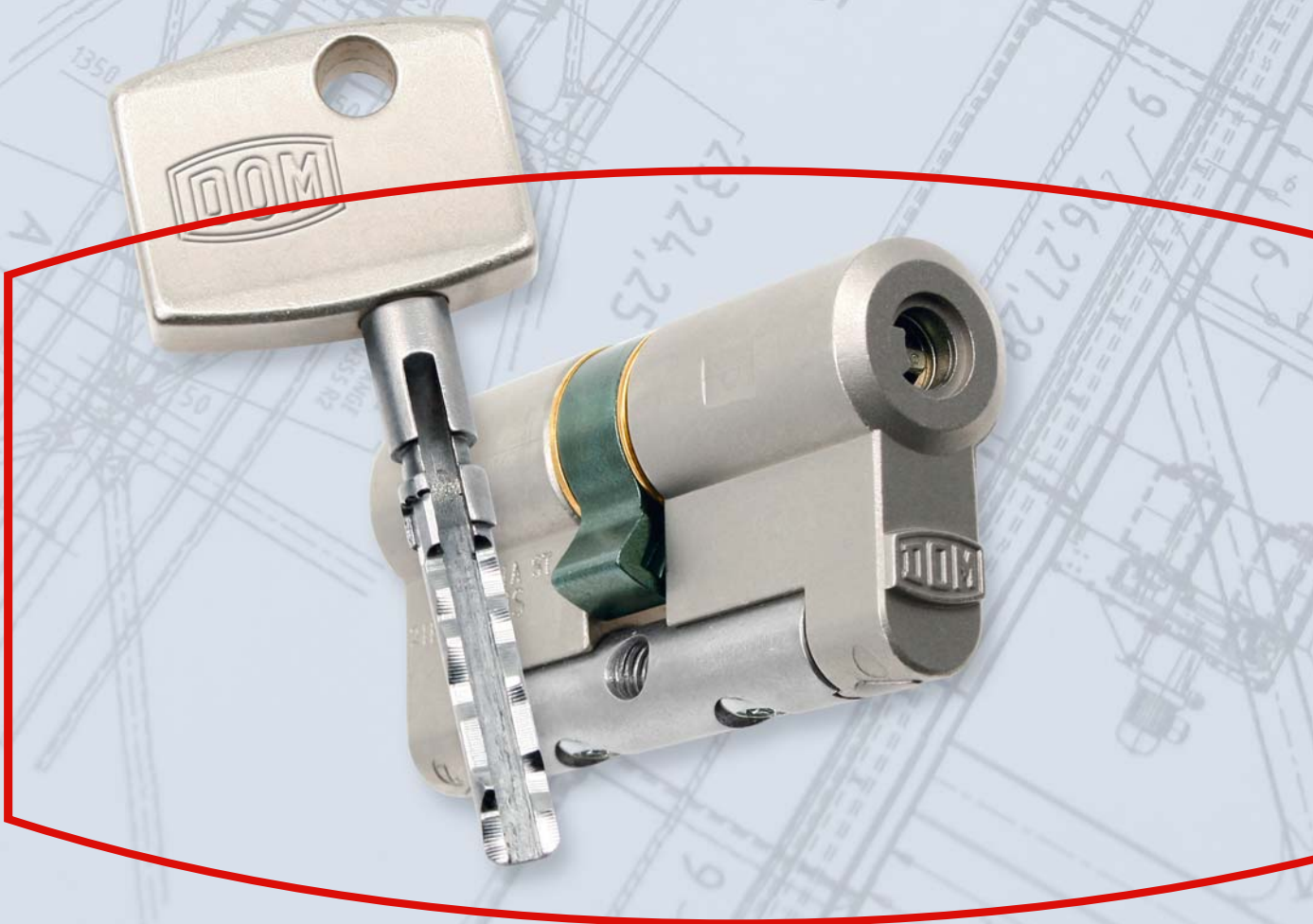
CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 2(54)/2007

ZABEZPIECZENIA

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



W NUMERZE:

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

CZASOPISMO ZABEZPIECZENIA

2/2007

w numerze

14
Z biometrią w podróży

34
Monitoring wizyjny stadionu Odry w Opolu

54
Jak uchronić dane znajdujące się na dysku twardym w trakcie jego przenoszenia?

63
Zabezpieczenie pieniędzy oraz informacji w firmie

TERMINARZ

Targi i wystawy branży security

MARZEC

14.03 – 17.03	**SEGUREX 2007** **International Exhibition for Security and Safety** Lizbona, Portugalia	www.segurex.fil.pt e-mail: segurex@aip.pt tel. +351 218 921 500
15.03 – 21.03	**CeBIT** Hannower, Niemcy	www.cebit.de www.hf-poland.com e-mail: info@hf-poland.com tel. 022 639 72 53
25.03 – 28.03	**ASIS** **International's 6th European Security Conference** Berlin, Niemcy	www.asisonline.eu e-mail: berlin@asisonline.org tel. +32 2 645 2674
27.03 – 29.03	**Global Security Asia 2007** Singapur	www.globalsecasia.com e-mail: andrewmarriott@globalsecasia.com tel. +44 195 956 92 97
28.03 – 30.03	**ISC WEST** Las Vegas, USA	www.iscwest.com e-mail: inquiry@isc.reedexpo.com tel. +1 800 840 56 02
28.03 – 30.03	**SECURA 2007** Bruksela, Belgia	www.secura-expo.be e-mail: mail@secura-expo.be tel. +32 3 350 19 50
30.03 – 01.04	**Prewencja 2007** **III Targi Zabezpieczeń i Ochrony Mienia** Szczecin	www.mts.pl e-mail: office@mts.pl tel. 091 464 44 01

KWIECIEŃ

11.04 – 13.04	**PRAGOALARM/PRAGOSEC 2007** Praga, Czechy	www.pragoalarm.cz e-mail: v.voriskova@incheba.cz tel. +420 220 103 307
16.04 – 18.04	**SECUTECH EXPO 2007** Tajpej, Tajwan	www.asmag.com www.secutech.com e-mail: int'l@asmag.com tel. +886 2 2659 9080
17.04 – 19.04	**INTERTELECOM** **Międzynarodowe Targi Komunikacji Elektronicznej** Łódź	www.mtl.lodz.pl e-mail: j.fratczak@mtl.lodz.pl tel. 042 637 29 34, 042 638 64 68
18.04 – 20.04	**EUROPOLTECH 2007 – III Międzynarodowa Konferencja Policyjna** **Międzynarodowe Targi Techniki i Wyposażenia Służb Policyjnych** **oraz Formacji Bezpieczeństwa Państwa** Warszawa	www.europoltech.pl e-mail: europoltech@mtgsa.com.pl tel. 058 554 92 13 tel. 058 554 93 28
24.04 – 26.04	**INFOSECURITY EUROPE 2007** Londyn, Wielka Brytania	www.infosec.co.uk e-mail: natalie.booth@reedexpo.co.uk tel. +44 208 910 7718
24.04 – 26.04	**MIPS 2007** **Protection, Security & Fire Safety** Moskwa, Rosja	www.mips.ru e-mail: mips@ite-expo.ru tel. +7 495 935 7350
25.04 – 26.04	**SECTECH** Oslo, Norwegia	www.sectech.nu e-mail: deniz@armedia.se tel. +46 8 556 306 80

MAJ

07.05 – 11.05	**ELFACK 2007** Gothenburg, Szwecja	www.elfack.com e-mail: elfack@swefair.se tel. +46 31 708 80 00
08.05 – 10.05	**SAFETY & SECURITY AMSTERDAM 2007** Amsterdam, Holandia	www.safetysecurityamsterdam.nl e-mail: ssa@rai.nl tel. +31 20 549 30 59

MAJ

09.05 – 13.05	**EXPO SECURITY – International Exhibition Of Security, Police, Alarm, Civil, Fire & Disasters Protection Systems** Bukareszt, Rumunia	www.exposecurity.ro e-mail: m.dicianu@romexpo.org tel. +40 21 207 70 00 wew. 1102 tel. +40 21 207 70 00 wew. 1005
15.05 – 17.05	**CARDTECH SECURTECH 2007** San Francisco, USA	www.ctst.com e-mail: abconferences@sourcemedia.com tel. +1 800 803 3424
16.05 – 18.05	**SECURITY & SAFETY** Budapeszt, Węgry	www.securityinfo.hu e-mail: eexpo@axelero.hu tel. +36 1 318 09 37
21.05 – 24.05	**IFSEC 2007** Birmingham, Wielka Brytania	www.ifsec.co.uk e-mail: ccracknell@cmpi.biz tel. +44 20 792 180 69
22.05 – 24.05	**E+R+P – ENTRY SK, RESCUE-SECUREX, PROTEC** Bratysława, Słowacja	www.incheba.sk e-mail: incheba@incheba.sk tel. +421 2 672 724 00
29.05 – 31.05	**EXPOSEC – X International Security Fair** Sao Paulo, Brazylia	www.cipanet.com.br e-mail: Lccipa@cipanet.com.br tel. +55 11 558 543 55
30.05 – 01.06	**LABORALIA 2007** **Integral Show for Prevention, Protection, Safety and Health at Work** Walencja, Hiszpania	http://laboralia.feriavalencia.com e-mail: feriavalencia@feriavalencia.com tel. +34 96 363 61 11

CZERWIEC

06.06 – 07.06	**GOVSEC EUROPE** Bruksela, Belgia	www.govseceurope.eu e-mail: info@govseceurope.eu tel. +32 2 474 85 35
11.06 – 13.06	**INFOSYSTEM – Informatyka Dla Przemysłu I Administracji** Poznań, Polska	www.infosystem.pl e-mail: infosystem@mtp.pl tel. 061 869 21 96
11.06 – 14.06	**CERTYFIKACJA – V Targi Usług Certyfikacyjnych, Badań Wyrobów i Wdrożenia Systemów Jakości** Poznań, Polska	www.sawo.pl e-mail: certyfikacja@sawo.pl tel. 052 581 11 72, 052 581 11 77
26.06 – 28.06	**SECURITY ISRAEL 2007** **The 21st International Homeland Security & Defense Exhibition** Tel Aviv, Izrael	www.securityisrael.com e-mail: sigmatim@netvision.net.il tel. +972 3 648 93 39
27.06 – 28.06	**TRANSEC WORLD EXPO** Amsterdam, Holandia	www.transec.com e-mail: pjones@simplygroupltd.com tel. +44 20 854 291 86
27.06 – 29.06	**SECURITYWORLD EXPO 2007** Seul, Korea Południowa	www.secuexpo.com e-mail: info@secuexpo.com tel. +82 2 719 69 31

WRZESIEŃ

03.09 – 06.09	**MSPO – XV Międzynarodowy Salon Przemysłu Obronnego** Kielce, Polska	www.targikielce.pl e-mail: biuro@targikielce.pl tel. 041 365 12 22
11.09 – 13.09	**SAFETY & SECURITY** Sofia, Bułgaria	www.bcci.bg e-mail: fairs@bcci.bg tel. +359 2 981 66 26
11.09 – 16.09	**INTERPROTEX** **International Fair for the Protection of People and Assets** Zagrzeb, Chorwacja	www.zv.hr e-mail: interprotex@zv.hr tel. +385 1 650 33 90
18.09 – 21.09	**A+A 2007** **SAFETY, SECURITY AND HEALTH AT WORK** Düsseldorf, Niemcy	www.aplusa-online.de e-mail: portalinfo@aplusa-online.de tel. +49 211 456 001
26.09 – 28.09	**ELEKTROTECHNIKA 2007** **V Międzynarodowe Targi Sprzętu Elektrycznego i Systemów Zabezpieczeń** Warszawa, Polska	www.elektroinstalacje.pl e-mail: soma@lightfair.pl tel. 022 649 76 69

PAŹDZIERNIK

03.10 – 04.10	**CŁO i GRANICA 2007 – XIII Międzynarodowa Wystawa Wyposażenia Dla Kontroli Celnej i Granicznej** Warszawa, Polska	www.cig.info.pl e-mail: elzbieta@brsa.com.pl tel. 022 849 60 06 wew. 104, 114
03.10 – 05.10	**FINNSEC** Helsinki, Finlandia	www.finnexpo.fi e-mail: peter.guthwert@finnexpo.fi tel. +358 503 504 645
09.10 – 12.10	**MILIPOL 2007** Paryż, Francja	www.milipol.com tel. +33 1 46 27 82 00
10.10 – 12.10	**LOGISPOL 2007 – VI Międzynarodowe Targi Zaopatrzenia Wojska, Straży Granicznej i Policji** Bydgoszcz, Polska	www.targi-pom.com.pl e-mail: targi-pom@bdg.pl tel. 052 323 07 13
16.10 – 19.10.	**BEZPEKA 2007** Kijów, Ukraina	www.bezpeka.ua tel. +38 044 461 92 01
23.10 – 24.10	**SECTECH** Sztokholm, Szwecja	www.sectech.nu e-mail: deniz@armedia.se tel. +46 8 556 306 80
23.10 – 25.10	**PREVENTIA 2007** Barcelona, Hiszpania	www.preventia.org e-mail: info@preventia.org tel. +34 93 237 09 01
23.10 – 25.10	**CHINA INTERNATIONAL HARDWARE SHOW POWERED BY PRACTICAL WORLD** Szanghaj, Chiny	www.koelnmesse.com.sg e-mail: p.mottmann@koelnmesse.de tel. +49 221 821 35 86
28.10 – 02.11	**INTERPOLITEX** **The 10th International Exhibition of Police and Defence Technologies** Moskwa, Rosja	www.interpolitex.ru e-mail: foreign@interpolitex.ru tel. +007 495 937 4081

LISTOPAD

03.11 – 06.11	**LOGISTYKA** **XIII Międzynarodowe Targi Logistyczne** Kielce, Polska	www.targikielce.pl e-mail: biuro@targikielce.pl tel. 041 365 12 22
05.11 – 10.11	**BATIMAT 2007** **International Bulding Exhibition** Paryż, Polska	www.batimat.com e-mail: emmanuelle.alexandre@reedexpo.fr tel. +33 1 47 56 51 91
06.11 – 09.11	**SFITEX 2007** **16th International Security & Fire Exhibition** St. Petersburg, Rosja	www.omega.spb.ru e-mail: omega@nodex.ru tel. +7 812 327 61 64, +7 812 321 05 40
07.11 – 08.11	**ALARM 2007** **VIII Konferencja i Wystawa Monitoringu Wizyjnego** Kielce, Polska	www.targikielce.pl e-mail: biuro@targikielce.pl tel. 041 365 12 22
07.11 – 10.11	**DEFENSE & SECURITY 2007** Bangkok, Tajlandia	www.asiandefense.com e-mail: defense@cmpthailand.com tel. +66 2 642 69 11 wew. 121
08.11 – 11.11	**SECURITY – International Specialized Exhibition** Skopje, Macedonia	http://en.security.moldexpo.md e-mail: info@moldexpo.md tel.: +373 22 592 683
13.11 – 16.11	**SICHERHEIT 2007** **Trade Fair For Safety And Security** Zurych, Szwajcaria	www.sicherheit-messe.ch e-mail: info@sicherheit-messe.ch tel. +41 44 806 33 99

GRUDZIEŃ

06.12 – 07.12	**KARTA 2006– Polish-International Smart Card Summit** **VI Międzynarodowa Wystawa Producentów i Użytkowników Kart i Systemów Kartowych** Warszawa, Polska	www.karta.info.pl e-mail: biuro_reklamy@brsa.com.pl tel. 022 849 60 06

Aktualny wykaz imprez branżowych na naszych stronach internetowych
www.zabezpieczenia.com.pl
Redakcja nie odpowiada za zmianę terminów targów.

Honeywell i Senspex zapewniają bezpieczeństwo kontroli granicznej

Koncern **Honeywell** poinformował o ukończeniu (wspólnie z firmą **Senspex** Inc. – dostawcą innowacyjnych rozwiązań w dziedzinie bezpieczeństwa, monitoringu, analizy chemicznej oraz systemów detekcji) instalacji zintegrowanego systemu bezpieczeństwa na posterunku patrolowym straży granicznej w miejscowości Alpine w stanie Texas.

Serce systemu, platforma Win-Pak Pro 2005 wyposażona w panel kontrolny Vista-128FBP, znacząco ogranicza czas potrzebny straży granicznej do zarejestrowania wydarzeń, oceny realnego zagrożenia oraz podjęcia decyzji o sposobie reakcji. Połączenie obu produktów zmniejszy również długość szkolenia nowych członków zespołu.

Dzięki zintegrowaniu wszystkich systemów bezpieczeństwa za pomocą jednej platformy strażnicy na posterunku mogą monitorować cały teren na pojedynczym monitorze. W ten sam sposób kontrolują również każdy element instalacji. Panel Vista-128FBP współpracuje ze zdalnym odbiornikiem alarmowym MX8000, a 32-kanałowe urządzenie DVR odbiera i nagrywa sygnały z 23 kamer stałych oraz pięciu kamer typu PTZ, zlokalizowanych na patrolowanym terenie. Oznacza to, że strażnicy są w stanie zdalnie monitorować i odpowiadać na alarmy, a także sterować kamerami. Każde działanie wymaga zalogowania, a przechowywane nagrania można w każdej chwili odtworzyć.

– *Nowy system zabezpieczeń dał straży granicznej narzędzie kontroli poziomu dostępu personelu do obszarów szczególnie chronionych, zdalnego monitorowania wszystkich wydarzeń oraz reagowania na zaistniałe sytuacje szybciej i wydajniej* – twierdzi William Renfro, starszy inżynier projektu w firmie Senspex.

– *Przy projektowaniu systemu bezpieczeństwa najważniejsze wydaje się słuchanie klientów oraz zrozumienie ich potrzeb, a także specyfiki działania* – podsumowuje Jacek Andruszkiewicz, regionalny kierownik sprzedaży w Honeywell Access Systems. – *Współpraca między firmami Senspex i Honeywell przewyższyła nawet wymagania inwestora* – dodaje Janelle Anthone, wiceprezes firmy Senspex.

Posterunek straży granicznej w Alpine jest jedną z 12 stanic w sektorze Marfa, obejmującym ponad 165 000 mil kwadratowych oraz 155 hrabstw w stanach Texas i Oklahoma. Jest to więc największy sektor wzdłuż całej południowo-zachodniej granicy Stanów Zjednoczonych. Strażnicy są tu również odpowiedzialni za ponad 520 mil granicy rzecznej.

Źródło:
www.securityworldhotel.com

Nowa nazwa stowarzyszenia

VI Zjazd Sprawozdawczy Ogólnopolskiego Stowarzyszenia Polalarm w listopadzie 2006 r. podjął nowe decyzje dotyczące zakresu działalności Polalarmu w branży ochrony – obszar zainteresowań stowarzyszenia ma objąć również zarządzanie bezpieczeństwem obiektów i firm. Nowy kierunek rozwoju zawodowego został uwzględniony w statucie, a także zmienionej nazwie stowarzyszenia, która obecnie brzmi:

Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „Polalarm”.

Uprzejmie informujemy, iż nowa nazwa została zarejestrowania przez Sąd Rejonowy m.st. Warszawy, XII Wydział Gospodarczy KRS i obowiązuje od dnia 8 lutego 2007 r.

Szczegółowe informacje o zmianach znajdziecie Państwo w uaktualnionym statucie stowarzyszenia Polalarm na naszej stronie *http://www.polalarm.com.pl*.

Bezp. Inf. inż. Bogdan Tatarowski, POLALARM

Forward Vision dostawcą kamer obrotowych dla służb ratowniczych Royal Navy

Kamera obrotowa **Mic1-400** firmy **Forward Vison** zapewnia monitoring wizyjny w trudnych warunkach akcji ratowniczych na pokładach Tamar – najnowszej klasy łodzi ratunkowych służących w Royal Navy.

Kamery te posiadają metalową kopułę zapewniającą sprawne użytkowanie w ekstremalnie trudnych warunkach morskich i pomagają oficerom Royal Navy wykonywać swoje obowiązki przez 24 godziny na dobę na wodach brytyjskich i irlandzkich. Od momentu założenia służb ratowniczych Marynarki Królewskiej w 1824 roku, łodzie ratunkowe ocaliły ponad 137000 osób. W 2005 roku łodzie uratowały 8104 osoby – średnio 22 dziennie.

Bezp. Inf. Forward Vison

Finał V edycji

studiów podyplomowych w Wojskowej Akademii Technicznej

W dniu 25 listopada 2006 roku w sali Rady Wydziału Mechatroniki (WMT) Wojskowej Akademii Technicznej (WAT) w Warszawie miało miejsce zakończenie V edycji niestacjonarnych studiów podyplomowych pn. ***Ochrona osób i mienia*** oraz ***Bezpieczeństwo lokalne i zarządzanie kryzysowe****, połączone z inauguracją ich VI edycji.

Podczas uroczystości dziekan WMT prof. dr hab. inż. Aleksander Olejnik wraz z dyrektorem Instytutu Elektromechaniki WMT prof. dr hab. inż. Józefem Gackiem, prezesem „Crimen II" mgr inż. pilotem Eugeniuszem Zduńskim i wiceprezesem Zarządu Polskiej Izby Ochrony Osób i Mienia Bogdanem Tatarowskim wręczyli nowym studentom symboliczne indeksy, a absolwentom – świadectwa ukończenia studiów podyplomowych. Ponadto uhonorowali najlepszych studentów. Nagrodę za ukończenie studiów z wyróżnieniem otrzymał mgr inż. Piotr Kierklo, który obronił pracę pt. *Świadomość użytkowników w zakresie zagrożeń bezpieczeństwa w strukturach informatycznych*, natomiast nagrodami za najlepsze prace końcowe zostali wyróżnieni: mgr Adam Banach za pracę pt. *Edukacja i aktywizacja społeczeństw w strategii walki ze współczesnym terroryzmem*, mgr Katarzyna Hołdak za pracę pt. *Polska w amerykańskim systemie obrony przeciwrakietowej*, mgr Jarosław Leśniowski za pracę pt. *Fałszerstwa znaków pieniężnych jako element terroryzmu międzynarodowego* oraz mgr Dariusz Wroniewicz za pracę pt. *Ustawodawstwo polskie w zakresie stosowania środków przymusu bezpośredniego i broni palnej – stan aktualny i propozycje nowych rozwiązań*.

* Studia podyplomowe, organizowane przez Instytut Elektromechaniki Wydziału Mechatroniki we współpracy ze Studium Ochrony Osób, Mienia i Usług Detektywistycznych „Crimen II", są przeznaczone dla osób pracujących na stanowiskach związanych m.in. z ochroną osób, mienia i informacji niejawnych oraz administrowaniem systemami bezpieczeństwa na poziomie lokalnym (przedsiębiorstwa, jednostki ratownictwa, straż miejska, administracja terenowa itp.).

V edycję studiów ukończyło 22 absolwentów, a VI edycję rozpoczęło 30 studentów.

Szczegółowe informacje na temat kolejnych edycji studiów można uzyskać u kierownika studiów – dra inż. Zbigniewa Leciejewskiego (Instytut Elektromechaniki WMT WAT); tel.: 022 683 95 08, 022 683 99 56; faks: 022 683 95 08; e-mail: Zbigniew.Leciejewski@wat.edu.pl; www.wat.edu.pl oraz mgr. inż. pilota Eugeniusza Zduńskiego („Crimen II"); tel.: 022 782 54 53; tel. kom.: 0600 253 907; e-mail: info@crimen2.prv.pl; www.crimen2.prv.pl.

Inf. Bezp. płk dr inż. Ryszard Woźniak, WAT

Kamera Forward Vision Mic1-400

Kamera firmy **Forward Visio Mic1-400** została wybrana do monitoringu nowej siedziby jednej z głównych nowojorskich firm medialnych. Produkt ten, często określany mianem „Metalowy Mickey", zyskał uznanie inwestora nie tylko ze względu na doskonałe właściwości i dużą odporność mechaniczną, ale również atrakcyjne industrialne wzornictwo.

Zastosowane urządzenie rozwiązuje jednocześnie kilka problemów napotykanych przez osoby odpowiedzialne za systemy zabezpieczeń we współczesnych biurowcach – konwencjonalne kamery typu **Speed Dome** nie pasują do nowoczesnych wnętrz, wydają się w nich nie na miejscu. Instalatorzy najczęściej poszukują kamer PTZ, wykorzystujących istniejące protokoły i działających w warunkach słabego oświetlenia, ale jednocześnie mających atrakcyjny wygląd.

