystkie informacje o zdarzeniach w systemie przedstawione są w postaci czytelnych i jednoznacznych sygnałów świetlnych. W przypadku gdy centrala ma pracować w wyjątkowo trudnych warunkach, można ją zaprogramować tak, aby reagowała dopiero po drugim sygnale z czujki.

Centrala może działać z osprzętem pracującym pod napięciem 12 lub 24 V. Napięcie zasilania systemu wybiera instalator. Niezależnie od tego wyboru, centrala wymaga tylko jednego akumulatora 12 V/7,2 Ah jako źródła napięcia podtrzymującego.

FP400 – duży wybór modeli

Przed rokiem, wraz z opisaną wcześniej rodziną central analogowych adresowalnych serii FP1500, firma GE Security wprowadziła również nową serię central konwencjonalnych FP400. Można powiedzieć, że seria ta to młodszy brat rodziny central FP1500. To doskonała propozycja dla tych, którzy mają ograniczony budżet na system pożarowy do małych lub średnich obiektów. Instalator ma do wyboru pięć modeli: FP402, FP404, FP408, FP412 oraz FP416 – ostatnie dwie cyfry mówią, ile stref (linii) obsługuje dana centrala. Użytkownik może zdecydować się na centralę obsługującą od dwóch do szesnastu linii.

Jeśli chodzi o wielkość obudowy, wszystkie opisane modele można podzielić na dwie kategorie. Do pierwszej należą modele FP402 i FP404, montowane w małej, estetycznej obudowie o wymiarach 297 x 307 x 105 mm. W obudowie jest miejsce na dwa akumulatory o pojemności 2,3 Ah każdy. Dzięki temu po utracie zasilania sieciowego system może pracować przez minimum 24 godziny na zasilaniu awaryjnym. Do drugiej kategorii należą centrale FP408, FP412 i FP416. Wyróżniają się one większą obudową o wymiarach 420 x 335 x 110 mm, która oczywiście pozwala na zamontowanie dwóch większych akumulatorów – o pojemności 7,5 Ah każdy. Dlatego przy większej liczbie linii nadal przez minimum 24 godziny podtrzymywane jest działanie systemu. Ponadto większa obudowa pozwala na zamontowanie większej liczby kart wyjść typu SB 404 i RB 404. Moduł RB 404 ma cztery wyjścia przekaźnikowe (styki NC/NO), a SB 404 wyposażony jest w cztery wyjścia monitorowane (na syreny lub inne urządzenia powiadamiające). Moduły te mogą pracować w kilku trybach, można indywidualnie ustawiać opóźnienia pracy wyjść. Możliwa jest też praca w trybie koincydencji – gdy do włączenia wyjścia wymagana jest informacja o pożarze z dwóch stref.

Podsumowanie

Przedstawiony powyżej opis central oferowanych obecnie przez firmę GE Security miał za zadanie pokazać rozwiązania, z których może skorzystać instalator. W niniejszej ofercie na pewno każdy znajdzie coś dla siebie, produkt najbardziej odpowiadający jego potrzebom.

Łukasz Wojtukiewicz
GE Security Polska

5 modeli do wyboru – szeroka oferta nowych central konwencjonalnych serii FP400

Zamki o zwiększonej odporności na włamanie

Wprowadzenie

Zamek to niezależne urządzenie, zwykle przymocowane do drzwi. Mogą być do niego wprowadzone nośniki kodu w celu porównania ich z kodem zapisanym w pamięci zamka. Prawidłowy dobór kodu pozwala na wykonanie ruchu przez urządzenia blokujące. Kod to wymagana informacja identyfikacyjna, która może być wprowadzona do zamka i która, jeżeli jest prawidłowa, pozwala na zmianę statusu jego zabezpieczenia.

Rozróżnia się następujące rodzaje kodów:
- kod materiałowy – określany przez właściwości fizyczne lub inne nośnika kodu;
- kod pamięciowy – zapamiętany, zawierający informację cyfrową i (lub) alfanumeryczną;
- kod biometryczny – działający z wykorzystaniem cech człowieka.

W zależności od formy nośnika kodu (obiektu, którego forma fizyczna lub własności określają kod wejściowy, np. klucza) rozróżnia się następujące rodzaje zamków:
1) mechaniczne – wyposażone jedynie w elementy mechaniczne;
2) elektroniczne – zabezpieczony częściowo lub całkowicie elementami elektrycznymi i (lub) elektronicznymi.

Zamki ze względu na przeznaczenie (zastosowanie) i kryteria oceny dzieli się na dwie grupy:
- zamki drzwiowe ogólnego stosowania;
- zamki skarbcowe, zwane zamkami o wysokim stopniu zabezpieczenia (ang.: *High Security Locks*, HSLs), stosowane w urządzenia i w drzwiach pomieszczeń do przechowywania wartości.

Zamek o wysokim stopniu zabezpieczenia HSL

Jest to niezależne urządzenie normalnie przymocowane do drzwi urządzeń bezpiecznego przechowywania. Mogą być do niego wprowadzone kodowane informacje w celu porównania ich z kodem zapisanym w pamięci urządzenia. Prawidłowy dobór kodów pozwala na wykonanie ruchu przez urządzenia blokujące.

Podstawowym dokumentem, na podstawie którego bada się i klasyfikuje zamki, jest Norma Europejska ENV1300.

Norma Europejska określa wymagania dla zamków o wysokiej skuteczności bezpiecznego przechowywania HSL w celu zabezpieczenia ich niezawodności, odporności na włamania i otwarcia przez osoby niepowołane, a także metody testowania. W normie podany jest również schemat klasyfikacyjny HSL w zależności od ich właściwości zabezpieczających.

Norma dotyczy mechanicznych i elektronicznych HSL. Nie obejmuje dodatkowych właściwości, które mogą podwyższyć całkowitą niezawodność systemu zabezpieczeń, takich jak:
1) kod główny (master) zabezpieczający przed zmianą kodu i (lub) pozwolenia/zakazu kodów równoległych;
2) kod czasowy dla zakazu nastaw czasowych;
3) integracja składowych alarmu lub funkcji;
4) działania przy sterowaniu zdalnym;
5) odporność na działanie kwasów;
6) odporność na promieniowanie Roentgena;
7) odporność na działanie materiałów wybuchowych.

W Polsce zamki HSL są badane i klasyfikowane według normy PN-EN 1300 w czterech klasach A, B, C, D, przy czym klasa A jest najniższa, D – najwyższa.

Zamki ogólnego stosowania

Zamki drzwiowe ogólnego stosowania obecnie klasyfikowane są na podstawie normy PN-EN 12209, a dla klasyfikacji, w odróżnieniu do zamków HSL przyjęto oznaczenie cyfrowe.

Aby ocenić skuteczność zamków w zakresie odporności na włamanie przyjęto następujące kryteria:
1) wymagania podstawowe,
2) odporność na manipulowanie,
3) odporność na wyśledzenie i kopiowanie kodu,
4) odporność na włamanie destrukcyjne,
5) odporność na fizyczne parametry środowiska,
6) niezawodność.

Zamki ogólnego stosowania były dotychczas klasyfikowane w pięciu klasach i oznaczane literowo O, T, A, B, C, co niejednokrotnie wprowadzało nieporozumienia w odniesieniu do zamków wysokiego bezpieczeństwa, klasyfikowanych wg PN-EN 1300.

Zamki w tych klasach powinny być odporne na atak przez przepiłowanie, ścięcie, rozwiercenie i inne niekonwencjonalne manipulacje niszczące, przez co najmniej:
- 0 min w klasie O oraz T,
- 1 min w klasie A,
- 3 min w klasie B,
- 6 min w klasie C.

Zamki ogólnego stosowania mocowane są głównie w drzwiach i służą do blokowania rygli lub uruchamiania innych elementów zabezpieczających.

Klasyfikacja i akty normatywne zamków ogólnego stosowania

Metody badań i oceny zamków ogólnego zastosowania określają następujące polskie normy:

PN-EN 12209	Okucia budowlane. Zamki. Zamki mechaniczne wraz z zaczepami. Wymagania i metody badań.
PN-EN 1906	Okucia budowlane. Klamki i gałki drzwiowe wraz z tarczami. Wymagania i metody badań.
PN-EN 1303	Okucia budowlane. Wkładki bębenkowe do zamków. Wymagania i metody badań.

Zamki powinny mieć konstrukcję uniemożliwiającą otworzenie ich kluczem o innym profilu lub kombinacji nacięć niż w kluczu dostarczonym w komplecie z zamkiem.

Zastawki powinny mieć zarys wewnętrzny obustronnie wyprofilowany. Blokowanie przesuwu zasuwki przez zastawkę powinno następować również wtedy, gdy wymiar klucza jest większy lub mniejszy od prawidłowego.

Konstrukcja zamka powinna uniemożliwiać wykonanie pomiarów lub odcisków w zamku przez otwór kluczowy, w celu wykonania klucza zastępczego.

Można przyjąć, że (w przybliżeniu) większa cyfra i dalsza litera alfabetu określa wyższe wymagania.

Dodatkowo, poza klasyfikacją, wprowadzono parametr odporności na włamanie, który istniał w dotychczasowych normach, natomiast w obecnych nie występuje. Głównie dotyczy to badań odporności na manipulacje bez użycia klucza.

Z jednej strony należy to traktować jako pewne niedopatrzenie, z drugiej, docelowo przewidziano, że ten parametr będzie określany przy badaniu drzwi. Na dziś taki sposób jest nie do

Tabela 1. Klasyfikacja zamków według normy PN-EN 12209

Kategoria użytkowania	Trwałość	Masa drzwi	Odporność ogniowa	Bezpieczeństwo	Odporność na korozję i temperaturę	**Zabezpieczenie**	Obszar zastosowania	Sposób uruchamiania, ryglowania	Typ działania trzpienia	Identyfikacja klucza	Odporność na włamanie
3	**C**	**1**	**0**	**0**	**C**	**2**	**E**	**A**	**0**	**D**	**C**

przyjęcia i odporność na włamanie należy oceniać podczas badania i klasyfikacji zamka.

Dlatego też wprowadzono dodatkową pozycję klasyfikacyjną, która jest podstawowa dla oceny zamka i jego przydatności jako wyrobu o zwiększonej odporności na włamanie.

Jeśli zamek posiada zastawki współpracujące z kluczem (dostarczonym w komplecie), istotna jest jego odporność na manipulacje, czyli otwarcie metodami nieniszczącymi. Ta cecha zamka jest zawarta w dodatkowej informacji literowej A, B, C, odpowiadającej odporności na włamanie zgodnej z dotychczas stosowanymi wymaganiami przedstawionymi na początku artykułu.

Ze względu na dość złożoną klasyfikację zamków, należy skoncentrować się na kilku najistotniejszych cechach zamków.

Na przykład tylko zamek w klasie 5 i 7 zabezpieczony jest przed wierceniem.

W pozostałych klasach zamki muszą przy montażu być kompletowane z odpowiednimi blachami zabezpieczającymi i szyldami ochronnymi dobrej jakości.

Wkładki bębenkowe do zamków wg PN-EN 1303:2007 (Wymagania i metody badań)

Wkładka bębenkowa – urządzenie, zwykle oddzielne od współpracującego zamka lub zatrzasku, uruchamiane kluczem. W praktyce współpracuje z zamkiem i z jego mechanizmem ryglowym, umiejscowionym w odpowiedniej kasecie.

Stosowanie wkładek jest bardzo praktyczne i poprawia bezpieczeństwo użycia. Bez konieczności wymiany zamka można, tylko wymieniając wkładkę, szybko zmienić kod. Ponadto wkładki są wyposażone w małe klucze, co znacznie ułatwia ich przechowywanie.

Tabela 2.: Klasyfikacja wkładek bębenkowych do zamków według normy PN-EN 1303

1	2	3	4	5	6	7	8	9
Kategoria użytkowania	Trwałość	Masa drzwi	Odporność ogniowa	Bezpieczeństwo	Odporność na korozję i temperaturę	Zabezpieczenie związane z kluczem	Odporność na atak	Odporność na włamanie
1	**6**	**–**	**0**	**–**	**0**	**6**	**2**	**C**

Objaśnienie:

1	Kategoria użytkowania	wkładki bębenkowe powinny być klasyfikowane w kategorii użytkowania 1
2	Trwałość (cykle próbne)	wkładki bębenkowe powinny być klasyfikowane w klasach trwałości 4, 5, 6 Klasa trwałości 4 – 25 000 cykli Klasa trwałości 5 – 50 000 cykli Klasa trwałości 6 – 100 000 cykli
3	Masa drzwi	nieklasyfikowana
4	Odporność ogniowa	wkładki bębenkowe powinny być klasyfikowane w klasach odporności ogniowej 0 lub 1; w klasie 0 – brak wymagań
5	Bezpieczeństwo	nieklasyfikowane
6	Odpornośc na korozję	wkładki bębenkowe powinny być klasyfikowane w klasach korozyjnych 0 lub 1; klasa 0 nie wymaga minimalnej odporności ma korozję
7	Bezpieczeństwo kodu	wkładki bębenkowe są klasyfikowane w klasach od 1 do 6: klasa 6 jest najwyższa
8	Odporność na atak	określa się trzy klasy (0, 1, 2); wkładki powinny być odporne na atak przepiłowanie, ścięcie, rozwiercenie i inne niekonwencjonalne manipulacje niszczące, przez co najmniej: 0 min – w klasie 0 3 min – w klasie 1 5 min – w klasie 2
9	Odporność na włamanie	pozycja dodatkowa, określa odporność na włamanie. Badania dodatkowe określające odporność wkładki na manipulację. Odpowiednio: klasa A – 1 min, B – 3 min i C – 6 min

Tabela 3. Okucia budowlane. Klamki i gałki drzwiowe wraz z tarczami wg PN-EN 1906 (Wymagania i metody badań)

1	2	3	4	5	6	7	8
Kategoria użytkowania	Trwałość	Masa drzwi	Odporność ogniowa	Bezpieczeństwo	Odporność na korozję i temperaturę	Zabezpieczenie	Tryb działania
1	**6**	**–**	**0**	**–**	**0**	**6**	U

Objaśnienie:

1	Kategoria użytkowania	określa cztery klasy (1, 2, 3, 4) w zależności od częstotliwości użytkowania; wkładki bębenkowe powinny być klasyfikowane
2	Trwałość (cykle próbne)	wyróżnia się dwie klasy trwałości: – klasa 6: średnia częstotliwość użytkowania: 100 tys. cykli – klasa 7: średnia częstotliwość użytkowania: 200 tys. cykli
3	Masa drzwi	nieklasyfikowana
4	Odporność ogniowa	Odporność ogniowa – określa się dwie klasy odporności ogniowej: – klasa 0: niedopuszczone do stosowania w drzwiowych przeciwpożarowych/dymoszczelnych – klasa 1: odpowiednie do stosowania w drzwiowych przeciwpożarowych/dymoszczelny
5	Bezpieczeństwo	określa się dwie klasy bezpieczeństwa: – klasa 0: normalne użytkowanie; – klasa 1: zastosowania wymagające podwyższonego bezpieczeństwach
6	Odpornośc na korozję	określa się pięć klas odporności na korozję według PN-EN 1670:1998
7	Zabezpieczenie	określa się pięć klas zabezpieczenia – klasa 0: okucie niedopuszczone do stosowania w drzwiach o zwiększonej odporności na włamanie; – klasa 1: niska odporność ma włamanie; – klasa 2: średnia odporność ma włamanie; – klasa 3: wysoka odporność ma włamanie; – klasa 4: bardzo wysoka odporność ma włamanie
8	Tryb działania	określa się trzy typy działania: – typ A: okucie wspomagane sprężyną; – typ B: okucie obciążone sprężyną; – typ U: okucie bezsprężynowe.

Badanie odporności wkładki na manipulację jest ważną cechą wkładki, która nie została ujęta w badaniach normy PN-EN 1303.

Pozycja 9 w tabeli nr 2 (odporność na włamanie) jest podstawowa dla oceny wkładki i przydatności jako wyrobu o zwiększonej odporności na włamanie.

W znaku siódmym (bezpieczeństwo kodu) są zawarte najważniejsze cechy wkładki bębenkowej.

Znak ósmy (odporność na atak) informuje, czy wkładka może funkcjonować niezależnie od klasy szyldu ochronnego. Znak ósmy „0" informuje, że wkładka nie jest odporna na atak metodami niszczącymi i wymaga wysokiej klasy szyldów ochronnych.

Okucia budowlane. Klamki i gałki drzwiowe wraz z tarczami wg PN-EN 1906 (Wymagania i metody badań)

Okucie stanowi istotny element zabezpieczenia zamka w drzwiach (tabela 3).

Sposoby zabezpieczeń zamków w drzwiach

Zamki stosuje się do bezpośredniego lub pośredniego uruchamiania mechanizmów ryglowych. Pośredni system uruchamiania systemów ryglowych stosuje się w przypadku potrzeby przeniesienia przez układ zamykający dużych obciążeń.

Zamki mieszkaniowe ogólnego zastosowania służą do bezpośredniego uruchamiania i blokowania systemów ryglowych.

Stosowane elementy zabezpieczające układy zamkowe to płytki z materiałów trudno obrabialnych umieszczane na powierzchni zamka.

Najczęściej stosuje się utwardzone płyty stalowe, które umieszcza się tak, aby chroniły zamek lub inne ważne elementy zespołu ryglowego przed destrukcyjnymi działaniami z zewnątrz.

Typowym zabezpieczeniem zamka drzwiowego są odpowiednie tarcze drzwiowe. Osłaniają one zamek lub jego najważniejsze elementy.

Inny sposób zabezpieczający zamki to wykonywanie niektórych ich elementów (jak np. zastawki kołkowe wkładek bębenkowych) z materiałów trudno obrabialnych.

Zakończenie

Zamki o zwiększonej odporności na włamanie mają zastosowanie w obiektach, dla których istnieje duże zagrożenie włamania.

Ponieważ zamek stanowi podstawowe zabezpieczenie, bardzo ważna jest dokładność i jakość wykonywanych produktów. Każdy dostawca, deklarując klasę danego wyrobu, powinien mieć świadomość, że spoczywa na nim duża odpowiedzialność. Odpowiedzialny dostawca powinien zawsze skorzystać z usług wyspecjalizowanych osób czy firm, by uzyskać ocenę swoich wyrobów.

Metoda kwalifikacji zamków czy też wkładek jest skomplikowana. Tylko dokładne opisanie zamków i wskazanie właściwych parametrów pozwoli na właściwy wybór. Oczywiście bardzo ważną cechą jest odporność na włamanie, manipulacje. Tylko zamek oznaczony tym parametrem dodatkowym, nadaje się do stosowania w przypadku wyrobów o zwiększonej odporności na włamanie.

Brak oznaczenia dodatkowej cechy na zamku czy też na wkładce oznacza tylko jedno – taki zamek czy wkładka nie są odporne na włamanie.

Inna kwestia to zamki wysokiego bezpieczeństwa, które przeznaczone są do wyrobów służących do przechowywania wartości czy też innych przedmiotów, takich jak broń i amunicja lub dokumenty niejawne.

Miron Durzewski
Instytut Mechaniki Precyzyjnej

Satel - Inteligentne systemy alarmowe

Przede wszystkim jakość

Od 17 lat specjalizujemy się wyłącznie w produkcji urządzeń do systemów alarmowych. Posiadamy własne laboratorium, dostosowujemy produkty do najwyższych standardów i norm Unii Europejskiej, przeprowadzamy kontrolę jakości na każdym etapie produkcji. Dbamy aby produkt, który trafia w Państwa ręce, był niezawodny, przyjazny w użytkowaniu, funkcjonalny i nowoczesny.

- posiadamy system nadzoru procesu produkcji, który umożliwia śledzenie produktu od momentu rozpoczęcia montażu, aż do chwili jego sprzedaży
- produkty wykonane są z wyselekcjonowanych elementów od najlepszych dostawców podzespołów
- posiadamy w pełni zautomatyzowany proces montażu SMD wykorzystujący super dokładne i szybkie maszyny firmy JUKI
- gwarantujemy, że 100% produktów jest testowana zanim trafi do sprzedaży
- stosujemy podczas produkcji pełną ochronę ESD
- posiadamy certyfikowany system zarządzania jakością zgodny z normą ISO 9001:2000
- zapewniamy obsługę gwarancyjną i pogwarancyjną naszych produktów
- do każdego produktu dołączamy jasną i zrozumiałą dokumentację montażu i obsługi pisaną w języku polskim
- produkty SATEL sprzedawane są w ponad 40 krajach na całym świecie, gdzie ich jakość i funkcjonalność została wysoko oceniona

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

Artykuł sponsorowany

Zabezpieczenia w dobie TERRORYZMU

Duże zaangażowanie Polski w działania wojskowe i misje międzynarodowe, mające na celu walkę z terroryzmem, niesie za sobą realne zagrożenie ataku skierowanego na najważniejsze obiekty administracji państwowej, lotniska, instalacje przemysłowe oraz militarne na terenie kraju

Jeszcze kilka lat temu ambasady, budynki rządowe i ministerstwa były uważane za miejsca względnie bezpieczne, a ich ochrona sprowadzała się jedynie do zabezpieczenia przed natarciem hałaśliwych demonstrantów. Również w przypadku obiektów takich jak bazy wojskowe, porty lotnicze, rafinerie podstawę systemu ochrony obwodowej stanowiły wysokie ogrodzenia i zasieki z drutu kolczastego, a dostępu do chronionej strefy bronił uzbrojony strażnik. Dzisiejsze czasy pokazują, że ochrona – tam, gdzie jest konieczna – powinna stać na najwyższym poziomie. Musi opierać się nie tyle na wykwalifikowanych specjalistach, ile na niezawodnym sprzęcie wysokiej klasy. Technologia XXI wieku stosowana przez firmę Gunnebo Polska pozwala na stworzenie systemu zabezpieczeń dla każdego obiektu i na każdą okoliczność. Zagrożenia, które niesie ze sobą rzeczywistość, wymagają przemyślanych rozwiązań. Realizując hasło *Gunnebo for a safer world*, koncern projektuje rozwiązania i technologie ułatwiające osiągnięcie celu.

Automatyczne blokady drogowe firmy Gunnebo należą do grupy produktów, które na całym świecie chronią przed atakami terrorystycznymi obiekty o szczególnym znaczeniu cywilnym oraz militarnym. Stanowią doskonałe zabezpieczenie przed wymuszonym lub nieautoryzowanym wjazdem pojazdów do chronionej strefy. Urządzenia znajdują zastosowanie wszędzie tam, gdzie liczy się czas reakcji i niezawodna oraz pewna ochrona. Charakteryzują się doskonałą jakością, sprawnością działania w każdych warunkach i ogromną wytrzymałością na zderzenia, czego dowiodły testy w Stanach Zjednoczonych, Niemczech i Wielkiej Brytanii.

Road Block DSP

Blokady drogowe Road Block DSP oferują maksymalną ochronę punktów kontrolnych prowadzących do chronionej strefy (bram wjazdowych). Stanowią najwyższy standard ochrony i bezpieczeństwa. Zabezpieczają przed nieautoryzowanym wjazdem pojazdów każdej wielkości i masy.

Blokady DSP zaprojektowano w taki sposób, by nawet po zderzeniu z ciężarówką zachowały całkowitą sprawność i dawały pełną ochronę wjazdu. By uzyskać niemiecki certyfikat TÜV, urządzenie poddano próbie zderzeniowej z jadącą z prędkością 80 km/h ciężarówką, której masa wynosiła 7,5 tony. Po wykonanym teście blokady DSP funkcjonowały normalnie, bez konieczności serwisowania. Blokady są produkowane w dwóch wersjach i czterech zakresach wytrzymałości, a ich parametry dobierane są w zależności od specyfiki miejsca instalacji oraz wymagań klienta.