Kamera Mic1-400, wykonana z polerowanej stali nierdzewnej oraz aluminium, doskonale współgra z wystrojem nowoczesnych wnętrz. Ponadto ma wszystkie zalety kamer obrotowych: 216-krotny zoom, wysokiej jakości układ optyczny oraz mechaniczny filtr IR, zapewniający wysokiej jakości obraz w warunkach słabego oświetlenia.

Zainstalowane we wspomnianym obiekcie kamery Mic1-400 doskonale harmonizują z wysmakowaną fasadą budynku. Stanowią one przyjemny dla oka detal architektoniczny, być może jeden z najbardziej charakterystycznych elementów budynku.

Ich widok chroni jednocześnie przed potencjalnymi przestępcami. Tym samym podwyższono poziom bezpieczeństwa osób przebywających w obiekcie oraz ich subiektywne poczucie bezpieczeństwa.

Źródło: Forward Visio

Big Brother używa Rayteca

Seria oświetlaczy podczerwieni **RAYMAX** firmy **Raytec** została wykorzystana w programie Big Brother w telewizji chilijskiej.

Chilijska telewizja użyła oświetlaczy **RAYMAX 50**, aby sporządzać materiał filmowy w godzinach nocnych. Transmisja programu w chilijskiej TV odbywa się 24 godziny na dobę, więc zapewnienie wysokiej jakości obrazu w warunkach słabego oświetlenia jest niezwykle ważne. RAYMAX 50 został wybrany ze względu na bardzo dobre parametry, estetyczny wygląd oraz pełny serwis techniczny.

Oświetlacze RAYMAX są dostępne w ponad 20 krajach. Każdy oświetlacz zapewnia wysokiej jakości oświetlenie w zakresie fal podczerwonych. Oświetlacze RAYMAX dostosowują się do poziomu oświetlenia i posiadają pięcioletnią, najdłuższą w tej klasie produktów dostępnych na rynku, gwarancję.

Bezp. Inf. Raytec

Protect Security Systems na rynku polskim

W dniu 02.01.2007 rozpoczęła działalność na rynku polskim firma **AWC Protect Global Security Systems**. Protect Global jest wiodącym światowym dostawcą emiterów dymu do zabezpieczania obiektów. Wizją firmy jest skuteczna ochrona wszystkiego, co stanowi wartość dla klientów.

Protect Global wdraża obecnie trzecią generację generatorów dymu. Pierwszą generację stanowiły urządzenia, które są znane z koncertów i dyskotek.

Urządzenia zabezpieczające Protect są konstruowane w sposób, który pozwala zintegrować je z tradycyjnymi alarmowymi systemami antywłamaniowymi. Kiedy włamywacz aktywuje alarm, Protect zaczyna funkcjonować, wypełniając pomieszczenie sklepowe, biuro lub magazyn gęstym lecz nieszkodliwym dymem. Zabezpieczenie to skutecznie zatrzymuje włamywacza w mniej niż 20 sekund, powodując kompletną dezorientację intruza, a co za tym idzie brak możliwości kradzieży czegokolwiek. Konwencjonalne alarmy antywłamaniowe **nie powstrzymują złodzieja** – aktywują sygnał dźwiękowy i przesyłają sygnał do centrali. Centrala wysyła wówczas patrol interwencyjny, który dojeżdża na miejsce zdarzenia, ale zdarza się, że za późno – gdy złodziej z łupem jest już daleko.

Bezp. Inf. Witold Drozdowicz
AWC Protect Global Security Systems

Adres przedstawicielstwa:
01-233 Warszawa, ul. Bema 87, tel. 022 456 87 79

Monitoruj.pl rozszerza ofertę produktów

Monitoruj.pl prezentuje nowy dział w ofercie – kamery IP. W sklepie internetowym monitoruj. pl znajdziecie Państwo już dziś 30 produktów siedmiu producentów oraz nieograniczoną ilość rozwiązań. Oferujemy urządzenia takich firm, jak: AXIS, D-Link, GrandTec, TRENDnet, Tokia, LYD oraz Camstar – wszystkie dostępne są w jednym miejscu i można je natychmiast nabyć.

Technologia IP to przyszłość. Nieograniczona ilość kamer, podgląd i obsługa z dowolnego miejsca na świecie, prosty montaż, nowoczesne technologie, takie jak *Power over Ethernet* – to wszystko przyczynia się do coraz większej popularności rozwiązań IP.

Monitoruj.pl obserwuje rynek urządzeń sieciowych, aby osiągnąć kompleksowość swojej oferty i proponować klientom najlepsze rozwiązania.

Bezp. Inf. monitoruj.pl

WV-NS202

kamera sieciowa o właściwościach lepszych niż ludzkie oko

Panasonic wprowadza nową szybkoobrotową kamerę sieciową **WV-NS202**, wyposażoną w technologię Super Dynamic III oraz progresywne skanowanie.

Kamera ma wysoką czułość oraz rozdzielczość, co zapewnia doskonałą jakość obrazu. Wytrzymałe mechanizmy oraz funkcja archiwizacji obrazu czyni z niej doskonałe narzędzie profesjonalnych systemów nadzoru. Technologia Super Dynamic III pozwala na 128-krotne rozszerzenie zakresu dynamiki, co z kolei umożliwia wierną reprodukcję obrazów w każdych warunkach oświetlenia. Dotyczy to zarówno generowania obrazów dla prędkości migawki 1/50 s, jak i 1/8000 s.

Kamera WV-NS202 wyposażona jest w wysokiej jakości obiektyw zmiennoogniskowy 3,79–83,4 mm, który zapewnia 22-krotne powiększenie optyczne. W połączeniu z 10-krotnym powiększeniem cyfrowym umożliwia to uzyskanie 220-krotnego powiększenia, gwarantującego obserwację odległych obiektów i tym samym znaczne zwiększenie obszaru nadzoru. Dzięki progresywnemu skanowaniu obrazu kamera generuje, w porównaniu do kamer skanujących międzyliniowo, o wiele gładszy i ostrzejszy obraz szybko poruszających się obiektów.

Minimalne oświetlenie konieczne do prawidłowego działania kamery WV-NS202 wynosi 0,7 lx, a więc obserwacja sceny w kolorze jest możliwa nawet przy bardzo niskim poziomie oświetlenia. Wyposażenie kamery w funkcję wydłużonej migawki (maks. do 32 razy) pozwala również na efektywną pracę urządzenia w warunkach nocnych.

Dla ułatwienia instalacji i montażu kamerę wyposażono w technologię *Power over Ethernet* (PoE) IEEE802.3af, która pozwala na zasilanie kamery oraz przesyłanie obrazu za pomocą jednego kabla. Również prosty mechanizm mocowania znacznie ułatwia instalację urządzenia w wyznaczonym miejscu.

Wielu ustawień WV-NS202 – między innymi balansu bieli, czułości oraz prędkości migawki – można dokonywać bezpośrednio podczas obserwacji obrazu z kamery. Dzięki temu użytkownik uzyskuje obrazy najwyższej jakości. Urządzenie wyposażone jest w gniazdo mikrofonowe oraz głośnikowe, co pozwala na dwukierunkową komunikację audio.

Z kolei wbudowane gniazdo kart SD umożliwia archiwizację nagrań w przypadku awarii sieci.

Wysoka jakość mechanizmów zastosowanych w kamerze Panasonic gwarantuje długotrwałe i bezproblemowe użytkowanie. Maksymalna prędkość obrotu kamery w poziomie to 300 stopni na sekundę, w pionie – 100 stopni na sekundę.

Kamera WV-NS202 ma funkcję automatycznego śledzenia obiektu (*auto tracking*), co pozwala na obserwację poruszających się obiektów bez udziału operatora. Pozostałe funkcje kamery to miedzy innymi: 64 programowalne pozycje, maskowanie stref prywatnych, rozbudowane funkcje alarmowe (wejścia i wyjścia alarmowe, detekcja ruchu itp.). W przypadku inicjacji alarmu odpowiednio zaprogramowana kamera jest w stanie wysłać pod cztery wskazane adresy e-mail powiadomienie o tym zdarzeniu wraz z dołączonym zdjęciem.

Wszystko to powoduje, że nowa kamera sieciowa Panasonic WV-NS202 doskonale nadaje się do stosowania w nawet najbardziej wymagających, profesjonalnych systemach monitoringu wizyjnego – znacznie zwiększa ich efektywność oraz bezpieczeństwo nadzorowanych obiektów.

Bezp. Inf. Panasonic

Nowy mówiący *FINGER*

Rynek urządzeń biometrycznych stale poszerza i udoskonala swoją ofertę. Jedną z ciekawszych nowości jest biometryczny czytnik kontroli dostępu **Finger LX007** o zaskakująco rozbudowanych możliwościach.

Najnowsze urządzenie firmy **IDTECK**, podobnie jak inne czytniki kontroli dostępu z rodziny Finger, łączy w sobie funkcje czytnika linii papilarnych, karty zbliżeniowej i kodu dostępu. W przeciwieństwie do starszych modeli ma on jednak więcej klawiszy funkcyjnych, co daje więcej możliwości kontroli czasu pracy.

– LX007 ma możliwość wyświetlania logo firmy użytkującej system – mówi Radosław Majkowski, dyrektor techniczny z Grupy T4B. *– Można również zapisać dźwięk lub komunikat głosowy i przypisać go do danej osoby. W ten sposób każdy pracownik może być przywitany przez urządzenie w specyficzny sposób.*

Urządzenie firmy IDTECK ma więcej możliwości określenia przerw w pracy. Oprócz rozpoczęcia i zakończenia pracy można dodatkowo zdefiniować wyjście na posiłek, wyjście służbowe, delegację itp.

Kolejną zaletą urządzenia Finger LX007 jest możliwość podłączenia go do sieci Ethernet.

– Do tej pory podłączenie urządzenia do sieci lokalnej było możliwe tylko przy użyciu dodatkowego konwertera TCP/RS-422. W przypadku LX007 konwerter jest wbudowany w urządzenie. Ta zaleta znacznie ułatwia instalację i usprawnia komunikację ze stacją roboczą – tłumaczy Radosław Majkowski.

Nowe czytniki biometryczne weryfikują tożsamość szybciej, przy mniejszym prawdopodobieństwie popełnienia błędu. Są one niezastąpione przy wejściach do pomieszczeń o znaczeniu strategicznym dla przedsiębiorstwa. Wykorzystuje się je wszędzie tam, gdzie chcemy mieć ścisłą kontrolę nad tym, kto do danego miejsca wchodzi, o której i ile czasu w nim spędza. Tego typu czytniki z całą pewnością powinny być instalowane przy wejściach do pomieszczeń, gdzie nawet obecność samych pracowników –z innych sektorów – jest niepożądana, np. w strefie kontroli jakości lub badania żywności.

Bezp. Inf. T4B

System GPS
w samochodzie zadziałał – złodziej złapany

Dzięki systemowi **GPS** i szybkiej akcji policji złodziej samochodowy został złapany w niecałą godzinę.

Dyżurny Komendy Miejskiej Policji w Poznaniu odebrał telefon z **Centrum Monitorowania Alarmów w Bytomiu**. Pracownik firmy zajmującej się monitorowaniem pojazdów w systemie GPS poinformował, że na jednym z osiedli poznańskiej dzielnicy Piątkowo skradziono Renault Kangoo.

W ciągu kilkunastu minut trasy wylotowe z Poznania zostały zablokowane. Przez cały czas trwania obławy dyżurny otrzymywał informacje o lokalizacji skradzionego pojazdu z centrum GPS i przekazywał je patrolom biorącym udział w akcji. Po 40 minutach złodziej był już w rękach policji, a Renault Kangoo wróciło do właściciela.

Zatrzymany 21-letni Bartosz S. był już wcześniej karany za inne przestępstwa. Za kradzież z włamaniem grozi mu kara pozbawienia wolności do lat dziesięciu.

Źródło: www.wiadomosci.epoznan.pl

Hybrydowa kamera AutoDome

Firma **Bosch Security Systems**, producent elementów systemów bezpieczeństwa, wprowadza innowacyjne urządzenie dozorowe – nową kamerę **AutoDome**.

Nowa kamera AutoDome stanowi platformę wymiennych modułów, umożliwiających szybkie i ekonomiczne dodawanie zaawansowanych funkcji, takich jak śledzenie obiektów czy praca w sieci TCP/IP. Podstawą konstrukcji tej kamery jest pięć typów wymiennych modułów. Kamerę AutoDome zaprojektowano w sposób umożliwiający wymianę lub dodanie modułów również w czasie pracy (*hot swap*).

Kamera umożliwia połączenie hybrydowe – możliwe jest jednoczesne przesyłanie strumienia wizyjnego przez sieci IP oraz analogowego sygnału wizyjnego przez konwencjonalny kabel koncentryczny. Nowe kamery AutoDome współpracują z całą gamą urządzeń dozorowych firmy Bosch, włączając w to przełączniki wizyjne, rejestratory i systemy zarządzania obrazem bazujące na sieciach IP. Kamery wykorzystują kodowanie i kompresję w standardzie MPEG-4, zapewniając obraz jakości DVD 4CIF o częstotliwości odświeżania maks. 25 obrazów na sekundę.

Firma Bosch oferuje modele kamer AutoDome wyposażone w inteligentne funkcje, takie jak stabilizacja obrazu, detekcja ruchu oraz automatyczne śledzenie ruchu AutoTrack II (kamera wykrywa i śledzi obiekty tylko w określonych obszarach, ignorując dodatkowy ruch w tle).

Oferta kamer obejmuje cztery modele, począwszy od podstawowej wersji stacjonarnej, poprzez dwa modele z mechanizmem uchylno-obrotowym i regulacją zoomu (PTZ), a skończywszy na wyposażonej we wszystkie funkcje inteligentnej kamerze PTZ serii 500i.

Kamery odznaczają się również wyjątkową niezawodnością – wszystkie obudowy posiadają stopień ochrony IP66 i wszystkie są wyposażone we wzmocnioną, wandaloodporną kopułkę poliwęglanową. Kamery objęte są również trzyletnią gwarancją, najdłuższą w branży *security* w zakresie kamer.

Bezp. Inf. Bosch Security Systems

Zamki
DOM D31 i D12

Informujemy, że zakończyły się badania zamków wpuszczanych DOM D31 i DOM D12.

Zamki zakwalifikowano do 4. klasy według PN-EN 12209:2005. Omawiane produkty charakteryzują się dużą trwałością i estetycznym wykończeniem. Blacha czołowa zamków wykonana jest ze stali nierdzewnej. Dzięki temu znajdują one szerokie zastosowanie w wielu projektach, stanowiąc idealne uzupełnienie oferty **DOM Polska** w zakresie obsługi inwestycji. Zamki dostępne są w wersjach: na wkładkę Euro-DIN, na klucz i do drzwi WC.

Więcej informacji znajduje się na stronie: http://www.dom-polska.pl.

Bezp. Inf. Dom Polska

Targi IIPSEC 2007

IIPSEC to cykliczne targi wraz imprezami towarzyszącymi, które promują **technologie IP w branży zabezpieczeń**. W tym roku impreza odbyła się w dniach 23–25 stycznia 2007 r. w Stoneleigh Park niedaleko Coventry w Anglii.

Organizatorzy przygotowali ponad 120 stanowisk dla czołowych firm z branży zabezpieczeń oraz IT. Według danych organizatorów targi odwiedziło około 3000 osób z ponad 65 krajów – głównie kadra kierownicza, menedżerowie firm instalacyjnych i dystrybucyjnych oraz producenci sprzętu sieciowego i szeroko pojętych systemów zabezpieczeń.

Dominowali wystawcy urządzeń telewizji dozorowej, bazującej na sieciach IP (IPTV), chociaż wiele miejsca poświecono także rozwiązaniom zintegrowanym, kontroli dostępu, zdalnemu monitoringowi, technologiom sieciowym, a w dalszej kolejności – systemom alarmowym, biometrycznym oraz przeciwpożarowym.

Targi wzbogacał cały szereg imprez towarzyszących – 22 stycznia odbyła się całodniowa konferencja, przeznaczona głównie dla menedżerów, kierowników i osób odpowiedzialnych za wprowadzanie nowych rozwiązań technologicznych w firmach z sektorów przemysłu, budownictwa publicznego i wielu innych. Poruszano tematy związane z przyszłością technologii ochrony i zapobiegania aktom przestępczym, jak również kosztami szeroko pojmowanego bezpieczeństwa.

Podczas targów zorganizowano wiele warsztatów i pokazów, pokrewnych tematycznie względem rozwiązań prezentowanych przez firmy. Wiele szkoleń i warsztatów zorganizowała firma Cisco. Szkolenia obejmowały zakres od podstaw technologii IP aż do profesjonalnego projektowania sieci oraz techniki zwiększania bezpieczeństwa i niezawodności sieci.

Niezależnie od programu firmy Cisco przygotowano szereg seminariów technicznych, poświęconych różnym aspektom wykorzystania sieci IP (od podstaw zagadnień sieciowych aż do integracji systemów kontroli dostępu, alarmowych, przesyłania dźwięku i obrazu oraz zagadnienia sieci bezprzewodowych i mobilnych systemów łączności).

Przewidziano również wiele seminariów dla użytkowników końcowych. Na seminariach tych dokonano prezentacji firm, przedstawiono projekty zrealizowane i planowane, jak również perspektywy rozwoju branży zabezpieczeń w różnych zastosowaniach – począwszy od środków transportu, poprzez przemysł, handel i edukację, a zakończywszy na systemach wdrożonych dla policji i służb więziennych.

Na targach nie zabrakło największych firm z branży. Obecne były firmy Dedicated Micros, Dallmeier, Axis, CBC, Cieffe, DVTel, Flir, Arecont Vision, Honeywell, JVC, Milestone, Mobotix, Siemens – Bewator, Indigo Vision, Norbain (główny sponsor targów) i wiele innych.

Dominującą pozycję na targach zajmowały systemy telewizji IP (kamery sieciowe, enkodery wideo, rejestratory sieciowe), a także specjalizowane oprogramowanie – od prostych aplikacji zmieniających komputer PC w wielokanałowy rejestrator cyfrowy aż po potężne platformy do zdalnego monitoringu sieciowego, wyposażone w wyrafinowane funkcje analizy i obróbki obrazu. Tegorocznym hitem były zaawansowane techniki obróbki obrazu (*Video Analytics*), pozwalające definiować w dowolny sposób obszary, strefy i linie detekcji ruchu, rozpoznawać obiekty i twarze, zliczać ludzi i obiekty, dokonywać pomiaru prędkości poruszających się obiektów czy wykrywać naruszenie stref ochronnych. W powiązaniu z bazami danych i silnymi jednostkami obliczeniowymi pozwala to na analizę zagrożeń w czasie rzeczywistym i przewidywanie zachowań ludzi w rozległych systemach cyfrowej rejestracji i analizy obrazu, np. na lotniskach, w halach produkcyjnych i handlowych, na autostradach czy w ruchu miejskim. Systemy te obecnie spełniają nie tylko funkcję przesyłania i rejestracji wideo. Umożliwiają również dostarczanie danych koniecznych do podejmowania kluczowych decyzji, pozwalają w porę rozpoznać zagrożenie, a dzięki sprzężeniu z systemami automatyki budynku – także zarządzać i sprawnie reagować na pojawiające się zagrożenia.

Tendencją branży *security*, która uwidoczniła się na targach, jest silne dążenie do integracji różnych systemów zabezpieczeń (CCTV, kontroli dostępu, alarmowych, pożarowych itd.) na wspólnej platformie IP z wykorzystaniem specjalizowanego oprogramowania znacznie zwiększającego funkcjonalność i łatwość obsługi, a z drugiej strony zapewniającego wielodostępowość, niezawodność oraz trwałość danych. Ciekawość zwiedzających targi mogły wzbudzić technologie bezprzewodowe i mobilne, pozwalające na znaczne rozszerzenie zakresu zastosowań technologii IP w branży zabezpieczeń i nie tylko.

Technologia IP wydaje się obecnie najbardziej przyszłościowa. Pomimo faktu, że jeszcze nie jest ona bardzo rozpowszechniona w systemach bezpieczeństwa, nowe możliwości systemów IP (jak chociażby zdolność generowania obrazów o wysokiej rozdzielczości przez kamery megapikselowe, możliwość łatwej integracji i sprzężenia z innymi systemami) pozwalają sądzić, że sytuacja ta może szybko ulec zmianie.

Mimo rozpowszechnienia i przystępnej ceny analogowych systemów CCTV, zdecydowanie widać wzrost zainteresowania w pełni cyfrowymi systemami IP oraz hybrydowymi systemami pośrednimi. Szacuje się, że nadchodzący okres – od roku do dwóch lat – będzie decydujący dla systemów IP. Po tym czasie powinny one osiągnąć status rozwiązania jeżeli nie dominującego, to przynajmniej preferowanego.

RED.

I znowu **były tłumy**

Ponad 1200 wystawców z kilkudziesięciu państw, 40 000 m² powierzchni ekspozycyjnej, a także bogaty program wydarzeń – to krótka charakterystyka **Międzynarodowych Targów Budownictwa „Budma" w Poznaniu**.

Budma 2007 odbyła się pod patronatem Ministra Budownictwa i Ministra Transportu oraz Stowarzyszenia Architektów Polskich.

Z uwagi na dobrą koniunkturę i ożywienie w budownictwie, organizatorzy byli pewni wysokiej frekwencji inwestorów z kraju i zagranicy. Duża liczba zapowiadanych nowości wskazuje na to, że jakość oferty wystawców spełni duże oczekiwania rynku. Znaczące są także wzrosty ilościowe – niektóre branże, np. zajmujące się stolarką okienną czy materiałami budowlanymi, były reprezentowane przez większą (w porównaniu z poprzednimi targami) liczbę wystawców; wzrosła też zajmowana przez nich powierzchnia ekspozycji. Dotyczy to przede wszystkim budownictwa sportowego – w tym sektorze targów ekspozycje wystawców zajmowały powierzchnię ponad dwukrotnie większą.

Ekspozycja targów Budma była podzielona na czytelne segmenty tematyczne, ułatwiające dotarcie do poszukiwanej oferty: salon materiałów budowlanych, salon stolarki otworowej, salon wykończenia, wystroju i małej architektury, salon usług budowlanych, dachy, centrum budownictwa drogowego i inżynieryjnego, centrum budownictwa sportowego oraz salon nieruchomości i inwestycji Investfield. Ich uzupełnieniem były strefy specjalne, np. Wyspa Nowości – eksponująca najnowsze hity wystawców, czy BudShow – pokazujący finalny efekt zastosowań nowoczesnych produktów i technologii.

W powyższej formule firmy uczestniczące w targach Budma 2007 przedstawiły materiały budowlane i izolacyjne, chemię budowlaną, nawierzchnie, posadzki i podłogi, dachy, wyroby metalowe i elementy mocujące, szkło, profile, okna, drzwi oraz okucia, bramy i ogrodzenia, schody i windy.

Program wydarzeń stworzono, biorąc pod uwagę potrzeby wszystkich grup wystawców i zwiedzających. Wiele interesujących informacji mogli zdobyć przedstawiciele samorządów – oferta dla nich to zarówno salon nieruchomości i inwestycji Investfield, jak i centrum budownictwa sportowego. Dla kadry inżynieryjno-technicznej zorganizowano Dni Inżyniera Budownictwa, dla architektów – Targowe Spotkania z Architekturą, a dla handlowców – Dzień Dystrybutora. Dla rzemieślników przygotowano liczne prezentacje i warsztaty (Dzień Dekarza, Dzień Glazurnika, Rzemieślnicze Forum Budowlane). Natomiast z myślą o inwestorach indywidualnych zorganizowano BudShow – aktywny pokaz materiałów i technologii budowlanych „na żywo".

Na targach Budma branżę *security* reprezentowały między innymi następujące firmy: **Info-Cam, D+H Polska, Alarmnet, Gunnebo Polska, Kaba Security, Genway, Lockpol, Metalkas, Metalplast Lob**.

Wyżej wymienione firmy posiadają w swojej ofercie między innymi elektroniczne systemy zabezpieczeń i systemy dozorowe CCTV (Info-Cam), systemy odprowadzania dymu i gorąca, systemy blokad drzwi przeciwpożarowych oraz systemy naturalnej wentylacji (D+H Polska), systemy domofonowe i wideodomofonowe Comelit (Alarmnet), systemy zewnętrznej ochrony budynków oraz przyległego terenu (Gunnebo Polska), wkładki mechaniczne, depozytory kluczy oraz przejścia kontrolowane, systemy kontroli dostępu (Kaba Security), systemy domofonowe oraz wideodomofonowe (Genway), zamki, wkładki, samozamykacze hydrauliczne, elektrozaczepy (Lockpol), sejfy, kasy pancerne, szafy do przechowywania dokumentów niejawnych, bezpieczne pojemniki, kłódki (Metalkas), zamki wierzchnie i wpuszczane, kłódki, wkładki bębenkowe, zamykacze hydrauliczne, okucia budowlane, drzwi antywłamaniowe, systemy Master Key (Metalplast Lob).

Zaprezentowano okna z szybami antywłamaniowymi, z antywyważeniowymi okuciami oraz wielostopniowe systemy zabezpieczeń antywyważeniowych do okien i drzwi, nawet z możliwością podłączenia do systemu alarmowego (między innymi: Roto, Siegenia-AUBI).

Na wielu stoiskach można było znaleźć drzwi antywłamaniowe wyposażone w system wielopunktowego ryglowania. W zależności od liczby i rodzaju stalowych trzpieni ryglujących, występują one w różnych wersjach, należących do różnych klas odporności antywyważeniowej. Warto nadmienić, że drzwi antywłamaniowe klasy C (atestowany musi być też użyty w drzwiach zamek) spełniają wymogi bezpieczeństwa, które są brane pod uwagę przy ubezpieczaniu mieszkania lub domu. W niektórych towarzystwach ubezpieczeniowych zniżka przysługująca dzięki zamontowaniu takich drzwi może wynosić nawet 30%.

Źródło: MTP

z BIOMETRIĄ w podróży

Obserwując nasze otoczenie, doniesienia z całego świata, nie sposób nie zgodzić się z wizją świata przyszłości wg Jacques'a Attalego (francuskiego ekonomisty i pisarza), przedstawioną w *Une breve historie de l'avenir*. W świecie tym panować będzie kontrola i nadzór, sprawowany m.in. przez coraz bardziej zminiaturyzowane elektroniczne urządzenia, niejednokrotnie będące częścią ludzkiego ciała (już dziś wszczepia się miniaturowe układy elektroniczne dzieciom w celu kontroli ich miejsca pobytu). Wszechobecny monitoring dostarczy informacji o pochodzeniu produktów i przemieszczaniu się ludzi, a dzięki nanowłóknom komputery zostaną zintegrowane z ubraniami i pozwolą „czytać" i nadzorować ludzkie ciało. Czy to wizja fantastyczno-naukowa, czy zapowiedź? Czy rzeczywistość dokona plagiatu powieści – nawiąże do Attalego, tak, jak do George'a Orwella, Alvina Tofflera, Marshalla McLuhana, Stanisława Lema etc.?

Istnieją instytucje/organizacje (np. Internet, Navstar GPS, The United Nations, Interpol, Total Information Awareness, Federal Communications Commission, The International Monetary, MI5, Mossad, Europol & Eurojust, Secret Service, Department of Justice, Federal Bureau of Investigation, Department Of Homeland Security, National Security Agency, The Central Intelligence Agency, Department of Defense, The Pentagon, The Peacekeeper Missile, The United States Strategic Command, Open Source Information System etc.) i projekty (np. Echelon, Keyhole, ELINT, SIGINT, banknoty z RFID, e-paszporty, AFIS, monitoring miast, rozpoznawanie numerów rejestracyjnych pojazdów, rejestracja czasu pracy i kontrola dostępu etc.), których działalność może mieć wiele wspólnego z działalnością Orwellowskiego Wielkiego Brata, chociaż wszystkie zostały powołane dla naszego wspólnego dobra i bezpieczeństwa. Ich siła staje się tym większa, im bardziej wzrasta uzależnienie od spektrum elektromagnetycznego. W społeczeństwach wiedzy zautomatyzowane pomiary unikatowych cech genotypowych i fenotypowych obywateli stają się konieczne dla zapewnienia im bezpieczeństwa.

Doświadczamy rozdźwięku pomiędzy pragnieniem większego bezpieczeństwa a niechęcią do ograniczania wolności i swobody.

Według Ericha Fromma (niemieckiego filozofa, socjologa, psychologa i psychoanalityka), lakonicznie mówiąc, uciekamy dziś od wolności rozumianej potocznie, rozumianej w sensie (nadmiernej) swobody. Uciekamy w:

- autorytaryzm – zaspokajamy potrzebę ładu i porządku poprzez podporządkowanie się innym lub podporządkowanie ich sobie;
- destruktywność – mamy potrzebę sprawstwa i szybkiego doświadczania własnego wpływu na bieg zdarzeń;
- mechaniczny konformizm – redukuje on niepewność; zmniejszając lęk zapewnia minimum bezpieczeństwa w niestabilnym, zagrażającym otoczeniu.

Postępy w rozwoju technologii biometrycznych powodują obawy społeczne, które z kolei negatywnie wpływają na dalszy rozwój i funkcjonalność metod. Istnieją różnego rodzaju społeczne obawy względem użycia biometrii.

Nieliczni uważają, że technologia ta może spowodować fizyczną szkodę, uszczerbek na zdrowiu użytkowników, albo że użycie skanerów biometrycznych jest niehigieniczne (choroby) – oczywiście nie ma to odzwierciedlenia w rzeczywistości, aczkolwiek w przypadku takiej katastrofy, jak np. epidemia SARS, która zmusza ludzi do noszenia masek i unikania kontaktu fizycznego, nie będzie można skłonić obywateli do przyłożenia dłoni lub palca do czytnika. W takiej lub podobnej sytuacji popularniejsze będą metody „nieinwazyjne", np. skanowanie tęczówki oka, żył, pomiar pojemności elektrycznej paznokcia wraz z wykorzystaniem RFID

(ang. *Radio Frequency Identification* – technologia wykorzystywana również w e-paszportach zawierających dane biometryczne) czy też metody behawioralne.

Innego rodzaju obawy dotyczą naszych personaliów. Niektórzy obawiają się, że pobrane dzięki biometrycznym metodom dane o osobach mogą być źle wykorzystywane. Chodzi tu o fałszowanie danych, manipulowanie nimi, wykorzystywanie danych biometrycznych przez złodziei – np. pozostawianie na miejscu przestępstwa cudzych śladów (zapachu, odcisku palca), wykorzystywanie nagrania głosu – wydaje się, że istnieje taka możliwość, choć można z pewnością takim sytuacjom zapobiec.

Nauka jest bardzo wszechstronnym wytrychem, potrafi otworzyć wrota wszechświata i wrota piekieł.

A. Majewski

Nowoczesne technologie wyprzedzają mentalność ludzką, sposób myślenia i przyzwyczajenia, dlatego też należy dobrze zrozumieć działanie systemów biometrycznych, oswoić się z nimi, przyzwyczaić do nich, do korzyści – komfortu i bezpieczeństwa – jakie niosą ze sobą nowoczesne technologie biometryczne (była już o tym mowa w naszych wcześniejszych artykułach, zamieszczonych w nr 4/2006, 5/2006, 6/2006, 1/2007 *Zabezpieczenia*).

Obecnie, jak wynika z badania przeprowadzonego w 2006 r. przez Ponemon Institute LLC na zlecenie firmy Unisys (ogólnoświatowej firmy consultingowej w zakresie technologii informatycznych), aż 70% respondentów z całego świata nie ma nic przeciwko biometrycznym metodom kontroli tożsamości. Przyzwolenie na stosowanie nowych technik zabezpieczeń rośnie szczególnie w obszarze bezpieczeństwa obiektów użyteczności publicznej, takich jak banki, metro, hale sportowe, przejścia graniczne, a zwłaszcza porty lotnicze.

Już przed zamachami terrorystycznymi z 11 września 2001 r. (które spowodowały wyznaczenie nowych kierunków w dziedzinie bezpieczeństwa) w transporcie lotniczym rozpoczęto projekty i badania związane z wykorzystaniem biometrii w systemach zabezpieczeń portów lotniczych. Na przykład: lotnisko Chicago O'Hare miało zainstalowany system wykorzystujący biometrię odcisku palca dla zwiększenia szybkości i bezpieczeństwa kontroli kierowców dostarczających ładunki na terminal cargo. Także międzynarodowy port Charlotte/Douglas, we współpracy z amerykańskimi liniami lotniczymi (US Airways), posiadał projekt pilotażowy wykorzystujący technologię rozpoznawania tęczówki do weryfikacji pracowników mających dostęp do wydzielonych obszarów bezpieczeństwa. Izraelski port lotniczy Ben Gurion wykorzystywał rozpoznawanie geometrii dłoni, by przyspieszać odprawy celne. Islandzkie lotnisko Keflavik używało technologii rozpoznawania twarzy w aplikacji nadzoru.

Dyskusje nad użyciem biometrii w celu zwiększenia poziomu bezpieczeństwa lotnisk niezwykle zaostrzyły się w pierwszych tygodniach po atakach terrorystycznych na WTC i objęły zarówno media, jak i inne społeczności (personel lotniczy, producentów technologii, obrońców prywatności i praw człowieka, liczne grupy obywatelskie oraz przywódców politycznych). Osobiste zaangażowanie amerykańskich polityków (np. senatora Johna Edwarda – demokraty, mianowanego na wiceprezydenta USA w 2004 r., oraz republikanina Jerrego Wellera), opowiadających się za poprawą bezpieczeństwa portów morskich i lotniczych poprzez wykorzystanie biometrii, niewątpliwie przyspieszyło wdrażanie projektów biometrycznych przeznaczonych do kontroli tożsamości.

Państwa, które do tej pory nie interesowały się wykorzystaniem biometrii przy odprawie celnej (porty lotnicze i morskie, przejścia graniczne), nie mogą długo zwlekać i nie powinno to być kwestią mody, będącej wynikiem naśladownictwa standardów bezpieczeństwa i obyczajów przyjętych w krajach wysokorozwiniętych (ale i takich jak np. pustynny Oman – kraj wielbłądów i biometri), mocno akcentowanych, a nieraz zaczerpniętych z filmów (np. 2001: *Odyseja Kosmiczna*, 1968 rok – rozpoznawanie głosu; *Golden Eye*, 1995 rok – głos, dłoń, tęczówka; *Ultraviolet*, 2006 rok – DNA, głos, tęczówka, twarz i struktura czaszki, fizjologiczna budowa głowy, struktura skóry, metabolizm – puls, oddech, analiza poligraficzna, czyli tzw. multimodalna biometria etc.), lecz koniecznością wynikającą z ewolucji zagrożeń współczesnego świata.

Po 11 września 2001 r. przeprowadzono specjalne kontrole w zakresie bezpieczeństwa na 32 lotniskach w Stanach Zjednoczonych, a ich wyniki wykazały, że wstępna kontrola pasażerów na lotniskach w 70% przypadków nie chroni przed wnoszeniem noży, w 3% przypadków – broni palnej oraz w 60% – imitowanych materiałów wybuchowym (płynne, wieloskładnikowe materiały wybuchowe). Z pewnością analogię do tych wyników znajdziemy w innych portach lotniczych. Dlatego też środki bezpieczeństwa na lotniskach zostały udoskonalone. Administracja Bezpieczeństwa Transportowego (ang. *Transport Security Administration*, TSA) zajmuje się doskonaleniem procedur związanych z kontrolą bagażu i osób, jak również opracowuje nowe, bardziej efektywne metody kontroli, które umożliwią wykrywanie różnych rodzajów zagrożeń.

Z kolei zastosowanie biometrii we wstępnej kontroli pasażerów ogranicza ryzyko popełnienia błędu, jeżeli nie eliminuje go zupełnie (może jest to zbyt optymistyczne stwierdzenie, lecz wyniki realizowanych projektów w najbliższym czasie z pewnością zweryfikują tę tezę). Szanse na zidentyfikowanie przez system rozpoznawania twarzy nieprzebranego Osamy bin Ladena wchodzącego w tłumie na lotnisko wynosiłyby aż 60% (jakie jest prawdopodobieństwo, że zostałby on zidentyfikowany na podstawie zwykłej obserwacji prowadzonej przez wybranych pracowników służby ochrony np. w porcie lotniczym we Frankfurcie?). Z kolei zaledwie jedna osoba na sto mogłaby być fałszywie rozpoznana jako słynny terrorysta.

Pierwszym warunkiem sprostania zmianom jest wyzbycie się lęku przed nimi.

F. Znaniecki

Okazuje się, że przedstawiciele linii lotniczych i towarzystw handlowych bardzo zainteresowali się wynikami eksperymentów wykonanych niedługo po tragicznych wydarzeniach w Ameryce, w których to wykorzystywano różne metody biometrycznej kontroli. Rozpoczęto kampanię antyterrorystyczną na dużą skalę, związaną z pracami i projektami na rzecz nowych technologii bezpieczeństwa.

Dla przykładu, na początku 2005 roku władze lotnictwa cywilnego Francji (franc.: *Direction Générale de l'Aviation Civile* – DGAC) rozpoczęły projekt sześciomiesięcznej analizy metod biometrycznego rozpoznawania tożsamości

– na podstawie odcisku palca, wzoru tęczówki i rysów twarzy – na lotniskach w Bordeaux, Lille, Lyon, Nicei, Paryżu i Tuluzie. W Australii zostały zastosowane systemy rozpoznawania twarzy, które działają równolegle z tradycyjnymi punktami odpraw celnych. Odprawa z zastosowaniem czytnika twarzy trwa sześć sekund i jest niezwykle popularna. Obecnie 98% osób przekraczających australijską granicę wybiera właśnie biometryczną odprawę zamiast klasycznej (czas odprawy to minimum 2,5 min). Podobny system, bazujący na rozpoznaniu twarzy, chce także rozwijać Francja. Z kolei Wielka Brytania postawiła na urządzenia skanujące tęczówkę oka. System opracowywany w Wielkiej Brytanii ma pozwolić na skrócenie czasu odpraw celnych z dwóch minut do 20 sekund, przy jednoczesnym zwiększeniu bezpieczeństwa.

Dziś wiele lotnisk na całym świecie posiada systemy biometryczne w postaci projektów pilotażowych, np. dla wydzielonej grupy pasażerów lub pracowników. Dla przykładu, londyńskie lotnisko Heathrow wprowadziło program Międzynarodowego Zrzeszenia Przewoźników Powietrznych (ang. *International Air Transport Association*, IATA) mający na celu uproszczenie podróży pasażerom (ang. *Simplifying Passenger Travel Programme*), z wykorzystaniem wzoru tęczówki. Jego sztandarowym celem jest pogodzenie ze sobą dwóch biometrycznych sprzeczności, jakimi są bezpieczeństwo i wygoda. Wprowadzono do bazy danych wzorce tęczówki oka dwóch tysięcy stałych klientów. Klienci ci poruszają się w specjalnych strefach, przechodząc przez wydzielone punkty kontrolne – pozwalające na szybszą odprawę.

W lotniskowych projektach pilotażowych systemów kontroli dostępu dominują techniki rozpoznawania tęczówki oka, odcisku palca i systemy rozpoznawania twarzy 2D oraz 3D, a także geometria dłoni z dodatkowo zastosowaną analizą głosu (multibiometria), choć istnieje znacznie więcej biometrycznych technik uwierzytelniania, które posiadają wiele zalet i również mogą być z powodzeniem zastosowane w lotniskowej kontroli tożsamości. Inne formy biometrycznych zabezpieczeń to między innymi karty magnetyczne z informacjami o pracownikach i pasażerach bądź też biometryczny e-paszport. System identyfikacji personalnej pasażerów musi być w miarę szybki i przyjazny. Powinno się stosować w nim bezkontaktowe metody biometryczne. Ponadto przyszła taktyka nadzoru mogłaby umożliwiać wykrywanie podejrzanych ludzi na podstawie cech fizjologicznych albo widocznego, charakterystycznego zachowania.

Rys. 1. System rozpoznający tęczówkę oka – wybrany w 2004 r. do projektu pilotażowego biometrycznej kontroli granicznej (ang. Automated and Biometrics – Supported Border Controls*, ABG) w porcie lotniczym we Frankfurcie nad Menem.*

Do projektu włączyło się 17 krajów UE i Szwajcaria. Pasażerowie niemieckiej Lufthansy, którzy zainteresowali się programem i zamieszkują w krajach UE albo Szwajcarii, mogli zarejestrować swoje dane – tęczówkę oka. W sumie zainstalowano siedem systemów rozpoznających tęczówkę oka przy punktach kontroli granicznej lotniska.

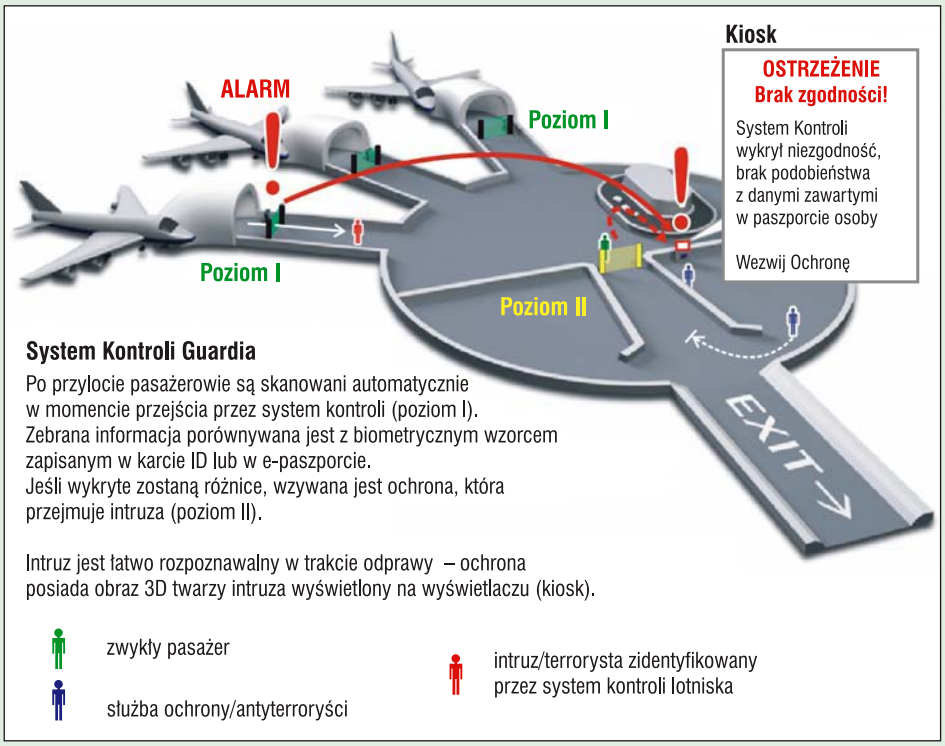
Osoba mająca poddać się biometrycznej kontroli podchodzi do specjalnego kiosku – urządzenia kontroli. Gdy stoi przed urządzeniem skanującym tęczówkę oka, np. firmy Oki –iris, kamera systemu automatycznie pozyskuje wzór tęczówki i weryfikuje tożsamość w kilka sekund (następuje dopasowanie pozyskanego wzorca biometrycznego z wzorcem zawartym w paszporcie oraz sprawdzenie danych osobowych odczytanych poprzez skanowanie MRTD strony personalizacyjnej paszportu przed wejściem do kiosku, z danymi dostępnymi w istniejących bazach danych).

Należy pamiętać, że obok systemów biometrycznego uwierzytelniania, porty lotnicze wykorzystują wiele innych systemów wpływających na bezpieczeństwo pasażerów. Obecnie wiele firm łączy wysiłki by zaoferować zintegrowane rozwiązania w dziedzinie bezpieczeństwa lotnisk integrujące systemy zarządzania, systemy bazodanowe i inne zaawansowane aplikacje IT, systemy dźwiękowego ostrzegania, ochrony ppoż., sterowania monitoringiem CCTV i właśnie biometryczną identyfikacją, systemy sterowania zasilaniem elektrycznym i klimatyzacją, systemy komunikacji i łączności alarmowej oraz zautomatyzowane systemy dokowania samolotów, systemy rozwiązania oświetlenia pasu startowego itp.

Jest kilka gotowych do wdrożenia systemów biometrycznej kontroli tożsamości w infrastrukturze lotnisk. Na uwagę zasługuje firma Guardia A/S, zajmująca się biometrycznymi technologiami w systemach zabezpieczeń, oferująca system rozpoznający twarz. Guardia Control jest systemem kontroli, który skanuje twarz, tworząc jej obraz w trzech wymiarach (z dokładnością do 1 mm), mierzy temperaturę skóry (z dokładnością do 0,2°C) i tworzy trójwymiarowy model twarzy. Powstaje trójwymiarowy model wizerunku twarzy oraz trójwymiarowy model termiczny twarzy. Na podstawie tych modeli z około 300 punktów charakterystycznych ustala się wzorzec biometryczny. Skanowanie temperaturowe w zakresie podczerwieni dodatkowo może dostarczyć informacji np. o chorobie osobnika. Zaletą systemu jest to, że działa w pełni autonomicznie, nie angażując żadnych osób w proces skanowania. Urządzenia skanujące nie są narażone na zabrudzenia wynikające z kontaktu fizycznego, jak w przypadku metod skanowania odcisku palca czy dłoni (również preferowanych w systemach ochrony lotnisk), i nie angażują naszej uwagi podczas procesu pobierania wzorca.

Specjaliści od biometrycznego systemu kontroli Guardia twierdzą, że technologia rozpoznawania 3D jest najbardziej godna zaufania i użyteczna dla celów bezpieczeństwa na rynku, a rozpoznawanie 2D i inne biometryczne systemy znajdą tylko ograniczone zastosowanie (wyniki projektów pilotażowych prowadzonych przez Guardia A/S, w których użyto odcisków palca, rozpoznawania twarzy 2D, tęczówki oka, analizy podpisu odręcznego i głosu, uwidaczniają ich niską niezawodność – pomiędzy 40% a 60% – w stosunku do zaprezentowanego systemu).

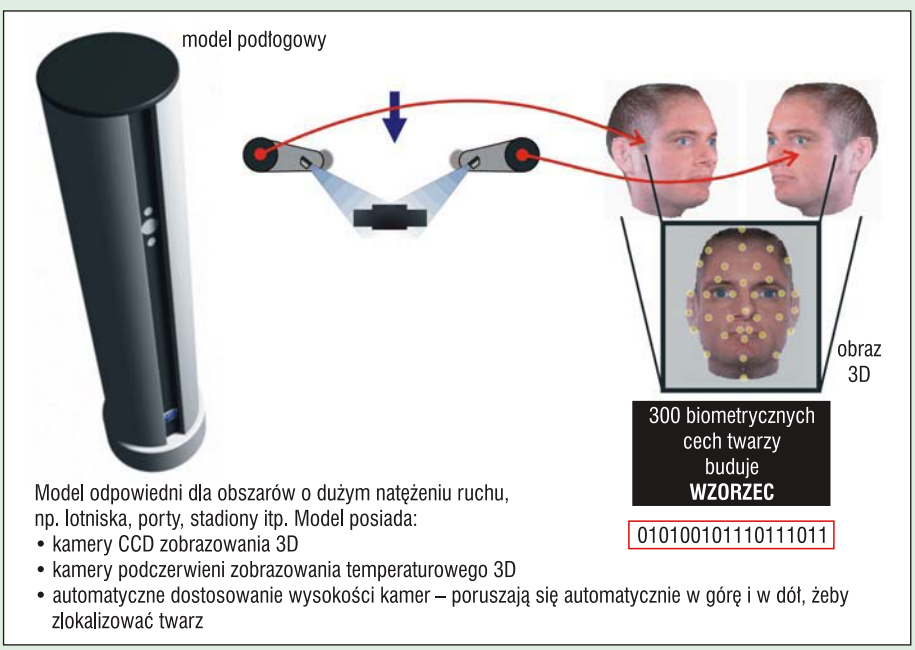
Niezwykle ciekawy jest projekt Cogito izraelskiej firmy Suspect Detection Systems Ltd. W sierpniu 2006 r. opublikowano, że spółka opracowała biometryczny system (biometryczny wykrywacz



Rys. 2. Zasada działania biometrycznego systemu kontroli Guardia (Guardia A/S; http://www.guardia.dk)

poddają swój dokument – paszport, dowód itp. – do skanowania. Następnie system zadaje pytania – są one wyświetlane na panelu dotykowym (np.: *Czy posiadasz materiały, przedmioty sklasyfikowane jako niebezpieczne? Czy posiadasz nielegalne narkotyki?* Odpowiedź musi być jednoznaczna i brzmi zawsze: tak albo nie) – i rejestruje odpowiedzi i zachowanie kontrolowanego, na bieżąco przesyłając uzyskane dane do stacji nadzorczej. System Cogito przeszedł pomyślnie testy TSA oraz izraelskich służb bezpieczeństwa.