Road Block DSP oferuje najwyższe bezpieczeństwo dzięki:
- wytrzymałości na uderzenia do 5000 kN,
- szybkości otwarcia wynoszącej 2 s,
- elementowi blokującemu wysokiemu na 650 mm i szerokiemu do 8 m,
- funkcji *Panic open*,
- wydajnemu napędowi elektrohydraulicznemu,
- zastosowaniu we wszystkich komponentach stali wysokogatunkowej przenoszącej duże obciążenia,
- przenoszonemu naciskowi (100 kN), zgodnemu z DIN 1072,
- napędowi ręcznemu pozwalającemu na obsługę np. w przypadku braku zasilania,
- spełnianiu warunków technicznych wymaganych przez Niemiecki Instytut Techniczny.

Tyre Killer

Blokady ostrzowe Tyre Killer gwarantują zatrzymanie pojazdu dzięki solidnym ostrzom. Stanowią doskonałe zabezpieczenie przed wymuszonym lub nieautoryzowanym wjazdem. Podczas próby sforsowania opony, a także podwozie pojazdu ulegają całkowitemu zniszczeniu.

Tyre Killer oferuje najwyższe bezpieczeństwo dzięki:
- solidnym ostrzom o wysokości 450 mm i kącie natarcia wynoszącym 60 stopni,
- elementowi blokującemu szerokości od 2,4 m do 6 m,
- szybkości otwarcia poniżej 3 s,
- instalacji w betonowej komorze głębokiej na 500 mm,
- kompaktowej budowie gotowej do natychmiastowego montażu,
- przenoszonemu naciskowi (100 kN), zgodnemu z DIN 1072,
- bardzo wydajnej elektrohydraulicznej jednostce napędowej ukrytej pod powierzchnią jezdni.

Lifted Barriers

Belki zaporowe Lifted Barriers – zastępują tradycyjne łatwe do pokonania rogatki, jednocześnie dając możliwość instalacji w niskich pomieszczeniach, bez względu na długość ramienia.

Charakteryzują się ponadprzeciętną wytrzymałością na uderzenia, czego dowiodły testy przeprowadzone w Stanach Zjednoczonych. Pojazd o masie 7,5 tony poruszający się z prędkością 50 km/h i przewożący niebezpieczny ładunek został zatrzymany w kontrolowany sposób gwarantujący pozostawienie ładunku przed blokadą. Blokada nie została sforsowana przez pojazd.

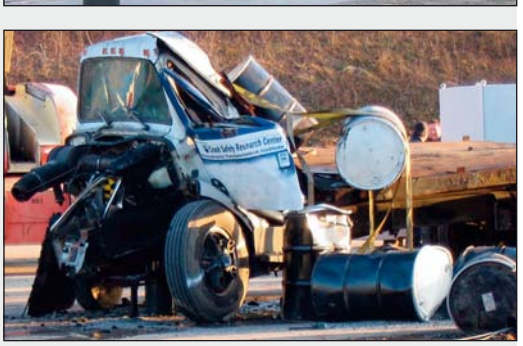
Belki zaporowe oferują wysokie bezpieczeństwo dzięki:
- wytrzymałości na uderzenia do 1300 kN,
- szybkości zamknięcia do 4 s,
- wydajnemu napędowi elektrohydraulicznemu,
- ramieniu blokowanemu przez zworę elektromagnetyczną,
- napędowi ręcznemu pozwalającemu na obsługę np. w przypadku braku zasilania.

Bollards System

Automatyczne słupki Bollards System są używane w miejscach ogólnie dostępnych dla przechodniów i częściowo wyłączonych z ruchu kołowego. Słupki nie kolidują z ruchem osobowym jednocześnie gwarantują dostęp uprawnionym pojazdom. Urządzenia znajdą zastosowanie wszędzie tam, gdzie wymagana jest maksymalna ochrona i niezawodność.

Podobnie jak wcześniej wymienione urządzenia automatyczne słupki Bollards System zostały poddane testom zderzeniowym, które dowiodły ich solidności.

Słupki oferują najwyższe bezpieczeństwo dzięki:
- wytrzymałości na uderzenia do 656 kN,
- elementowi blokującemu wysokiemu na 750 mm lub 900 mm,
- szybkości otwarcia wynoszącej około 2 s w zależności od typu,
- wydajnemu napędowi elektrohydraulicznemu,
- przenoszonemu naciskowi (100 kN), zgodnemu z DIN 1072,
- napędowi ręcznemu pozwalającemu na obsługę np. w przypadku braku zasilania.



Produkty firmy Gunnebo Polska symbolizują: jakość, trwałość, nowoczesność i niezawodność, o czym świadczą spełniane normy, posiadane certyfikaty, zdobyte nagrody i uznanie klientów. Gunnebo zapewnia kompleksową obsługę na najwyższym poziomie w fazie projektowania, montażu i szkolenia oraz w każdej innej sytuacji wymagającej fachowej pomocy, doradztwa lub wiedzy merytorycznej.

Bartosz Kędzia
Gunnebo Polska
www.gunnebo.pl

Teoria ochrony informacji

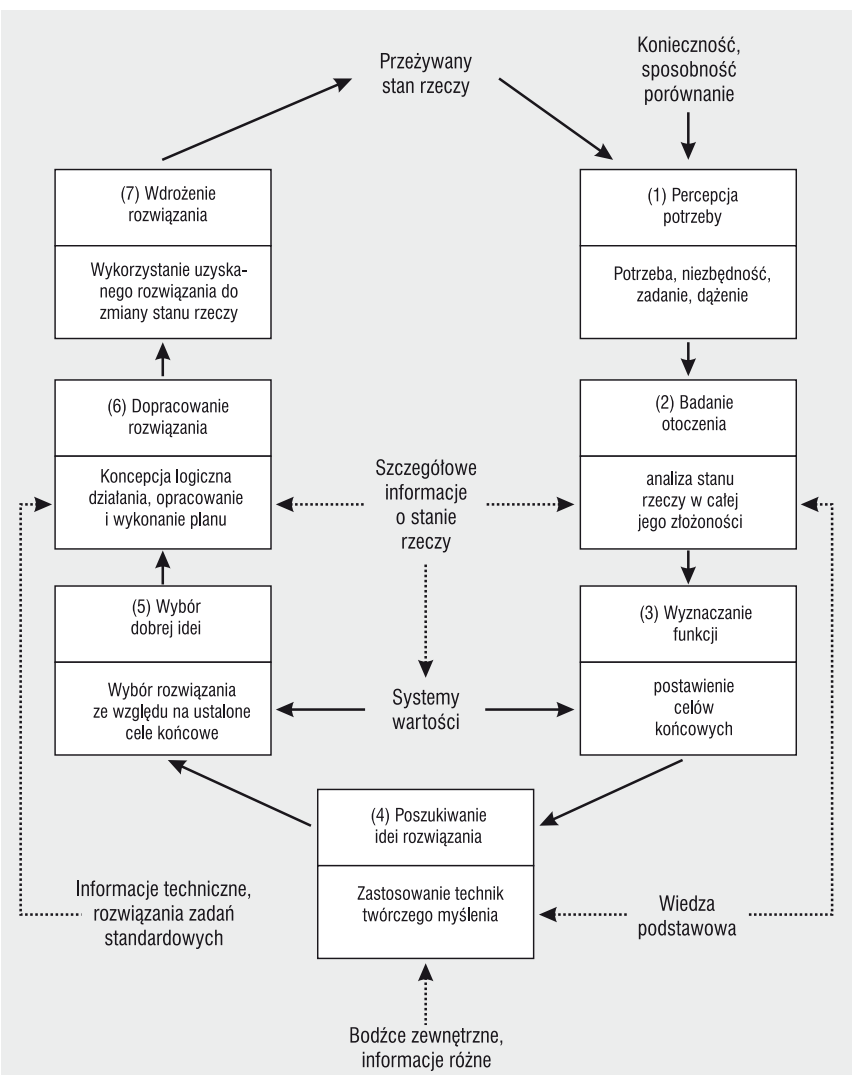
(część 1.)

Cykl, składający się z trzech artykułów publikowanych w kolejnych numerach *Zabezpieczeń*, ma (w zamierzeniu autora) w sposób prosty, łatwy i przyjemny – przy wykorzystaniu zasad analizy funkcjonalnej – przybliżyć PT Czytelnikom rolę inżynierii bezpieczeństwa w ochronie informacji. Jest to więc rodzaj ściągi tematycznej przeznaczonej dla najwyższego kierownictwa firm

1. Wstęp

W bezpiecznym społeczeństwie informacyjnym („trzeciej fali" wg A. H. Toffflerów[1]) wszelkie działania muszą i powinny opierać się na świadomym kontrolowaniu bezpieczeństwa ogólnego przez nadzorowanie bezpieczeństwa informacji – tej, którą gromadzimy, wykorzystujemy i udostępniamy otoczeniu. Inżynieria bezpieczeństwa informacji to przede wszystkim umiejętność analizowania otoczenia pod względem zbierania i wykorzystywania każdej z wielu dostępnych danych [Ross Anderson[2] i jego analizy] na potrzeby bieżące bezpieczeństwa instytucji/organizacji/grupy społecznej.

Użycie systemowej metody analizy funkcjonalnej[3] na potrzeby opisu przedstawionego zagadnienia i jego



Rys. 1. Pętla algorytmu badawczego metody analizy funkcjonalnej

1) Alvin Toffler (1928) – socjolog i publicysta, jest jednym z najbardziej znanych w świecie futurologów. Jego książka *Szok przyszłości* (1970, wyd. polskie: 1975) została przełożona na ponad 30 języków i ukazała się w łącznym nakładzie ponad 10 milionów egzemplarzy. Wydał też m.in. *Ekospazm* (1975) i, wspólnie z żoną Heidi, *Trzecią falę* (1980, wyd. polskie: 1989). Laureat wielu nagród i doktoratów *honoris causa*.
2) Ross Anderson: *Inżynieria zabezpieczeń,* WNT, Warszawa, 2005.
3) Michel Fustier: *Analiza funkcjonalna*, rozdz. 4., zbiór 4. serii „Techniki twórczego myślenia" pod red. A. Góralskiego, WNT, Warszawa, 1982, s. 80–109.

rozwiązania wydaje się tu ze wszech miar zasadne. Sama metoda charakteryzuje się wyjątkową prostotą pętli podstawowego algorytmu postępowania w prowadzonym procesie analizy problemu i w podejściu do generacji praktycznie sprawdzalnego rozwiązania, którego warunkowe przyjęcie jest przede wszystkim zobligowane możliwościami pomyślnego wdrożenia. Takie postępowanie ma zarazem zachowane wszelkie pierwiastki rozwiązań *a posteriori*, tych ujawnionych w trakcie analizy, a zarazem z różnych względów (organizacyjnych, materialnych, osobowych itp.) niezbyt możliwych do bezpośredniego włączenia we wdrażane rozwiązanie (mimo ich słuszności i zgodności z wybraną dobrą ideą).

Analiza funkcjonalna składa się z siedmiu etapów:

1) percepcji potrzeby;
2) badania otoczenia;
3) wyznaczenia funkcji;
4) poszukiwania idei rozwiązania;
5) wyboru dobrej idei;
6) dopracowania rozwiązania;
7) wdrożenia rozwiązania.

Schemat realizacji algorytmu metody przedstawia rys. 1.

Należy zwrócić szczególną uwagę na zgodność formalną między oceną stanu przeżywanego będącą inspiracją działania oraz wskazywane mierniki wartości wykorzystywane w budowaniu kolejnych ocen – ich podstawa powinna być ujednolicona (dopuszcza się określoną na wstępie prac kompatybilność pojęć).

Pragnę zwrócić tutaj szczególną uwagę zarówno na wielokrotne czerpanie informacji z zasobu wiedzy podstawowej (2. i 4. krok), jak i na wykorzystanie doświadczeń oraz wyników objętych ogólnie znanymi rozwiązaniami standardowymi (6. krok), bez których trudno by było mówić o wdrożeniu jakiegokolwiek rozwiązania (nieufność przełożonych wobec nowości, nawet dla najbardziej słusznych nowatorskich rozwiązań, jest ogólnie znana).

Technologie obronne i bezpieczeństwa informacji są obecnie na etapie bardzo intensywnego rozwoju we wszystkich warstwach społeczeństwa (od gminy po władze centralne państwa), choć nie wszyscy z nas zdają sobie sprawę ze skutków i wagi przypadkowego (zbędnego) ujawniania nawet drobnych „okruchów informacyjnych", dotyczących rzeczy istotnych dla bezpieczeństwa danej społeczności (jej spraw życiowych), stąd też niniejszy cykl.

Jego ideą jest pokazanie znaczenia prawidłowej oceny każdego (nawet drobnego) incydentu z zakresu naruszania bezpieczeństwa i uświadomienie (sobie i innym), jak ważne jest niedopuszczenie do powstawania ryzyk i ich materializacji w postaci widocznych szkód i (czasami nieodwracalnych) strat materialnych oraz osobowych.

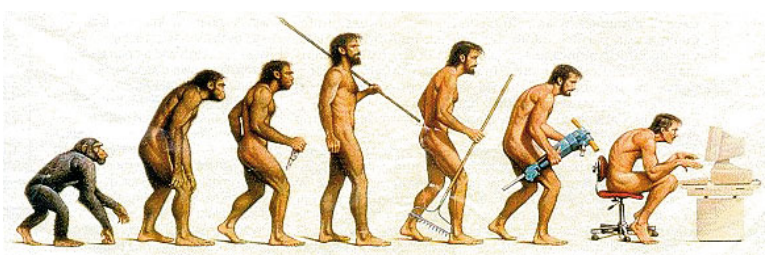
Podstawą są teoretyczne (securitologia – dziedzina nauki od 1989 roku zajmująca się wieloaspektowością postrzegania i „odczytywania" bezpieczeństwa jako obiektu badań) oraz praktyczne (materiały seminaryjne Polalarm, Techom, OSPOIN, Instytutu Bezpieczeństwa Biznesu Grupy Konsalnet, Komitetu Bezpieczeństwa Biznesu Krajowej Izby Gospodarczej oraz informatory Biura Prewencji Komendy Głównej Policji) opracowania związane z aspektami ochrony informacji o osobach i rzeczach (nie tylko w rozumieniu biznesowym).

Odniesienia do problemu pokazywane są w zmieniającym się pod względem komunikacji oraz współdziałania otoczeniu ludzkim, ze szczególnym zwróceniem uwagi na konieczność wyjścia na przeciw tym (nie zawsze korzystnym) zmianom w danym środowisku. Uzupełnieniem odniesień są okresowo przywoływane zobowiązania o charakterze biznesowym (np. OECD, ale nie tylko) wynikające z sojuszy (NATO, EUMS), unii (UZE/WE/UE) i umów międzynarodowych, zasadniczo związane z ochroną i obroną państwowości, porządkiem publicznym i zobowiązaniami militarnymi.

2. Ochrona informacji jako reakcja człowieka

Kiedy mówimy o ochronie informacji, bardzo często odnosimy nasze działania do systemów jej przetwarzania (teleinformatycznych, telekomunikacyjnych, telekodowych itd.) oraz nośników (trwałych, bezpośrednio czytelnych – *hard-copy*; okresowych, czytelnych systemowo – OEM, czyli opto-elektroniczno-magnetycznych), przy czym zapominamy o najważniejszym – człowieku, który przez wieki tę informację zbierał, agregował i wykorzystywał (mniej lub bardziej świadomie – zobacz rysunek).

Człowiek, jako obiekt analizy stanowi zagadnienie samo w sobie, dlatego też w obszarze prowadzonych dywagacji trudno się ustrzec modelowych uproszczeń i uprzedzeń w ocenie (związanych z niefrasobliwością osób na kierowniczych stanowiskach, zaobserwowaną przeze mnie w trakcie pracy jako konsultant, audytor czy biegły sądowy) poszczególnych postaci i grup ze świata biznesu.



Rys. 2. Od małpy i pitekantropa (homo erectus) do współczesności (homo computerus?)

Skrót myślowy na rysunku wydaje się zbyt duży, tymczasem to właśnie człowiek jest źródłem informacji. Czasami mimowolnie ujawnia innym pewne szczegóły, zdradza się ze swoją wiedzą. Od zarania dziejów bowiem wykorzystywał tą wiedzę dla siebie, ukrywał przed innymi i (jak nas uczy historia) manipulował nią dla własnych (osobistych, plemiennych czy też narodowych) celów.

To właśnie konieczność dzielenia się fragmentaryczną wiedzą z innymi w grupie, niezbędna dla osiągnięcia założonych (ukrytych przed innymi członkami populacji) celów, wywołała potrzebę ochrony informacji, stworzyła formy i metody niezbędne do jej realizacji.

Rozwijały się różnymi drogami (od szyfru Cezara po steganografię), ale zawsze chodziło przede wszystkim o ogólnie rozumianą ochronę istotnych wartości i informacji dotyczących meritum sprawy (pieniądza – Fenicjanie, tajemnic wiary – templariusze, tajemnic grupy – loże masońskie itd.) na poziomie maksymalnego, możliwego do osiągnięcia bezpieczeństwa.

Czy pojedynczy człowiek, sam z siebie, jest w stanie na tyle opanować swoje świadome i nieświadome (mowa ciała) reakcje, aby nie poddać się bezpośredniej ocenie i odczytowi własnych emocji (kod werbalny, werbalne zachowania maskujące – wokalne i wizualne sygnały stanu) w odniesieniu do chronionych przezeń informacji?

Czy i na ile jest świadomy oddziaływań celowych na jego postawę, realizowanych z wykorzystaniem socjotechnik tylko po to, aby sprowokować go/zmusić do niekorzystnego zachowania (wybujałe ambicje i wstyd idą tutaj w parze)?

„Zrozumienie istoty bezpieczeństwa oraz zdobywanie i ochrona informacji stały się we współczesnym biznesie problemem, który wymaga nie tylko praktycznych umiejętności, ale także poprawnych procedur uwzględniających analizy naukowe i doświadczenia praktyczne”[4].

Wszystko to należy zatem badać i ujmować nie tylko w teoretyczne rozważania, lecz także sprowadzać do przejrzystych i czytelnych procedur oraz prostych i zrozumiałych instrukcji.

3. Ochrona informacji jako dziedzina nauki – securitologia[5]

Zasoby informacyjne to współcześnie najistotniejszy składnik struktury zasobów dowolnej organizacji – nie sposób tu mówić o jego cenności. Podstawowym pojęciem wymagającym analizy jest bezpieczeństwo informacji.

Charakterystyczne dla jego opisu jest uwzględnienie wielorakich czynników obiektywnych i subiektywnych, socjopsychologicznych i kulturowych, politycznych i prawnych, przyrodniczych i technicznych, makro- i mikroekonomicznych warunkujących zagrożenia i pozostających także wzajemnie w nierozerwalnych związkach, funkcjonujących w bliskim otoczeniu systemowym, wpływających zarówno na strukturę samego pojęcia, jak i jego materialną realizację w danych warunkach.

Pierwsze publikacje podejmujące próbę wyodrębnienia nauki o zarządzaniu bezpieczeństwem życia człowieka – securitologii jako dyscypliny naukowej pochodzą z lat 90. ubiegłego wieku, co można wyjaśnić przede wszystkim nowymi potrzebami i oczekiwaniami, a także warunkami kształtującymi się po rewolucyjnej zmianie ustrojów społeczno-politycznych w Europie, kiedy to życie człowieka, elementu demokratycznego ustroju, wraz z jego wszystkimi atrybutami informacyjnymi (jawnymi i chronionymi) stało się ewenementem w na nowo określanej polityce wewnętrznej państw środkowoeuropejskich. Samego określenia securitologia (Секюримология) z propozycją jego definicji użył w 1989 roku w Rosji W.I. Jaroczkin, który w sposób nowatorski wskazał na wyodrębniającą się wśród innych dyscyplin naukowych[7] nową naukę o bezpieczeństwie życia człowieka. Szerzej informują o samym problemie i sposobach jego badania, liczne prace polskich naukowców z tej dziedziny: Janusza Świniarskiego, Stanisława Piochy, Leszka Korzeniowskiego[8], Jana Maciejewskiego[9] i innych.

Co w nowych teoriach jest najistotniejsze dla menedżera biznesu?

Oczywistość i prostota naukowego postępowania, jeżeli bowiem „istnieje możliwość (przynajmniej teoretyczna) minimalizacji lub eliminacji zagrożenia poprzez celowe, regulacyjne oddziaływania ludzkie, to zarządzanie bezpieczeństwem – przeciwstawieniem niebezpieczeństwa, czyli zagrożenia – jest możliwe i wskazane”, a skoro takie zarządzanie jest możliwe, to powinno ono mieć swoją bazę teoretyczną, czyli musi istnieć i rozwijać się nauka o zarządzaniu bezpieczeństwem niezależnie od wciąż licznych sporów pomiędzy samymi naukowcami o jej ostateczną nazwę (Tadeusz Hanausek[10]).

To m.in. Uniwersytet w Żylinie na Słowacji preferuje w publikowanych pracach określenie zarządzanie bezpieczeństwem (*bezpečnostný manažment – security management*), przez które to rozumiana jest „specyficzna czynność umysłowa, skierowana na odwrócenie albo minimalizację ryzyka lub zagrożeń różnej natury względem: życia i mienia obywateli, grupy i społeczeństwa, zawierająca pierwiastki zarządzania ryzykiem, zarządzania kryzysowego, zarządzania katastrofą (wypadkiem), zarządzania wartościami”[11].

Zarządzanie realizowane w praktyce dotyczy działań profesjonalnych, to znaczy opartych na rzetelnej wiedzy, fachowych umiejętnościach, racjonalnych metodach, sprawnych i skutecznych sposobach i technikach postępowania. Tak więc można powiedzieć, że zarządzanie jest profesją, i to profesją łączącą wizję artysty, szacunek dla społecznych wartości, znajomość rzemiosła i umiejętność komunikowania się.

Pomijając opis zasadności tych n-powodów dotyczących związków profesjonalnego zarządzania z bezpieczeństwem: przedsiębiorstwa, informacji itd., warto jednak wskazać na dwa aspekty tego problemu.

Po pierwsze, zawodowy kodeks etyczny menedżerów nie tylko wskazuje wartości społeczne, które mają być uniwersalne, ale oczekuje od swoich wyznawców, aby poświęcili interes własny dla wyższych celów. Etyka zawodowa musi być ukierunkowana na wyższe wartości społeczne, a nie na własne interesy danej grupy zawodowej.

Po drugie, oparcie sposobów działania na naukowo opracowanych zasadach, a nie na prostych, rutynowych umiejętnościach, co pozwala uniknąć zaskoczeń, zidentyfikować zagrożenia i uprzedzić materializację stwierdzonych ryzyk.

Tutaj potrzeba jedynie:
- chcieć się nauczyć samemu lub wnikliwie słuchać rad konsultantów/ekspertów;
- umieć wyciągać wnioski z cudzych i własnych niedorobek, pomyłek oraz ewentualnych błędów;
- potrafić wycofać się z podjętych w pośpiechu i jedynie ambicją uzasadnionych nietrafnych decyzji;

bowiem w każdym innym przypadku te, nawet najlepsze: teorie, zasady, aspekty, rady, uwagi, zalecenia, procedury *et cetera* nie są w stanie uchronić menedżera biznesu przed negatywnymi skutkami jego własnego działania.

Istota działań menedżera na rzecz bezpieczeństwa firmy – praktyka

Obiektywny stan bezpieczeństwa firmy należy odnosić do istnienia lub nieistnienia zagrożeń realnych niezależnych od czyichkolwiek spostrzeżeń. Pamiętając konsekwentnie

4) Leszek Korzeniowski: *European Association for Security,* Kraków – cytat z wystąpienia na Kongresie Ochrony Informacji Niejawnych i Biznesowych, Bielsko-Biała, 18–20 maja 2005 r.

5) *security* (ang.), bezpieczeństwo, inaczej: nauka o bezpieczeństwie; zob.: Świniarski J.: *Filozoficzne podstawy edukacji dla bezpieczeństwa,* Egros, Warszawa 1999, str. 20; Piocha S., Makroekonomia a problemy bezpieczeństwa w: Problemy bezpieczeństwa ekonomicznego wobec procesów globalizacji, red. naukowa S. Piocha, PTE, Koszalin 2004, str. 9.