Czego system szuka? Wzorów zachowań, które wskazują na coś, czym można scharakteryzować wszystkich potencjalnych sprawców, a mianowicie na obawę bycia złapanym! System może izolować tych podejrzanych, kłamstw) do wykrywania nienaturalnych zachowań, emocji podczas odpowiedzi na serię wyselekcjonowanych pytań, na podstawie których można domniemać złe zamiary podróżnego. System, nazwany Cogito, używa technik wzorowanych na badaniach poligraficznych. W ciągu kilku minut system określa, czy pasażer może kontynuować podróż, czy też powinien być poddany dalszej i bardziej szczegółowej kontroli.



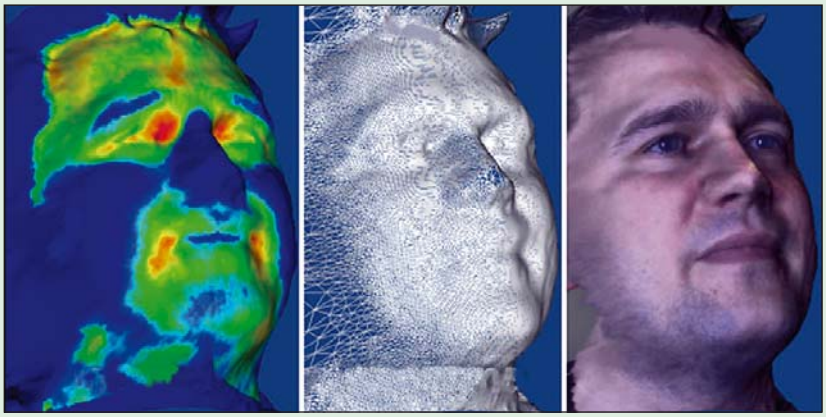
Rys. 3. Model podłogowy biometrycznego systemu kontroli Guardia. System skanuje wizerunek twarzy oraz obraz rozkładu temperatury skóry w formacie 3D i na podstawie tych modeli z około 300 punktów charakterystycznych ustala wzorzec biometryczny

Suspect Detection to technologia, która wykorzystuje oprogramowanie emulujące oficera dochodzeniowego, ujawniającego modus operandi sprawcy. Na system bazujący na technologii *Suspect Detection* składa się:

– *Test Station* – stacja dokonująca pomiaru – ergonomiczny kiosk funkcjonujący jako punkt, w którym dokonuje się badania poligraficznego (bazującego na wskazaniach biologicznego sprzężenia zwrotnego);

– *Back Office* – jednostka centralna przeznaczona do zarządzania i kontroli wszystkich stacji dokonujących pomiarów. Jednostka ta przechowuje wszystkie wyniki testów i profile podróżnych i jest odpowiedzialna m.in. za dystrybucję danych i połączenie z zewnętrznymi systemami i bazami danych.

System testowany był m.in. na lotnisku w Knoxville. Pasażerowie poddawani kontroli siadają w specjalnej kabinie (kiosku) przed komputerem (panelem dotykowym) i czytają instrukcje. Zakładają słuchawki, by słyszeć polecenia systemu, wkładają dłoń w sensor badający tętno i ciśnienie krwi oraz rzy kwalifikują się do drugiego etapu badania, prowadzonego przez wytrenowanych, doświadczonych badaczy (psychologów). Badania wykazują, iż system jest w wysokim stopniu dokładny i skuteczny (najwyżej czteroprocentowe prawdopodobieństwo wystąpienia fałszywego alarmu). Jest również bardzo elastyczny – może mieć różne zastosowania, np.:



Rys. 4. Model 3D. Na podstawie modelu 3D tworzony jest wzorzec wyznaczony przez 300 charakterystycznych punktów twarzy, który jest później przechowywany w bazie danych.

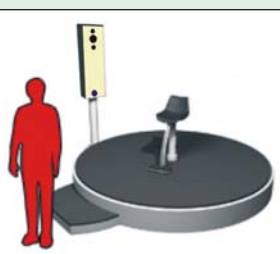
Trójwymiarowy obraz twarzy zawiera więcej informacji niż płaskie zdjęcie w formacie 2D. Model 3D zawiera informację o głębi (jak długi jest nos, jak głęboko osadzone są oczodoły etc.), która umożliwia wizualizację twarzy z każdej strony i pod każdym kątem. System dostarcza wystarczającą ilości informacji do tego, by układ sterowania zbudował, w kombinacji z trójwymiarową mapą podczerwieni – IR, model twarzy.

Podczerwień. Ludzie widzą widmo światła dlatego, że fale o określonej długości pobudzają receptory oka. Kolory w widmie świetlnym występują w następującej kolejności: czerwony, pomarańczowy, żółty, zielony, niebieski, indygo, fiolet. Wynika to z faktu, że każdy z tych kolorów ma inną długość fali. Postrzegamy światło o największej długości fali jako kolor czerwony (ok. 780 nm), natomiast światło o najkrótszej długości fali – jako kolor fioletowy (ok. 380 nm). Zakres długości fal, które widzi człowiek, nosi nazwę „światła widzialnego". Światło o długości fali większej niż najdłuższa fala z zakresu widzialnego nazywane jest promieniowaniem podczerwonym (od 760 nm do ok. 2 mm fal radiowych). Oko ludzkie nie jest w stanie dostrzec promieni podczerwonych, można je tylko zmierzyć. Promieniowanie to emitowane jest przez ciepłą twarz, a jego rozkład zależy od temperatury poszczególnych części twarzy. Detektory podczerwieni, z których zbudowana jest kamera podczerwieni, wykrywają promieniowanie IR (ang. infra-red), a układ sterowania kamery pozwala stworzyć termiczną mapę twarzy z rozdzielczością (zdolnością rozdzielczą) 0,08°C

Model siatkowy. Model siatkowy twarzy (tzw. obraz szkieletowy) to wizualna prezentacja elektronicznej reprezentacji trójwymiarowego fizycznego obiektu używana w komputerowej grafice 3D. Model siatkowy jest tworzony przez wyodrębnienie każdej krawędzi obiektu (np. twarzy), gdzie dwie matematycznie ciągłe gładkie powierzchnie spotykają się, albo przez połączenie składowych wierzchołków obiektu (twarzy) za pomocą linii prostych albo krzywych. Obiekt (twarz) jest widoczny na ekranie komputera w postaci rysunku linii (tworzących model siatkowy) będących stykiem każdej krawędzi. Model siatkowy pozwala na elektroniczną wizualizację obiektu fizycznego w formacie 3D.

– w walce z terroryzmem,
– w ochronie portów lotniczych i morskich,
– w kontroli granicznej,
– w kontroli imigracyjnej,
– w zapobieganiu przerzutu narkotyków,
– w pracach organów dochodzeniowo-śledczych policji,
– w ochronie zakładów penitencjarnych,
– w przeciwdziałaniu korupcji,
– w procesie naboru kadr.

Inny projekt zasługujący na uwagę to miSense, będący kolejną „biometryczną próbą ułatwienia podróży i sprawienia, by była ona bezpieczniejsza. IATA uruchomiło na lotnisku w Heathrow program uproszczenia ruchu pasażerów (ang. *Simplifying Passenger Travel,* SPT), obejmujący testy nowych technologii i rozwijanie nowych projektów, czyniących podróż przyjemniejszą i bezpieczną. Program objął wszystkich klientów podróżujących z lotniska Heathrow (terminal 3) do Hong Kongu liniami Cathay Pacific, a także do Dubaju, liniami Emirates. Wykorzystano system biometrycznego rozpoznawania tożsamości miSense.



Model z krzesłem

Model z krzesłem do rejestracji ludzi w bio-bazie danych:
- kamera CCD
- kamera podczerwieni – pomiar temperatury
- krzesło
- ruchoma podstawa

Rys. 5. Model do rejestracji (ang. enrolment) w systemie Guardia. Krzesło obraca się tak, by kamery stworzyły model fizyczny 3D twarzy osoby, a system skatalogował uzyskany wzorzec w bazie danych biometrycznych.

Koncepcja programu SPT bazuje na automatycznym przetwarzaniu danych pasażerów „znanych", przez co uwaga zostaje skupiona na pasażerach „nieznanych" – to wśród nich poszukuje się potencjalnych intruzów (przyrost bazy danych znanych użytkowników zmniejsza krąg podejrzanych). SPT ma na celu optymalne powiązanie kluczowych elementów procesu podróży, takich jak pasażerowie, linie lotnicze, porty lotnicze, władze kontroli i dostawcy technologii. Program ten koncentruje swoje wysiłki na całym procesie podróży, ujmując problem bezpieczeństwa całościowo, a nie na poszczególnych jego elementach, za które każda z zaangażowanych stron jest odpowiedzialna.

Sam projekt SPT wykorzystujący system miSense trwał do końca stycznia 2007 roku. Pasażerowie podróżujący na określonych trasach byli zapraszani przy punktach odprawy do wzięcia udziału w projekcie. Skanowano ich paszporty i pobierano wzorzec odcisku palca wskazującego prawej dłoni w specjalnie zaprojektowanym samoobsługowym kiosku miSense. Zebrane dane (przechowywane na czas lotu w bazie *United Kingdom Immigration Service* i, ze względu na ochronę danych osobowych, kasowane po zakończeniu lotu) umieszczano na mikroprocesorowej karcie wstępu, która, po potwierdzeniu tożsamości poprzez zeskanowanie odcisku palca, pozwalała na sprawny dostęp do stref bezpieczeństwa i samolotu. Druga część projektu, miSenseplus, uzupełniała zamieszczone w rejestrze bazy biometrycznej dane podróżnego poprzez rejestrację dziesięciu odcisków palców, jednej fotografii twarzy i szczegółowego obrazu obu oczu (wykorzystanie multimodalnego systemu biometrycznego). Na podstawie tych danych wydawana była osobista karta członkostwa miSenseplus. Programy miSense i miSenseplus łączyły wysiłki

Rys. 6. „Test Station" – stacja dokonująca pomiaru – urządzenie izraelskiej firmy Suspect Detection Systems Ltd. (SDS) – Cogito 1002, które bada, np. w trakcie kontroli granicznej, czy osoba wchodząca na pokład samolotu nie ma złych zamiarów, czegoś nie ukrywa. Jest w pełni zautomatyzowanym systemem, nie wymagającym ludzkiej kontroli. (źródło: www.suspectdetection.com)

służb imigracyjnych Wielkiej Brytanii i Hongkongu, by stworzyć międzynarodową, zautomatyzowaną, szybką usługę kontroli paszportowej. Trzecia część projektu, miSenseallclear, miała na celu wykorzystanie zewnętrznych źródeł informacji o pasażerze (takich, jak wywiad, krajowe rejestry policyjne i sądowe) do zebrania kluczowych informacji o przeszłości kryminalnej (terrorystycznej) pasażera (ang. *Advance Passenger Information*, API). Po zarejestrowaniu się system ten miał w jak najkrótszym czasie umożliwić połączenie pomiędzy systemem bezpieczeństwa portu lotniczego a rządowym systemem analizy danych. Ideę tę próbują wykorzystywać z powodzeniem takie kraje, jak Australia, Bahrajn, Kuwejt i Nowa Zelandia.

Do końca 2007 r. mają zostać określone zasady działania ogólnoświatowego systemu danych biometrycznych (wykorzystującego dane policyjne, administracyjne itp. z poszczególnych krajów dla wspólnych celów), co niewątpliwie przyspieszy wdrażanie systemów biometrycznych na lotniskach i wpłynie na ich skuteczność.

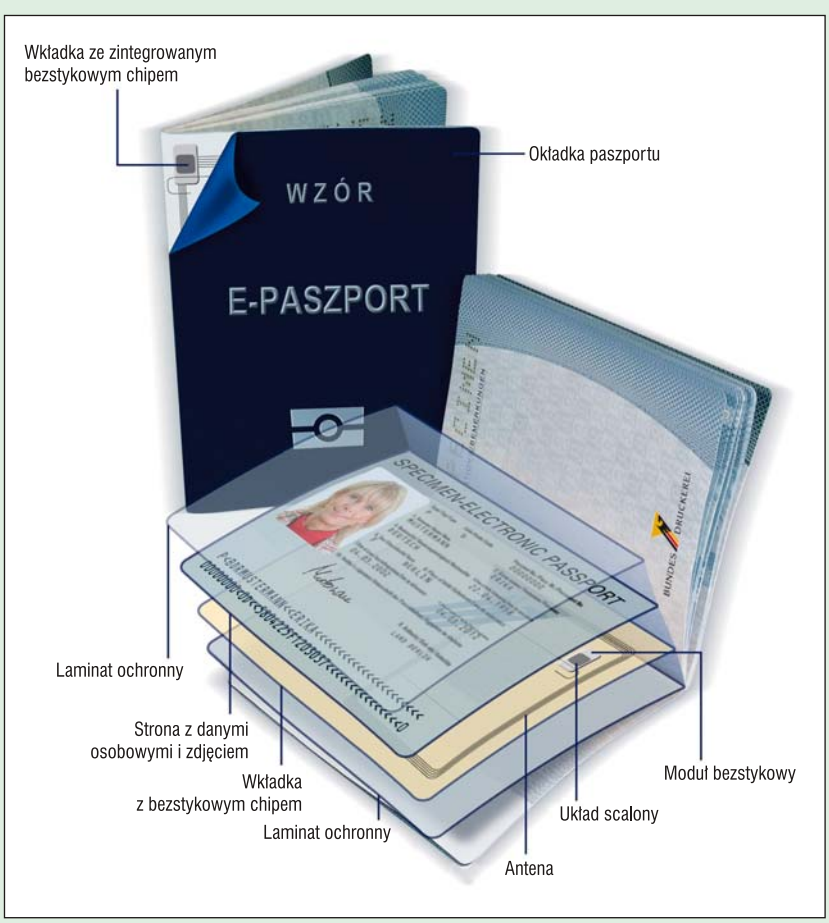
W styczniu 2006 roku na międzynarodowym lotnisku w San Francisco rozpoczęto program testujący paszport elektroniczny (e-paszport). Pomysł szybkiego wprowadzenia paszportów wyposażonych w elektroniczne identyfikatory powstał w USA przed pięcioma laty. Amerykanie zdecydowali w uchwalonym wówczas pakiecie ustaw *Patriot Act* (uchwała z dnia 26 października 2001 roku), że wszyscy cudzoziemcy przybywający do USA muszą posiadać paszport obdarzony namiastką „inteligencji" lub wizę wyposażoną w elektroniczny identyfikator. Oczywiście celem takich posunięć jest przeciwdziałanie fałszerstwom dokumentów tradycyjnych oraz kradzieży dokumentów na zamówienie.

Testy elektronicznego paszportu przeprowadzono w czterech krajach: Stanach Zjednoczonych, Australii, Nowej Zelandii i Singapurze. Celem testów było zebranie informacji, które mogłyby ułatwić innym krajom decyzję o wprowadzaniu w życie e-paszportów. Elektroniczny paszport powstał w oparciu o standardy wypracowane przez Międzynarodową Organizację Lotnictwa Cywilnego (ang. *International Civil Aviation Organization*, ICAO).

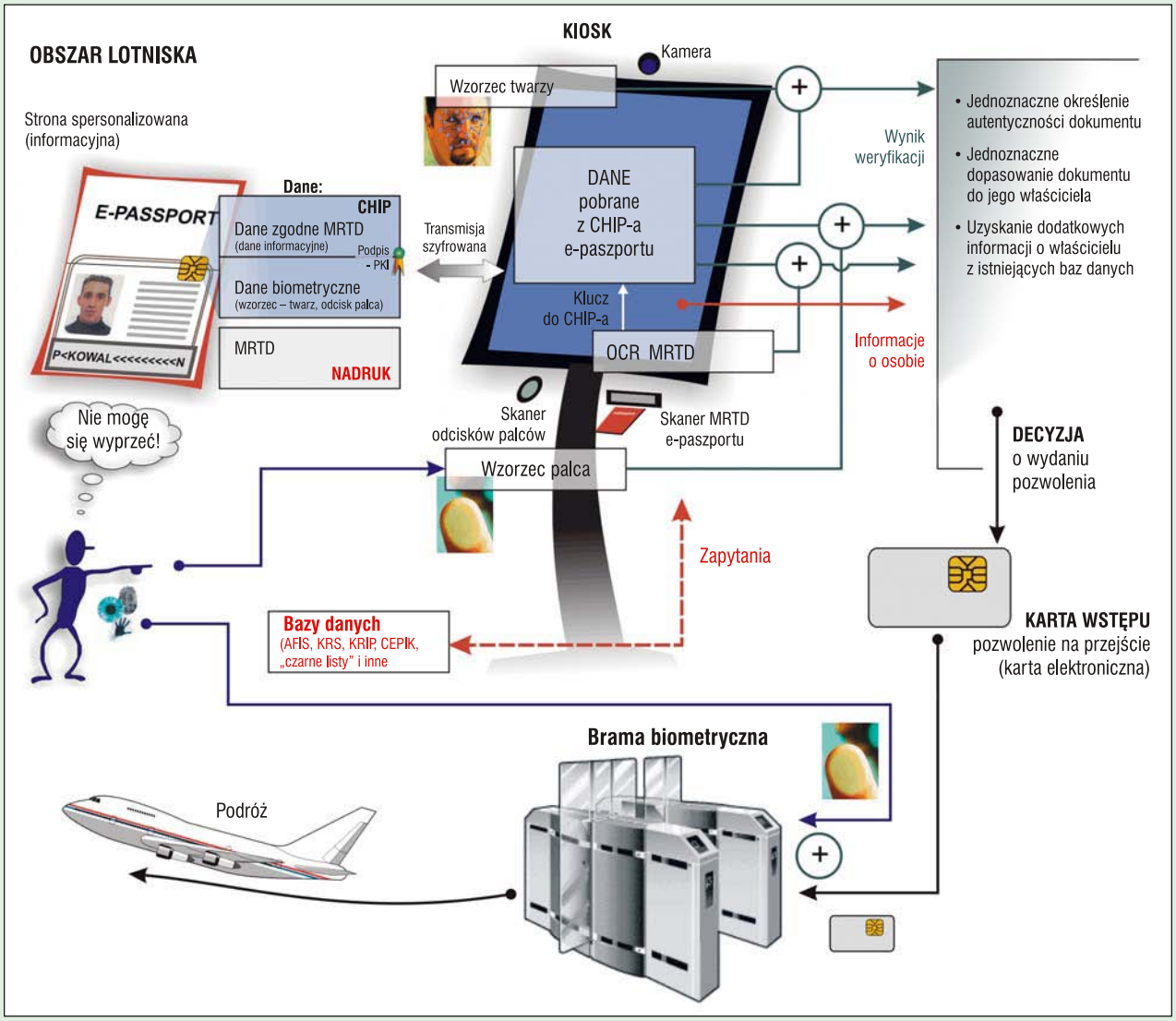
ICAO, mając na względzie chęć zdecydowanie lepszego powiązania dokumentów z ich właścicielami, od dawna, bo już od 1997 roku, prowadziła prace nad rozszerzeniem specyfikacji dotyczącej maszynowego czytania dokumentów podróży, czyli MRTD (ang. *Machine Readable Travel Documents*). W ramach tychże prac dążono do rozszerzenia obowiązujących zaleceń o dodatkowe wskazania, które dotyczyłyby zabezpieczeń biometrycznych. Prace te uległy gwałtownemu przyśpieszeniu po atakach na WTC.

W listopadzie 2003 r. ICAO przedstawiła opinii publicznej pierwsze wstępne wymagania stawiane nowym dokumentom podróżnym. ICAO zdecydowała się na wykorzystanie istniejącego od 2001 roku międzynarodowego standardu ISO 14443, opisującego techniki identyfikacji związane z użyciem bezstykowych kart mikrochipowych. Zgodne z tym standardem karty i czytniki używają do komunikacji technologii RFID (częstotliwość 13,56 MHz). Aby mogła nastąpić komunikacja, karta musi zostać zbliżona do czytnika na odległość co najmniej 10 cm. Standard opisuje jedynie sposób komunikacji pomiędzy kartą a czytnikiem, nie rozwiązuje jednak kwestii bezpieczeństwa komunikacji.

Specyfikacje ICAO sugerują różne warianty umieszczenia danych biometrycznych w paszporcie. Jedne z nich przewidują lokalizację układu elektronicznego



Rys. 8. Elektroniczny układ bezstykowy może być zintegrowany z okładką paszportu lub stroną spersonalizowaną.
Źródło: Bundesdruckerei GmbH (http://www.bundesdruckerei.de)



Rys. 9. Przykładowa koncepcja biometrycznego systemu wspomagającego ochronę lotniska

w którejś z okładek. Inne zalecają zamieszczenie anteny i układu elektronicznego w karcie spersonalizowanej, zawierającej dane osobowe. Do umieszczenia wspomnianych elementów w karcie wykorzystuje się folię poliwęglanową, podobnie jak w przypadku klasycznych kart plastikowych, stosowanych np. w systemie komunikacji miejskiej. Inną możliwością jest umieszczenie układu elektronicznego pomiędzy stronami wizowymi paszportu.

Standardy ICAO przewidują także zastosowanie mechanizmów bezpieczeństwa, których celem jest minimalizacja zagrożeń wynikających z potencjalnych prób fałszowania paszportów oraz uniemożliwienie odczytu danych bez otwierania dokumentu.

Kierując się zaleceniami organizacji ICAO oraz wymaganiami administracji USA, Unia Europejska rozpoczęła prace nad określeniem własnych wymagań dotyczących paszportów zawierających zapisane w formie cyfrowej dane biometryczne, zgodnych ze standardem komunikacji kart bezstykowych ISO 14443. W wyniku prac Rada Europy wydała dnia 13 grudnia 2004 roku rozporządzenie (nr 2252/2004) w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie Unii Europejskiej.

Polski paszport biometryczny spełnia zalecenia Unii Europejskiej oraz jest w pełni zgodny z międzynarodowym standardem ISO 14443. Układ elektroniczny z danymi biometrycznymi wraz z anteną został umieszczony wewnątrz strony zawierającej odpowiednio sformatowane zdjęcie oraz dane właściciela. Paszport jest podobny do wcześniejszych i oprócz zabezpieczeń biometrycznych posiada również szereg innych (m. in. odpowiednio zabezpieczony papier ze znakiem wodnym). W układzie elektronicznym zarejestrowany jest biometryczny wzorzec twarzy właściciela, a także inne dane personalne, termin ważności oraz dodatkowe dane potwierdzające, że informacje przechowywane w układzie zostały zapisane przez uprawniony do tego organ (jest to po prostu cyfrowe odzwierciedlenie tekstu wydrukowanego na stronie spersonalizowanej paszportu). Dokument uniemożliwia odczytanie danych zapisanych w układzie elektronicznym bez otwarcia książeczki. W systemie paszportowym przewidziano również możliwość rozwoju paszportów poprzez zastosowanie w nich innych technologii biometrycznych, m.in. wykorzystujących wzór tęczówki oka czy też odciski palców (wymóg obowiązuje od dnia 28 lutego 2008 roku).