6) W.I. Jaroczkin: „Секюримология - наука о безпасносми жизнедеямелносми”, Moskwa, 1989.

7) Dyscyplina naukowa jest to więc doniosła społecznie, ukształtowana i wyodrębniona ze względu na przedmiot i cel badań lub kształcenia część nauki w znaczeniu instytucjonalnym i uznana za podstawową jednostkę jej klasyfikacji. Zob.: Krzyżanowski L.J.: *O podstawach kierowania organizacjami*, PWN, Warszawa 1999, str. 130.

8) Korzeniowski L.: *Menedżment. Podstawy zarządzania,* EAS, Kraków, 2003, str. 183–205.
Korzeniowski L.: „Управлыния безпекою”, Aktualne Problemy Ekonomii, Nr 1(31)/2004, s. 147–154.

9) Maciejewski J.: *Oficerowie Wojska Polskiego w okresie przemian społecznej struktury i wojska. Studium socjologiczne,* Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław, 2002.

10) Hanausek T.: *Zarządzanie bezpieczeństwem – nowa dziedzina nauki,* w: *Bezpecnost' a ochrana majetku LIPORT LFK*, Koszyce, 2001, str. 37.

11) Šimâk L.: *Krizový manaźment vo verejnej správe,* Uniwersytet Żyliński, Żylina, 2001, s. 39.

o jego potencjalnym lub aktywnym charakterze, możemy odnieść go pod względem oceny do czasu już minionego. Zachowanie obiektywizmu naukowego wymaga uświadomienia wszystkim zainteresowanym, że stan bezpieczeństwa nie jest zjawiskiem trwałym, ale należy traktować go jako proces realizowany w analizowanym systemie (tutaj systemem jest firma, jakkolwiek byśmy to rozumieli) w odniesieniu do wszystkich bliższych i dalszych oddziaływań systemowych (od prawa lokalnego po przepisy unijne; od skutków skręcenia kostki przez petenta przed wejściem do biura po zagrożenie terroryzmem mafijnym lub politycznym itd., itp.) nie zawsze branych świadomie pod uwagę w trakcie prowadzonych (wobec tego stanu i warunków jego zachowania) analiz.

Subiektywne aspekty bezpieczeństwa to przede wszystkim odniesienia do pojedynczego człowieka i jego poczucia bezpieczeństwa: jest to świadomość istnienia lub nieistnienia bezpieczeństwa, brak takiej świadomości lub brak świadomości możliwego przeciwdziałania niebezpieczeństwu albo też istnienie fałszywej świadomości zagrożenia w rzeczywistości w ogóle niewystępującego.

Ta różnorodność obiektywnych i subiektywnych kategorii może być przedstawiona w postaci uproszczonego modelu przedstawionego na rys. 3. (za: Leszek Korzeniowski, *Securitology*...[12]), zawierającego cztery zasadnicze segmenty oceny sytuacji (gdzie odpowiednio:

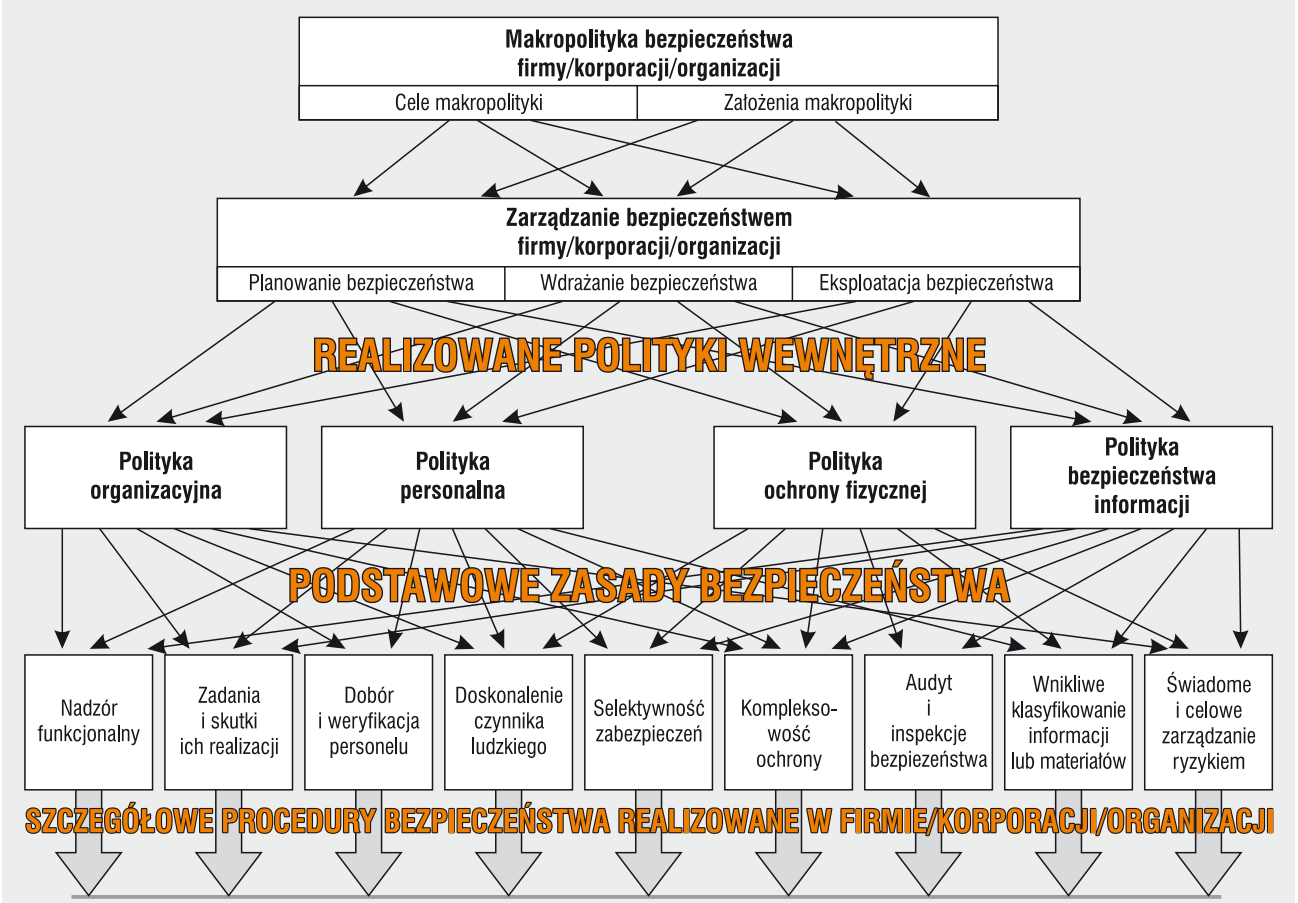
– czarna linia oznacza poziom zagrożeń;
– pole wykrzykników to poziom percepcji;
– symbol literowy /A–D/ identyfikuje analizowany segment).

Na potrzeby firmy, jej główny szef, na co dzień dbający o bezpieczeństwo (stan A), dysponujący odpowiednimi informacjami o zagrożeniu (stan C), działając jako jej przywódca i włodarz, ma szanse podjąć odpowiednie decyzje, by przeciwdziałając zagrożeniom i ryzykom, dotrzeć z nimi do pracowników i współpracujących z nim osób, organizacji,

Rys. 3. Uproszczony model kategorii poczucia bezpieczeństwa

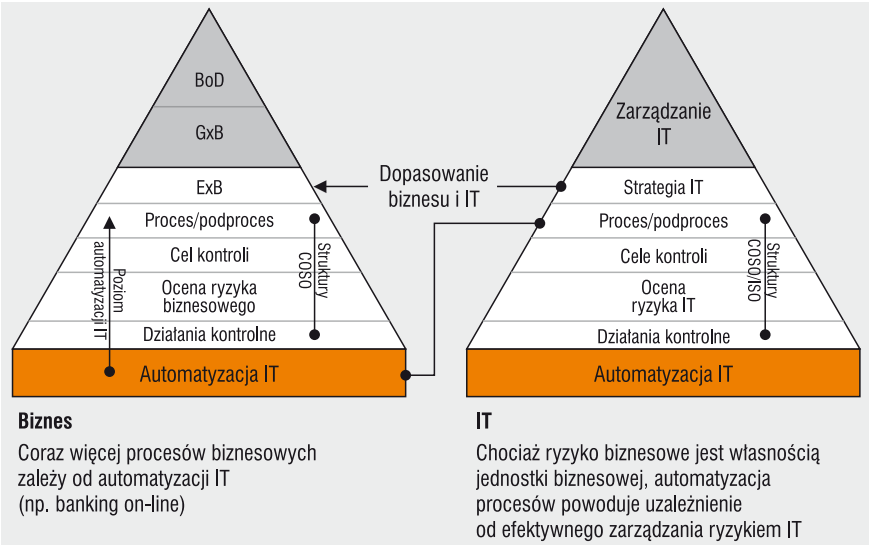
Opisy poszczególnych segmentów:
A – Stan bezpieczeństwa, gdy poziom zagrożeń jest mały i postrzegany jako niewielki,
B – Fałszywe bezpieczeństwo, gdy poziom zagrożeń jest duży, a postrzegany jest jako mały,
C – Stan zagrożenia, gdy poziom zagrożeń jest duży, a postrzeganie tych zagrożeń jest prawidłowe (adekwatne do ryzyk i skutków ich ewentualnej materializacji),
D – Obsesja, gdy zagrożenia są małe, ale postrzegane jako duże.

Analiza systemowa realizacji polityki bezpieczeństwa



Rys. 4. Makropolityka bezpieczeństwa jako strategia wieloetapowego i wielopoziomowego działania

12) Korzeniowski L.: *Securitology. The concept of safety,* Communications, Nr 3/2005, s. 20–23.



Rys. 5. Problemy – Biznes kontra IT
Źródło – Michał Jarski: *Wdrażanie norm ISMS,* Sarbanes-Oxley i Basel II)

agend i służb, a w konsekwencji – we współpracy z nimi zminimalizować lub wyeliminować poszczególne rodzaje zagrożeń (co tylko w teorii jest tak proste).

Istotnym, żeby nie powiedzieć głównym, elementem budowania warunków bezpieczeństwa i przeciwstawiania się zagrożeniom jest wiedza menedżera o charakterze samych zagrożeń oraz jego sposób komunikowania się z personelem zarządczym średniego szczebla i pracownikami – otwarty, bezpośredni (o ile to możliwe), na poziomie ich percepcji, co w dobie rozwoju współczesnych środków przekazu zapewnia nieosiągalną w innym układzie pełnię porozumienia (werbalny i niewerbalny kontakt osobisty).

Uzupełnieniem jest wnikliwa strategiczna analiza systemowa wdrożonej polityki bezpieczeństwa, znajomość jej zasad i umiejętność skutecznego odwołania się do jej ustaleń na każdym (polityki cząstkowe/procedury) poziomie działania (zobacz schemat na rys. nr 4).

4. Ochrona informacji jako obszar dobrych praktyk – na przykładzie GMITS/ISMS

Wprowadzenie pojęcia dobrych praktyk, czyli, innymi słowy, ogólnych zasad wynikających jako powtarzalne z zastosowanych z dobrym skutkiem, choć w różnych okolicznościach rozwiązań praktycznych, jest niczym innym jak odwołaniem się do uogólnionych pozytywnych doświadczeń.

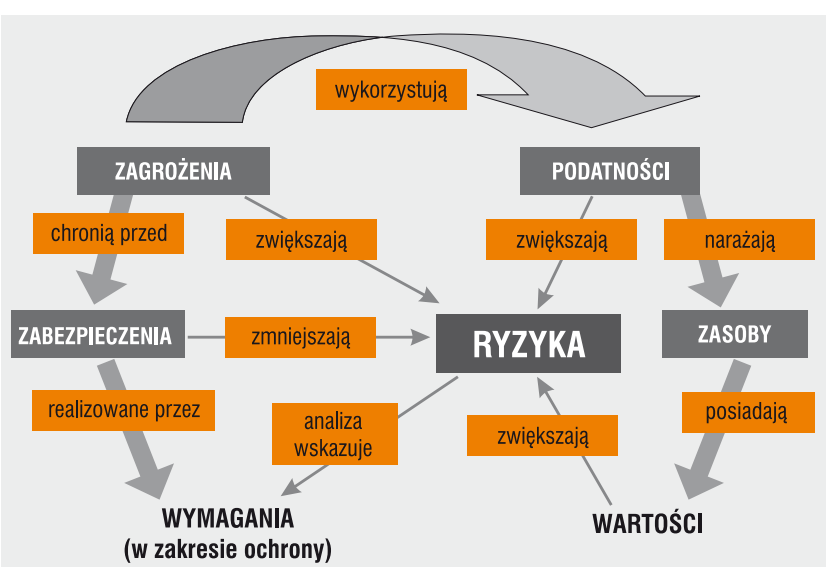
Postać, pod jaką są one prezentowane, może być rozmaita:
- reguły i sprawdzone zasady stowarzyszeniowe;
- zalecenia i protokoły organizacji zawodowych oraz normalizacyjnych;
- uzgodnienia techniczne stanowiące podstawy dla opracowania norm i specyfikacji normatywnych;
- regionalne i środowiskowe rozwiązania techniczne, technologiczne i organizacyjne;
- nieujęte formalnie, ale zastosowane z sukcesem i wielokrotnie powielane porozumienia zawodowe o charakterze *gentleman's agreement*;
– rozwiązania (np. organizacyjne) sprawdzone praktycznie w kilku różnych dziedzinach i zachowujące swoją skuteczność i poprawność działania.

Obecnie, jedyną poprawną formą upowszechniania i dobrowolnego udostępniania takich *best practices* są normy (krajowe, regionalne, międzynarodowe) – w swej wyspecjalizowanej treści dostatecznie ogólne, aby móc je dopasować do swojej firmy, i zarazem wyposażone w zdefiniowane wskaźniki/mierniki stanu, co pozwala (z dużym prawdopodobieństwem) upewnić się zainteresowanym, co do tego, że są poprawnie stosowane (samodzielnie lub z wykorzystaniem trzeciej strony, jako audytora certyfikującego).

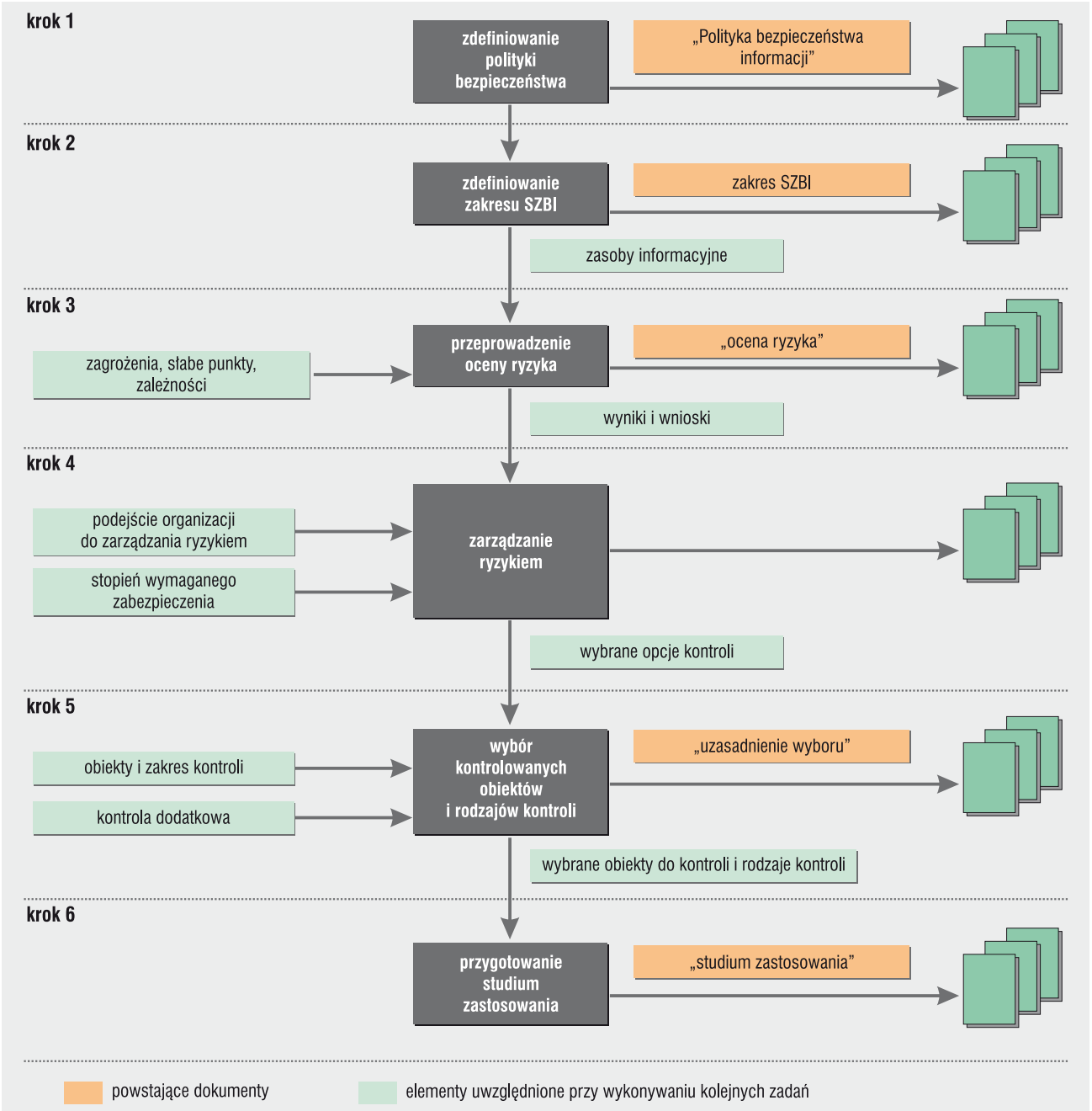
Dlaczego zatem, mówiąc o dobrych praktykach w ochronie informacji, warto zaczynać od GMITS (ang.: *Guidelines for the Management of IT Security*)? Uzasadnienie jest proste i nad wyraz oczywiste, jego podstawą jest bowiem szybkość przetwarzania informacji w procesie, czyli zobrazowana prędkość narastania strat wobec choćby minimalnego:
- popełnionego błędu;
- zaistniałego zagrożenia;
- zmaterializowanego ryzyka;

która to w systemach informatycznych po wielokroć przewyższa zdolność podjęcia takiej obserwacji w tradycyjnym systemie statystyki papierowej. Szybsze narastanie „niepokojących objawów" w systemie informatycznym dopinguje decydenta do wypracowania wniosków w zakresie oceny niekorzystnego stanu i wprowadzenia odpowiednich działań/czynności korygujących/naprawczych.

Trudno dziś wyobrazić sobie jakiekolwiek działanie biznesowe bez wsparcia systemami IT, choć tak naprawdę niewielu decydentów zdaje sobie dokładnie sprawę, że ich ryzyka, podejmowane w imię realizowanego interesu zwielokrotniają się, niezależnie od ich zamierzeń i oczekiwań. Dzieje się tak, na ogół, w wyniku nie do końca bezpiecznych operacji realizowanych w sposób zautomatyzowany, z użyciem systemów IT i przy wykorzystaniu (nie zawsze w pełni bezpiecznego) oprogramowania.



Rys. 6. Model wymagań ochrony wartości w systemach wg ISO 13335-1



Rys. 7. Wykorzystanie zasad kodeksowych normy ISO 17799

Współzależności biznesu i IT przedstawia rysunek 5.

A przecież w praktyce mamy przed sobą problem ochrony informacji (biznesowej, technicznej, organizacyjnej) stanowiącej wartość i zasób firmy. Wprowadzane przewodniki (GMITS) stały się zatem w latach 1993–1996 kolejno: uzgodnionymi protokołami TR 13335 (1–3) następnie normami ISO 13335 (1–5), a ich kolejne edycje zostały wpisane co do treści i założeń w rodzinę norm ISO 2700x dotyczących zarządzania bezpieczeństwem informacji – ISMS (ang.: *Information Security Management System*).

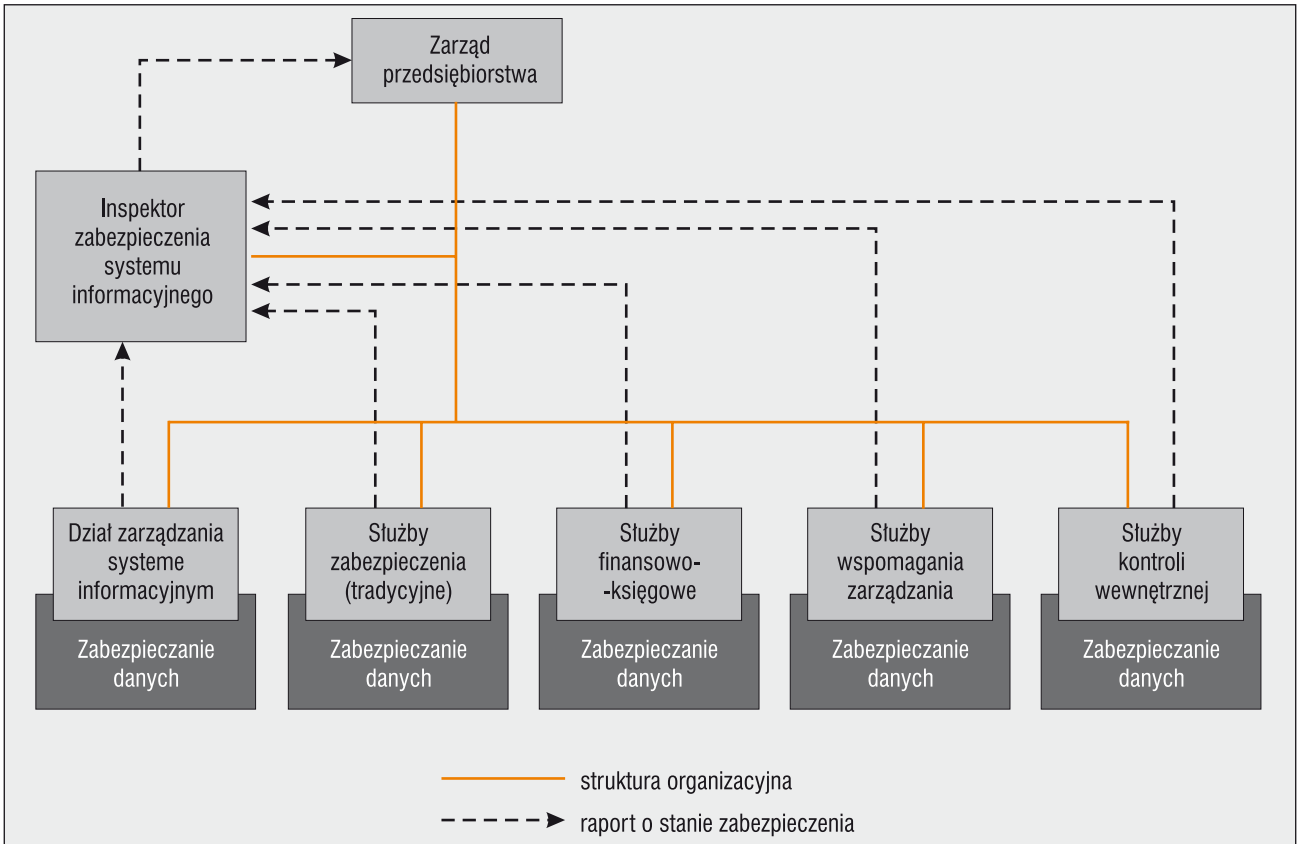
Patrząc na podstawowe założenia normatywne Systemu Zarządzania Bezpieczeństwem Informacji SZBI – ISMS, jego wskaźniki (zał. A do normy PN-I-07799-2:2005), jak i ogólne założenia (PN-ISO/IEC 17799:2003, obecnie 2. ed. ISO 17799:2005 ⇔ ISO 27002:2007) prezentowane w ujęciu kodeksu wymagań[13], powinniśmy świadomie i celowo w każdym z planowanych działań analizować potencjalne zagrożenia, oceniać ryzyko ich wystąpienia i materializacji oraz przewidywać koszty utrzymania ciągłości działania biznesowego w ramach podjętych wcześniej przedsięwzięć ochrony naszego zasobu informacyjnego.