W australijskim paszporcie elektronicznym chip (zwykle 32–64 kB pamięci) jest osadzony w centrum strony. Przechowuje on cyfrową kopię fotografii oraz dane: imię, nazwisko, płeć, datę urodzenia, narodowość, numer paszportu i datę wygaśnięcia jego ważności. Jest to ta sama informacja, która znajduje się na wydrukowanej stronie personalizacyjnej (informacyjnej) każdego

paszportu. Dane w postaci cyfrowej pozwalają na wykrycie fałszerstwa informacji drukowanych lub zdjęcia poprzez porównanie zawartości cyfrowej i wydrukowanej. Technologia rozpoznawania twarzy użyta w e-paszporcie ulepszy sprawdzanie tożsamości (automatyczne porównanie cyfrowego wzorca z galerią istniejących zdjęć terrorystów) i ograniczy sensowność kradzieży takiego paszportu.

Dane zapisane w mikroukładzie będą chronione poprzez Infrastrukturę Klucza Publicznego (ang. *Public Key Infrastructure,* PKI) gwarantującą, że dane zostały wprowadzone do chipa przez certyfikowaną jednostkę, że są kompletne i do chwili obecnej nie zostały zmienione. Podpis cyfrowy chipa odpowiada wymaganiom ICAO. Algorytm *Basic Access Control* (BAC) zapobiega uzyskaniu dostępu do danych umieszczonych na chipie do momentu aż MRZ rozpocznie proces czytania przez specjalny skaner OCR. Technologia *Basic Access Control* wykorzystuje klucz elektroniczny, uzyskiwany dzięki odczytaniu danych wydrukowanych w paszporcie, do odblokowania danych w mikroukładzie, a cyfrowy podpis chroni integralność tych cyfrowych danych. BAC i PKI na dzień dzisiejszy czynią e-paszport dokumentem wysoce bezpiecznym.

Rys. 10. Australijski e-paszport, wprowadzony 24 października 2005 r. MRZ – pas na stronie personalizacyjnej (informacyjnej) czytelny dla urządzenia z czytnikiem MRTD.
Źródło: www.dfat.gov.au/dept/passports

Tradycyjna lotniskowa odprawa graniczna jednej osoby trwa od półtorej do 2,5 minuty (pomijając przypadki kontroli szczegółowej). Według testów ICAO odprawy automatyczne nie trwają dłużej niż pół minuty, z czego większość czasu zajmują czynności pasażera (wyjęcie paszportu, jego odpowiednie umieszczenie w czytniku, wyjęcie z czytnika). Ponieważ strona paszportu zawierająca drukowane dane pasażera spełnia wymagania MRTD, kontrolę można w całości scedować na system kontroli.

Wygoda oraz oszczędność czasu pasażerów i personelu jest wielkim plusem wynikającym z zastosowania paszportów elektronicznych. Jednakże z wprowadzeniem takich paszportów wiążą się liczne (nawet banalne na pierwszy rzut oka) problemy.

Pierwszym z nich jest na pewno zagrożenie w ujęciu zdrowotnym. Powszechnie nagłaśniany jest problem szkodliwego dla zdrowia działania pola elektromagnetycznego (nieuzasadniona obawa przed np. rozpoznawaniem tęczówki, czy też rzekomo szkodliwą emisją czytnika RFID), jak również chorób przenoszonych przez bezpośredni kontakt (SARS, żółtaczka). Jak na ironię, skutecznie odstrasza to zainteresowanych podniesieniem poziomu bezpieczeństwa. Trzeba jednak przyznać, że problemy te nie zostały do końca zbadane i nie można w 100% wykluczyć zasadności związanych z tymi – faktycznymi albo wyimaginowanymi – zagrożeniami obaw.

Kolejnym problemem wydaje się być nieznana trwałość paszportów. Zainteresowane strony wymagają zazwyczaj od producentów udzielenia 10-letniej gwarancji na trwałość dokumentu, obejmującej m.in. prawidłowe działanie wbudowanego układu elektronicznego. Czy jednak można aż tak zabezpieczyć układ elektroniczny przed wszelkiego rodzaju uszkodzeniami mechanicznymi, żeby przetrwał aż dziesięć lat? Wydaje się to niemożliwe.

Inne zagrożenie, które *de facto* wynika ze standardowego w wielu państwach 10-letniego okresu użytkowania paszportu, wiąże się z bezpieczeństwem przechowywanych w paszporcie i przetwarzanych z jego udziałem danych elektronicznych. Obecnie wydaje się, iż zastosowane w paszporcie techniki i algorytmy są bezpieczne, jednakże, jak pokazuje historia, wiele technik i algorytmów uważanych za niezawodne nie spełniło swego zadania. Przykładowo, holenderskiej firmie Riscure udało się wykazać możliwość przechwycenia danych wymienianych między holenderskim paszportem elektronicznym (wykorzystującym ten sam układ elektroniczny zgodny z ISO 14443 i standard szyfrowania BAC, jakie zastosowano w e-paszportach Stanów Zjednoczonych i innych krajów) a czytnikiem i rozszyfrowania zapisu wzorca biometrycznego oraz pozostałych danych personalnych. Ponadto, podczas ostatniej konferencji o tematyce hackerskiej Black Hat, niemieccy hackerzy zademonstrowali możliwość kopiowania zawartości układu elektronicznego paszportu, chociaż nie udało się im dokonać zmiany jego zwartości.

Kolejnym problemem wydaje się być sama dojrzałość technik biometrycznych i ich wykorzystanie w pełni bezobsługowych systemach kontroli. O ile w kryminalistyce automatyczne porównywanie odcisków palców podejrzanych wspomaga tylko pracę policjantów, w przypadku systemów automatycznych wykorzystanie biometrii (przy obecnym stanie wiedzy i techniki – patrz poprzednie numery *Zabezpieczeń*), mimo solidnych podstaw teoretycznych, jest swego rodzaju eksperymentem naukowym. Dopiero długotrwałe aplikacje praktyczne mogą zweryfikować, czy promowane rozwiązania z dziedziny bezpieczeństwa spełnią pokładane w nich nadzieje (osiągnięcie poprawności automatycznej weryfikacji/identyfikacji tożsamości osoby w różnych warunkach pracy, przy zapewnieniu jak największego komfortu i wygody).

Jeszcze innym problemem wydaje się być brak pełnej zgodności pomiędzy różnymi czytnikami paszportów i różnymi układami elektronicznymi, które mogą znaleźć zastosowanie w paszportach. Brak tej zgodności może wynikać z nie

do końca precyzyjnych zapisów standardu ISO 14443, będącego podstawą paszportów biometrycznych. W praktyce oznacza to, iż możemy znaleźć się w sytuacji, w której nasz polski paszport biometryczny nie zostanie odczytany i zweryfikowany, np. na lotnisku w Wenezueli.

Warto również wspomnieć o dość powszechnych obawach (nie wiadomo do końca, czy nieuzasadnionych) związanych z możliwością naruszania praw obywatelskich i utraty prywatności za sprawą nieuprawnionego odczytu zawartości układów elektronicznych w paszportach. Wydaje się jednak, iż prywatność może być znacznie bardziej i łatwiej naruszana w inny sposób (np. przez systemy monitoringu miast, telefony komórkowe, bazy danych obywateli i inne, związane z uczestnictwem obywateli w społeczeństwie wiedzy – banki i płatności elektroniczne, Internet itp.).

* * *

Obecnie świat oszalał na punkcie bezpieczeństwa. Jak nigdy dotąd zwiększyło się zapotrzebowanie na technologie weryfikujące tożsamość. Znajdują one zastosowanie w obiektach użyteczności publicznej (na stadionach, w centrach handlowych, portach lotniczych czy też na przejściach granicznych). W większości przypadków technologie te wykorzystywane są eksperymentalnie i mają jedynie na celu wspomagać odpowiedzialne służby. Być może w przyszłości role ulegną zamianie i to człowiek będzie je wspomagać, a zadania przejmą systemy i urządzenia wykorzystujące te technologie.

Zdajemy sobie sprawę, że coraz to nowsze rozwiązania techniczne inspirowane są wzrostem zagrożeń i mają na celu poprawę naszego bezpieczeństwa. Z drugiej jednak strony obawiamy się, iż rozwiązania te umożliwią, na wzór Wielkiego Brata, inwigilację i ogromne sproceduralizowanie naszego życia. Musimy być jednak świadomi faktu, iż przed postępem nie ma odwrotu. Powinniśmy pogodzić się z myślą, że dla poczucia bezpieczeństwa warto w pewnym stopniu ograniczać swoją wolność i prywatność.

* * *

W Polsce, na konferencji Wymagania Techniczne w Bezpieczeństwie Lotniczym (Wrocław, 19–21 października 2005 r.) można było odnieść wrażenie, że biometria w bezpieczeństwie polskich lotnisk może być zaledwie dodatkiem, który raczej ubogaca design niż ulepsza system bezpieczeństwa. Pojawiała się również sugestia, jakoby poprawa bezpieczeństwa na lotnisku miała zależeć od szeregu dodatkowych, różnorodnych kontroli, i zaostrzenia procedur bezpieczeństwa – nieco ulepszonych, ale zasadniczo takich samych, jak dotychczas. Warto zauważyć, że w przypadku kilku tysięcy lotów dziennie (w USA jest ich codziennie około 65 000) wzmożenie tradycyjnych kontroli jest fizycznie niemożliwe. Największy entuzjazm na konferencji wzbudziła instytucja tzw. skymarshala, strażnika obecnego podczas każdego lotu, uzbrojonego i dobrze wyszkolonego, czuwającego nad bezpieczeństwem pasażerów. Taki rodzaj „narzędzia" bezpieczeństwa w świadomości podróżnych daje większą gwarancję bezpieczeństwa, ale dla terrorystów przygotowujących atak może być swoistym ułatwieniem: po co przemycać broń na pokład samolotu – ona już tam jest...

Ireneusz Krysowaty
Paweł Niedziejko
WEL WAT

KABE

Najnowsza
technologia ochrony
rozległych terenów zewnętrznych

RADARY

Idealne zabezpieczenie
dla lotnisk i baz wojskowych


Radar RDTS
na granicy USA


Wizualizacja PSRS
z kamerą THV


Radar PSRS
z kamerą THV

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

KABE

43-190 MIKOŁÓW
ul. Waryńskiego 63

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

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

artykuł sponsorowany

Bezdotykowe karty inteligentne
HID iCLASS 13,56 MHz

Przygotowane z myślą o przyszłości

Obecnie większość użytkowników systemów kontroli dostępu wybiera technologię zbliżeniową, działającą na niskiej częstotliwości 125 kHz i uważaną za bezpieczną, wygodną oraz ekonomiczną. Umożliwia ona jedynie odczyt danych, co oznacza, że nie da się dopisywać, usuwać lub modyfikować informacji znajdujących się na karcie zbliżeniowej. W kontroli dostępu nie stanowi to problemu, ponieważ odpowiedzialne za nią systemy odczytują numer seryjny karty i za jego pomocą dokonują w systemie komputerowym tych decyzji, które są do niego przypisane. Jednak w innych branżach rozwinięto oprogramowanie wykorzystujące numery seryjne kart do bardziej różnorodnych zastosowań, na przykład do kontroli obecności, logowania do sieci komputerowych oraz obsługi internetowych punktów sprzedaży. Zamierzeniem twórców tych rozwiązań było umożliwienie użytkownikom szerszego zastosowania posiadanych kart.

Choć technologia zbliżeniowa przez wiele lat stanowiła akceptowalne rozwiązanie, postęp technologiczny sprawił, że użytkownicy wyrażają dziś duże zainteresowanie inną technologią – „inteligentnymi" kartami. Słyszy się obecnie liczne głosy stwierdzające, że stanowią one przyszłość branży zabezpieczeń

Inteligentne karty i rynek zabezpieczeń elektronicznych

Na pierwszy rzut oka inteligentna karta to mały kawałek plastiku o wielkości karty kredytowej z zatopionym chipem. Do niedawna technologia ta była stosowana głównie do zbierania opłat drogowych oraz bezpiecznego logowania się do sieci komputerowych. Jednak w opublikowanym przez Freedonia Group raporcie World Smart Card oceniono, że światowe zapotrzebowanie na ten typ kart będzie wzrastać jedenastokrotnie co roku, począwszy od roku 2006. Chociaż pozostaną one najbardziej rozpowszechnione w komunikacji i handlu, wyraźnie zwiększy się liczba zastosowań rządowych i instytucjonalnych. Będą one stosowane częściej także do automatycznej identyfikacji i w systemach zabezpieczeń.

Eksperci zgadzają się, że aby taki gwałtowny wzrost udziału inteligentnych kart w rynku zabezpieczeń rzeczywiście nastąpił, muszą one posiadać wszystkie zalety kart zbliżeniowych, czyli oferować bezpieczeństwo, wygodę oraz korzyści ekonomiczne. Właśnie dlatego narodziła się w firmie HID *smart card* 13,56 MHz!

Podstawową barierą dla szerszego wykorzystania tej technologii w systemach zabezpieczeń były do tej pory czynniki ekonomiczne. Jednak rozwój tego rodzaju zastosowań będzie napędzany przez spadające koszty instalacji i rosnącą łatwość zastosowania.

HID wprowadza iCLASS na rynek zabezpieczeń elektronicznych

Jako lider rynku, HID oferuje również rozwiązania działające na częstotliwości 13,56 MHz Seria *iCLASS* obejmuje następujące urządzenia:

– czytniki i urządzenia umożliwiające odczyt i zapis danych,
– czytniki i urządzenia umożliwiające odczyt i zapis danych wyposażone w klawiaturę,
– kompletną rodzinę identyfikatorów (karty, klucze i zawieszki), dostępną w wariancie 2 kb (256 bajtów) lub

16 kb (2 kB), z obszarem pamięci zarezerwowanym dla dwóch lub 16 aplikacji,
– moduły urządzenia umożliwiającego odczyt i zapis danych do wykorzystania w produkcji OEM,
– programator identyfikatorów i zestaw do rozbudowy oprogramowania (SDK),
– czytniki biometryczne.

Urządzenia *iCLASS* są zgodne z następującymi normami ISO:
– 15693 – identyfikatory *iCLASS* umożliwiające odczyt lub odczyt i zapis 2 kb lub 16 kb;
– 14443A – urządzenia tylko do odczytu; standard MIFARE (numer seryjny);
– 14443B2 – identyfikatory *iCLASS* umożliwiające odczyt lub odczyt i zapis, 16 kb.

Zastosowania produktów *iCLASS* obejmują kontrolę dostępu, bezpieczną identyfikację w IT, obsługę bankomatów oraz zdalnej sprzedaży, identyfikację osób na podstawie zdjęć, identyfikację pojazdów, kontrolę trasy patrolowania, parkingów oraz procesów produkcji, weryfikację biometryczną, a także kontrolę czasu pracy i obecności.

Wymagania użytkowników

Od momentu wprowadzenia na rynek urządzenia *iCLASS* pojawiły się w dużych instytucjach finansowych, na uniwersytetach, w agendach rządowych, sklepach, szpitalach i fabrykach. Poniżej przedstawiono niektóre powody wyboru *iCLASS*.

1. *iCLASS* oferuje łatwość instalacji oraz przygotowuje użytkownika pod kątem przyszłych rozwiązań. Dzięki rozwiązaniom firmy HID, które umożliwiają korzystanie z jednej karty w różnych zastosowaniach, można ograniczyć inwestowanie w istniejące systemy, a jednocześnie łatwo je unowocześnić, podążając za nowymi technologiami. Ponadto program HID Connect ułatwia dodawanie nowych aplikacji.

2. *iCLASS* pozwala dostosować istniejącą technologię do nowego systemu. Ponieważ większość oprogramowania kontroli dostępu nie potrafi odczytać pełnego numeru seryjnego karty bez jego skracania, uniemożliwia to duplikowanie numerów kart. Dodatkowo, dla użytkowników posiadających wielosystemowe identyfikatory, standardowy format zbliżeniowy oraz *iCLASS* można połączyć tak, że użytkownik posiada tylko jeden wpis w bazie danych.

3. *iCLASS* umożliwia zapisanie wielu aplikacji na jednej karcie. Wśród danych mogą znajdować się numery PIN oraz wzorce biometryczne, co pozwala na budowę wielopoziomowych systemów zabezpieczeń.

4. *iCLASS* jest przystępny cenowo. W zależności od typu identyfikatora, koszt systemu dostępu wykorzystującego technologię *iCLASS* 13,56 MHz może być porównywalny z kosztem rozwiązań wykonanych w technologii zbliżeniowej 125 kHz (albo taki sam).

Migracja technologii

Wiele organizacji zainwestowało już w kontrolę dostępu starszego typu, a jednak chcą one poszerzać swoje systemy o nowe aplikacje. Wiodący uniwersytet w Wielkiej Brytanii zdecydował się na instalację *iCLASS* i obecnie przechodzi z technologii pasków magnetycznych na technologię *iCLASS*. Zastosowane karty będą początkowo posiadały również paski magnetyczne przystosowane do istniejących czytników, ale w przyszłości urządzenia te będą również stopniowo zastępowane technologią *iCLASS*.

Wiele zastosowań, jedna karta

Liczne uniwersytety na świecie unowocześniają swoje systemy kontroli dostępu. Dawniej student mógł posiadać nawet cztery karty do różnych celów – kontroli dostępu, zdalnej sprzedaży, identyfikacji, korzystania z biblioteki. Dziś panuje trend zastępowania ich wszystkich jedną kartą wielofunkcyjną. Podobne działania podejmują rozmaite organizacje.

Zwiększanie poziomu bezpieczeństwa – biometria

Ponieważ skanowanie linii papilarnych jest uważane za najbardziej niezawodną technologię biometryczną, HID uzupełnił rodzinę *iCLASS* o produkt *bioCLASS*. Oferuje on opcję wielopoziomowego potwierdzania tożsamości, łącząc bezstykową technologię z weryfikacją linii papilarnych, realizowaną przez porównanie z wzorcem biometrycznym przechowywanym w pamięci karty.

Produkty *bioCLASS* zapewniają trzy poziomy weryfikacji linii papilarnych. Urządzenia z serii *bioCLASS* są podłączane do komputera przez port USB. Wyposażone są w wyświetlacz i klawiaturę, umożliwiające odczyt i zapis danych. W procesie weryfikacji urządzenie skanuje linie papilarne danej osoby. Oprogramowanie prowadzi ją przez proces skanowania przy pomocy jasnych instrukcji. Stworzony wzornik jest natychmiast zapisywany na karcie i tylko tam. Podczas weryfikacji tożsamości wyświetlacz LCD czytnika pokazuje użytkownikowi, jak należy dokonać autoryzacji.

Nowe rozwiązania i sprawdzeni partnerzy – HID Connect

Aplikacje stworzone przez partnerów rozwojowych HID Connect obejmują następujące elementy:
– weryfikację biometryczną,
– obsługę punktów sprzedaży,
– dostęp logiczny,
– zdalną weryfikację,
– czytniki wandaloodporne,
– drukowanie i obsługę fotoidentyfikatorów (*Photo ID*).

HID oferuje kompletny zestaw narzędzi HID Connect. Dzięki nowym pakietom modułów OEM oraz zestawom rozwoju oprogramowania (SDK – *Software Development Kit*) inni producenci mogą w sposób łatwy i ekonomiczny zintegrować technologię *iCLASS* ze swoimi produktami.

Zakończenie

Ponieważ różne organizacje stale poszukują nowych sposobów zarządzania ryzykiem oraz optymalizacji działań w środowisku, w którym uczymy się lub pracujemy, bezdotykowe, inteligentne karty będą zdobywały coraz większą popularność, przyczyniając się do poprawy bezpieczeństwa i wygody użytkowania systemów kontroli dostępu. Koszty implementacji przestaną stanowić barierę, zwłaszcza wtedy, gdy karty będą miały wiele zastosowań. Dzięki pojawianiu się innowacyjnych rozwiązań proponowanych przez doświadczonych producentów technologia ta będzie w stanie nadążyć za postępem technologicznym – została przygotowana z myślą o przyszłości.

HID

Opracował:
Andrzej Sosiński

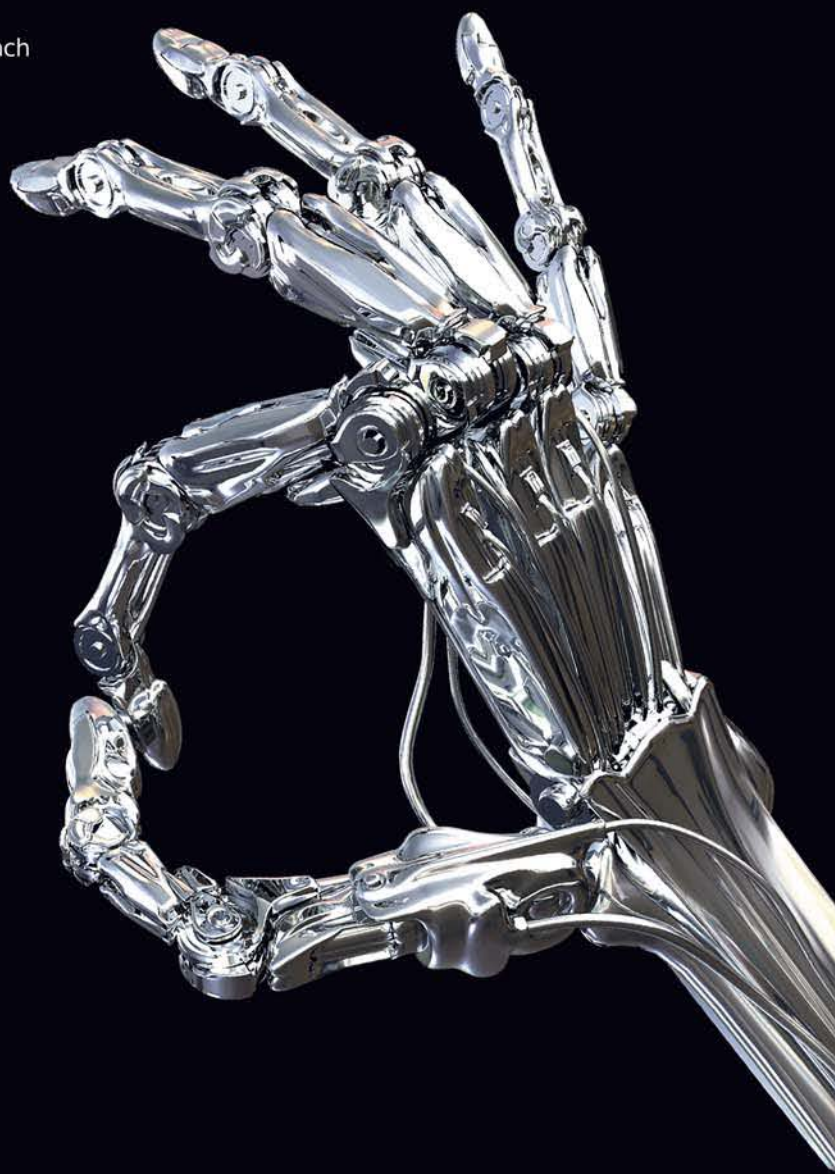
Dodatkowych informacji udziela
Czesław Półtorak, Regional Sales Manager dla Polski, Litwy, Estonii, Węgier i Łotwy.
e-mail: cpoltorak@hidcorp.com
Tel.: +48 507 445 361,
www.hidcorp.com

Satel - Inteligentne systemy alarmowe

Zaawansowana technologia

Od 17 lat specjalizujemy się wyłącznie w produkcji urządzeń do systemów alarmowych. Inwestycje w wysoko wykwalifikowaną kadrę inżynierską, zaawansowane technologie oraz innowacyjne rozwiązania przekładają się na produkt, który jest oceniany jako niezawodny, pewny w działaniu i zgodny z najnowszymi trendami technologicznymi.

- urządzenia SATEL powstają w naszych działach konstrukcyjnych, począwszy od fazy projektu, aż po produkt finalny
- posiadamy własne laboratorium, gdzie przeprowadzamy badania funkcjonalności, stabilności parametrów i kompatybilności elektromagnetycznej naszych produktów
- wykorzystujemy do produkcji w pełni zautomatyzowane linie technologiczne, gwarantujące powtarzalność produktów i perfekcyjny montaż elementów
- przeprowadzamy proces testowania 100 % naszych produktów za pomocą specjalizowanych testerów komputerowych
- posiadamy nowoczesną narzędziownię i wtryskownię, dzięki czemu możemy samodzielnie projektować i zmieniać design naszych produktów
- wykorzystujemy w procesie produkcyjnym technologię bezołowiową



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

Integracja wideofonów Bpt z telefonami

Niniejszy artykuł omawia zagadnienia współdziałania systemu wideofonowego Bpt serii 300/X2 z instalacją telefoniczną i centralami telefonicznymi Bpt. Przy zastosowaniu aparatów wideofonowych Bpt posiadających funkcję telefonu oraz wykorzystaniu central telefonicznych można w łatwy sposób zrealizować łączność wideofonową, telefoniczną oraz interkomową pomiędzy odbiornikami. Artykuł przedstawia sposób wykorzystania zwykłych telefonów do łączności z wideofonowymi panelami wejściowymi oraz do sterowania ryglami elektrycznymi, bramami i innymi urządzeniami towarzyszącymi.