Prezes ISMS International User Group Polish Chapter, dr inż. Elżbieta Andrukiewicz, od ponad 10 lat, na wszystkich swoich wykładach i wystąpieniach odwołuje się do sześciu podstawowych kroków, wynikających z normy kodeksowej, czyli pierwowzoru brytyjskiego (BS 7799:1996 ⇔ BS 7799-1:1999) oraz jego późniejszej pierwszej edycji międzynarodowej (ISO 17799:2000), dostępnej po polsku jako PN-ISO/IEC 17799:2003.

Proponuje również przed wdrażaniem SZBI/ISMS rozważenie działania przykładowej osoby zajmującej się zabezpieczeniem systemu i zasobów informacyjnych przedsiębiorstwa.

Warto zdać sobie sprawę z tego, że „rozmienione” na działy duże ryzyko firmy, wcale nie jest mniejsze i łatwiejsze do zapoznania i opanowania.

13) E. Andrukiewicz, D. Gaj: *Nowe wydanie normy ISO/IEC 17799:2005*, materiały ISMS International User Group Polish Chapter.



Rys. 8. Propozycja rozwiązań organizacyjnych: za: E. Andrukiewicz, PCkurier 26/1998

5. W uzupełnieniu wywodów...

... czyli w podsumowaniu części pierwszej cyklu, wypada jedynie stwierdzić, że większość spostrzeżeń przedstawionych PT Czytelnikom dla ich późniejszych rozważań ma (niestety) kryzysowy rodowód. Krytyczne uwagi i wskazania są pochodnymi od namacalnych skutków braku znajomości prawa oraz ograniczonej wyobraźni poszczególnych decydentów co do efektów ich uproszczonego myślenia i postępowania w procesie ochrony zasobów informacyjnych.

Wniosek nie jest budujący i da się zamknąć w znanym od wieków łacińskim stwierdzeniu: *Ignorantia iuris nocet* (*Nieznajomość prawa szkodzi* – zobacz: prawa rzymskie z IV w. p.n.e.), które to przedkładam niniejszym, do wzięcia pod rozwagę, wszystkim menedżerom.

OPRACOWAŁ: DR INŻ. MAREK BLIM

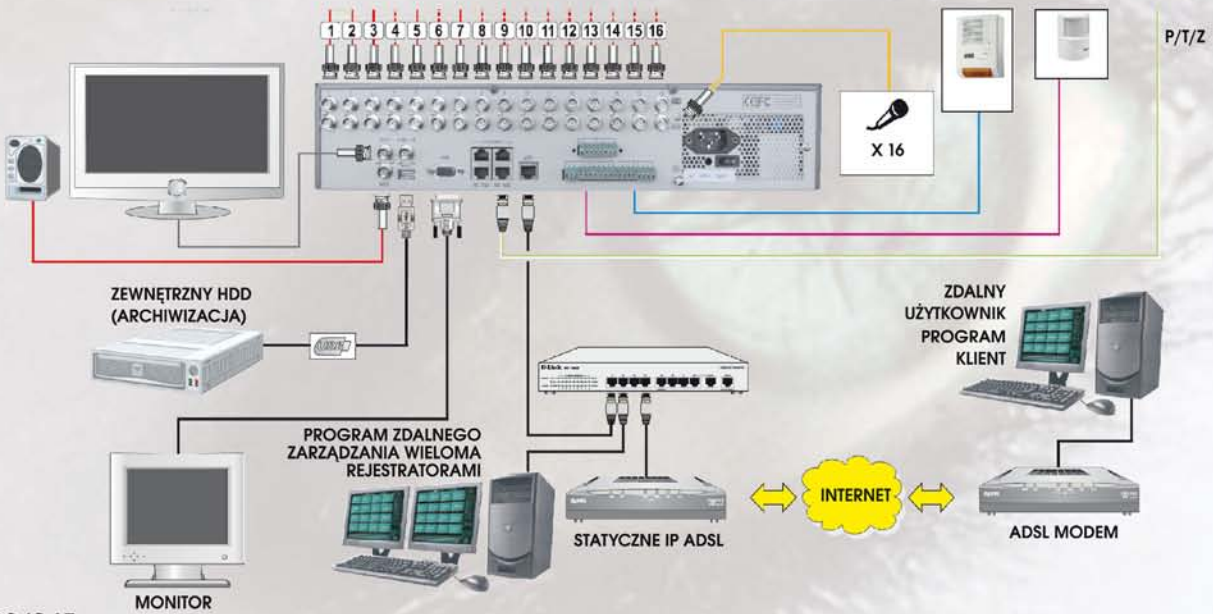
Bibliografia:

1. Ross Anderson: *Inżynieria zabezpieczeń,* WNT, Warszawa, 2005.
2. Elżbieta Andrukiewicz: *Bezpieczeństwo systemów informacyjnych,* Zarządzanie, PCkurier, nr 26/1998.
3. Elżbieta Andrukiewicz: *ISO/IEC 27005 – Zarządzanie ryzykiem w procesie budowania systemu zarządzania bezpieczeństwem informacji,* materiały Forum Zarządzania Bezpieczeństwem Informacji, Warszawa, 30 marca 2006.
4. Elżbieta Andrukiewicz, Dorota Gaj: *Nowe wydanie normy ISO/IEC 17799:2005,* materiały ISMS International User Group Polish Chapter, *http://www.ismspolska.org.pl*
5. Witold T. Bielecki: *Informatyzacja zarządzania,* PWE, Warszawa, 2000.
6. Jadwiga Bizon-Górecka: *Strategie zarządzania ryzykiem w organizacji gospodarczej,* Przegląd Organizacji, nr 1/2001, s. 13–15.
7. Doroty E. Dening: *Wojna informacyjna i bezpieczeństwo informacji,* WNT, Warszawa, 2002.
8. Piotr Jedynak, Stanisław Szydło: *Polityka ryzyka w procesie zarządzania marketingowego polskich przedsiębiorstw,* materiały konferencyjne, Poznań, 1995.
9. Robin Kendall: *Zarządzanie ryzykiem dla menedżerów. Praktyczne podejście do kontrolowania ryzyka,* Liber, Warszawa, 2000.
10. Zygmunt Kor: *Świadomy podwójnie chroniony,* CXO Custom Publishing, Warszawa, maj 2004, str. 7.
11. Józef Penc, *Decyzje w zarządzaniu,* PSB, Poznań–Kraków, 1996.
12. Carl L. Pritchard, *Zarządzanie ryzykiem w projektach. Teoria i praktyka MT&DC*, WIG-PRESS, Warszawa, 2002
13. Magdalena A. Powolna, Roksana Curysek: *Uprzedzić ryzyko,* e-zin e-Forum Zarządzanie z 7 maja 2002 roku.
14. Robert Simmons: *Kalkulator ryzyka*, Neuman Management Review, październik 1999; polskie opracowanie M. Bańkowski, Forum Zarządzania, nr 6/2001, s. 11–14.
15. Wiktor Samecki: *Ryzyko i niepewność w działalności przedsiębiorstwa przemysłowego*, wyd. III, PWE, Warszawa, 1986.
16. Waldemar Tarczyński, Magdalena Mojsiewicz: *Zarządzanie ryzykiem. Podstawowe zagadnienia,* PWE, Warszawa, 2001.
17. *Terroryzm. Bezpieczeństwo i ryzyko,* materiały z konferencji, Emowo, 28 listopada 2002.
18. *Wprowadzenie do analizy ryzyka*, materiały AEA Technology-Consulting, Risley, Warrington, UK, 2000.
19. *Wybrane aspekty zarządzania wiedzą w przedsiębiorstwach UE*, Oficyna Wydawnicza PTZP, Opole, 2006.
20. Kazimierz Zimniewicz: *Błędy w procesie podejmowania decyzji*, Zeszyty Naukowe WSZiB, nr. 1. Poznań, 1996.
21. Kazimierz Zimniewicz: *Współczesne koncepcje i metody zarządzania*, PWE, Warszawa, 2003.

NOWA JAKOŚĆ OBRAZU

NOWE REJESTRATORY SIECIOWE Z KOMPRESJĄ H.264

MONITORING STADIONÓW
MONITORING OBIEKTÓW PRZEMYSŁOWYCH
MONITORING KOMPLEKSÓW BIUROWYCH



1093/045

Nowy rejestrator cyfrowy firmy URMET posiada najnowszą kompresję H.264. Kompresja ta charakteryzuje się niemal bezstratną jakością obrazu oraz wydajnością do 40 % wyższą w stosunku do standardowego MPEG-4. Urządzenie łączy w sobie cechy wysokiej jakości rejestratora oraz serwera sieciowego. W rejestratorach firmy URMET istniej możliwość transmisji dwóch niezależnych strumient wysokiej jakości do transmisji w sieci LAN oraz jakości ograniczonej, dopasowanej do łącza internetowego. Do urządzenia dostępne jest oprogramowanie zdalne do zarządzania wieloma rejestratorami (do 100 kamer w jednym ekranie - opcja) oraz oprogramowanie typu klient.

- 16 kanałów video
- 16 kanałów audio
- Jednoczesna rejestracja, przeglądanie zapisu, archiwizacja i transmisja do sieci
- Wyjścia monitorowe: 1 x BNC, 1 x VGA, 1 x S-Video
- Wyswietlanie 400kl/s w rozdzielczości 720x576
- Zapis 400 kl/s (25 kl/s na kanał) z jakością ok. 450 linii analogowych (DCIF) dla każdego kanału
- Maks. 8 dysków montowanych w urządzeniu
- USB oraz DVD-RW(opcjonalnie) do archiwizacji
- Współpraca ze sprzętowymi klawiaturami 1090/046, 1090/048
- Profesjonalne oprogramowanie do zarządzania poprzez sieć komputerową
- Znak wodny
- Polska wersja językowa

MIWI-URMET Sp. z o. o.
tel. (042) 616 21 00, fax (042) 616 21 13
www.miwiurmet.com.pl
miwi@miwiurmet.com.pl

Jak się zachować w przypadku incydentu bombowego

W związku ze wzrostem zagrożenia atakami terrorystycznymi w Europie, także w Polsce, warto podjąć działania mające na celu uświadomienie istoty zagrożeń, jakie niesie ze sobą terroryzm, oraz przygotowanie społeczeństwa do właściwego zachowania się w przypadku wystąpienia ryzyka ataku

Efektywność wszelkich działań ukierunkowanych na przeciwdziałanie aktom terroryzmu jest pochodną skuteczności służb odpowiadających za bezpieczeństwo kraju i gotowości społeczeństwa do wspierania tych działań oraz wzajemnego zaufania i odpowiedzialności za dobro wspólne.

Terroryzm to szeroki termin. Oznacza użycie siły lub przemocy w stosunku do osób lub własności w celu zastraszenia, przymuszenia lub okupu.

Do jego skutków można zaliczyć znaczną liczbę ofiar, uszkodzenia budynków, zakłócenia w dostępie do podstawowych usług, takich jak: elektryczność, dostawy wody, opieka medyczna, telekomunikacja, komunikacja miejska.

W strukturach polskiej policji funkcjonują wydziały antyterrorystyczne i komórki minersko-pirotechniczne, których pracownicy mają specjalne przygotowywanie do tego, aby zapobiegać aktom terroru i stawiać im czoła.

Jednym z możliwych aktów terrorystycznych jest zamach bombowy. Jest to działanie specyficzne: u jego podstaw nie ma podziału ludzi na „swoich" czy „obcych". O ile pistolet może być wycelowany w konkretną osobę, a porwania dotyczą określonego człowieka, to ofiarą zamachu bombowego może być każdy, kto będzie przebywał w pobliżu miejsca wybuchu. Kryteriami wyboru ofiary nie są ani jej poglądy polityczne, ani stan majątkowy. Ofiarami równie dobrze mogą być matka z dzieckiem, jak i emeryt wychodzący z banku.

W strukturach polskiej policji funkcjonują wydziały antyterrorystyczne i komórki minersko-pirotechniczne

Na określenie zamachu bombowego specjaliści posługują się również terminem incydent bombowy – często zdarza się, że zanim nastąpi eksplozja, bomba zostanie w taki czy inny sposób ujawniona.

Incydent bombowy to sytuacja stwarzająca zagrożenie życia lub zdrowia przez podłożenie materiału lub urządzenia wybuchowego albo groźbę ich podłożenia. Jeśli dojdzie do incydentu bombowego, właściwe zachowanie jest niezwykle ważne dla przebiegu zdarzenia, jego skutków i działania specjalistów policyjnych. Informacji o zagrożeniu incydentem bombowym nie wolno bagatelizować ani lekceważyć.

Podstawową cechą terroryzmu jest to, że nie ma wyraźnych sygnałów ostrzegawczych o możliwości wystąpienia zamachu lub trudno je dostrzec. Trzeba więc zwracać uwagę na to, co dzieje się w naszym najbliższym otoczeniu, np. na zakupach, podczas uczestnictwa w imprezach masowych i w miejscach o dużych skupiskach ludzi.

Należy zwrócić uwagę na:
- rzucające się w oczy lub po prostu nietypowe zachowania innych,
- rzeczy pozostawione bez opieki, takie jak teczki, paczki, pakunki itp.,
- wyglądających na obcokrajowców,
- ubranych nieodpowiednio do pory roku,
- samochody, a w szczególności furgonetki, parkujące nietypowo, tj. w pobliżu miejsc, w których organizowane są imprezy masowe i zgromadzenia.

Warto jednak pamiętać o tym, że terrorysta nie zawsze musi być odmiennej narodowości i wyróżniać się z tłumu wyglądem. O swoich spostrzeżeniach należy informować służby odpowiedzialne za bezpieczeństwo obiektu, straż miejską lub policję.

Nasuwa się pytanie, jak postępować w sytuacjach zagrożenia incydentem bombowym.

Oto kilka rad ekspertów z Biura Operacji Antyterrorystycznych Komendy Głównej Policji.

Można przygotować się na wypadek powstania tego typu zagrożenia w budynkach użyteczności publicznej, tzn.:
- zawczasu pomyśleć o tym, którędy można się w pośpiechu ewakuować z budynku lub zatłoczonych miejsc – zapamiętać, gdzie znajdują się klatki schodowe i wyjścia ewakuacyjne,
- zwrócić uwagę na ciężkie lub łatwo tłukące się przedmioty, które mogą być przesunięte, zrzucone lub zniszczone podczas wybuchu – zapamiętać elementy z najbliższego otoczenia.

Należy również pamiętać o tym, aby nie przyjmować od obcych żadnych pakunków oraz nie pozostawiać bagażu bez opieki.

Jeżeli przyjęliśmy zgłoszenie o podłożeniu ładunku wybuchowego lub ujawniliśmy przedmiot niewiadomego pochodzenia, co do którego istnieje podejrzenie, że może stanowić zagrożenie dla osób i mienia, powinniśmy to zgłosić służbom odpowiedzialnym za bezpieczeństwo w danym miejscu, administratorowi terenu, policji lub straży miejskiej. Informacji takiej nie należy przekazywać osobom niepowołanym, gdyż jej niekontrolowane rozpowszechnienie może doprowadzić do paniki i w konsekwencji utrudnić przeprowadzenie sprawnej ewakuacji z zagrożonego miejsca.

Zawiadamiając policję, należy podać następujące informacje:
- rodzaj zagrożenia i źródło informacji o nim (informacja telefoniczna, ujawniony podejrzany przedmiot);
- treść rozmowy z informującym o podłożeniu ładunku wybuchowego;
- numer telefonu, pod który przekazano informację o zagrożeniu, oraz dokładny czas jej przyjęcia;

– adres, numer telefonu zgłaszającego;
– opis miejsca i wyglądu ujawnionego przedmiotu.

Po ogłoszeniu alarmu bombowego należy realizować procedury postępowania w czasie zagrożenia bombowego:

1. Do czasu przybycia policji akcją kieruje administrator obiektu, terenu lub osoba odpowiedzialna za jego bezpieczeństwo.
2. Na miejsce zagrożenia incydentem bombowym należy wezwać służby pomocnicze, takie jak: pogotowie ratunkowe, straż pożarną, pogotowia gazowe, wodno-kanalizacyjne, energetyczne.
3. Po przybyciu policji na miejsce incydentu bombowego przejmuje ona kierowanie akcją.
4. Należy bezwzględnie wykonywać polecenia policjantów.
5. Jeśli brak informacji o konkretnym miejscu podłożenia bomby użytkownicy pomieszczeń służbowych powinni sprawdzić miejsce pracy i jego bezpośrednie otoczenie pod kątem obecności przedmiotów nieznanego pochodzenia.
6. Pomieszczenia ogólnodostępne (korytarze, klatki schodowe, windy, toalety, piwnice, strychy) oraz najbliższe otoczenie obiektu sprawdzają i przeszukują osoby wyznaczone lub służby odpowiedzialne za bezpieczeństwo w danej instytucji.
7. Podejrzanych przedmiotów nie wolno dotykać! O ich lokalizacji należy powiadomić administratora budynku oraz osoby odpowiedzialne za bezpieczeństwo w nim.
8. Po ogłoszeniu ewakuacji należy zachować spokój i opanowanie, pozwoli to sprawnie i bezpiecznie opuścić zagrożony rejon.
9. Po ogłoszeniu ewakuacji w miejscu pracy należy je opuścić, zabierając rzeczy osobiste (torebki, siatki, nesesery itp.).

Telefony alarmowe	
999	Pogotowie Ratunkowe
998	Straż Pożarna
997	Policja
987	Wojewódzkie Centra Zarządzania Kryzysowego
112	Telefon alarmowy dla użytkowników telefonów komórkowych
0 800 120 226	Infolinia Policji (połączenie bezpłatne)

10. Identyfikacją i rozpoznawaniem zlokalizowanego ładunku wybuchowego oraz jego neutralizacją zajmą się uprawnione i wyspecjalizowane osoby i komórki organizacyjne policji.

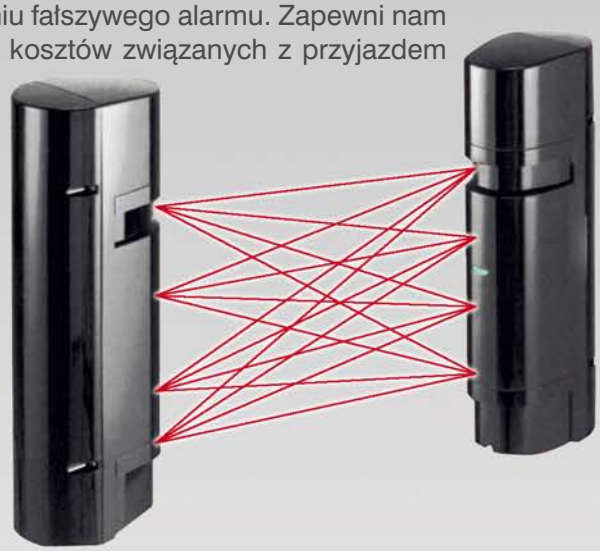
Po otrzymaniu informacji o podłożeniu lub groźbie podłożenia bomby i zarządzeniu ewakuacji w obiektach publicznych, np. supermarketach, hurtowniach, magazynach, niezwłocznie udajemy się do wyjścia zgodnie ze wskazaniami administratora budynku lub upoważnionych osób. Wielu z pracujących 11 września 2001 roku w World Trade Center uratowało się dzięki kilkorgu ludziom, którzy mieli pewne doświadczenia w obronie cywilnej i potrafili zorganizować szybką ewakuację. W przypadku konieczności ewakuacji obiektów handlowych należy strzec się paniki. Przydaje się zaś planowanie, wcześniejsze przygotowanie się i cykliczne szkolenia pracowników.

Ekspert Wydziału Prewencji KWP w Poznaniu
nadkom. mgr Henryk Gabryelczyk

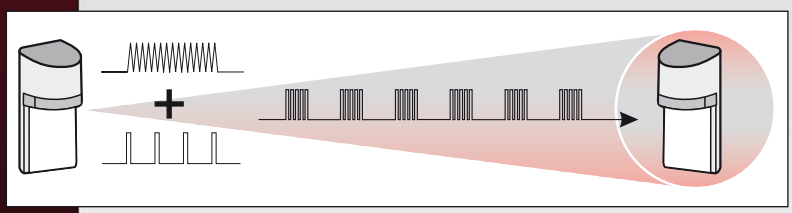
Bariery podczerwieni

TAKEX

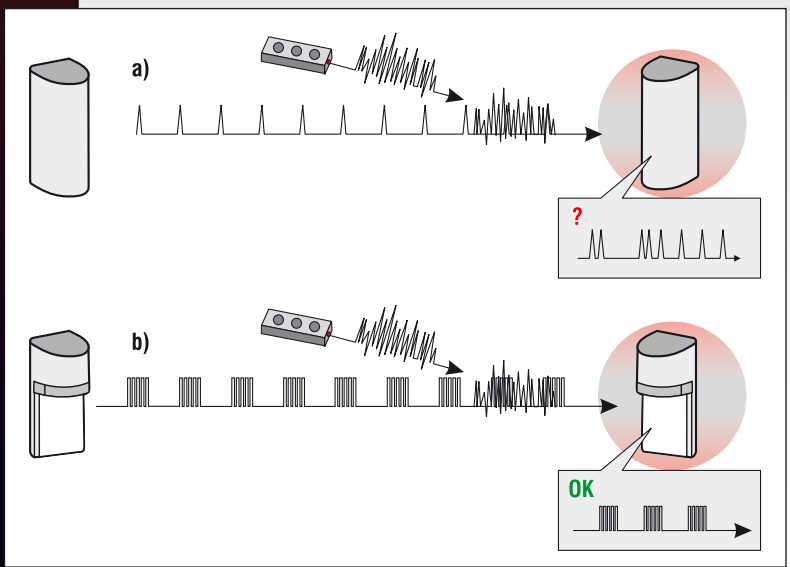
W dobie ogromnej konkurencji oraz przy obecnej różnorodności urządzeń systemów zabezpieczeń możemy czuć się nieco zagubieni. Czym zatem powinniśmy się kierować przy wyborze urządzeń służących do ochrony naszego życia i mienia? Nieustanna walka o klientów wymaga od producentów elektronicznych systemów zabezpieczeń wprowadzania na rynek coraz to nowszych rozwiązań. Dlatego decydując się na ochronę barierami podczerwieni, musimy brać pod uwagę przede wszystkim te parametry, które świadczą o wysokiej skuteczności detekcji intruza przy jak najmniejszym wskaźniku wystąpieniu fałszywego alarmu. Zapewni nam to bezpieczeństwo, a przy okazji pozwoli uniknąć kosztów związanych z przyjazdem grupy interwencyjnej po nieuzasadnionym alarmie



Japońska firma Takex (dawniej znana pod nazwą Pulnix), będąca częścią organizacji Takenaka, należy do najbardziej prestiżowych producentów detektorów ruchu. Jej produkty od ponad 25 lat cieszą się dużym uznaniem wśród instalatorów i użytkowników na całym świecie. Obok produkcji pasywnych detektorów ruchu, zarówno wewnętrznych jak i zewnętrznych, wizytówką firmy są aktywne bariery podczerwieni, zwane też torami podczerwieni. Ponad kilkadziesiąt modeli w ofercie świadczy o dużej różnorodności sprzętu i umożliwia użytkownikowi wybór odpowiedniego urządzenia. Nowatorskie rozwiązania, takie jak opatentowana podwójna modulacja wiązki, klasyfikują urządzenia do najbardziej zaawansowanych technicznie torów podczerwieni dostępnych na rynku.