Wprowadzenie

Rozwiązania techniczne Bpt w zakresie integracji systemu wideofonowego z instalacją telefoniczną mają na celu:

1) połączenie funkcji odbiornika wideofonowego z aparatem telefonicznym w celu zredukowania liczby urządzeń oraz ilości okablowania,
2) przekazywanie (transferowanie) wywołań z wejściowych paneli wideofonowych do numerów telefonicznych wewnętrznych i zewnętrznych (np. komórkowych) w czasie nieobecności lokatorów w domu,
3) wykorzystanie zwykłych dostępnych na rynku aparatów telefonicznych do realizacji funkcji łączności z panelami wejściowymi instalacji wideofonowej w celu zwiększenia wygody obsługi systemu i zmniejszenia kosztów tej instalacji.

Realizacja powyższych funkcji wymaga zastosowania systemowych rozwiązań Bpt, tj. aparatów serii Exedra lub Integra oraz interfejsu telefonicznego IT/300 dla systemu cyfrowego (S300, X2 lub X1), IT/200 dla systemu analogowego serii 200 lub central telefonicznych CT1/6U (jedna linia zewnętrzna, sześć linii wewnętrznych) i CT2/8U (dwie linie zewnętrzne, osiem linii wewnętrznych). W niniejszym artykule omówione zostaną rozwiązania dla systemu cyfrowego.

Interfejs telefoniczny IT/300

Najprostszy sposób podłączenia telefonów do instalacji wideofonowej (lub domofonowej) Bpt, zarówno tych systemowych, jak i standardowych, wymaga zastosowania interfejsu linii telefonicznej IT/300. Umożliwia on podłączenie jednej linii zewnętrznej oraz kilku aparatów telefonicznych, nie wykluczając zarazem możliwości zastosowania w systemie dowolnej liczby odbiorników wideofonowych

Na rys. 1 przedstawiono schemat instalacji z interfejsem IT/300 dla dwóch użytkowników A i B, z których jeden posiada odbiorniki wideo i audio Bpt z funkcją telefonu (XT/200+XV, XT/200+XVC, XT/200, IM/TC), a drugi odbiorniki audio Bpt i standardowe aparaty telefoniczne. Oprócz panelu wejściowego wideo serii Targha kolor, do systemu podłączona jest dodatkowa kolorowa kamera CCTV do obserwacji bramy wjazdowej oraz moduł przekaźników do sterowania bramą i zapalania światła. Każdy z użytkowników posiada również standardowe odbiorniki wideofonowe, nie powiązane z instalacją telefoniczną (Nova, Ophera). W układzie użytkownika A zastosowano rozdzielacz wizji XDV/304 ze względu na odbiorniki wideo (XV/200+XKP/300, XVC/200+XKP/300, IM/TC) oraz wzmacniacz sygnału wizji XDV/300A ze względu na kaskadowe połączenie rozdzielaczy XDV/304. Zagregowane sygnały wizji, fonii i sterowań (dla instalacji wideofonowej i telefonicznej) przesyłane są od interfejsu IT/300 do odbiorników po jednej parze skrętki.

FUNKCJA	Domofon BPT z funkcją telefonu	Standardowe aparaty telefoniczne DTMF
Programowanie modułu IT/300	tak	tak
Połączenie telefoniczne	bezpośrednio	bezpośrednio
Odbieranie połączeń z paneli/połączeń telefonicznych	tak	tak
Dostęp do usługi DTMF	tak	tak
Łączenie z panelem wejściowym wideo	(monitor)	R+86
Otwieranie rygla elektrycznego		R+85
Sterowanie dodatkowe (otwieranie bramy, zapalanie światła)		R+88
Połączenie z portierem		R+87
Przełączanie pomiędzy rozmową telefoniczną a rozmową z panelem		R+80

Tab. 1. Klawisze funkcyjne w telefonach Bpt oraz kody sterujące dla standardowych aparatów telefonicznych

Użytkownik A widzi obraz z kamery panelu wejściowego, jeśli w czasie rozmowy telefonicznej zadzwoni ktoś z panelu. Dodatkowo wywołanie z panelu sygnalizowane jest sygnałem dźwiękowym w słuchawce. Odbiorniki wideo wymagają doprowadzenia drugiej pary zasilającej od zasilacza XA/300LR (lub innego zasilacza systemowego: VAS/100.20, AS/200).

Użytkownik B wykorzystuje aparaty telefoniczne Bpt i standardowe aparaty telefoniczne i nie ma możliwości podglądu obrazu z kamery w trakcie połączenia z panelem wejściowym.

Aparaty wideofonowe Bpt z funkcją telefonu posiadają dedykowane przyciski do realizacji takich funkcji, jak: łączenie z panelem wejściowym, otwieranie rygla elektrycznego, dodatkowe sterowanie (otwieranie bramy, zapalanie światła), komunikacja z portierem, przełączanie między rozmową telefoniczną a połączeniem z panelem wejściowym. Te same funkcje w standardowych telefonach mogą być realizowane za pomocą odpowiednich kodów DTMF zestawionych w tabeli 1.

Interfejs IT/300 generuje różne sygnały dzwonka dla połączeń telefonicznych, wywołań z panelu wejściowego i połączenia pochodzącego od portiera, umożliwiając rozróżnienie źródła przychodzącego połączenia.

Maksymalna odległość aparatu telefonicznego od modułu IT/300 wynosi 100 m. Jeden moduł może obsłużyć maksymalnie pięć aparatów w dowolnej kombinacji.

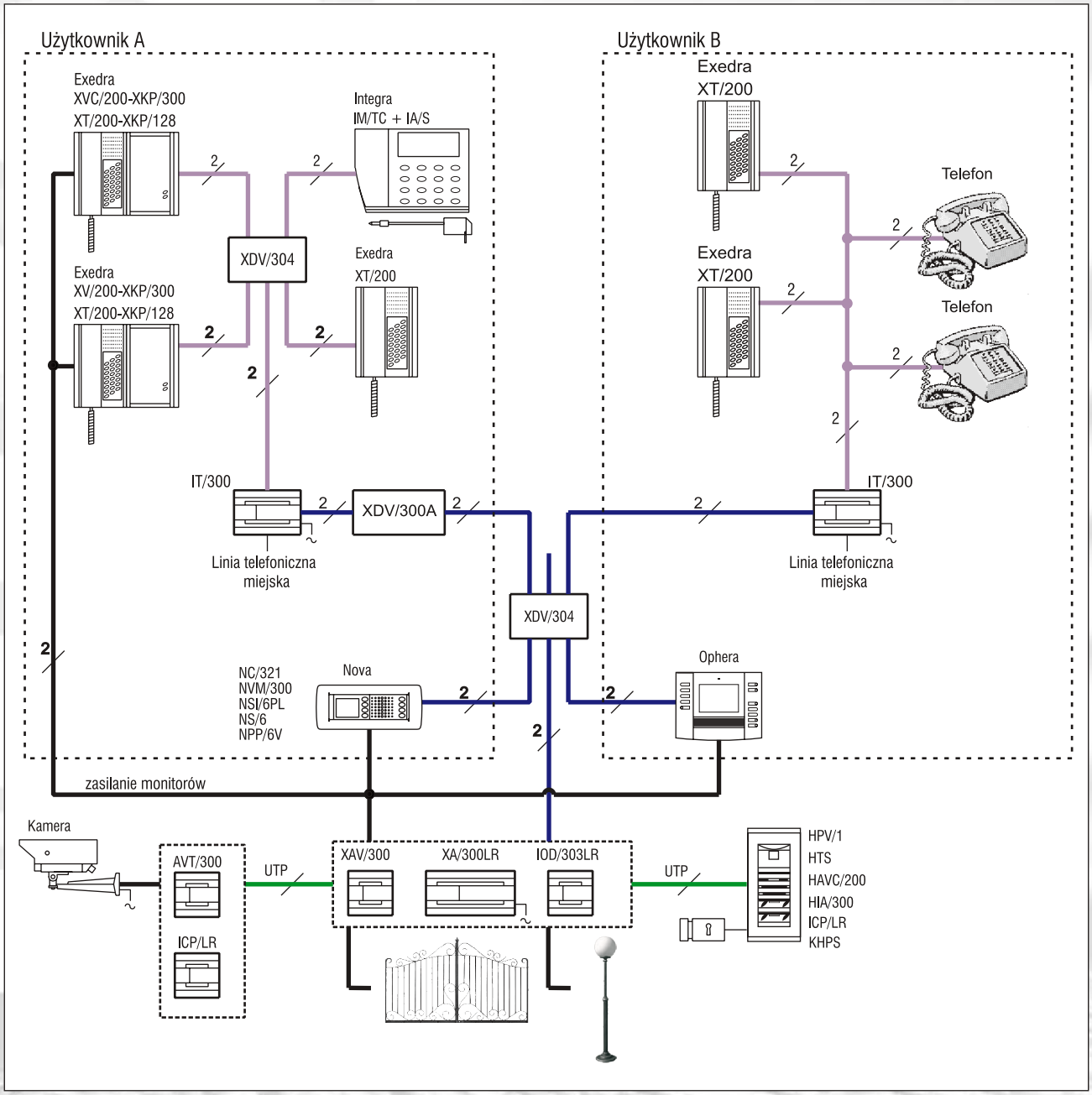
Centrala telefoniczna CT2/8U (CT1/6U)

Centrale telefoniczne Bpt CT1/6U i CT2/8U umożliwiają zrealizowanie większej liczby funkcji niż interfejs IT/300.

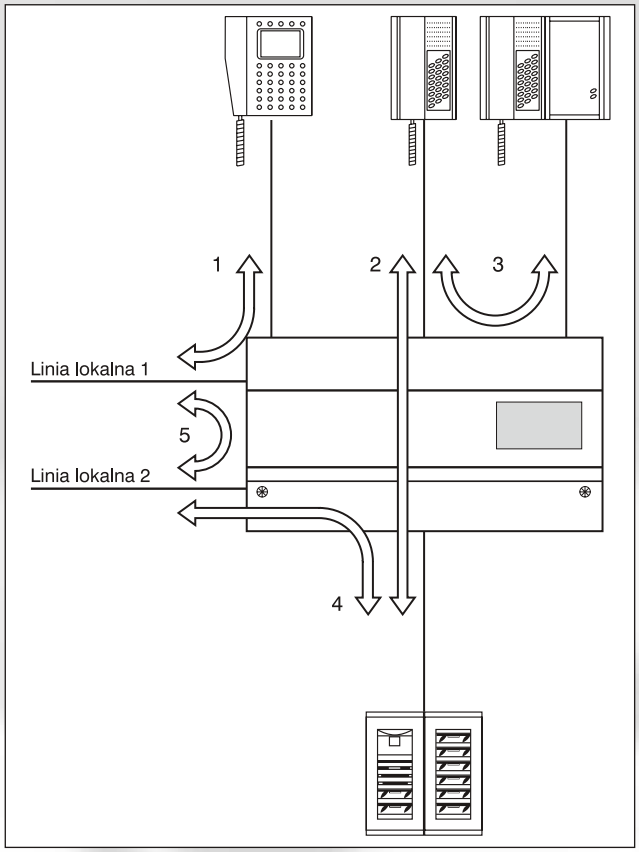
Funkcjonowanie central telefonicznych Bpt we współpracy z instalacją wideofonową przedstawione jest w poglądowy sposób na rys. 2. Ponumerowane połączenia oznaczają odpowiednio:

1 – zwykłe połączenie telefoniczne,
2 – połączenie pomiędzy panelem wejściowym a aparatem,
3 – połączenie interkomowe pomiędzy aparatami,
4 – połączenie pomiędzy panelem wejściowym a zewnętrznym numerem telefonicznym,
5 – transferowanie zewnętrznego połączenia z jednej linii na inny numer zewnętrzny poprzez drugą linię.

Centrala telefoniczna CT2/8U (z interfejsem CTI/300) może być funkcjonalnie podzielona między dwóch użytkowników, a poszczególne linie wewnętrzne mogą być aktywowane przez wciśnięcie pierwszego lub drugiego przycisku wywołania w panelu wejściowym.



Rys. 1. Schemat instalacji z interfejsem IT/300 dla dwóch użytkowników



Rys. 2. Funkcjonalność central telefonicznych Bpt CT2/8U i CT1/6U

Centrala CT2/8U może obsługiwać maksymalnie osiem aparatów w dowolnej kombinacji z zestawu: domofon z funkcją telefonu Exedra XT/200, wideofon z funkcją telefonu Exedra XT/200+XKP/128+XKP/300+XV/200 (XVC/200 w wersji kolorowej), wideofon z funkcją telefonu Integra IM/T (IM/TC w wersji kolorowej) lub standardowy telefon.

Użycie wideofonu z funkcją telefonu wymaga zastosowania modułu CTI/304, który odpowiednio formuje i selekcjonuje sygnały do poszczególnych aparatów wideo. Domofony Bpt z funkcją telefonu lub standardowe aparaty mogą być podłączone bezpośrednio do centrali telefonicznej.

Na rys. 3 przedstawiono schemat rozwiązania dla pojedynczego użytkownika, który korzysta z czterech odbiorników telefonicznych wideo, dwóch odbiorników telefonicznych audio, jednego standardowego telefonu i faksu. Ponadto w systemie znajdują się odbiorniki wideofonowe nie powiązane z instalacją telefoniczną (Nova i Ophera).

Magistrala standardu X2, wychodząca z rozdzielacza XDV/304, dołączona jest najpierw do interfejsu CTI/304, skąd prowadzi dalej do modułu CTI/300 w centrali CT2/8U. Z centrali CT2/8U wychodzą cztery linie wewnętrzne, które dochodzą do czterech odpowiednich wejść modułu. Z czterech wyjść modułu CTI/304 (skojarzonych z czterema wspomnianymi wejściami) wychodzi sygnał po jednej parze skrętki do aparatów wideo z funkcją telefonu. Wybór przycisku wywołania z panelu wejściowego dla każdego wyjścia modułu CTI/304 dokonywany jest za pomocą czterech zworek. O tym, którym przyciskiem dokonano wywołania, informują dwie linie aktywacji doprowadzone do modułu CTI/304 z centrali CT2/8U. W układzie można zastosować maksymalnie dwa moduły CTI/304, jeśli liczba aparatów wideo z funkcją telefonu jest większa niż cztery.

Aparaty audio z funkcją telefonu podłączone są bezpośrednio do pozostałych wyjść centrali CT2/8U z pominięciem modułu CTI/304.

Na każdej linii centrali CT2/8U (lub interfejsu CTI/304) można podłączyć tylko jeden aparat telefoniczny.

Funkcje realizowane przez odbiorniki wideofonowe Bpt z funkcją telefonu i odpowiadające im przyciski funkcyjne, a także kody sterujące DTMF dla standardowych aparatów telefonicznych, zestawione są w tabeli 2.

Oprócz typowych funkcji sterujących podanych w tabeli, centrala telefoniczna może realizować wiele innych ciekawych funkcji. Oto niektóre możliwości, jakie daje:

- automatyczne przekierowywanie miejskiego połączenia telefonicznego na inny numer zewnętrzny (poprzez drugą linię zewnętrzną),
- automatyczne przekierowywanie wywołania z panelu wejściowego na numer zewnętrzny (np. w trakcie naszej nieobecności),
- funkcja telekonferencji pomiędzy trzema aparatami (w tym jedną linią zewnętrzną),
- wybór aparatów, które mają odpowiadać na wywołanie z panelu wejściowego,
- transferowanie połączeń telefonicznych i połączeń z panelem wejściowym do innych aparatów,
- możliwość połączenia się z innym, dodatkowym aparatem (np. w celu przeprowadzenia konsultacji) w trakcie rozmowy telefonicznej lub połączenia z panelem wejściowym,
- połączenie z wszystkimi aparatami wewnętrznymi;
- możliwość przełączania się między rozmową telefoniczną i rozmową z panelem wejściowym przy równoległych połączeniach,
- przechwytywanie połączenia do innego aparatu, jeśli nasz aparat nie dzwoni,
- wybieranie automatyczne numeru alarmowego (jeśli słuchawka jest podniesiona, a klawisz nie został wciśnięty w ciągu dziesięciu sekund),
- dzwonienie do jednej wybranej grupy użytkowników (spośród czterech),

Opis komendy (sterowań)	Dedykowany przycisk	Odpowiednie kody DTMF	
		System 200	System 300 i X2
Otwieranie rygla elektrycznego nr 1	⊶	R 5 0	R * 5 0
Łączenie z panelem wejściowym wideo (audio)	⇦	R 5 2	
Łączenie z panelem wejściowym wideo (audio)	⇦		* 5 2 / R * 5 2
Dodatkowe sterowanie nr 1	•	R 5 3	
Dodatkowe sterowanie nr 1	•		R * 5 3
Połączenie z portierem lub przycisk dodatkowego sterowania	⇨	R * 5 4	R * 5 4
Przełączanie pomiędzy rozmową telefoniczną a rozmową z panelem wejściowym	⇦⇨	R 4 4	R 4 4
Otwieranie rygla elektrycznego nr 2		R 5 1	
Dodatkowe sterowanie nr 3			R * 5 1
Połączenie z portierem lub przycisk dodatkowego sterowania nr 2		R * 5 5	
Dodatkowe sterowanie nr 4			R * 5 5

Tab. 2. Klawisze funkcyjne w odbiornikach wideofonowych Bpt z funkcją telefonu oraz kody sterujące DTMF dla centrali CT2/8U

– możliwość wybrania z zewnątrz numeru wewnętrznego aparatu po odebraniu połączenia przez centralę,
– możliwość sterowania P1 i P2 przez telefon – z zewnątrz, po podaniu hasła (np. otwarcie bramy).

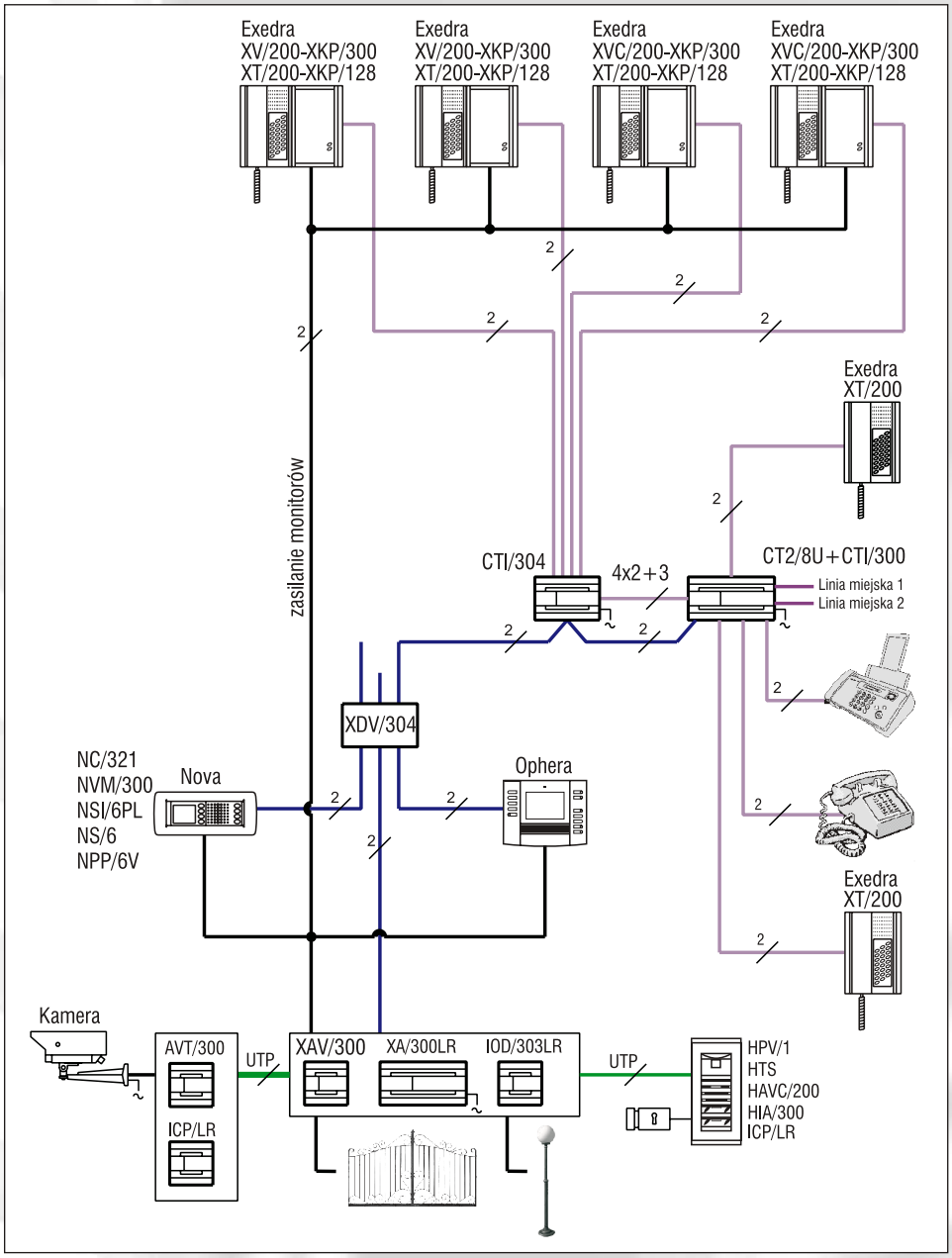
Centrala telefoniczna CT2/8U może być wyposażona dodatkowo w opcjonalne moduły: CTM – karta muzyczna, CTM/GV – karta muzyczna z czterema zapowiedziami (komunikatami) głosowymi, CT/ST – skrzynka głosowa z pamięcią 17 minut nagrań.

Odbiorniki domofonowe i wideofonowe z funkcją telefonu

Bpt posiada dwie linie odbiorników domofonowych i wideofonowych z funkcją telefonu. Seria Exedra jest systemem modułowym przeznaczonym do montażu na ścianie lub na biurku. Wersja audio składa się tylko ze słuchawki XT/200.

Exedra w wersji wideo składa się ze słuchawki XT/200, podstawki pod słuchawkę XKP/128, podstawki monitora XKP/300 oraz monitora w wersji czarno-białej XV/200 lub kolorowej XVC/200. Wersja na biurko wymaga zastosowania dodatkowo przystawek XKT/128 i XKT/200. Exedra jest dostępna również w kolorze antracytowym.

Odbiornik XT/200 posiada klawisz funkcji głośnomówiącej.



Rys. 3. Schemat instalacji z centralą CT2/8U dla jednego użytkownika

Odbiorniki serii Integra w wersji czarno-białej IM/T i kolorowej IM/TC posiadają wbudowany monitor. Zasilane są z lokalnego zasilacza IA/S. Przeznaczone są do pracy na biurku.

Podsumowanie

Integracja systemu wideofonowego Bpt z systemem telefonii daje duże możliwości funkcjonalne realizacji zarówno zewnętrznej, jak i wewnętrznej łączności między użytkownikami. Ponadto umożliwia połączenie się z osobami, które pod naszą nieobecność dzwonią do domu z linii miejskiej lub z panelu wejściowego przed domem.