Rys. 1. Podwójna modulacja częstotliwości wiązki



Rys. 2. Wpływ obcego źródła IR na odbierany sygnał:
a) dla pojedynczej modulacji częstotliwości wiązki
b) dla podwójnej modulacji częstotliwości wiązki

Podwójna modulacja częstotliwości wiązki

Firma Takex, szukając niezawodnych rozwiązań, wykorzystała w swojej technologii podwójną modulację częstotliwości wiązki. Podwojenie częstotliwości polega na nałożeniu sygnału, zawierającego informację o alarmie, na falę nośną wielkiej częstotliwości. Nakładanie realizuje się w celu przesłania właściwego sygnału w paśmie większej częstotliwości. Rys. 2. przedstawia wpływ obcego źródła promieniowania podczerwonego na pracę bariery z pojedynczą oraz podwójną modulacją częstotliwości wiązki. Widzimy, że w przypadku zastosowania podwójnej modulacji sygnał nadawany równy jest odbieranemu, z wyeliminowaniem zakłóceń pochodzących z obcego źródła. W barierach podczerwieni z pojedynczą modulacją sygnał odbierany stanowi wypadkową sumę sygnału nadawanego i zakłócającego. Dlatego też tradycyjne tory podczerwieni z pojedynczą modulacją wiązki charakteryzują się dużą wrażliwością na zakłócenia zewnętrzne i inne źródła promieniowania podczerwonego lub fluorescencyjnego.

Układ PLL

W parze z podwojeniem modulacji wiązki w barierach podczerwieni Takex zastosowano układ PLL (*Phase Locked Loop*). Filtruje on wszystkie wyższe harmoniczne sygnału docierające do odbiornika i wprowadza w obwód sygnału odbieranego z przeciwnym znakiem. Taka kompensacja sygnału gwarantuje wyeliminowanie zakłóceń przy zachowaniu najwyższej czułości układu.

Gama produktów

dwuwiązkowe bariery podczerwieni o zasięgach zewnętrznych 30 m (PB-30TK), 60 m (PB-60TK), 100 m (PB-100TK, PB-100ST) z jedną częstotliwością pracy
dwuwiązkowe bariery podczerwieni o zasięgach zewnętrznych 20 m (PB-20TE), 40 m (PB-40TE), 60 m (PB-60TE) z czterema częstotliwościami pracy
czterowiązkowe bariery podczerwieni o zasięgach zewnętrznych 50 m (PB-50F), 100 m (PB-100F), 200 m (PB-200F) z jedną częstotliwością pracy
czterowiązkowe bariery podczerwieni o zasięgach zewnętrznych 50 m (PB-IN-50HF), 100 m (PB-IN-100HF), 200 m (PB-IN-200HF) z czterema częstotliwościami pracy, wyjściem pogodowym, pamięcią alarmu, regulacją mocy wiązek i wbudowanym sygnalizatorem ułatwiającym prawidłowe zestrojenie toru optycznego
czterowiązkowa bariera podczerwieni o zasięgu zewnętrznym 100 m (PB-IN-100AT), która ma parametry takie same, jak w przypadku barier serii (PB-IN-HF), a dodatkowo funkcję *Antyprzeczołganie* oraz osobną regulację czasu naruszenia dla dwóch i czterech wiązek
bariery podczerwieni z reflektorem pryzmowym o zasięgu wewnętrznym 1 m (PR-1B), 5 m (PR-5B), 10 m (PR-10B) i zasięgu zewnętrznym 11 m (PR-11B)
bariera mikrofalowa MW-50 o zasięgu zewnętrznym 50 m, dwóch częstotliwościach pracy, regulacji czasu naruszenia wiązki, z układem automatycznej regulacji wzmocnienia, przeznaczoną do montażu ściennego lub na słupku
czujka zewnętrzna MS-12-FE o zasięgu detekcji 2 x 12 m, kącie detekcji 2 x 90°, czterech torach detekcji, z trybem pracy dzień/noc oraz AND/OR, płynną regulacją czułości i brakiem reakcji na zwierzęta.

Model 16-wiązkowy

W modelach czterowiązkowych każda z czterech synchronizowanych wiązek jest odbierana przez cztery odbiorniki. W ten sposób tworzy się 16 torów podczerwieni (górny – górny, górny – dolny, dolny – dolny, dolny – górny) dla jednego kompletu barier. Wszystkie 16 torów musi być zablokowane, aby odbiornik wygenerował alarm. Taki sposób pracy znacząco redukuje liczbę fałszywych alarmów spowodowanych np. przez małe zwierzęta lub spadające liście.

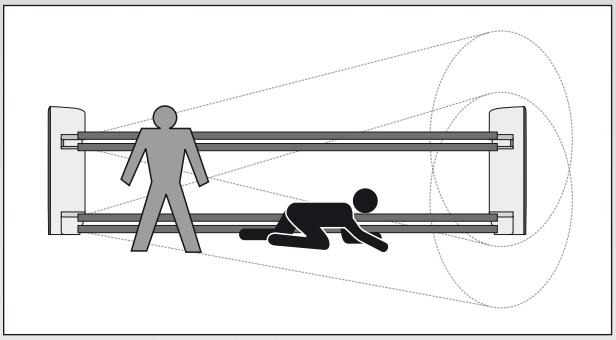
Eliminacja fałszywych alarmów

Wiele różnorodnych rozwiązań zastosowanych w barierach podczerwieni Takex gwarantuje dużą odporność na fałszywe alarmy oraz utrzymywanie czułości na wysokim poziomie. Bariera będzie pracować poprawnie nawet w przypadku 99-procentowego tłumienia wiązki pomiędzy nadajnikiem a odbiornikiem. Decydują o tym:

– podwójna modulacja częstotliwość wiązki,
– układ PLL,
– synchronizacja wiązki,
– cztery kanały pracy,
– regulacja czasu naruszenia wiązki,
– układ AGC,
– regulacja mocy wiązki nadawanej,
– wyjście pogodowe,
– zasilanie do 30 VDC,
– znakomity układ kompensacji światła białego,
– specjalna obudowa odporna na zlodowacenie.

Model czterowiązkowej bariery podczerwieni PB-IN-100AT został dodatkowo wyposażony w funkcję Antyprzeczołganie i ma możliwość aktywacji wyjścia alarmowego w przypadku naruszenia tylko dwóch dolnych wiązek. Aby wyeliminować przy tym większe ryzyko przypadkowego alarmu, możemy ustawić osobne czasy naruszenia dla dolnej pary wiązek oraz dla wszystkich czterech wiązek jednocześnie.

Dodatkowe wyposażenie barier podczerwieni stanowią grzałki i termostaty, które zapewniają bezawaryjną pracę nawet podczas najostrzejszej zimy. Dostępne obudowy kolumnowe o wysokościach od jednego do trzech metrów, w wersji jednostronnej oraz dwustronnej, pozwalają na tworzenie układów wielobarierowych o zwiększonym bezpieczeństwie (bariera ukryta w obudowie; intruz nie wie, ile kompletów i na jakiej wysokości zostało zamontowane) oraz dużej estetyce wykonania.



Rys. 3. Funkcja Antyprzeczołganie w barierze PB-IN-100AT

Podsumowanie

Bariery podczerwieni Takex cieszą dużym uznaniem w branży. Wysoka jakość wykonania oraz wiele zaawansowanych rozwiązań technicznych gwarantują skuteczną ochronę i wykluczają ryzyko fałszywego alarmu. Bariery podczerwieni Takex stanowią alternatywę dla tanich torów podczerwieni, których wykonanie, łatwość instalacji i przede wszystkim poprawna praca pozostawia wiele do życzenia.

Jakość barier Takex potwierdzają otrzymane świadectwa kwalifikacyjne klasy S, wydane przez Zakład Rozwoju Technicznej Ochrony Mienia „Techom".

Wszystkie opisane produkty są dostępne w firmie **ICS Polska**, autoryzowanego przedstawiciela firmy Takex w Polsce.

Paweł Penczonek
ICS Polska

artykuł sponsorowany

Bariery podczerwieni

AX-350TF AX-650TF

Fot. 1. Nowa bariera AX-350TF

Aktywne czujki podczerwieni, nazywane torami lub barierami podczerwieni, są nadal – pomimo postępu technologicznego – najczęściej wykorzystywanymi urządzeniami do ochrony obwodowej. Są stosunkowo łatwe w obsłudze, mechanizm ich działania nie jest skomplikowany, mają przystępną cenę, więc zyskały uznanie wielu instalatorów i użytkowników

Firma OPTEX jest liderem w produkcji urządzeń ochrony zewnętrznej, w tym aktywnych czujek podczerwieni. Oferuje wiele produktów, m.in. urządzenia ochrony obwodowej, od najprostszych detektorów krótkiego zasięgu do stosowania jako pojedyncze czujki do bardziej zaawansowanych, umożliwiających tworzenie skomplikowanych aplikacji składających się z wielu detektorów. Największym uznaniem zarówno instalatorów, jak i użytkowników cieszą się m.in. bariery AX-350MKII i AX-650MKII. Te sprzedawane na całym świecie detektory doczekały się następców, nowych czujek AX-350TF i AX-650TF o zasięgu, odpowiednio, 150 i 200 m. Ponieważ klienci zaakceptowali rozwiązania zastosowane w poprzedzających modelach, postanowiono, że kolejny będzie jak najbardziej zbliżony do poprzednika. Obie wersje mają te same obudowy, w ten sam sposób rozmieszczono zaciski czy przełączniki zadające parametry pracy, tak samo regulowany jest układ optyczny. Właściwie, poza tym, że zrezygnowano ze wskaźnika dostrojenia bariery w nadajniku, innych zmian nie widać, ponieważ dotyczą głównie układów sterujących. Instalatorzy mogą montować nowe produkty bez czasochłonnych szkoleń. Nie dochodzi też do kosztownych pomyłek podczas pierwszych instalacji nowego modelu urządzenia.

Modernizacja układów sterujących polegała na zastosowaniu nowoczesnych materiałów i układów o wyższej skali integracji, co w sposób istotny ograniczyło liczbę komponentów. Poza tym zastosowano elementy o znacznie lepszych parametrach pracy w szerokim zakresie temperatur itp. Nowe modele czujek charakteryzują się znacznie bardziej stabilną pracą, zwłaszcza w zmiennych warunkach otoczenia, oraz mniejszym o 20 procent zużyciem energii.

Fot. 2. Nowa bariera AX-350TF - bez pokrywy przedniej.

Zastosowane technologie

Tak jak poprzedniczka, nowa bariera ma wiele rozwiązań technicznych umożliwiających stabilną i długoletnią pracę urządzenia niezależnie od miejsca instalacji. Dzięki układowi automatycznej regulacji wzmocnienia (ARW) odbiornik dostosowuje parametry pracy do zmian natężenia docierającej do niego wiązki podczerwieni, zmieniającego się w zależności od warunków otoczenia. Po stronie analizatora otrzymujemy zatem zawsze ten sam poziom sygnału, co znacznie ogranicza wpływ zmiennych warunków propagacji promieniowania podczerwonego na właściwą detekcję intruza – czyli w wypadku barier podczerwieni na czas przerwania wiązek, wymagany, aby powstał alarm.

Zastosowanie ARW umożliwia pośrednią ocenę warunków pracy detektora. W przypadku stopniowo pogarszającej się pogody (np. powstającej mgły) zaobserwowany powolny spadek natężenia odbieranej wiązki, powodujący wzrost wzmocnienia, zostaje zinterpretowany jako zakłócenie środowiskowe i w chwili, kiedy detektor nie może już zapewnić skutecznej detekcji, aktywowane jest wyjście (DQ), sygnalizujące zbyt niski poziom sygnału. Można je wykorzystać do bramkowania sygnału alarmu w celu uniknięcia fałszywych pobudzeń systemu alarmowego lub lokalnej sygnalizacji, że ochrona obwodowa jest wyłączona. Taka informacja w obiektach posiadających ochronę fizyczną może spowodować podjęcie odpowiednich działań przez pracowników ochrony.

Wszystkie bariery firmy OPTEX charakteryzują się wysoką odpornością na zakłócenia powstałe w wyniku wyładowań atmosferycznych (do 15 kV) oraz wyjątkową stabilnością pracy w zróżnicowanych warunkach. Bariery podczerwieni serii AX mogą poprawnie pracować nawet przy 99-procentowym tłumieniu wiązki z nadajnika. Wykorzystanie tych parametrów jest uzależnione od dokładności wzajemnego pozycjonowania głowic nadajnika i odbiornika. Tu również bariery OPTEX są bezkonkurencyjne. Sposób pozycjonowania głowic pozwala na regulację wstępną przy zastosowaniu wizjerów, a następnie – przy wykorzystaniu wskaźnika diodowego lub multimetru – umożliwia bardzo dokładne ustawienie położenia nadajników i odbiorników. Głowice detektorów są starannie wykonane z wysokiej jakości tworzyw sztucznych oraz elementów metalowych. Bardzo długo zachowują ustawione precyzyjnie położenie. Dzięki temu nie wymagają częstych wizyt serwisowych i ponownego pozycjonowania głowic.

W barierach AX-350TF i AX-650TF można wybrać cztery częstotliwości modulacji wiązek podczerwieni. Zastosowanie różnych częstotliwości modulacji umożliwia tworzenie skomplikowanych konfiguracji detektorów do realizacji najbardziej nawet wyszukanych aplikacji ochrony obwodowej. Dostępna liczba kanałów wystarcza, żeby można było łączyć do czterech detektorów pionowo w jeden moduł ochrony lub do dwóch detektorów pionowo – w szeregowo ustawionych modułach, właściwie bez ograniczeń ich łącznej długości. Prawidłowy dobór kanałów w poszczególnych urządzeniach eliminuje ich wzajemne zakłócanie się bez konieczności wykonywania skomplikowanego okablowania synchronizującego.

Interesującym dodatkiem jest wejście alarmowe po stronie nadajnika. Możemy do niego podłączyć dowolny czujnik alarmowy o stykach normalnie zamkniętych. Rozwarcie styków spowoduje wyłączenie wiązek nadajnika i, w rezultacie, aktywację wyjścia alarmowego odbiornika. Można to wykorzystać np. do zainstalowania dodatkowych pasywnych czujek podczerwieni lub czujek mikrofalowych, które będą uzupełniały system ochrony obwodowej. Nie musimy wówczas wykonywać dodatkowego okablowania. Jest to niezmiernie istotne w instalacjach już istniejących lub kiedy okablowanie dodatkowych czujników jest niemożliwe.

Bariery AX-350/650TF można stosować również w obudowach kolumnowych. Firma OPTEX ma w ofercie zestawy obudów kolumnowych dwustronnych stojących oraz jednostronnych do montażu na ścianie. Dostępne są również typowe akcesoria do obudów kolumnowych, czyli: termostaty, grzałki, wentylatory oraz pokrywy wyposażone w dodatkowe styki sabotażowe, pozwalające wykryć próbę przeskoczenia przez kolumnę.

Podsumowanie

Nowe bariery AX-350TF (150 m) i AX-650TF (200 m), w niczym nie ustępując poprzednikom, w wielu aspektach są od nich lepsze. Znane i doceniane cechy użytkowe zostały uzupełnione o niższe zużycie energii oraz potencjalnie wydłużoną żywotność urządzeń w wyniku mniejszej liczby zastosowanych komponentów. Wraz z zestawem obudów kolumnowych i ich akcesoriów tworzą kompletne rozwiązanie do realizacji najbardziej nawet skomplikowanych systemów ochrony obwodowej.

Wszystkie opisane w niniejszym artykule urządzenia są do nabycia w przedstawicielstwach firmy AAT-T, która jest autoryzowanym dystrybutorem firmy OPTEX w Polsce.

Jarosław Gibas
Optex Security

MULTIPLEKSER CYFROWY

NV-DVR 400 series

NV-DVR404/CD

CECHY CHARAKTERYSTYCZNE

- 4 wejścia wideo
- Tryb pracy tripleks
- System operacyjny oparty na systemie Linux
- Prędkość nagrywania do 100 obr/s
- Algorytm kompresji M-JPEG z możliwością wyboru jednego z 5 poziomów kompresji
- Sterowanie kamerami PTZ (z poziomu rejestratora oraz przez sieć komputerową)
- Wbudowana nagrywarka CD-RW

PARAMETRY TECHNICZNE

Model	NV-DVR404/CD
System operacyjny	Linux
Wejścia wideo	4 x BNC
Wyjścia wideo	monitor główny (1 x BNC), monitor pomocniczy (1 x BNC)
Wejścia/wyjścia alarmowe	4/1
Prędkość nagrywania	do 100 obr/s (360 x 288), do 50 obr/s (720 x 288)
Kompresja	M-JPEG
Tryby nagrywania	ciągły, wyzwalany (alarmem i/lub detekcja ruchu)
Format wyświetlania	1, 4, PIP, sekwencja, zoom cyfrowy, zamrożenie obrazu
Detekcja ruchu	siatka 16 x 12, regulacja czułości
Detekcja utraty sygnału	tak
Harmonogram	odrębne ustawienia dla każdego dnia tygodnia i każdej kamery, możliwość łączenia różnych trybów nagrywania
Sposób wyszukiwania	według czasu/daty, zdarzeń, paska nagrań
Kopiowanie obrazów	na płyty CD, pamięć Flash USB, przez sieć komputerową
Nagrywarka CD	wbudowana
Protokoły sterowania PTZ	Novus-C, Novus-C1, Novus-C2, Pelco-D
Obsługa	mysz komputerowa PS2, sieć komputerowa
Menu	wyświetlane na ekranie (w języku polskim)
Oprogramowanie	N-Viewer 400
Zabezpieczenie systemu	WATCHDOG sprzętowy
Zasilanie/pobór mocy	12 VDC (zasilacz 230 VAC w zestawie)/48 W

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

Rejestrator NV-DVR404/CD

Przy pierwszym kontakcie z rejestratorem NV-DVR404/CD rzuca się w oczy jego unikatowy i bardzo efektywny sposób obsługi przez użytkownika. Urządzenie nie posiada przycisków w panelu czołowym. Czynności administracyjne wykonuje się za pomocą podłączonej do rejestratora myszy PS2. I choć interfejs nie decyduje o funkcjonalności urządzenia, to sposób komunikacji ma duże znaczenie dla użytkownika końcowego – pozwala mu na łatwe i szybkie programowanie ustawień menu.

Menu urządzenia, chronione hasłem dostępu składającym się z maksimum dziesięciu cyfr, jest dostępne w dwunastu wersjach językowych, w tym polskiej.

Rejestrator oparto na systemie operacyjnym Linux, co gwarantuje niezawodność działania. To ważne, zwłaszcza że powyższe rejestratory w zdecydowanej większości pracują bezobsługowo w trybie ciągłym, 24 godziny na dobę. NV-DVR404/CD jest urządzeniem 4-kanałowym i pracuje w trybie triplex, pozwalając na równoczesny podgląd na żywo, nagrywanie oraz połączenia sieciowe, np. zdalne odtwarzanie zarejestrowanych materiałów.

Rejestrator, niezależnie od definiowanej przez administratora rozdzielczości zapisu (360 x 288 lub 720 x 288), pozwala na rejestrację do 100 obrazów na sekundę, więc zapewnia zapis obrazów w czasie rzeczywistym ze wszystkich czterech kamer, nawet w wysokiej rozdzielczości. Obrazy są kompresowane algorytmem M-JPEG w pięciu różnych poziomach gwarantujących różną jakość obrazu – od niskiej (17 kB) do najwyższej (32 kB).

W urządzeniu może być zamontowany jeden dysk o maksymalnej pojemności 500 GB, umożliwiający pracę w trybie nadpisywania. W trybie zapisu ciągłego i najwyższej jakości z prędkością 1 kl/s. dla kamery gwarantuje to 30 dni archiwizacji.

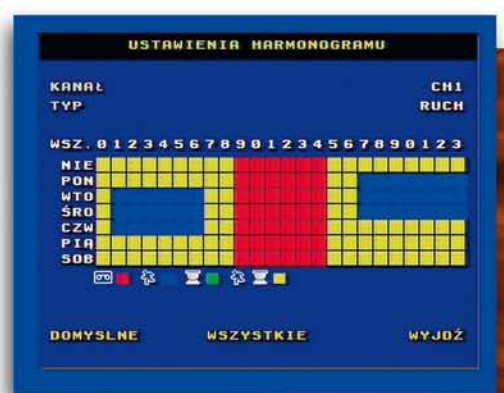
Rejestrator ma dwa wyjścia monitorowe: główne BNC i VGA, mogące działać równocześnie, oraz pomocnicze BNC. Wyjście VGA, dzięki możliwości ustawienia formatu pracy, tzn. rozdzielczości i częstotliwości odświeżania w zakresie od 640 x 480/60 Hz do 1280 x 1024/75 Hz zapewnia współpracę z praktycznie wszystkimi modelami monitorów LCD. Na wyjściu pomocniczym wyświetlana jest pełnoekranowo sekwencja obrazów z kamer o definiowanym przez użytkownika czasie przełączania. Dodatkowo na wyjściu monitorowym pomocniczym może być wyświetlany obraz z kanałów, dla których wystąpiła detekcja ruchu lub zostało uaktywnione odpowiednie wejście alarmowe.

Rejestrator NV-DVR404/CD dysponuje zaawansowanym graficznym harmonogramem nagrywania. Można zróżnicować tryb nagrywania dla poszczególnych dni i godzin tygodnia niezależnie dla każdej z kamer. Dla ustawionego numeru kanału i trybu nagrywania należy na graficznym harmonogramie ustawić czasowy zakres nagrywania, zaznaczając odpowiednie pola kursorem (rys. 1.).

Rejestrator NV-DVR404/CD posiada niezależne ustawienia detekcji ruchu dla każdego kanału. Ustawienia detekcji realizowane są za pomocą siatki pól 16 x 12. Można zdefiniować również czułość detekcji w zakresie od 1 do 5 oraz próg zadziałania, tzn. minimalną liczbę komórek siatki, które muszą być aktywne, aby system rozpoznał to jako ruch.

Rejestratory NV-DVR404/CD pozwalają sterować czterema kamerami wyposażonymi w interfejs RS485. Mogą to być zarówno kamery obrotowe, jak i stacjonarne z zoomem optycznym i cyfrowym. Istnieje możliwość sterowania kamerami w protokołach NOVUS-C1, NOVUS-C2, N-CONTROL i PELCO-D.

Sterowanie kamerami może być realizowane lokalnie lub z poziomu oprogramowania sieciowego. Rejestrator posiada intuicyjny i efektywny system sterowania kamerami obrotowymi za pomocą myszy. Aby sterować funkcją zoom, należy



Rys. 1. Ustawienia graficznego harmonogramu nagrywania

Rejestrator NV-DVR404/CD dysponuje zaawansowanym graficznym harmonogramem nagrywania. Można zróżnicować typ nagrywania dla poszczególnych dni i godzin tygodnia niezależnie dla każdej z kamer. Dla ustawionego numeru kanału i typu nagrywania należy na graficznym harmonogramie ustawić czasowy zakres nagrywania, zaznaczając odpowiednie pola kursorem.

ustawić kursor w centralnej części ekranu (ikona lupy) i użyć przewijania (*scroll*). W celu sterowania kamerami z obrotem i uchyłem (PAN/TILT) należy przemieścić kursor w wybrane miejsce (ikona strzałki) i nacisnąć lewy przycisk myszy. Dodatkowo w menu można definiować prędkość sterowania poszczególnymi funkcjami: obrotu, uchyłu oraz ogniskowania w zakresie od 0 do 7.

Rejestratory NV-DVR404/CD posiadają wbudowaną nagrywarkę płyt CD. Dzięki niej możliwe jest tworzenie kopii nagrań na płytach CD-R i CD-RW.

Rejestratory NV-DVR404/CD posiadają wbudowaną nagrywarkę płyt CD. Dzięki niej możliwe jest tworzenie kopii nagrań na płytach CD-R i CD-RW. Dodatkowo rejestrator jest wyposażony w złącze USB pozwalające na kopiowanie zapisanych plików do pamięci Flash z interfejsem USB. Kopiowane pliki z rozszerzeniem ajp mogą być odtwarzane za pomocą dołączanego oprogramowania N-BackUpPlayer. Aplikacja pozwala też na edycję i zapis poszczególnych klatek w formacie jpg, a następnie ich drukowanie oraz konwersję do formatu avi, który może być odtwarzany za pomocą standardowych aplikacji.

Dodatkowe złącze USB rejestratora przeznaczone jest do aktualizacji jego oprogramowania (*firmware*). W ramach niej producent będzie udostępniał kolejne wersje, bogatsze w nowe możliwości i, w razie potrzeby, z poprawionymi błędami.

Rejestrator jest wyposażony również w złącze USB pozwalające na kopiowanie zapisanych plików do pamięci Flash z interfejsem USB. Kopiowane pliki z rozszerzeniem ajp mogą być odtwarzane za pomocą dołączanego oprogramowania N-BackUpPlayer. Aplikacja pozwala też na edycję i zapis poszczególnych klatek w formacie jpg, a następnie ich drukowanie oraz konwersję do formatu avi, który może być odtwarzany za pomocą standardowych aplikacji.

Dodatkowe złącze USB rejestratora przeznaczone jest do aktualizacji jego oprogramowania (*firmware*). W ramach niej producent będzie udostępniał kolejne wersje, bogatsze w nowe możliwości i, w razie potrzeby, z poprawionymi błędami.

Kamery mogą być wyświetlane na monitorze głównym pełnoekranowo, w podziale 2x2, w sekwencji, funkcji „obraz w obrazie", a także w powiększeniu cyfrowym.

Rejestrator NV-DVR404/CD pozwala na szybkie odnalezienie zarejestrowanych obrazów na trzy sposoby – za pomocą procentowego paska wyszukiwania, przez wybranie określonej daty i czasu oraz poprzez rejestr zdarzeń. W przypadku procentowego paska wyszukiwania datę i czas odtwarzanych obrazów wybiera się kursorem myszy na pasku wyszukiwania reprezentującym całość dotychczas zarchiwizowanych materiałów jako 100%.

Rejestratory NV-DVR404/CD umożliwiają pracę w sieci komputerowej z wykorzystaniem protokołu TCP/IP. Połączenie realizowane jest z poziomu dedykowanego oprogramowania N-Viewer 400. Możliwe jest zdalne połączenie jednego użytkownika z rejestratorem w trybie na żywo lub odtwarzanie i podgląd kamer pełnoekranowo lub z podziałem 2 x 2.

Zdalny dostęp do rejestratora wymaga autoryzacji za pomocą loginu oraz hasła. Komunikacja z rejestratorem odbywa się definiowanym przez użytkownika jednym portem TCP/IP, który powinien być otwarty w urządzeniach sieciowych odpowiadających za realizację połączenia.

Program może być uruchamiany pełnoekranowo lub ze standardową rozdzielczością 800x600. Oprócz podglądu na żywo aplikacja N-Viewer 400 oferuje możliwość przejrzenia nagrań zarejestrowanych na rejestratorze. Tak jak przy obsłudze lokalnej można odszukać nagrania z konkretnej daty – z dokładnością co do sekundy – lub odtworzyć zdarzenia.

W trakcie odtwarzania można zapisać obrazy z kamer w formacie jpg lub strumienia avi. Tak zapisywane strumienie mogą być odtwarzane np. za pomocą programu Windows Media Player.

Na bardzo konkurencyjnym rynku rejestratorów 4-kanałowych NV-DVR404/CD jest wyróżniającym się produktem pozwalającym na spełnienie oczekiwań potencjalnych użytkowników. W kolejnym modelu urządzenia planowane jest zastąpienie systemu kompresji M-JPEG bardziej efektywnym dla transmisji sieciowej algorytmem H-264. Pozwoli to na znaczne zwiększenie częstotliwości odświeżania obrazów z kamer.

Rys. 2. Aplikacja sieciowa N-Viewer400

Patryk Gańko
Novus

Tango+L – drukarka i laminator w jednym

MAGICARD

Tango+L jest termosublimacyjną drukarką kart identyfikacyjnych ze zintegrowaną stacją laminującą. Wykonana z metalowych elementów konstrukcyjnych gwarantuje wysoką niezawodność w długim okresie użytkowania. Wysoka funkcjonalność oraz zabezpieczenia drukarki i nadruku sprawiają, że jest ona profesjonalnym rozwiązaniem do masowej produkcji kart ID

Proces laminacji, podczas którego karta pokrywana jest folią poliestrową znacznie zwiększa odporność nadruku na ścieranie lub inne uszkodzenia mechaniczne. Zastosowanie folii laminacyjnych z hologramem zabezpiecza karty przed podrobieniem. Możliwe jest zastosowanie folii z hologramem użytkownika (dowolna grafika).

Tempo+L wyposażona jest w panel z przyciskami funkcyjnymi, diodami LED oraz wyświetlaczem LCD informującym o statusie drukarki.

W standardzie:

Holokate™ – znak wodny drukowany na całej powierzchni karty. Widoczny przy patrzeniu pod kątem.

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

Nadruk od krawędzi do krawędzi. Nadruk z jakością 300 dpi na całej powierzchni karty.

Interfejs Ethernet

Dwustronny nadruk

Stacja laminująca

2 lata gwarancji (łącznie z głowicą). Możliwość przedłużenia gwarancji do 4 lat.

Opcje:

Dowolna grafika lub tekst w znaku wodnym.

Możliwość kodowania kart magnetycznych.

Możliwość kodowania kart chipowych i zbliżeniowych.

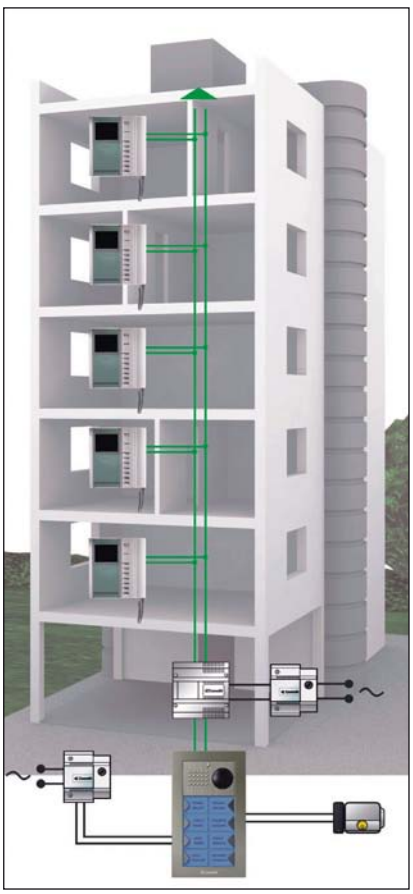
SPECYFIKACJA TECHNICZNA
PRĘDKOŚĆ NADRUKU
Nadruk z laminacją od 36 do 55 s (w zależności od ustawień)
Nadruk dwustronny z laminacją od 82 do 120 s (w zależności od ustawień)
ZABEZPIECZENIA URZĄDZENIA
Dostęp do folii laminacyjnej, podajnika oraz odbiornika kart chroniony kluczem
Zabezpieczenie przed nieautoryzowanym użyciem drukarki opcjonalną kartą flash
ZABEZPIECZENIA KART
HoloKote – znak wodny drukowany na całej powierzchni karty
Laminator (możliwość użycia folii holograficznych)
TYPY TAŚM
LC1: YMCKO – 350 wydruków
LC3: monochromatyczna – 1000 wydruków
LC6: KO (czarny i overlay) – 600 wydruków
LC8: YMCKOK – 300 wydruków
Taśmy laminacyjne czyste i holograficzne (dostępne hologramy z wzorem klienta)
Akceptowane karty
PVC/PET ISO CR80 – z paskiem magnetycznym, zbliżeniowe, HoloPatch, samoprzylepne (bez laminacji)
Grubość kart
Z laminacją – 0,76 mm
Bez laminacji – od 0,38 mm do 1.6 mm
Pojemność magazynków
Podajnik 100 szt.
Pojemnik kart nadrukowanych 50 szt.
Głowica
300 dpi
Interfejs
Port LPT i USB, Ethernet
Sterowniki
Win 2000, 2003 Server user-mode, XP
Zasilanie
240 V/50-60 Hz
Wymiary (szer. x wys. x dł.)
300 mm x 260 mm x 700 mm
Masa
20 kg
Temperatura pracy
od 10°C do 30°C

DYSTRYBUTOR w Polsce:

ACSS Sp. z o.o.
ul. Rydygiera 12, 01-793 Warszawa
tel.: 022 8324744
faks 022 8324644
e-mail:biuro@acss.com.pl
www.acss.com.pl
www.magicard.com.pl

2-przewodowy system wideodomofonowy

firmy COMELIT



SIMPLEBUS2

Cechy charakterystyczne:

- 2 przewody łącznie z zasilaniem monitora
- 4 magistrale na zasilacz (np. 4 piony w budynku mieszkalnym)
- do 8 monitorów z funkcją intercomu 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
- wyeliminowano konieczność stosowania zasilacza monitora

Oprócz standardowych funkcji systemów wideodomofonowych, monitory Bravo i Genius umożliwiają sterowanie programowalnym modułem przekaźnikowym lub innym zewnętrznym urządzeniem. Standardowo możliwe jest podłączenie przycisku dzwonka lokalnego i dodatkowej (oddalonej) sygnalizacji wywołania. Ponadto monitor Bravo można wyposażyć w kartę 4 dodatkowych przycisków realizujących inne funkcje w systemie (np. przełączanie obrazu z kamer zewnętrznych, interkom itp.)

W systemie Simlpebus2 można zastosować panele wejściowe serii Powercom jak i wandaloodporne Vandalcom. Oba panele występują w wersji cyfrowej z elektronicznym spisem nazwisk oraz z indywidualnymi przyciskami wywołania. Kamera panelu wejściowego posiada płynną regulację położenia w obu płaszczyznach oraz podświetlanie diodami podczerwieni. Ramki zewnętrzne paneli dostępne są w różnych kolorach.

DYSTRYBUTOR w Polsce:

alarmnet®

ALARMNET Sp. j.
ul. Rydygiera 12
01-793 Warszawa

tel.: (22) 663 40 85
fax: (22) 833 87 95
www.alarmnet.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 VDC (10-15 VDC)
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 VDC
Ostrzeżenie o zbyt niskim napięciu: <10 VDC
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

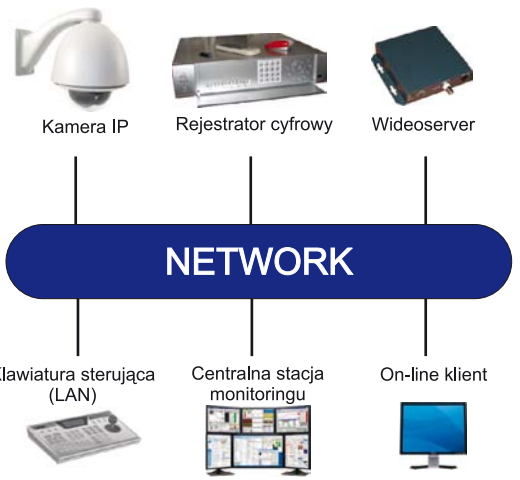
alarmnet®

ALARMNET Sp. j.
ul. Rydygiera 12
01-793 Warszawa

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

Urządzenia systemu CCTV IP – seria PROTEC-D

- Podgląd i rejestracja 16 rejestratorów lub wideoserwerów w tym samym czasie (dowolny wybór istotnych kamer)
- Dual streaming dla każdej z kamer lub rejstratorów
- Opcja nagrywania lokalnego każdej z zobrazowanych kamer
- Opcja robienia zdjęć
- Opcja obsługi audio
- Jednoczesny podgląd, nagrywanie i odtwarzanie nagrań
- Tworzenie planów połaczeń z kamerami i rejestratorami
- Sterowanie kamerami obrotowymi poprzez rejestratory i wideoserwery
- Obserwacja w trybie on-line obciążenia sieci LAN i procesora komputera stacji monitorowania
- Pełny podgląd i konfiguracja każdego rejestratora i wideoserwera
- Rejestr działania systemu



Wideoserwer serii Protec DNVS-01

System operacyjny	Zaimplementowany system LINUX
Rozdzielczość	VGA/QVGA/HD1/D1/CIF/QCIF
Kompresja wideo	MPEG-4 (VBR, CBR), audio-PCM
Prędkość transmisji	1-25 kl./s
Szerokość pasma	1,3 Mb/s dla transmisji PAL D1(704X576), 25 kl./s
Audio	1-4 wejść przełączanych (liniowe lub mikrofonowe), 1 wyjście, wsparcie dla VoiceIP
Wideo	1-4 wejść wideo w zależności od wersji
Wideodetekcja	192 obszary (16x12) – 3 stopnie czułości na kanał wideo
Jakość obrazu	6 poziomów ustawień
Wejścia alarmowe	4 wejścia, 1 wyjście przekaźnikowe
Porty komunikacyjne	RJ 45 LAN 10M/100M, RS 232,
Sterowanie PTZ	RS 485, 60 protokołów
Zasilanie	12 V_{DC}
Pobór mocy	5 W
Opcje dodatkowe	Możliwość nagrywania w zależności od wersji
Interfejs komunikacyjny	WEB, program klienta – do 10 klientów jednoczesnie, pełna konfiguracja zdalna serwera za pomocą oprogramowania

Klawiatura sterująca IP D-NKB (LAN)

Opcje sterowania	Sterowanie do 1024 rejestratorów, kamer obrotowych lokalnie lub po sieci LAN
Zasilanie	12 V_{DC}, 1 A
Porty	LAN – RJ 45 10M/100M, RS 232, RS 485, podczerwień
Inne	Pełne sterowanie rejestratorów, kamer obrotowych, krosownic wizyjnych

Głowica szybkoobrotowa seri PR-60C

Głowice szybkoobrotowe zewnętrzne/wewnętrzne	Opcja – wyposażone w moduł IP
PR-60C09	Kamera szybkoobrotowa zewnętrzna; 1/4"; dualna – dzień/noc; 35x zoom optyczny oraz 12x zoom cyfrowy; kamera z przetwornikiem SONY 540 TVL; 0,01 lx; 0 lx (IR); S/N>50 dB; WB; Gain Control; BLC; SWDR; obiektyw: F=3,4 (wide)–119 (tele) mm; kamera kompletna z obudową, uchwytem, zasilaczem
PR-60C08	j.w., 23x zoom optyczny
PR-60C04	Kamera szybkoobrotowa zewnętrzna; 1/4"; dualna – dzień/noc; 26x zoom optyczny oraz 12x zoom cyfrowy; kamera z przetwornikiem SONY 540 TVL; 0,01 lx; 0 lx (IR); S/N>50 dB; WB; Gain Control; BLC; obiektyw: F=3,5 (wide)–91 (tele) mm; kamera kompletna z obudową, uchwytem, zasilaczem
PR-60C03	j.w., 18x zoom optyczny

PROTECTOR

Protector Polska Sp. z o.o.
ul. Tyniecka 28, 71-019 Szczecin
tel.: 091 431 83 10, faks 091 431 83 11
www.protector-polska.pl, e-mail: biuro@protector-polska.pl

Urządzenia systemu CCTV IP – seria PROTEC-D
(ciąg dalszy)

Rejestratory serii Protec D PR-D1604/0804/0404R H.264 (Real Time)

4/8/16 kanałów audio/wideo
(krosownica wizyjna 16x4)

System operacyjny	Zaimplementowany system LINUX
Rozdzielczość podglądu i rejestracji	Rejestracja D1 (704x576)/HD1 (704x288)/CIF(352x288), podgląd D1 (704x576),
Kompresja wideo	MPEG-4/H.264 (VBR, CBR), audio-PCM
Prędkość transmisji i nagrywania	1-25 kl/s na każdy kanał (do 400 kl./s dla 16 kanałów w HD1, CIF), 200 kl./s w D1
Szerokość pasma	1,3 Mb/s dla transmisji PAL D1(704X576), 25 kl./s – multicast lub osobno dla każdego kanału wideo (dual streaming)
Audio	4-16 wejść (liniowe), 1 wyjście, wsparcie dla VoiceIP
Wejścia wideo	4-16 wejść wideo w zależności od wersji
Wyjścia wideo	1 Main, 1 Spot (BNC), VGA-Main
Wideodetekcja	192 obszary (16x12) – osobna na każdy kanał wideo
Jakość obrazu	6 poziomów ustawień
Wejścia alarmowe	4-16 wejść, 2-6 wyjść przekaźnikowych
Porty komunikacyjne	RJ-45 LAN 10M/100M, RS 232, 2xUSB
Sterowanie PTZ	RS 485, 60 protokołów
Zasilanie	230 V_{AC}
Pobór mocy	25 W-45 W
Interfejs komunikacyjny	WEB, program klienta, do 10 klientów jednocześnie, program multiklienta, pełna zdalna konfiguracja rejestratora
Harmonogram nagrywania	Oddzielny dla każdej kamery na każdy dzień tygodnia, godzinę i rodzaj zdarzeń (wideodetekcja, alarm z wejść, nagrywanie ciągłe)
Współpraca	Współpraca z klawiaturą sterującą typu NET (w sieci LAN), sterowanie myszą lub pilotem
Inne	Maskowanie kamer, strefy prywatności, osobne ustawienie parametrów pracy kamer dla trybu dziennego i nocnego
Ilość dysków	Do 8 dysków wewnętrznych po 500 GB (4 TB)
Opcje dodatkowe	Rejestrator z funkcją krosownicy wizyjnej 16x4 z wejściami przelotowymi i dodatkowymi 4 wyjściami na monitory

Rejestratory serii Protec D PR-D 0414

PR-D 0414 slim
(non-real time)

PR-D 0414NRL
(non-real time)

System operacyjny	Zaimplementowany system LINUX
Rozdzielczość	Rejestracja CIF (352x288), podgląd D1 (704x576),
Kompresja wideo	MPEG-4 (VBR, CBR), audio-PCM
Prędkość nagrywania	1-36 kl./s na 4 kanały
Audio	2 wejścia (liniowe), 1 wyjście, wsparcie dla VoiceIP
Wejścia wideo	4-wejścia video BNC
Wyjścia wideo	1 Main, 1 Spot (BNC), VGA-Main
Wideodetekcja	192 obszary (16x12) – osobna na każdy kanał wideo
Jakość obrazu	6 poziomów ustawień
Wejścia alarmowe	4 wejścia, 2 wyjścia przekaźnikowe
Porty komunikacyjne	RJ-45 LAN 10M/100M, RS 232, 2xUSB
Sterowanie PTZ	RS 485, 60 protokołów
Zasilanie	230 V_{AC}
Pobór mocy	25 W
Interfejs komunikacyjny	WEB, program klienta – do 10 klientów jednocześnie, program multiklienta, pełna zdalna konfiguracja rejestratora
Harmonogram zapisu	Oddzielny dla każdej kamery
Współpraca	Sterowanie myszą lub pilotem
Ilość dysków	1-2 dysków wewnętrznych 500 GB (1 TB) w zależności od wersji
Opcje dodatkowe	Wbudowany LCD – w zależności od wersji

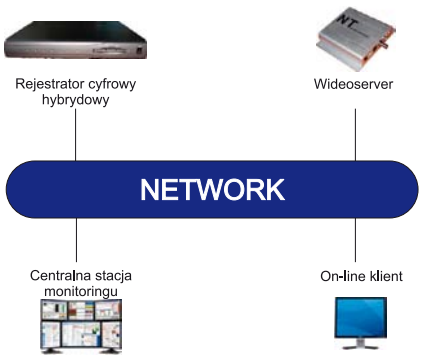
PROTECTOR

Protector Polska Sp. z o.o.
ul. Tyniecka 28, 71-019 Szczecin
tel.: 091 431 83 10, faks 091 431 83 11
www.protector-polska.pl, e-mail: biuro@protector-polska.pl

Urządzenia systemu CCTV IP – seria PROTEC-M

Możliwości oprogramowania Centralnej Stacji Monitorowania i Klienta

Podgląd i rejestracja 256 kamer podłaczonych do rejestratorów lub wideoserwerów. *Dual streaming* dla każdej z kamer lub rejstratorów. Opcja nagrywania lokalnego każdej z zobrazowanych kamer. Opcja robienia zdjęć. Opcja obsługi audio. Jednoczesny podgląd, nagrywanie i odtwarzanie nagrań. Tworzenie graficznych planów rozmieszczenia kamer. Sterowanie kamerami obrotowymi poprzez rejestratory i wideoserwery. Obserwacja *on-line* obciążenia sieci LAN i procesora komputera stacji monitorowania. Pełny podgląd i konfiguracja każdego rejestratora i wideoserwera. Rejestr działania systemu, alarmów i innych zdarzeń.



Wideoserwer serii Protec M NT-24

System operacyjny	Zaimplementowany system LINUX
Rozdzielczość	D1 (704x576), CIF 352x288
Kompresja wideo	MPEG-4, audio-PCM
Prędkość transmisji	1-25 kl./s
Szerokość pasma	3 Mb/s dla transmisji PAL D1(704X576), 25 kl./s
Audio	1 wejście (liniowe), 1 wyjście, wsparcie dla VoiceIP
Wideo	1 wejście wideo przelotowe
Wideodetekcja	Czułośc i rozróżnialność regulowana od 1-99 poziomów
Funkcje specjalne	Funkcja dekodera sprzętowego obrazu z kamery podłączonej do innego serwera
Wejścia alarmowe	2 wejścia, 2 wyjścia przekaźnikowe
Porty komunikacyjne	RJ 45 LAN 10M/100M, RS232 – modem, USB
Sterowanie PTZ	RS485
Zasilanie	12 V_{DC}
Pobór mocy	5 W
Opcje dodatkowe	Możliwość nagrywania na kartach SD lub poprzez USB
Interfejs komunikacyjny	WEB, program klienta – do 99 klientów jednocześnie, pełna konfiguracja zdalna serwera za pomocą oprogramowania

Rejestrator hybrydowy serii PR-M NC 04 slim (Real-time)

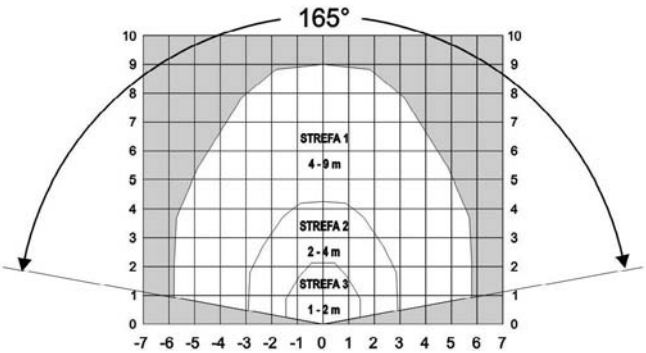
System operacyjny	System LINUX (PC Based)
Rozdzielczość podglądu	D1 (704x576)/HD1 (704x288)/CIF (352x288)
Kompresja wideo	MPEG-4, audio-PCM
Prędkość transmisji i nagrywania	1-25 kl./s na każdy kanał (do 400 kl./s dla 16 kanałów w D1, HD1, CIF)
Audio	4-16 wejść (liniowe), 1 wyjście, wsparcie dla VoiceIP
Wejścia wideo	4-16 wejść wideo w zależności od wersji
Wyjścia wideo	1 Spot (BNC), VGA-Main
Videodetekcja	192 obszary (16x12) – osobna na każdy kanał wideo
Funkcje specjalne	Hybrydowy sposób pracy. Możliwy podgląd i rejestracja zarówno kamer analogowych podłączonych bezpośrednio do rejestratora, jak i kamer IP poprzez sieć LAN
Wejścia alarmowe	4-16 wejść, 2-8 wyjść przekaźnikowych
Porty komunikacyjne	RJ-45 LAN 10M/100M, RS232, 2xUSB
Sterowanie PTZ	RS232
Zasilanie	230 V_{AC}
Pobór mocy	25 W-45 W
Interfejs komunikacyjny	WEB, program klienta, do 99 klientów jednocześnie, program multiklienta, pełna zdalna konfiguracja rejestratora
Harmonogram nagrywania	Oddzielny dla każdej kamery na każdy dzień tygodnia ,godzinę i rodzaj zdarzeń (wideodetekcja, alarm z wejść, nagrywanie ciągłe)
Współpraca	Sterowanie myszą
Inne	Maskowanie kamer, strefy prywatności
Ilość dysków	Od 2 do 4 dysków wewnętrznych po 500 GB (2 TB)

PROTECTOR

Protector Polska Sp. z o.o.
ul. Tyniecka 28, 71-019 Szczecin
tel.: 091 431 83 10, faks 091 431 83 11
www.protector-polska.pl, e-mail: biuro@protector-polska.pl

Akustyczne detektory zbicia szyby klasy S z serii AD 700

Zakresy detekcji przy montażu na ścianie w metrach:



Produkowane przez Alarmtech detektory z serii AD 700 są nowoczesnymi, akustycznymi detektorami zbicia szyby, dającymi informację w postaci alarmu przy próbach włamania do chronionych obiektów przez okna, przeszklone drzwi, oszklone elementy ścian. Zbudowane są w oparciu o najnowszą technologię z dziedziny mikrokontrolerów, ich oprogramowanie uwzględnia wiele czynników związanych z akustyką pomieszczeń. Opracowany przez Alarmtech algorytm detekcji metodą „data fission – data fusion" uwzględnia najnowsze osiągnięcia z dziedziny techniki rozpoznawania dźwięków. Umożliwia również cyfrową kompensację akustyki pomieszczenia (DRC). Dzięki temu możliwe jest precyzyjne rozróżnianie sygnałów, powstających w wyniku zbicia szyby od innych, zakłócających.