Andrzej Grodecki
ADD
WWW.ADD.PL

Absolutely perfect

Dualna Kamera Kolorowa Wysokiej Rozdzielczości

DCC-500F

- 540 TV lines
- DAY/NIGHT- wysoka czułość do 0,002 lux
- DNR - perfekcyjny system redukcji szumów
- OSD - menu ekranowe

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

ALPOL HURTOWNIA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ

D-max DONGYANG UNITECH

tel: 0 801 77 77 90

Bielsko-Biała	Gliwice	Katowice	Kraków	Łódź	Poznań	Sopot	Szczecin	Warszawa Mokotów	Warszawa Praga	Wrocław
0 32 7907621	0 32 7907623	0 32 7907656	0 32 7907646	0 32 7907625	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

artykuł sponsorowany

Monitoring wizyjny stadionu Odry w Opolu

Zabezpieczenie imprez masowych za pomocą środków technicznych jest aktualnie zarówno wymogiem Ministerstwa Spraw Wewnętrznych i Administracji, jak i absolutną koniecznością. Tylko wyeliminowanie z tłumu kibiców jednostek agresywnych, zakłócających przebieg imprez, jest gwarancją pełnych trybun oraz spokojnego przebiegu zawodów. Dlatego też zarządzający największym stadionem w Opolu, obiektem Odry, podjęli decyzję o zainstalowaniu systemu monitoringu wizyjnego.

Wykonawcą projektu oraz systemu wizyjnego została firma Konsalnet Inowopol z Opola. Projekt zakładał monitoring najważniejszych części stadionu z wykorzystaniem odpowiednich rodzajów i typów kamer oraz nagrywanie materiału na rejestratorze cyfrowym przy spełnieniu wytycznych rozporządzenia MSWiA.

Wspomniane rozporządzenie bardzo jasno precyzuje, jakie obszary muszą być monitorowane:

1) ogrodzenie zewnętrzne obiektu, granica terenu, na którym odbywa się impreza masowa;
2) kasy biletowe na terenie imprezy masowej (w przypadku imprezy odpłatnej);
3) bramy, furtki i inne miejsca przeznaczone do wejścia uczestników na teren imprezy masowej;
4) ciągi komunikacyjne na terenie imprezy masowej, w tym drogi dla służb ratowniczych i drogi ewakuacyjne;
5) parkingi zorganizowane na terenie imprezy masowej;
6) sektory dla uczestników imprezy masowej;
7) płyta boiska, scena itp.

Cechą charakterystyczną tego typu obszarów jest występowanie silnych kontrastów, szczególnie przy słonecznej pogodzie. Zadaszone trybuny czy też zabudowane wejścia na stadion znajdują się wtedy w bardzo mocnym cieniu, pozostała część boiska jest silnie oświetlona. Sytuacja taka wymaga zastosowania kamer o szerokim zakresie dynamiki. Ponadto należy pamiętać o konieczności identyfikacji kibiców (obiekt musi zajmować 120% wysokości ekranu) i w związku z tym, w przypadku kamer stacjonarnych, należy użyć obiektywów o odpowiedniej ogniskowej.

Pierwszą barierę, mającą zapobiegać wejściu osób niepożądanych (z zakazami stadionowymi) oraz umożliwiającą uzyskanie zbliżenia twarzy w celu późniejszej identyfikacji, stanowią kamery przy wejściu na stadion. Ponieważ kamery te pracują w skrajnych warunkach, jeśli chodzi o kontrasty, zadecydowano o zastosowaniu kamer JVC TK-WD310E (A). Kamery te są wyposażone w przetwornik CMOS firmy Pixim, a naświetlenie każdego piksela odbywa się indywidualnie, z pięcioma różnymi prędkościami migawki. Dzięki tej funkcji rozpoznanie twarzy osób wchodzących na stadion jest możliwe niezależnie od oświetlenia sceny: zarówno w bardzo pogodny dzień, przy bardzo silnym nasłonecznieniu i dużych cieniach, jak i w warunkach słabego oświetlenia (kamera przełącza się

Fot. 1. Porównanie obrazów z kamery tradycyjnej (po lewej) i z kamery JVC TK-WD310E

w tryb czarno-biały). Rysunek 1 ilustruje zalety wykorzystania kamery TK-WD310E (A) – po lewej obraz z tradycyjnych kamer CCD (wyraźne problemy z prawidłowym, równoczesnym oświetleniem ciemnego wnętrza i bardzo jasnego parkingu na zewnątrz), po prawej obraz z TK-WD310E (A).

Łącznie wejście dla widzów miejscowych oraz osobne wejście dla widzów przyjezdnych są monitorowane przez osiem kamer JVC TK-WD310E (A).

Nie mniej istotne z punktu widzenia bezpieczeństwa są ciągi komunikacyjne. Ich podgląd uzyskujemy na dwa sposoby: z kamer stacjonarnych wysokiej rozdzielczości JV TK-C920E (A) oraz wykorzystując bardzo duże możliwości kamer obrotowych JVC TK-C655E. Ponadto kamery obrotowe umożliwiają obserwowanie niezwykle istotnych miejsc, jakimi są trybuny oraz płyta stadionu. Ważną cechą użytych kamer, która między innymi zdecydowała o ich zastosowaniu, jest funkcja ExDR (ang. *Extended Dynamic Range*, w skrócie znana także jako XDR), czyli rozszerzony zakres dynamiki. Ponieważ część trybun jest kryta, a część odsłonięta, w słoneczny dzień mamy do czynienia z głębokimi cieniami i bardzo jasnymi, oświetlonymi obszarami. Rozpoznanie twarzy kibiców jest możliwe tylko przy poprawnej ekspozycji. Funkcja ExDR to dwukrotne naświetlenie przetwornika z dłuższym i krótszym czasem migawki, a następnie kompilacja tych dwóch obrazów. Dzięki temu zabiegowi wyraźnie widzimy zarówno zacienione, jak i mocno oświetlone fragmenty sceny. Kamery JVC TK-C655E wyposażone są w obiektyw z zoomem optycznym x25. Jest to ważna cecha, gwarantująca spełnienie wymogów rozporządzenia w zakresie identyfikacji i rozpoznawania obiektów (odpowiednio 120% i 50% wysokości obrazu).

Fot. 2. Kamera JVC TK-920E

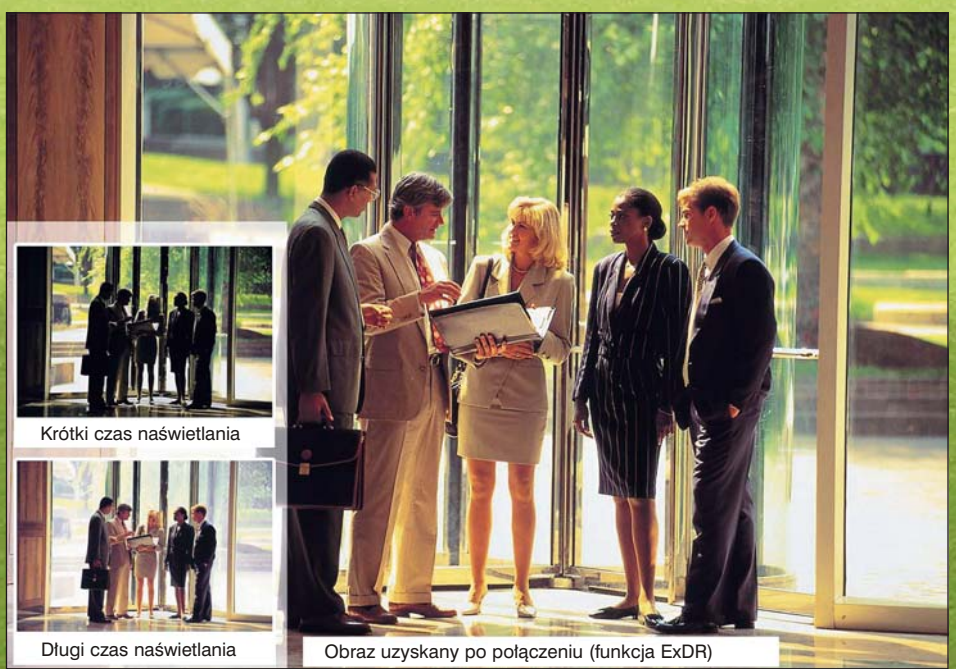
Kamery obrotowe zainstalowano również przed terenem stadionu – na parkingu. Poza umożliwieniem obserwowania płyty parkingu pozwalają na podgląd kilku ważnych miejsc: kas biletowych i wejść na stadion oraz przyległej ulicy, spełniając dodatkowo funkcję kamery monitoringu miejskiego.

Fot. 3. Kamera szybkoobrotowa JVC TK-C655E

Centrum monitoringu znajduje się w specjalnie wydzielonym pomieszczeniu, pod krytą trybuną dla kibiców – gospodarzy. Sterowanie kamerami obrotowymi odbywa się za pomocą panelu sterowania JVC RM-P2580E. W systemach monitoringu stadionów sportowych niezwykle istotna jest jakość wyświetlanego obrazu. Dlatego zdecydowano o zastosowaniu monitorów CRT firmy JVC o przekątnej 17" i 21". Dokładniejsze ukazanie szczegółów umożliwia operatorowi trafniejszą ocenę sytuacji na trybunach i płycie stadionu oraz w jego otoczeniu.

Rozporządzenie w sprawie zabezpieczania imprez masowych za pomocą środków technicznych stawia szczególnie wysokie wymagania urządzeniom rejestrującym. Rejestrator zastosowany w monitoringu na stadionie Odry w Opolu spełnia wszystkie wymogi rozporządzenia, czyli m.in. nagrywa z prędkością 400 kl/s dla 16 kamer oraz posiada 16 wejść audio. Wyszukiwanie zdarzeń jest bardzo proste i intuicyjne, a łatwość archiwizacji pozwala na szybkie przekazanie materiału, np. na płycie CD, do dyspozycji policji lub innych służb.

Zaprojektowanie oraz wykonanie systemu monitoringu takiego obiektu, jak stadion sportowy, wymaga wzięcia pod uwagę wielu czynników (silne światło słoneczne lub światło jupiterów, duże kontrasty itp.) oraz doboru odpowiednich urządzeń. Efekty pracy firmy Konsalnet Inowopol na stadionie Odry w Opolu są kolejnym dowodem na najwyższą jakość i przydatność urządzeń telewizji dozorowej JVC w najbardziej wymagających systemach.



Fot. 4. Przykładowy obraz uzyskany za pomocą funkcji XDR

Sławomir Janiso
Radioton

reklama

ZAPRASZAMY DO WSPÓŁPRACY PARTNERSKIEJ !

AXIS COMMUNICATIONS

milestone

FORMUŁA 1 W WIDEO IP

DYSTRYBUCJA NOWOCZESNYCH CYFROWYCH ROZWIĄZAŃ DOZOROWYCH

SOFTEX Data

Tel. 022 33 11 990
e-mail: softex@softex.com.pl

SYSTEMY WIDEODOMOFONOWE COMELIT

Comelit GROUP S.P.A.

POWERCOM

BRAVO

GENIUS

VANDALCOM

DIVA

BRAVOkit

Zestaw wideodomofonowy z panelem wejściowym POWERCOM oraz monitorem BRAVO z wbudowaną funkcją interkom. Wersje dla 1 i 2 użytkowników. Możliwość zbudowania systemu składającego się z 30 lokali, wspólnego panela wejściowego oraz centrali portierskiej. System w okablowaniu 4-przewodowym.

DIVAkit

Zestaw składający się z panelu wejściowego POWERCOM oraz ekskluzywnego monitora Diva z kolorowym 3,5" wyświetlaczem LCD. Okablowanie tradycyjne lub uproszczone (bez kabla koncentrycznego).

SIMPLEBUS2

Cyfrowy system w okablowaniu 2-przewodowym (łącznie z zasilaniem monitora). Do 240 użytkowników z nieograniczoną ilością głównych i dodatkowych paneli wejściowych, interkomem, centralą portierską i wieloma innymi funkcjami.

COMELBUS

Cyfrowy system wideodomofonowy. Okablowanie z 7-przewodową magistralą komunikacyjną oraz kablem koncentrycznym. Do zastosowania przy projektach od 200 lokali do 9999 lokali.

TRADYCYJNY i UPROSZCZONY

System w okablowaniu tradycyjnym i uproszczonym (bez kabla koncentrycznego).
Nieograniczona liczba użytkowników i paneli wejściowych.

Dystrybutor domofonów i wideodomofonów COMELIT w Polsce:

alarmnet®

ALARMNET Sp. J.
ul. Rydygiera 12, 01-793 Warszawa
tel. 022 663 40 85, fax 022 833 87 95
biuro@alarmnet.com.pl, www.alarmnet.com.pl, www.comelit.com.pl

Firma Axis Communications wprowadziła na rynek rozwiązanie serwerowe, które obejmuje przeznaczoną do zabudowy w stojaku (*rack*) obudowę z wbudowanym przełącznikiem sieciowym i obsługą do trzech serwerów wideo w wersji Blade.

Razem z nowym wideoserwerem AXIS 243Q Blade, takie rozwiązanie może konwertować sygnały z maksymalnie 12 analogowych kamer wideo, umożliwiając użytkownikom zdalny dostęp do cyfrowej wizji z pełną szybkością transmisji obrazu w sieci IP.

Rozwiązanie to nadaje się idealnie do zastosowania w kasynach i na lotniskach, do monitorowania ruchu ulicznego i wszędzie tam, gdzie potrzebna jest migracja z analogowego systemu wideo do cechującego się wysoką efektywnością rozwiązania cyfrowego.

Serwerowe rozwiązanie AXIS dla kamer analogowych

AXIS COMMUNICATIONS

Fot. 1. Lars Wilson z Axis Communications (w środku) z działem dystrybucji wideo IP Softex Data

– Rozwijający się rynek wideoserwerów z wyższej półki domaga się pełnej szybkości transmisji obrazu lub 30/25 klatek na sekundę na kanał wideo w MPEG-4 lub Motion JPEG, a połączone rozwiązanie złożone z serwerów AXIS 243Q Blade i obudowy stojakowej AXIS 291 1U zaspokaja tę potrzebę – powiedział Anders Laurin, wiceprezes wykonawczy ds. strategii korporacyjnej w firmie Axis Communications. *– Rozwiązanie to jest efektywne ekonomicznie i łatwe w instalacji oraz umożliwia użytkownikom analogowych systemów wideo wykorzystanie w pełni zalet rozwiązania cyfrowego bazującego na protokole IP.*

Serwer AXIS 243Q Blade konwertuje sygnały z maksymalnie czterech kamer analogowych do wysokiej jakości cyfrowego sygnału wideo z usunięciem przeplotu. Dostarcza 30/25 (NTSC/PAL) klatek na sekundę na kanał przy rozdzielczości 4CIF w standardzie kompresji MPEG-4 lub Motion JPEG. Oprócz tego oferuje on użytkownikowi różne zaawansowane funkcje, takie, jak wideodetekcja ruchu, wysyłanie obrazów, obsługa zaplanowanych i wyzwalanych zdarzeń czy powiadomienie o alarmie. Port szeregowy wideoserwera umożliwia zdalne sterowanie analogowymi kamerami uchylno-obrotowymi (*Pan/Tilt/Zoom*). Obszerny zestaw funkcji bezpieczeństwa, włącznie z różnymi poziomami dostępu użytkowników, szyfrowaniem HTTPS, standardem uwierzytelniania IEEE 802.1X oraz filtrowaniem adresów IP, zapewnia bezpieczną obsługę wideo i konfigurację. Serwer AXIS 243Q obsługuje także technologię jakości usługi (*Quality of Service* – QoS) oraz adresację IPv4 i IPv6 (*Internet Protocol version 6*).

Wideoserwer AXIS 291 1U to 19-calowa obudowa, mieszcząca trzy wymienne serwery wideo firmy Axis w wersji Blade. Poprzez wbudowany przełącznik gigabitowy, przy użyciu pojedynczego portu Ethernet, rozwiązanie to pozwala na migrację do rozwiązań na bazie protokołu IP sygnałów z 4 do 12 kamer analogowych. AXIS 291 1U wyposażony jest z tyłu każdego gniazda karty w złącza dla sieci, portu szeregowego i wejścia/wyjścia oraz zintegrowane zasilanie, co zapewnia prostotę instalacji. Umożliwia on także wymianę wideoserwerów Blade na bieżąco, co eliminuje konieczność wyłączania zasilania przy ich instalowaniu lub wymianie.

Radykalna obniżka cen istniejących wideoserwerów

Jednocześnie z wprowadzeniem na rynek produktów AXIS 243Q Blade i AXIS 291 1U, firma Axis znacznie obniżyła ceny swych starszych wideoserwerów.

– Zainteresowania rynku przesuwają się z analogowego nadzoru wizyjnego na systemy na bazie protokołu IP. Tworzy to zapotrzebowanie na efektywne rozwiązania w dziedzinie serwerów wideo dla różnych typów instalacji – powiedział Anders Laurin. *– Przez zmianę cen linii naszych wideoserwerów pokazujemy zaangażowanie naszej firmy w ten rynek i umożliwiamy coraz większej liczbie użytkowników korzystanie z zalet nowoczesnych rozwiązań w dziedzinie nadzoru wizyjnego na bazie protokołu IP.*

– Mamy dużo zapytań od klientów firm, które rozpoczynają stosowanie wideo IP, dotyczących działania systemów monitoringu bazujących na urządzeniach AXIS-a. Czasami trudno im wykonać pierwszy krok. Myślę, że najnowsza oferta wideoserwerów pomoże w podjęciu decyzji o zainwestowaniu w rozwiązania IP. Ich ogromnym atutem jest możliwość integracji rozwiązań analogowych oraz „czystych" IP. Nareszcie nasi partnerzy i potencjalni klienci mogą bez obaw myśleć o ewolucyjnym przechodzeniu od rozwiązań analogowych do sieciowych, pozwalającym im nie tylko w pełni korzystać z nowych możliwości, ale też wykorzystać istniejące zasoby analogowe, chroniąc tym samym poniesione na nie nakłady inwestycyjne. Co więcej, rozwiązania bazujące na wideoserwerach pozwalają w pełni utrzymać dotychczasowe procedury i zasady obsługi części analogowej systemu monitoringu bez wprowadzania rewolucyjnych zmian – powiedział Aleksander M. Woronow.

Nowe produkty są dostępne u dystrybutora firmy Axis w Polsce – w firmie Softex Data.

Aleksander M. Woronow
Softex Data

Fot. 2. Rodzina wideoserwerów Axis

Obiektywnie patrząc najlepszy

Computar – szeroka gama
najczęściej na świecie kupowanych obiektywów CCTV.

computar®

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

artykuł sponsorowany

Systemy szybkoobrotowych kamer kopułkowych

Na rynku systemów CCTV można zaobserwować coraz większą rozbieżność pomiędzy dążeniami producentów a oczekiwaniami użytkowników. Producenci koncentrują się na osiąganiu coraz lepszych parametrów technologicznych, natomiast dla klientów najważniejsza jest funkcjonalność produktów, a w związku z tym – poprawa elastyczności systemu, inteligencji urządzeń oraz komunikacji pomiędzy nimi. Biorąc to pod uwagę, postaramy się w niniejszym artykule pokazać, w którą stronę zmierzają systemy kamer kopułkowych.

BOSCH
Technologia bliżej nas

Dlatego podczas gdy producenci żądni są technologicznego boomu i fundamentalnych zmian, użytkowników systemów znacznie bardziej interesują inne kwestie, a mianowicie:

– elastyczność systemu,
– komunikacja pomiędzy urządzeniami (analogowa, poprzez kabel koncentryczny lub sieciowa),
– inteligencja kamer.

Do czasu, kiedy branża przejdzie na rozsądne cenowo kamery HDTV lub sieciowe kamery z megapikselowymi przetwornikami, realnie dostępna rozdzielczość w konwencjonalnych kamerach kolorowych PAL lub NTSC jest ograniczona do około 500 linii TV. Może zdarzyć się oczywiście niewielka poprawa, ale mało prawdopodobna jest drastyczna zmiana (na przykład do 600 linii TV) bez dużego skoku technologicznego do formatu HDTV lub megapikselowych przetworników. Podobnie jest w przypadku czułości – zbliżamy się do praktycznego limitu, nawet przy zastosowaniu najnowszych przetworników obrazu oraz technologii redukcji szumów.

Ostatnie udoskonalenia obiektywów zoom zwiększyły w znacznym stopniu ich zakres. Poprawa dotyczy jednak największego zakresu oddalenia, a nie przybliżenia, podczas gdy najbardziej cenna byłaby właśnie możliwość dużego przybliżenia. Zaskakujące jest, że dostępne w kamerach kopułkowych typowe obiektywy 18x mogą przybliżać w takim samym stopniu, jak obiektywy z zoomem 26x lub 30x. Podobnie, możliwe jest zwiększenie prędkości obrotu i pochylenia kamery, jednak czy przywołanie żądanej sceny w 1/3 sekundy zamiast w 1/2 sekundy ma jakiekolwiek znaczenie praktyczne?

Elastyczność systemu

Zastosowanie szybkoobrotowych kamer kopułkowych bardzo szybko rozszerzyło się. Ich naturalnym środowiskiem były pierwotnie sklepy i kasyna. Teraz bywają wykorzystywane w ekstremalnie trudnych warunkach, na przykład do dozoru ruchu ulicznego oraz budynków przemysłowych, a także do ochrony terenu szpitali i innych obiektów komercyjnych. W wyniku tego dozór wizyjny obejmuje swym zasięgiem sąsiednie domy, podwórka szkolne oraz inne tereny. Z tego powodu jest absolutnie niezbędne (a w niektórych przypadkach nakazane prawnie), aby te obszary były chronione przed obserwacją. Na początku ewolucji techniki maskowania stref prywatności

Fot. 1. Maski w kamerach modułowych AutoDome są bardziej precyzyjne i śledzą scenę płynniej niż konkurencyjne technologie, dzięki czemu prywatność jest zachowywana bez uszczerbku dla celu oraz jakości dozoru wizyjnego

Większość zainstalowanych obecnie systemów nadal wykorzystuje analogowe techniki transmisji oraz kable koncentryczne, skrętkę lub światłowód. Nowoczesna kamera kopułkowa powinna posiadać wszystkie te opcje komunikacyjne, ale dodatkowo oferować wbudowaną transmisję sieciową, aby umożliwić podgląd obrazu oraz sterowanie i konfigurację kamery przez sieci TCP/IP. Wbudowany nadajnik powinien zapewniać jakość obrazu równą jakości obrazu analogowego. Ogólnie akceptowany standard rozdzielczości obrazu to D1 lub 4CIF (704 x 480 NTSC lub 704 x 576 PAL). Najnowsze nadajniki używają kompresji MPEG-4 i przesyłają 25 lub 30 obrazów na sekundę w rozdzielczości 4CIF. Niektóre nadajniki mają możliwość transmisji dwóch różnych strumieni wizyjnych. Standardowo jeden strumień służy do przesyłania obrazu bieżącego w pełnej rozdzielczości oraz zapisu alarmowego.

można było zdefiniować tylko proste obszary wyłączone z obserwacji. Obecnie użytkownicy wymagają możliwości zdefiniowania więcej niż 20 precyzyjnych obszarów, które są dokładnie śledzone i zamaskowane w czasie, w którym kamera obraca się, pochyla lub przybliża obraz. W celu zagwarantowania prywatności, bez konieczności ukrywania przed kamerą miejsc krytycznych z punktu widzenia dozoru, obszary maskowania mają często nieregularne kształty.

Kamery kopułkowe zainstalowane na zewnątrz budynków wymagają grzejników i wentylatorów, które, kierując przepływem powietrza, zapobiegają parowaniu kopułki, nawet w temperaturach do -60°C. Do pracy w gorącym klimacie niezbędnym wyposażeniem jest osłona, która umożliwia przepływ powietrza nad kamerą oraz chroni ją przed bezpośrednim działaniem promieni słonecznych. Nie tylko pogoda stanowi wyzwanie dla kamery kopułkowej. Uszkodzenie fizyczne może zostać spowodowane nieprawidłowym użytkowaniem lub wandalizmem, chyba że zastosowano specjalne środki zabezpieczające, takie jak wzmacniane obudowy oraz kopułki, które odporne są na uderzenia nawet kijem baseballowym.

Znaczące udoskonalenia zoomu optycznego sprawiły, że stabilizacja obrazu stała się absolutnie niezbędna. Dla przykładu wiele kamer kopułkowych zostało zainstalowanych na wysokich słupach rozmieszczonych wokół dozorowanego terenu, gdzie silny wiatr powoduje niestabilność platformy. Nieznaczny, sześciomilimetrowy ruch słupa może przesunąć pole widzenia o ponad 6 m, kiedy zoom kamery ma wysoką wartość. Może to spowodować, że obraz stanie się bezużyteczny. W warunkach nieustannego ruchu, na przykład na pokładzie statku lub w otoczeniu przemysłowym, gdzie pracują urządzenia wytwarzające drgania (np. generatory, kompresory itp.), kamery są często narażone na duże wibracje. W takich warunkach, podczas zbliżeń, można przekonać się, że zaawansowana stabilizacja obrazu oferuje znaczną przewagę.