Przeznaczone są do stosowania wewnątrz pomieszczeń – mogą być montowane na ścianach (najlepiej przeciwległych do chronionych powierzchni tak, aby okna znajdowały się w „polu widzenia" mikrofonu – 165°) i na sufitach. Instalacja na suficie nie wymaga dodatkowych akcesoriów, kształt detektora zapewnia swobodę montażu. Przy maksymalnej odległości detektora od chronionej powierzchni – 9 m, zabezpieczają szyby o grubości do 6,5 mm i wymiarach od 30 x 30 cm do 600 x 600 cm.

Kryteria dające AD 700 pozycję jednego z najbardziej interesujących akustycznych detektorów zbicia szyby:

- **Wysokiej klasy detekcja sygnału**

Dzięki algorytmowi DRC zapewniona jest znakomita detekcja sygnału rozbijanego szkła.

- **Doskonała odporność na fałszywe alarmy**

Ponownie algorytm DRC odgrywa tutaj ważną rolę razem z zaawansowanymi algorytmami rozpoznawania fałszywych alarmów.

- **Uniwersalność**

Jeden detektor może chronić wiele płaszczyzn szklanych znajdujących się w obszarze detekcji.

- **Wszechstronność**

Detektor wykrywa zbicia szkła różnego rodzaju.

- **Ulepszony sposób instalacji**

Mocowanie bez potrzeby wyjmowania płytki drukowanej. Dobry dostęp do złącz z zabezpieczeniami dla końcówek podłączanych przewodów. Łatwość programowania za pomocą przełączników – DIP.

UWAGA

Wprowadzone ostatnio do sprzedaży detektory AD 700 S i AD 700 SAM są ekonomicznymi odmianami serii AD 700, w których zrezygnowano z funkcji D/N oraz AIS **przy zachowaniu wszystkich pozostałych parametrów charakterystycznych dla pełnej wersji AD 700 i decydujących o zaletach detektora.**

Atesty Techom: 130/06, 131/06

Obszary zastosowań detektorów z serii AD 700		
Konstrukcja szyby		**Rodzaj szkła w szybie wewnątrz pomieszczenia**
1.	Szyby pojedyncze	Zwykłe Hartowane Laminowane
2.	Szyby podwójne zaspolone	Zwykłe Hartowane Laminowane
3.	Szyby potrójne zaspolone	Zwykłe Hartowane Laminowane
4.	Szyby pojedyncze i zespolone z folią antywłamaniową	Zwykłe z folią naklejoną od strony pomieszczenia

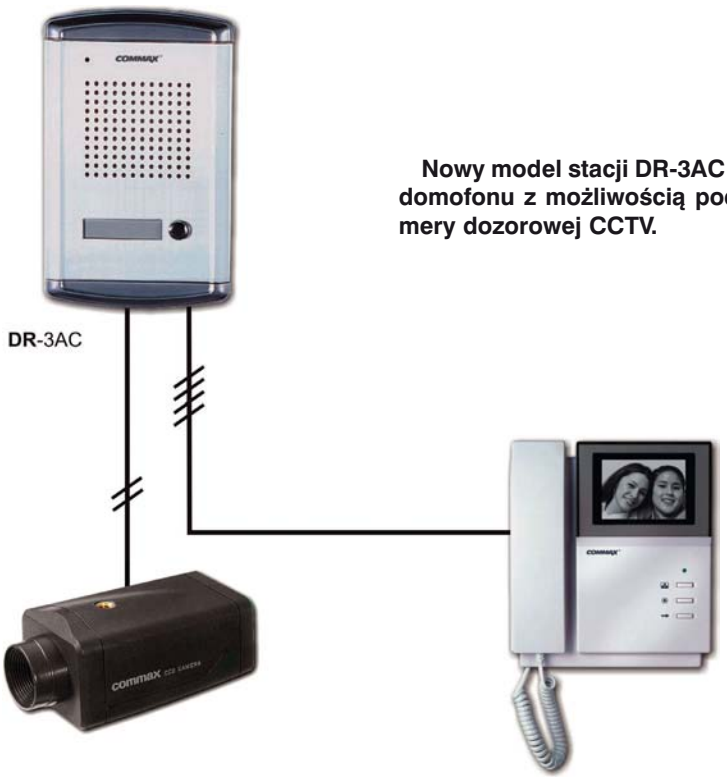
Dane techniczne	
Napięcie zasilania	9–15 V DC
Kontrola napięcia	alarm przy <7 V+/-0,5 V
Pobór prądu przy 12 V	
• w stanie spoczynkowym	ok. 25 mA
• w stanie alarmu	ok. 24 mA
Przekaźnik alarmu NC	500 mA/maks. 100 V DC R<40 ohm
Obciążalność styków przełącznika sabotażowego	50 mA/maks. 50 V DC
Zakresy	
• zasięg (maks.)	promień 9 m/165°
• zakres działania	strefa 3 = 1–2 m
	strefa 2 = 2–4 m
	strefa 1= 4–9 m
Wymiary chronionej szyby	min. 30x30 cm, maks. 6x6 m
Grubość szyby (maks.)	6,5 mm
Rodzaje szkła	zwykłe (float) – hartowane – laminowane – zwykłe foliowane
Kubatura chronionego pomieszczenia	min. 20 m^3, maks. 250 m^3
Zakres temperatury pracy	-10 do +55°C
Wilgotność, DIN 40040	maks. 90% r.h. (klasa F)
Kategoria ochr. obud. EN60529	IP 31

ALARMTECH POLSKA Sp. z o.o.

Alarmtech Polska Sp. z o.o.
80-299 Gdańsk – Osowa, ul. Kielnieńska 115
tel. 058 340-24-40, faks 058 340-24-49
http://www.alarmtech.pl; e-mail: info@alarmtech.pl

Stacja bramowa DR-3AC

Stacja domofonowa z możliwością podłączenia kamery przemysłowej w systemie wideodomofonowym

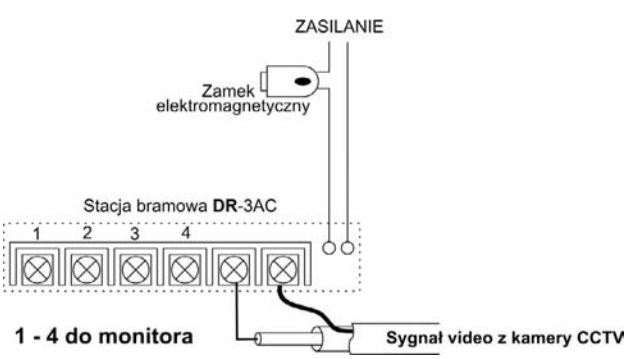


Nowy model stacji DR-3AC pełni funkcję domofonu z możliwością podłączenia kamery dozorowej CCTV.

Charakterystyka:

– stacja domofonowa do systemu wideodomofonowego (funkcja audio)
– metalowa, podtynkowa, kolor srebrny
– współpracuje z monitorami: DPV-4P**, DPV-4***, CDV-50, CDV-4HC
– możliwość podłączenia zewnętrznej kamery przemysłowej
– wymiary puszki podtynkowej (wys. x szer. x gł.) 168 x 100 x 40 mm
– wymiary panela czołowego (wys. x szer. x gł.) 186 x 124 x 18 mm
– dostępna osłona/daszek ODRC-4BANps
– możliwość montażu natynkowego z obudową ODRC-4BANns
– estetyczny wygląd

Parametry techniczne	
Zasilanie	DC 12 V (z monitora)
Okablowanie	4 przewody spolaryzowane 2 przewody (wejście wideo)
Otwieranie drzwi	2 przewody niespolaryzowane (styk)
Wejście wideo	1 Vp-p, 75 Ohm
Masa	760 g
Wymiary	124 x 186 x 50 mm



GDE POLSKA
GLOBAL DISTRIBUTOR OF ELECTRONICS

GDE Polska
ul. Koniecznego 46
32-040 Świątniki Górne

tel./fax: 012 256 50 35, 256 50 25
fax: 012 270 56 96
e-mail: biuro@gde.pl

CAV-71B
Monitor kolorowy z łącznością interkomową

CAV-71B to nowy kolorowy monitor w ofercie firmy GDE POLSKA z 7-calowym, panoramicznym wyświetlaczem LCD, na którym oprócz obrazu z kamery wyświetlane są dodatkowe informacje systemowe (data, godzina, menu systemowe, funkcje interkomu).

Elementem łączącym monitory z kamerami jest centrala systemowa CDS-4CM umożliwiająca podłączenie maksymalnie 4 kamer DRC-4C** (obsługa 4 wejść) i 20 monitorów CAV-71B. Centrala CDS-4CM dodatkowo wyposażona jest w moduł pamięci 128 obrazów umożliwiający zapis zdjęć osób odwiedzających np. podczas nieobecności domowników. Zapisane obrazy można przeglądać z dowolnego monitora podłączonego do systemu (1 lub 6 zdjęć jednorazowo wyświetlanych na ekranie).

Ciekawą funkcją monitorów CAV-71B jest interkom pomiędzy użytkownikami systemu. Przy instalacji kilku odbiorników (max. 20) możliwe jest wywołanie z dowolnego monitora CAV-71B każdej innej stacji końcowej (monitora) i rozmowa tylko pomiędzy dwoma użytkownikami końcowymi (selektywne wywołanie interkomowe).

Monitor CAV-71B wyposażony został również w funkcję alarmu. Po uzbrojeniu wejścia kontaktronem (podłączonym do centrali CDS-4CM) i uaktywnieniu funkcji alarmu, w momencie przerwania obwodu zabezpieczeń zostaniemy o tym powiadomieni poprzez generator dźwięku zainstalowany w monitorach.

Charakterystyka monitora:

- kolorowy wyświetlacz panoramiczny 7" TFT-LCD
- obsługa czterech wejść (poprzez centralę CDS-4CM)
- możliwość podłączenia dodatkowych monitorów (maks. 20 w systemie)
- interkom z selektywnym wyborem innej stacji końcowej (monitora)
- obsługa modułu pamięci 128 obrazów (moduł wbudowany w centralę CDS-4CM)
- współpraca z kamerami analogowymi czteroprzewodowymi (poprzez CDS-4CM)
- zasilanie 230 V

Okablowanie	Monitor – centrala systemowa: 6 przewodów Centrala systemowa – kamera: 4 przewody
Zasilanie	100-240 V AC; 50-60 Hz
Pobór mocy	Czuwanie: 6 W Praca: 19 W
Temperatura pracy	od 0°C do 40°C
Wymiary (szer. x wys. x gł.)	315 mm x 175 mm x 53 mm
Masa	1,7 kg

GDE POLSKA
GLOBAL DISTRIBUTOR OF ELECTRONICS

GDE Polska
ul. Koniecznego 46
32-040 Świątniki Górne

tel./fax: 012 256 50 35, 256 50 25
fax: 012 270 56 96
e-mail: biuro@gde.pl

Zewnętrzna czujka PIR MS-12FE

(dwie czujki w jednej obudowie)

TAKEX

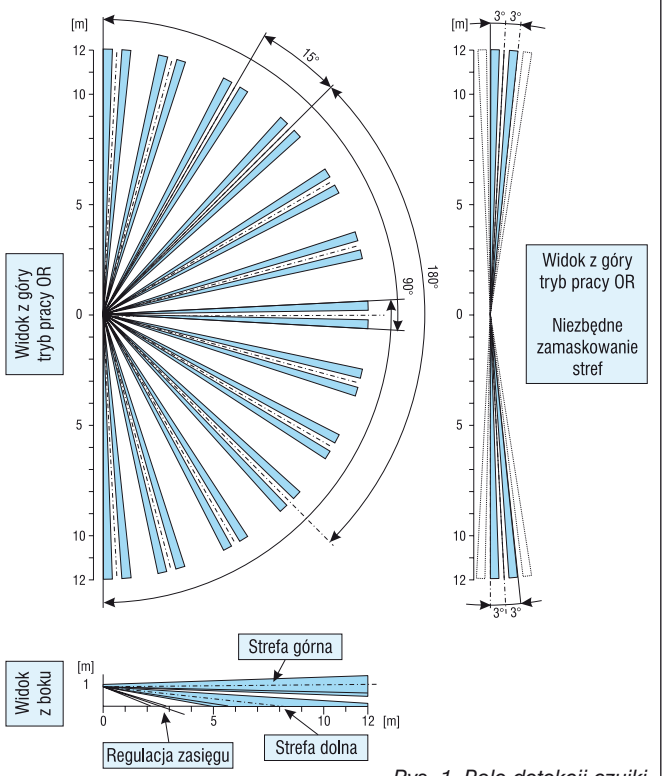
MS-12FE to zewnętrzna czujka ruchu o jak dotąd niepowtarzalnych parametrach technicznych i użytkowych. Dwa niezależnie regulowane układy optyczne pozwalają na zabezpieczenie powierzchni o długości 24 m (2 x 12 m) i kącie detekcji 180° (2 x 90°). Jest to obszar o powierzchni 226m^2. To dwa razy więcej niż możliwości popularnych czujek oferowanych na naszym rynku. MS-12FE to czujka wyposażona w 4 elementy PIR (dwa na każdy układ) oraz System Podwójnej Strefy (ang. *Dual Zone System*). Pole widzenia czujki zostało podzielone na obszar górny i dolny. Dopiero w przypadku wykrycia intruza w obu obszarach czujka wygeneruje alarm. Taki system zapewnia skuteczną eliminację fałszywych alarmów wywołanych przez ptaki lub małe zwierzęta.

Dowolna regulacja pola detekcji w zakresie długości oraz kąta detekcji pozwala na montaż czujki w każdym miejscu oraz konfiguracji. Możliwość zamaskowania wybranych wiązek pozwala na tworzenie charakterystyki kurtynowej, niezbędnej na niektórych obiektach (rys. 2.).

Czujka MS-12FE posiada świadectwo kwalifikacyjne klasy C.

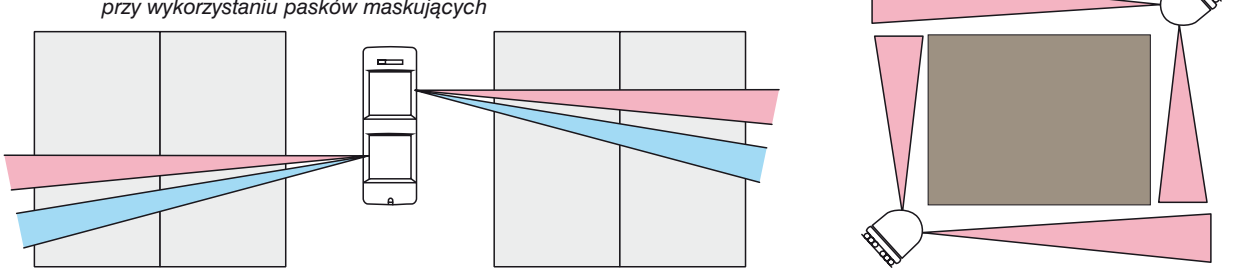
Podstawowe parametry czujki:

- Dwie tradycyjne czujki w jednej obudowie
- Japońska precyzja wykonania
- Brak reakcji na zwierzęta
- Pole detekcji: 2 x 12 m, 2 x 90°
- Cztery elementy PIR
- 2 układy optyczne, regulowane osobno: regulacja pola detekcji: od 3 do 12 m, od 15° do 180°
- System Podwójnej Strefy
- Tryb pracy AND/OR
- Tryb pracy dzień/noc
- Licznik impulsów: 1 lub 3
- Regulacja czasu aktywacji wyjścia alarmowego: od 2 s do 5 min.
- Wodoszczelna obudowa
- Płynna regulacja czułości od 30% do 170%
- Wysokość montażu: od 0,8 m do 1,2 m
- Montaż ścienny lub na słupku (opcjonalnie)
- Paski maskujące w komplecie
- Napięcie zasilania: 12 V_{DC} – 30 V_{DC}
- Maksymalny pobór prądu: 40mA
- Temperatura pracy: od -20°C do +50°C



Rys. 1. Pole detekcji czujki

Rys. 2. Przykład stworzenia charakterystyki kurtynowej przy wykorzystaniu pasków maskujących



ICS POLSKA

ICS Polska
ul. Żuławskiego 4/6, 02-641 Warszawa
tel. 022 646 11 38, faks 022 849 94 83
http://www.ics.pl

Kamera serii ICE firmy BAXALL
ICE-CM3M/LV i ICE-CM3M/M

- Kamera kolorowa DSP
- Przetwornik 1/3" CCD
- Rozdzielczość – 330 TVL

DANE TECHNICZNE	
Przetwornik	1/3" Sony Super HAD CCD
Obróbka obrazu	cyfrowa DSP
Efektywna liczba pikseli	500 (H) x 582 (V)
Czułość	0,6 lx dla obrazu użytecznego z włączoną automatyczną regulacją wzmocnienia (AGC), przysłona obiektywu F1.2
Rozdzielczość	330 TVL
Wyjście wizyjne	1 Vp-p composite video, 75Ω, BNC
Stosunek sygnał/szum	> 50 dB
Balans bieli	2500 K ~ 9500 K
Automatyczna regulacja wzmocnienia (AGC)	28 dB, z możliwością włączenia/wyłączenia
Migawka elektroniczna	1/50 s ~ 1/100 000 s, z możliwością włączenia/wyłączenia
Kompensacja tylnego oświetlenia (BLC)	1 okno konfiguracji (środkowa część obrazu); z możliwością włączenia/wyłączenia
Korekcja gamma	0,45
Synchronizacja	line-lock lub wewnętrzna

OBIEKTYW	
Mocowanie obiektywu	C lub CS 1/3", 1/2", 2/3", 1"
Automatyczna przesłona sterowana sygnałem wideo (video drive)	podłączenie przez 4-wejściowy zacisk z tyłu kamery
Automatyczna przesłona sterowana napięciem DC (DC drive)	4-pinowe, kwadratowe gniazdo z boku kamery; poziom DC jest ustawiany za pomocą potencjometru umieszczonego z tyłu kamery

ZASILANIE	
Wersja niskonapięciowa	24 V AC +/-15%/50 Hz; 12 V DC -10% +15%
Wersja sieciowa	od 98 V do 260 V AC/50 Hz
Złącze zasilania	/LV: dwutorowe złącze z tyłu kamery; /M: przewód sieciowy 2 m
Pobór mocy	< 4,2 W
Wskaźnik zasilania	niebieska dioda LED z tyłu kamery

PARAMETRY MECHANICZNE	
Wymiary (dł. x wys. x szer.)	123 x 60 x 52 mm
Masa	/LV: 0,35 kg; /M: 0,5 kg
Obudowa	uchwyt obiektywu odlany z cynku

ŚRODOWISKO PRACY	
Temperatura pracy	-10÷+50°C
Wilgotność względna pracy	20÷80 % (bez kondensacji)
Temperatura przechowywania	-10÷+70°C
Wilgotność względna przechowywania	20÷90% (bez kondensacji)

ID ELECTRONICS Sp. z o.o.
02-793 Warszawa, ul. Przy Bażantarni 11
tel. 022 649 60 95, faks 022 649 61 00
e-mail: sales@ide.com.pl
www.ide.com.pl

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

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

---

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

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

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

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

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

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

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

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

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

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

ACIE Polska Sp. z o.o.
ul. Poleczki 21
02-822 Warszawa
tel./faks (22) 894 61 63
e-mail: info@acie.pl
www.acie.pl

ACSS Sp. z o.o.
ul. Rydygiera 12
01-793 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. Puławska 597
02-885 Warszawa
tel. (22) 750 89 12
faks (22) 750 89 26
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. Rydygiera 12
01-793 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. Fabryczna 5a
31-553 Kraków
tel. (12) 411 88 88
faks (12) 294 18 88
e-mail: biuro@aldom.pl
www.aldom.pl

ALPOL Sp. z o.o.
ul. H. Krahelskiej 7
40-285 Katowice
tel. (32) 790 76 56
faks (32) 790 76 61
e-mail: alpol@e-alpol.com.pl
www.e-alpol.com.pl

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

ul. Portowa 14, 44-100 **Gliwice**
tel. (32) 790 76 23
faks (32) 790 76 65
e-mail: gliwice@e-alpol.com.pl

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

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

ul. Os. Na Murawie 10/2, 61-655 **Poznań**
tel. (32) 790 76 37
faks (32) 790 76 70
e-mail: poznan@e-alpol.com.pl

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

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

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

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

ul. Stargardzka 7, 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

ASSA ABLOY Poland Sp. z o.o.
ul. Warszawska 76
05-092 Łomianki
tel. (22) 751 53 54
faks (22) 751 53 56
biuro@assaabloy.com.pl
www.assaabloy.pl

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. Dworcowa 7
64-200 Wolsztyn
tel. (68) 347 09 25
faks (68) 347 09 26
e-mail: office@merlaud.com.pl
www.merlaud.com.pl

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

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

P.W.H. BRABORK Laboratorium Sp. z o.o.
ul. Postępu 2
02-676 Warszawa
tel. (22) 457 68 12, 457 68 32
faks (22) 457 68 95
e-mail: brabork@braborklab.pl
www.braborklab.pl

---

bt electronics
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

C&C PARTNERS TELECOM Sp. z o.o.
WYŁĄCZNY AUTORYZOWANY DYSTRYBUTOR SAMSUNG TECHWIN W POLSCE
ul. 17 Stycznia 119,121
64-100 Leszno
tel. (65) 525 55 55
faks (65) 525 56 66
e-mail: cctv@ccpartners.pl
www.samsungcctv.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

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. Olejniczaka 22, 41-902 **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
Arkadiusz Beck
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, 18
faks (22) 855 00 19
e-mail: cs@cs.pl
www.cs.pl, www.ckp.com.pl

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

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

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

ul. Płochocińska 19 lok. 43, 03-191 **Warszawa**
tel. (22) 614 39 52
faks (22) 614 39 64

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

DANTOM s.c.
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. Polnej Róży 2/4
02-798 Warszawa
tel. (22) 498 60 62,
tel./faks (22) 649 27 97
e-mail: handlowy@darsystem.pl
www.darsystem.pl
www.tvtech.com.pl

PW DELTA 2 s.c.
A. Piotrowski, J. Piotrowska
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
www.el-mont.com

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, (12) 278 48 91
faks (12) 288 14 26
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
www.ebs.pl

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

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

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

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

Elza Elektrosystemy
ul. Ogrodowa 13
34-400 Nowy Targ
tel. (18) 266 46 10
faks (18) 264 92 71
e-mail: elza@ceti.pl
www.elza.com.pl

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

Oddział:
ul. Jana Kazimierza 61, 01-267 **Warszawa**
tel./faks (22) 836 54 05, 837 75 93
tel. 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

EUROSAP – LTD Eugeniusz Klowan
ul. Tarniny 28
70-763 Szczecin
tel. (91) 466 60 45, 461 21 50
faks (91) 466 60 46
e-mail: eurosap@go2.pl, eurosap@eurosap.pl
www.eurosap.pl

FALARM Systemy Wykrywania Pożaru i Włamań
ul. Powązkowska 13b
01-797 Warszawa
tel. (22) 633 08 30
faks (22) 669 07 53
e-mail: biuro@falarm.pl
www.falarm.pl

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

GERARD – Systemy Alarmowe
ul. Suwalska 36d/8
03-252 Warszawa
tel. (22) 675 66 20
faks (22) 674 11 44
e-mail: biuro@alarmy-gerard.pl
www.alarmy-gerard.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.
Al. Jana Pawła II 61/233
01-031 **Warszawa**
tel. (22) 831 56 81, 831 28 52
faks (22) 636 13 73
tel. kom. 693 029 278
e-mail: warszawa@gvpolska.com.pl

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

ul. Hallera 40a/4b
53-324 **Wrocław**
tel. (71) 361 66 02
faks (71) 361 66 23
tel. kom. 695 583 292
e-mail: wroclaw@gvpolska.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

Inter-Sicherheits-Service Sp. z o.o.
ul. Kobylogórska 2
66-400 Gorzów Wielkopolski
tel. (95) 723 97 77
faks (95) 723 97 82
e-mail: sprzedaz@iss.net.pl
www.iss.net.pl

P.W. IRED
Kazimierzówka 9
21-040 Świdnik
tel. (81) 751 70 80
tel. kom. 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

KABA SECURITY Sp. z o.o.
ul. Połczyńska 51
01-336 Warszawa
tel. (22) 665 88 27
faks (22) 665 88 62
e-mail: kaba@kpw.kaba.com
www.kaba.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

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

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

KONSALNET SYSTEM Sp. z o.o.
ul. Przasnyska 6 A
01-756 Warszawa
tel. (22) 560 50 60
faks (22) 560 50 56
e-mail: system@konsalnet.com.pl
www.konsalnet.com.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

autoryzowany dystrybutor ABLOY®

KSC Sp. z o.o.
ul. Ks. Bpa Bernarda Bogedaina 2
40-749 Katowice
tel. (32) 604 50 70
faks (32) 604 50 79
e-mail: biuro@ksc.com.pl
www.ksc.com.pl

PPUH LASKOMEX
ul. Dąbrowskiego 249
93-231 Łódź
tel. (42) 671 88 00
faks (42) 671 88 88
e-mail: handel@laskomex.com.pl
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 25
faks (75) 642 45 35
e-mail: info@micronix.com.pl
www.micronix.com.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

NOKTON – DOCZKAL, NIZIO – Sp. J.
ul. Zamorska 41
93-478 Łódź
tel. (42) 250 62 51, 680 08 52
faks (42) 680 08 84
e-mail: info@nokton.com.pl
www.nokton.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.noma2.com.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. Serocka 10, 04-333 **Warszawa**
tel. (22) 610 40 13
faks (22) 610 37 28

infolinia: 0 801 055 075

OBIS CICHOCKI SLĄZAK Sp. J.
ul. Rybnicka 64
52-016 Wrocław
tel./faks (71) 343 16 76, 341 78 52, 341 98 54
e-mail: 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

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 Sp. z o.o.
Zakład Urządzeń Dozymetrycznych
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

PROXIMA Spółka Jawna
W. M. Fredrych, A. Kwiatkowski
ul. Filtrowa 23
87-100 Toruń
tel./faks (56) 660 20 00

PROXIMA Spółka Jawna
W. M. Fredrych, A. Kwiatkowski
Hurtownia Systemów Sygnalizacji
Włamania i Napadu

ul. Grudziądzka 11, 87-100 **Toruń**
tel. (56) 661 18 96
tel./faks (56) 661 18 97
e-mail: alarmy@proxima.pl
www.proxima.pl

Oddziały:
Białystok tel. (85) 740 35 35
Częstochowa tel. (34) 361 62 91
Gdańsk tel. (58) 554 83 04
Gdynia tel. (58) 620 69 77
Gliwice tel. (32) 230 47 27
Konin tel. (63) 245 61 61
Kraków tel. (12) 266 62 22
Bydgoszcz tel. (52) 375 41 41
Legnica tel. (76) 854 05 55
Leszno tel. (65) 520 44 67
Łódź tel. (42) 676 72 81
Lublin tel. (81) 745 30 35
Olsztyn tel. (89) 533 86 52
Poznań tel. 0 602 232 159
Rzeszów tel. (17) 857 49 49
Szczecin tel. (91) 482 40 99
Warszawa tel. (22) 838 45 46
Wrocław tel. (71) 333 49 43

PULSAR K. Bogusz Sp. J.
Siedlec 150
32-744 Łapczyca
tel. (14) 610 19 40
faks (14) 610 19 50
biuro@pulsarspj.com.pl
www.pulsarspj.com.pl, www.zasilacze.pl

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

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

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

ROPAM Elektronik s.c.
os. 1000-lecia 6A/1
32-400 Myślenice
tel./faks (12) 272 39 71
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. (22) 813 44 25
faks (22) 813 34 70
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

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

SECURITY SYSTEM
INTEGRATION Sp. z o.o.
ul. Irysowa 4
55-040 Bielany Wrocławskie
tel. (71) 311 04 30
faks (71) 311 28 63
e-mail: ssi@ssi-tv.pl
www.ssi-tv.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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Biura Handlowe:
ul. Winogrady 10
61-663 **Poznań**
tel. (61) 852 19 02,
faks (61) 825 09 03
e-mail: poznan@spstrading.com.pl

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

ul. Inflancka 6
91-857 **Łódź**
tel. (42) 617 00 32
faks (42) 659 85 23
e-mail: lodz@spstrading.com.pl

www.aper.com.pl
www.spstrading.com.pl

STRATUS
CENTRUM SYSTEMÓW ZABEZPIECZEŃ
ul. Nowy Świat 38
20-419 Lublin
tel./faks (81) 743 87 72
e-mail: info@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

TAP Systemy Alarmowe Sp. z o.o.
Os. Armii Krajowej 125
61-381 Poznań
tel. (61) 876 70 88
faks (61) 875 03 03
e-mail: tap@tap.com.pl
www.tap.com.pl

Biuro Handlowe:
ul. Rzymowskiego 30, 02-697 **Warszawa**
tel. (22) 843 83 95
faks (22) 843 79 12
e-mail: tap5@tap.com.pl

TAC Sp. z o.o.

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

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

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

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

TALCOMP SYSTEMY BEZPIECZEŃSTWA
ul. A. Dauna 70
30-629 Kraków
tel. (12) 655 85 85
faks (12) 425 63 68
e-mail: talcomp@talcomp.pl
www.talcomp.pl

TAYAMA POLSKA Sp. J.
ul. Słoneczna 4
40-135 Katowice
tel. (32) 258 22 89, 357 19 10, 357 19 20
faks (32) 357 19 11, (32) 357 19 21
e-mail: biuro@tayama.com.pl
www.tayama.com.pl

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

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

– Laboratorium Badawcze Elektronicznych Urządzeń Alarmowych

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

TECHNOKABEL S.A.
ul. Nasielska 55
04-343 Warszawa
tel. (22) 516 97 97
faks (22) 516 97 87
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl

TP TELTECH

TP TELTECH Sp. z o.o.
ul. Tuwima 36
90-941 Łódź
tel. (42) 639 83 60, 639 88 72
faks (42) 639 89 85
e-mail: teltechinfo@tpteltech.pl
www.tpteltech.pl

Oddziały:
ul. Długa 22/27
80-801 **Gdańsk**
tel. (58) 302 52 12
faks (58) 346 25 09
e-mail: michal.mikolajski@telekomunikacja.pl

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

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

ul. Rzeczypospolitej 5
59-220 **Legnica**
tel./faks (76) 856 60 71
e-mail: marian.sitko@telekomunikacja.pl
ul. Kosmonautów 82
20-358 **Lublin**
tel. (81) 745 39 83
faks (81) 745 39 78
e-mail: zbigniew.chodkiewicz@telekomunikacja.pl

TRIKON
32-447 Siepraw 556
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. Żupnicza 17
03-821 Warszawa
tel. (22) 518 21 00
faks (22) 518 21 01
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 do 10
faks (61) 872 96 30

W2 Włodzimierz Wyrzykowski
86-005 Białe Błota
ul. Czajcza 6
tel. (52) 345 45 00, 584 01 92
faks (52) 584 01 92
e-mail: biuro@w2.com.pl
www.w2.com.pl

WIZJA Sp. z o.o.
ul. Zakładowa 6
62-052 Komorniki k. Poznania
tel. (61) 810 08 00
faks (61) 810 08 10
www.wizja.com.pl

VISION POLSKA Sp. z o.o.
ul. Unii Lubelskiej 1
61-249 Poznań
tel. (61) 878 13 00
faks (61) 878 13 82
e-mail: biuro@visionpolska.pl
www.visionpolska.pl

DZIAŁALNOŚĆ

firma	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
2M Elektronik	-	TAK	-	TAK	-
3D	TAK	TAK	-	-	TAK
4 COM	-	TAK	TAK	TAK	TAK
AAT Trading Company	-	TAK	TAK	-	TAK
ACIE	TAK	-	TAK	TAK	TAK
ACSS	-	-	TAK	-	TAK
ADT Poland	-	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
ASSA ABLOY Poland	-	-	TAK	-	-
Atline Sp. J.	-	TAK	TAK	-	TAK
AVISmedia	-	TAK	TAK	-	TAK
Bitner Zakłady Kablowe	TAK	-	-	-	-
BOSCH	-	-	TAK	-	TAK
P.W.H. Brabork - Laboratorium	-	TAK	TAK	TAK	-
bt electronics	TAK	-	TAK	TAK	-
C&C Partners	-	TAK	TAK	-	TAK
CAMSAT	TAK	TAK	TAK	-	-
CBC Poland	TAK	-	TAK	-	TAK
Cezim	TAK	TAK	TAK	-	TAK
CMA Sp. z o.o.	TAK	-	-	TAK	-
COM-LM	-	TAK	TAK	TAK	TAK
CONTROL SYSTEM FMN	-	TAK	TAK	TAK	TAK
D+H Polska	TAK	TAK	TAK	TAK	-
DANTOM	TAK	-	TAK	-	-
DAR-ALARM	-	TAK	TAK	TAK	TAK
P.W. Delta 2 s.c.	TAK	-	TAK	TAK	-
DG Elpro	-	TAK	TAK	TAK	TAK
DOM Polska	TAK	TAK	TAK	-	-
DPK System	-	-	TAK	TAK	TAK
Dravis	-	TAK	-	TAK	-
Dyskret	-	TAK	TAK	TAK	-
EBS	TAK	TAK	TAK	-	TAK
EDP Support Polska	TAK	TAK	TAK	TAK	TAK
ela-compil	TAK	TAK	TAK	-	TAK
Elproma	-	TAK	-	TAK	-
Eltcrac	TAK	TAK	TAK	TAK	TAK
Elza Elektrosystemy-Instalacje	-	TAK	-	TAK	TAK
Emu	-	-	TAK	-	-
Eureka	-	TAK	-	TAK	-
Eurosap – LTD	-	TAK	TAK	TAK	-
Falarm	-	TAK	TAK	TAK	-
FES	TAK	TAK	TAK	TAK	-
Gerard Systemy Alarmowe	TAK	TAK	TAK	-	-
GE Security Polska	-	-	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	-

DZIAŁALNOŚĆ

firma	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Intel	-	TAK	TAK	TAK	TAK
Ired	TAK	TAK	TAK	TAK	-
ISS	TAK	-	-	-	-
Janex International	-	-	TAK	-	TAK
Kaba Security Sp. z o.o.	TAK	TAK	TAK	TAK	-
KABE	TAK	TAK	TAK	TAK	TAK
Kolektor	-	TAK	-	TAK	-
Kolektor MR	-	TAK	TAK	TAK	-
Konsalnet System	-	TAK	-	TAK	-
Krak-Poż	-	TAK	-	TAK	-
KSC Sp. z o.o.	TAK	TAK	TAK	TAK	TAK
Laskomex	TAK	TAK	TAK	-	TAK
MAXBAT	TAK	TAK	TAK	TAK	TAK
MicroMade	TAK	-	-	-	-
Micronix	-	TAK	TAK	-	-
Miwi-Urmet	TAK	-	TAK	-	-
Nokton Sp. J.	TAK	-	-	-	-
Noma 2	-	TAK	-	TAK	-
NORBAIN Polska	-	-	TAK	-	-
OBIS Sp. J.	-	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	-	-	-	-
PROXIMA Sp. J.	TAK	-	TAK	-	TAK
Pulsar	TAK	-	TAK	-	-
PPH Pulson	TAK	TAK	TAK	-	-
Radioton	-	-	TAK	-	-
Ramar	TAK	-	TAK	TAK	TAK
ROPAM Elektronik	TAK	-	-	-	-
Sagitta Sp. z o.o.	TAK	-	TAK	-	-
Samax	-	TAK	-	TAK	-
Satel	TAK	TAK	-	-	TAK
Sawel	-	TAK	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
SSI	TAK	TAK	-	TAK	-
STRATUS	-	TAK	TAK	-	TAK
SYSTEM 7 SECURITY	TAK	-	TAK	-	TAK
TAC	-	TAK	TAK	TAK	-
Talcomp	-	TAK	TAK	TAK	-
Tap – Systemy Alarmowe	-	TAK	TAK	-	TAK
Tayama	TAK	TAK	TAK	TAK	TAK
Techom	-	-	-	-	TAK
Technokabel	TAK	-	-	-	-
TP TELTECH	-	TAK	TAK	TAK	-
Trikon	TAK	TAK	-	TAK	-
TYCO	TAK	TAK	TAK	TAK	TAK
UNICARD S.A.	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	-	-
Wizja	-	-	TAK	TAK	-
Vision Polska Sp. z o.o.	-	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
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	-	TAK	-	-	-	-	-	-
ACSS	systemy identyfikacji								
ADT Poland	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
Alarm System	TAK	TAK	TAK	-	-	-	-	-	-
Alarmnet Sp. J.	-	TAK	TAK	-	-	TAK	-	-	-
Alarmtech Polska	TAK	-	-	-	-	-	-	-	-
Aldom	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Alkam System	TAK	TAK	TAK	TAK	-	-	TAK	-	TAK
Alpol Sp. z o.o.	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Ambient System	TAK	TAK	TAK	TAK	-	-	-	-	TAK
ANB	TAK	TAK	-	TAK	-	TAK	TAK	-	TAK
ANMA	TAK	TAK	TAK	TAK	-	TAK	-	-	-
ASSA ABLOY Poland	-	-	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
bt electronics	-	-	TAK	-	-	TAK	-	TAK	-
C&C Partners	-	TAK	-	-	-	-	TAK	-	-
CAMSAT	-	TAK	-	-	-	-	TAK	-	-
CBC Poland	-	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
CONTROL SYSTEM FMN	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	-
D+H	-	-	-	TAK	-	TAK	-	-	TAK
DANTOM	TAK	TAK	TAK	TAK	-	-	-	TAK	-
DAR-ALARM	TAK	TAK	TAK	TAK	-	-	TAK	-	-
P.W. Delta 2 s.c.	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
EBS	TAK	-	TAK	-	TAK	TAK	TAK	-	-
EDP Support Polska	TAK	TAK	TAK	-	-	TAK	-	TAK	TAK
ela-compil	-	-	-	-	-	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	-	-	-
Eurosap LTD	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Falarm	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
FES	TAK	TAK	TAK	TAK	-	-	-	-	TAK
Gerard Systemy Alarmowe	TAK	TAK	TAK	-	-	-	-	TAK	-
GE Security Polska	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	-
Gunnebo	-	-	TAK	-	-	-	-	TAK	-
GV Polska	-	TAK	-	-	-	-	TAK	-	-
HSA	TAK	TAK	TAK	TAK	TAK	-	-	-	-
ICS Polska	TAK	TAK	TAK	-	-	-	-	-	-
ID Electronics	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	-
Info-Cam	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	-	-
ISS	-	-	-	-	-	-	-	TAK	-
Janex International	TAK	TAK	TAK	TAK	-	-	TAK	-	TAK
Kaba Security Sp. z o.o.	TAK	TAK	TAK	TAK	-	TAK	TAK	TAK	-
KABE	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Konsalnet System	TAK	TAK	TAK	TAK	-	-	TAK	-	-
Krak-Poż	-	-	-	TAK	-	-	TAK	-	TAK
KSC Sp. z o.o.	TAK	TAK	TAK	-	-	-	-	TAK	-
Laskomex	TAK	TAK	TAK	-	-	TAK	TAK	TAK	TAK
MAXBAT	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	-
MicroMade	-	-	TAK	-	Rejestracja czasu pracy			-	-
Micronix	TAK	TAK	TAK	TAK	-	-	-	TAK	-
Miwi-Urmet	TAK	TAK	TAK	-	-	-	Domofony	-	-
Nokton Sp. J.	TAK	-	-	-	-	-	TAK	-	-
Noma 2	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
NORBAIN Polska	TAK	TAK	-	-	TAK	-	-	-	-
OBIS Sp. J.	TAK	TAK	TAK	TAK	-	-	-	-	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	-	-	-	-	TAK	-
PAG	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
Panasonic	-	TAK	TAK	-	-	-	-	-	-
Petrosin	TAK	TAK	TAK	-	-	-	-	-	-
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
POL-ITAL	-	-	TAK	-	-	-	-	TAK	-
Polon-Alfa	-	-	-	TAK	-	-	-	-	-
PROXIMA Sp. J.	TAK	TAK	TAK	TAK	-	-	-	TAK	-
Pulsar	TAK	TAK	TAK	-	-	-	TAK	TAK	-
PPH Pulson	-	-	-	-	-	TAK	TAK	-	-
Radioton	-	TAK	-	-	-	-	-	-	-
Ramar	TAK	TAK	TAK	-	TAK	-	TAK	-	-
ROPAM Elektronik	TAK	-	-	TAK	-	-	TAK	-	-
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	-	-
Secural	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.M.A.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFTEX Data	-	TAK	-	-	-	TAK	TAK	-	-
Solar	TAK	TAK	TAK	TAK	-	-	-	-	TAK
Sprint Sp. z o.o.	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
S.P.S. Trading	-	TAK	-	-	-	-	-	-	-
SSI	TAK	TAK	TAK	TAK	-	TAK	-	-	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	-	-	-	TAK
SYSTEM 7 SECURITY	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	TAK	-	-	-
Tayama	TAK	TAK	TAK	-	-	TAK	-	-	TAK
Techom	TAK	-	-	-	-	-	-	-	-
Technokabel	wszystkie rodzaje kabli								
TP TELTECH	TAK	TAK	TAK	TAK	-	-	TAK	-	-
Trikon	-	-	TAK	-	-	-	-	TAK	-
TYCO	TAK	TAK	TAK	TAK	-	TAK	-	-	TAK
UNICARD S.A.	-	-	TAK	-	-	TAK	-	TAK	-
W2	TAK	-	-	TAK	-	-	-	-	-
Wizja	-	-	-	-	-	-	-	-	TAK
Vision Polska Sp. z o.o.	-	-	-	TAK	-	-	-	-	-

ZABEZPIECZENIA
dwumiesięcznik
Redaktor naczelny
Teresa Karczmarzyk
teresa@zabezpieczenia.com.pl
Redaktor merytoryczny
Adam Bułaciński
adam@zabezpieczenia.com.pl
Dział 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
rafał@zabezpieczenia.com.pl
Andrzej Sosiński
andrzej@zabezpieczenia.com.pl
Współpraca
Jarosław Barszcz
Daniel Kamiński
Sławomir Wagner
Marcin Pyclik
Dział DTP
Jarosław Witkowski
jarek@zabezpieczenia.com.pl
Korekta
Izabela Jesiołowska
Adres redakcji
ul. Puławska 431, 02-801 Warszawa
tel. (22) 546 07 81, 83
faks (22) 546 07 89
www.zabezpieczenia.com.pl
Wydawca
AAT Trading Company Sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. (22) 546 05 46
faks (22) 546 05 01
Druk
Poligrafus
ul. Oszmiańska 9
03-503 Warszawa
tel. (22) 679 28 18

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

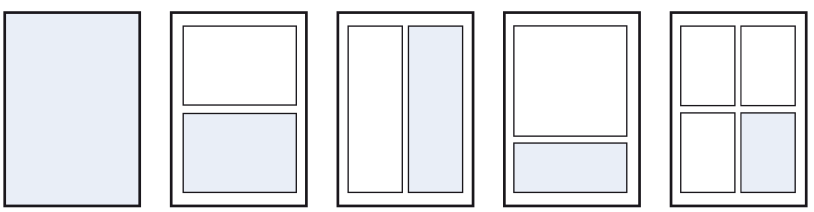
jednorazowy wpis	– 60 zł

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

PROFESJONALNY MONITORING WIZYJNY IP

Megapikselowa dualna kamera IP
WV-NP1000 Series

Wandaloodporna dualna kamera kopułowa IP
WV-NW470S

Kamera kolorowa IP
WV-NP240

Szybkoobrotowa kolorowa kamera IP
WV-NS202

Dualna kamera IP
WV-NP472

Oprogramowanie zarządzające
WV-AS65

Cyfrowy rejestrator IP
WJ-ND300

i-pro – profesjonalne, kompleksowe rozwiązania monitoringu wizyjnego IP

Rozwiązania IP wkraczają bardzo intensywnie w każdą dziedzinę naszego życia. Dotyczy to również systemów zabezpieczeń, a w szczególności systemów telewizji dozorowej.
Technologia IP w systemach CCTV, w porównaniu z konwencjonalnymi systemami analogowymi, oferuje olbrzymie możliwości oraz korzyści. Dlatego też firma Panasonic, bazując na długoletnim doświadczeniu oraz najnowocześniejszej technologii, stworzyła profesjonalną linię produktów IP ***i-pro***. Kompletna gama produktów ***i-pro*** umożliwia tworzenie bardzo efektywnych i najwyższej jakości cyfrowych systemów monitoringu wizyjnego. W jej skład wchodzą kamery IP, których jakość oraz funkcjonalność pozwala spełnić oczekiwania najbardziej wymagających klientów, cyfrowe rejestratory IP gwarantujące ciągłą stabilną pracę systemu oraz oprogramowanie zarządzające WV-AS65 umożliwiające użytkownikowi łatwe zarządzanie rozległymi systemami IP oraz integrowanie ich z systemami analogowymi Panasonic.
Nadszedł czas abyś stosując profesjonalne rozwiązania ***i-pro*** Panasonic zaczął korzystać ze wszystkich dobrodziejstw systemów wizyjnych opartych na technologii IP.

więcej informacji na:
http://panasonic.co.jp/pss/products/en/i-pro/

i-pro to połączenie: technologii IP, inteligencji i profesjonalizmu, to doskonała nazwa dla systemu dozoru wizyjnego IP Panasonic

Panasonic
ideas for life

Nowe czytniki iCLASS:

Cena ▶ taka sama jak Prox

Montaż ▶ taki sam jak Prox

Pobór mocy ▶ taki sam jak Prox

Bezpieczeństwo ▶ takie jak w Alcatraz

hidcorp.com

Czytniki iCLASS oferują zwiększony poziom bezpieczeństwa z zachowaniem wszystkich funkcji technologii zbliżeniowej. Nowe czytniki iCLASS posiadają identyczne parametry czytników Prox, dotyczące poboru mocy, łatwości instalacji i użytkowania oraz ceny. Jedyną znaczącą różnicą jest zwiększone bezpieczeństwo uzyskane dzięki kodowaniu i wspólnej identyfikacji kart. Możliwość odczytu/zapisu umożliwia wykorzystanie dodatkowych funkcji takich jak biometria, rejestracja czasu pracy, bezpieczne logowanie do komputerów i wiele innych. Ponadto, technologia iCLASS jest dostarczana przez HID. Dlatego też, możecie się czuć bezpiecznie.

HID

ACCESS security.

iCLASS