W przeszłości proste algorytmy stabilizacyjne były wbudowane w same kamery. Standardowo algorytmy te stabilizowały obraz tylko w jednej osi (pionowej lub poziomej) i znacząco obniżały czułość kamery, ograniczając jej efektywność pracy w złych warunkach oświetleniowych. Nowoczesne systemy używają skomplikowanych algorytmów przetwarzanych przez dedykowane cyfrowe procesory sygnałowe (DSP) w celu zapewnienia stabilizacji zarówno w osi poziomej, jak i pionowej, co gwarantuje najlepszy możliwy obraz, nawet wtedy, gdy kamera jest zainstalowana na niestabilnym podłożu. Ponadto najnowsze, zaawansowane rozwiązania stabilizacji obrazu nie powodują obniżenia czułości kamery.

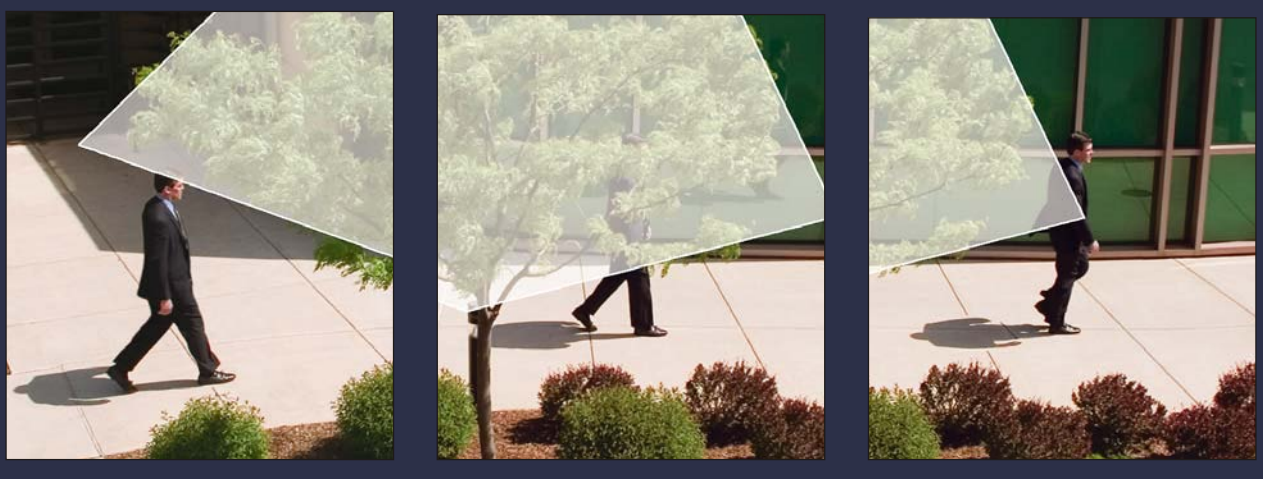
Duży asortyment opcji montażowych jest niezbędny z punktu widzenia elastyczności instalacji. Pojedynczy system może wymagać różnych mocowań, począwszy od konwencjonalnego wspornika sufitowego, aż do wewnętrznych i zewnętrznych wsporników oraz zawieszanych zasilaczy do kamer. Coraz bardziej wymagający użytkownicy i instalatorzy oczekują także od producentów kamer uproszczenia procesu instalacji za pomocą fabrycznie okablowanych wsporników i zasilaczy, a także wymiennych kamer i modułów, które umożliwią dostosowanie i uaktualnienie instalacji do zmieniających się wymagań dotyczących bezpieczeństwa oraz dozoru wizyjnego. Również podczas montażu na wsporniku oraz w trakcie wykonywania połączeń kamera musi utrzymywać się sama, aby obydwie ręce instalatora były wolne.

Fot. 2. Dzięki zaawansowanemu oprogramowaniu do stabilizacji obrazu kamer serii 500i, drgania kamery zostały wyeliminowane, co gwarantuje wyjątkowo klarowny obraz

Komunikacja pomiędzy urządzeniami

Większość zainstalowanych obecnie systemów nadal wykorzystuje analogowe techniki transmisji oraz kable koncentryczne, skrętkę lub światłowód. Nowoczesna kamera kopułkowa powinna posiadać wszystkie te opcje komunikacyjne, ale dodatkowo oferować

Fot. 5. Funkcja AutoTrack II z mechanizmem wirtualnych masek pozwala precyzyjnie śledzić wybrane obiekty bez negatywnego wpływu poruszających się obiektów, np. gałęzi drzew kołyszących się na wietrze



wbudowaną transmisję sieciową, aby umożliwić podgląd obrazu oraz sterowanie i konfigurację kamery przez sieci TCP/IP. Wbudowany nadajnik powinien zapewniać jakość obrazu równą jakości obrazu analogowego. Ogólnie akceptowany standard rozdzielczości obrazu to D1 lub 4CIF (704 x 480 NTSC lub 704 x 576 PAL). Najnowsze nadajniki używają kompresji MPEG-4 i przesyłają 25 lub 30 obrazów na sekundę w rozdzielczości 4CIF. Niektóre nadajniki mają możliwość transmisji dwóch różnych strumieni wizyjnych. Standardowo jeden strumień służy do przesyłania obrazu bieżącego w pełnej rozdzielczości oraz zapisu alarmowego.

Drugi strumień jest używany do zapisu poklatkowego oraz podglądu obrazu przez sieci o bardzo ograniczonej przepustowości, takie jak łącza ADSL. Najlepsze systemy będą mogły transmitować trzy strumienie, oferując dodatkowy strumień JPEG do integracji z wieloma systemami lub na przykład do wysyłania obrazów na serwer FTP w przypadku alarmu. Kolejną zaletą transmisji sieciowej jest to, że bez dodatkowych kabli, wraz z obrazem, może być przesyłany sygnał foniczny, co pozwala operatorowi zobaczyć i usłyszeć, co dzieje się na wybranym obszarze.

Sterowanie kamerą, konfiguracja oraz aktualizacja oprogramowania układowego przez kabel wizyjny posiada oczywiste zalety, niezależnie od tego, czy stosowana jest komunikacja analogowa, czy cyfrowa przez sieć. W przeszłości inteligentne produkty wizyjne były stosowane w drogich, scentralizowanych systemach, bazujących na komputerach PC. Teraz „inteligentne" są same kamery. Eliminuje to konieczność stosowania dużych i drogich serwerów oraz specjalistycznego oprogramowania. Wraz z wdrażaniem w coraz większym stopniu inteligencji do systemów kamer kopułkowych, dodawanie nowych funkcji – w momencie, kiedy będą już dostępne – będzie miało decydujące znaczenie. Użytkownicy wymagają teraz systemów kamer, które umożliwiają zdalną aktualizację, eliminującą przerwy w pracy oraz kosztowne wizyty w miejscu instalacji.

Świat systemów CCTV, zachęcony wszechobecną możliwością nawiązywania połączeń przez sieć, błyskawicznie przechodzi do ery cyfrowej. Jednakże nadal istnieje wielka liczba zainstalowanych systemów transmisji i sterowania analogowego, których całkowite dostosowanie do technologii cyfrowej zajmie lata, jeśli nie dekady. Kamery kopułkowe muszą więc być zdolne do pracy hybrydowej – umożliwiać jednoczesne przesyłanie strumienia sygnału cyfrowego i analogowego. Gwarantuje to kompatybilność z istniejącymi systemami analogowymi oraz zapewnia możliwość migracji do w pełni cyfrowych systemów CCTV w przyszłości.

Wbudowana inteligencja

Tendencja do dodawania inteligentnej obsługi sygnału wizyjnego do systemów CCTV staje się coraz bardziej powszechna i wiąże się między innymi z potrzebą ograniczania kosztownej szerokości pasma transmisji oraz przestrzeni dyskowej. Inteligentne systemy, filtrujące niechcianą lub niepotrzebną transmisję danych lub nagrania, są od wielu lat standardem w krosownicach oraz rejestratorach cyfrowych. Kupienie rejestratora cyfrowego, który nie zapewnia jakiejkolwiek formy wizyjnej detekcji ruchu (VMD), wyzwalającej alarm lub uruchamiającej zapis przy większej prędkości zapisu lub o lepszej jakości obrazu, kiedy rzeczywiście dzieje się coś poważnego, jest już dziś praktycznie niemożliwe. Jednakże większość systemów wizyjnej detekcji ruchu współpracuje tylko z kamerami stałopozycyjnymi.

Wykorzystanie inteligencji wizyjnej detekcji ruchu w systemach szybkoobrotowych kamer kopułkowych wiąże się zarówno z wyzwaniami, jak i z nowymi możliwościami. Oczywistym wyzwaniem jest to, że obraz regularnie się zmienia. Jest to w końcu celem pracy systemu kamer kopułkowych, ale trzeba pamiętać, że w ruchomej scenie trudno jest niezawodnie wykrywać ruch. Jednak większość kamer kopułkowych, szczególnie w większych systemach, pracuje wykorzystując zaprogramowaną trasę składającą się z tylko kilku położeń. W nowszych systemach można zaprogramować różne konfiguracje wizyjnej detekcji ruchu dla każdego położenia zaprogramowanego. Systemy te mogą także, uwzględniając koszty zapisu i transmisji cyfrowej, zatrzymywać obraz podczas obracania kamery pomiędzy położeniami w celu ograniczenia ilości przesyłanych i zapisywanych w tym czasie danych.

Wyobraźmy sobie kamerę kopułkową zainstalowaną w narożniku centrum logistycznego. Można zaprogramować położenia kamery obejmujące ogrodzenie terenu, główne wejścia do budynków oraz rampy załadowcze. Dzięki wbudowanej bezpośrednio w kamerę wielokanałowej technologii VMD, każdej scenie można przypisać osobną, indywidualną konfigurację wizyjnej detekcji ruchu. Ale korzystanie z inteligencji kamery wykraczające poza ten etap dozoru przynosi jeszcze większą korzyść. To, co system robi po wykryciu ruchu jest równie ważne, jak samo wykrywanie ruchu.

Zamiast polegać wyłącznie na przesyłaniu alarmu do zdalnego sterownika CCTV, gdzie rozpoczyna się działanie, inteligentna, nowoczesna kamera kopułkowa będzie oferowała wielopłaszczyznową, inteligentną i programowalną reakcję obejmującą kilka stanów wejściowych, które uaktywniają sekwencje reakcji. Na przykład, wykrycie ruchu może być powiązane z innymi wejściami alarmowymi, takimi jak system detekcji zainstalowany na ogrodzeniu w celu uruchomienia przesyłania sygnału alarmowego przez sieć, włączenia świateł, zwiększenia prędkości zapisu oraz rozpoczęcia śledzenia wykrytego obiektu.

W takim przypadku połączenie kamery kopułkowej oraz inteligentnej technologii wizyjnej ujawnia swoje zalety. Zapoczątkowane przez firmę Bosch automatyczne śledzenie obiektów z wykorzystaniem wbudowanej inteligencji przetwarzania obrazu umożliwia kamerze podążanie za intruzem i zapisywanie obrazu nawet wówczas, gdy teren jest pozbawiony dozoru. Większość widoków z kamery umiejscowionej na zewnątrz budynku zawiera obszary z nieistotnym ruchem, takie jak ścieżki lub drogi poza ogrodzeniem, a także drzewa lub rośliny poruszane przez wiatr. Dlatego ważne jest, aby systemy śledzące ruch mogły tworzyć „wirtualne maski" na obszarach, na których spodziewany jest nieistotny ruch. Ostatnie postępy w technologii umożliwiają dokładne wykrywanie oraz pewne śledzenie obiektów nawet w złożonym środowisku na zewnątrz budynków.

Nowoczesny, inteligentny system kamer kopułkowych umożliwia wykrywanie ruchu w wielu różnych widokach z kamery, w razie potrzeby wyzwala alarm, nawiązuje połączenie transmisyjne z centralną stacją monitoringu oraz śledzi intruza – a wszystko to bez interwencji operatora.

Każdy użytkownik myślący kategoriami rozwojowymi będzie domagał się uzyskania gwarancji, że inwestycja jest bezpieczna oraz zabezpiecza przyszłe wyzwania. Modułowa budowa, która umożliwia łatwą i szybką aktualizację sprzętu oraz oprogramowania układowego, jest niezwykle istotna. Najnowsze systemy kamer kopułkowych, np. Bosch AutoDome, składają się z wymiennych modułów pozwalających użytkownikowi na szybkie i tanie dodawanie zaawansowanych funkcji, takich jak transmisja przez sieć, oraz śledzenie obiektów lub zmianę układów optycznych kamery na najnowsze modele, bez konieczności wymiany całego systemu.

Każdy producent utrzymuje, że jego produkt jest niezawodny. Prawdziwa różnica pomiędzy podobnie wyglądającymi urządzeniami często tkwi nie w specyfikacji funkcjonalnej, ale w gwarancji oferowanej na kompletne urządzenie. Długość gwarancji często odzwierciedla sposób budowy oraz jakość procesu produkcji stosowanego przez producenta. Zaawansowane standardy jakości wymagają wdrożenia procesów jakości Six Sigma i SIE (*Software Engineering Institute*), oraz zgodności procesów wytwarzania, konserwacji i naprawy ze standardami ISO. Najlepsi producenci oferują trzyletnią lub nawet dłuższą gwarancję. Ponadto rygorystyczne procesy testowania, takie jak HALT (*Highly Accelerated Life Testing*) oraz HASS (*Highly Accelerated Stress Screening*), mierzą solidność produktu, wyrażając ją w jednostkach MTBF (*Mean Time Before Failure*), które określają, jak długo urządzenie będzie działać poprawnie – ile czasu przypuszczalnie pozostało do jego awarii.

Kamery kopułkowe są zwykle instalowane w trudno dostępnych miejscach, dlatego posiadają zaawansowane funkcje diagnostyczne, które pozwalają zdiagnozować stan urządzenia zdalnie, bez potrzeby korzystania z drabiny lub podnośnika hydraulicznego. Dzięki funkcjom diagnostycznym można zorientować się, czy kamera pracuje w zakresie dopuszczalnych limitów, sprawdzić krytyczne parametry, takie jak temperatura wewnętrzna czy poziom napięcia zasilającego.

Szybkoobrotowe kamery kopułkowe przeszły bardzo długą drogę od czasu, kiedy kamera i obiektyw z funkcją zoom były mocowane na konwencjonalnym mechanizmie uchylno-obrotowym i instalowane w dużej obudowie. Obecnie kamery są mniejsze i charakteryzują się znacznie lepszymi parametrami, wykorzystując technologiczne nowinki, które zostały zaadaptowane do systemów bezpieczeństwa.

Kamery kopułkowe są zwykle instalowane w trudno dostępnych miejscach, dlatego posiadają zaawansowane funkcje diagnostyczne, które pozwalają zdiagnozować stan urządzenia zdalnie, bez potrzeby korzystania z drabiny lub podnośnika hydraulicznego. Dzięki funkcjom diagnostycznym można zorientować się, czy kamera pracuje w zakresie dopuszczalnych limitów, sprawdzić krytyczne parametry, takie jak temperatura wewnętrzna czy poziom napięcia zasilającego.

Szybkoobrotowe kamery kopułkowe przeszły bardzo długą drogę od czasu, kiedy kamera i obiektyw z funkcją zoom były mocowane na konwencjonalnym mechanizmie uchylno-obrotowym i instalowane w dużej obudowie. Obecnie kamery są mniejsze i charakteryzują się znacznie lepszymi parametrami, wykorzystując technologiczne nowinki, które zostały zaadaptowane do systemów bezpieczeństwa.

Dzięki nieustannemu rozwojowi technologii szybkoobrotowe kamery kopułkowe stały się urządzeniami wysoce inteligentnymi i są istotnym elementem nowoczesnego systemu analogowego lub sieciowego.

Robert Bosch Security Systems

PROTECTOR

SYSTEM KONTROLI DOSTĘPU
i
ROZLICZANIA CZASU PRACY
Z
ELEMENTAMI AUTOMATYKI
„SOYAL"

- Darmowy program obsługi systemu KD oraz RCP
- Pojemność systemu - 15 tysięcy użytkowników
- Praca kontrolerów samodzielna lub w sieci
- Możliwość kontroli 4064 drzwi
- Zakres temperatur pracy kontrolerów do -10°C, czytników do -20 °C
- Współpraca z wieloma czytnikami w różnych formatach (WG26/34, ABA, 125 KHz, 13,56 MHz Mifare, 2,4 GHz)
- Pełna integracja z systemami CCTV oraz SSWiN

Kontroler z wew. czytnikiem oraz wyświetlaczem LCD, wodoszczelny, już od:

540zł netto

Czytnik z klawiaturą już od:

189zł netto

Czytnik już od:

144zł netto

www.protector-polska.pl

tel.: +48 (091) 431 83 10

fax: +48 (091) 431 83 11

biuro@protector-polska.pl

Na polski rynek coraz odważniej wkraczają systemy CCTV IP. Megapikselowa rozdzielczość, w pełni cyfrowa obróbka oraz transmisja obrazu, a także skalowalność systemu to niepodważalne zalety rozwiązań IP. Autor postara się odpowiedzieć na pytanie, czym tak naprawdę są systemy IP i czy rzeczywiście należy spodziewać się, że w najbliższym czasie klasyczne analogowo-cyfrowe rozwiązania odejdą do lamusa

Systemy CCTV IP

Elementy systemu IP

Kamera IP

Najważniejszym i często jedynym elementem systemu IP jest **kamera IP**. Kamery stosowane w systemach IP, mimo kilku wspólnych cech (optyka), znacznie różnią się od swoich poprzedniczek – kamer analogowych. Do ich najważniejszych elementów zaliczyć można matrycę CCD (*Charge Coupled Device*) lub CMOS (*Complementary MOS*), procesor odpowiedzialny za analizę i kompresję obrazu, wbudowany interfejs sieciowy oraz zastosowane oprogramowanie.

Światło wpadające do obiektywu, po przejściu przez szereg filtrów dolnoprzepustowych (m.in. filtr podczerwieni) pozwalających na zachowanie poprawnej kolorystyki i jakości obrazu, ogniskowane jest na matrycy CCD. Matryca przetwarza światło – a tym samym obraz – na sygnały elektryczne, które mogą zostać poddane kompresji przez zastosowany w kamerze procesor. Otrzymany w ten sposób materiał jest transmitowany przez interfejs sieciowy.

W tym miejscu uwidacznia się przewaga kamer IP nad kamerami analogowymi. Obraz powstający w wyniku zastosowania matrycy CCD nie jest ograniczony rozmiarem PAL D1 (720x576 pikseli) i może znacznie przekraczać tę rozdzielczość. Obecnie najpopularniejsza rozdzielczość stosowana w kamerach IP to 1,3 MPix czyli 1280x1024 piksele, spotyka się jednak kamery pracujące w jeszcze wyższych rozdzielczościach, dochodzących nawet do 5 Mpix (2560x1920 pikseli). Ilość szczegółów zarejestrowanych z taką rozdzielczością jest z pewnością nie do przecenienia i nie ma swojego odpowiednika wśród kamer analogowych.

Kamery IP posiadają wbudowany *webserwer*, cała instalacja polega zatem na podłączeniu zasilania kamery (na rynku dostępne są także kamery zasilane bezpośrednio z kabla UTP), przypisaniu jej adresu IP i podłączeniu za pomocą dedykowanej aplikacji bądź przeglądarki internetowej. Instalacja kilku czy nawet kilkunastu kamer przebiega w podobnych sposób, a obraz transmitowany przez kamery może być zapisany na dowolnym z komputerów podłączonych do systemu.

Widoeserwer i wideodekoder

W sytuacji, w której przystosowujemy istniejący system CCTV do standardów IP, konieczne może stać się podłączenie do systemu IP kamer analogowych. Pomocny może być wówczas kolejny element, tzw. **wideoserwer**. Zadaniem tego urządzenia jest digitalizacja analogowego obrazu i jego transmisja poprzez sieć już w postaci cyfrowej, kompatybilnej z pozostałymi strumieniami systemu IP. Wideoserwery posiadają najczęściej od jednego do czterech wejść analogowych, przetwornik obrazu oraz procesor odpowiedzialny za jego kompresję. Podobnie jak w przypadku kamer IP, wbudowany w wideoserwer *webserwer* pozwala na połączenie się z nim bezpośrednio poprzez przeglądarkę internetową. Warto zauważyć, że stosowanie wideoserwerów pozwala na wyeliminowanie z systemu rejestratorów DVR, gdyż zapis może odbywać się na dowolnym z komputerów PC podłączonych do sieci.

Odwrotną do wideoserwera funkcję pełni **wideodekoder**. Urządzenie to pozwala na dekompresję obrazu z systemu IP i wyświetlenie go na monitorze analogowym lub zarejestrowanie przez DVR. Niektóre z widedekoderów pełnią jednocześnie funkcję dzielnika obrazu, gromadząc dane np. z czterech kamer i wyświetlenie ich w widoku typu *Quad*. Urządzenia te mają zastosowanie najczęściej w sytuacji, gdy do dużego systemu analogowo-cyfrowego podłączana jest jedna bądź kilka pojedynczych kamer IP.

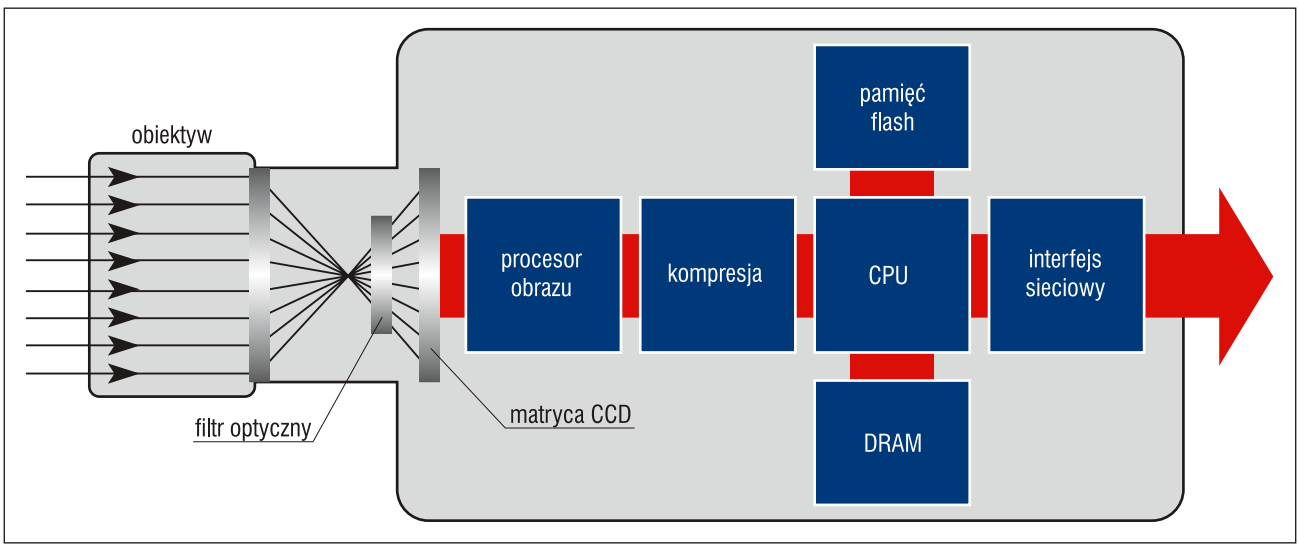
Rejestrator IP

Na samym końcu w systemie IP może zostać umieszczony **rejestrator**, który służy, jak sama nazwa wskazuje, do zapisywania i archiwizacji materiału. Funkcję rejestratora, jak wspomniano wyżej, może pełnić również każdy z komputerów osobistych podłączonych do systemu, dlatego też nie wszyscy producenci rozwiązań IP posiadają w swojej ofercie rejestratory. Oprogramowanie pełniące funkcję rejestratora pozwala najczęściej na zapis obrazu z 4–16 kamer. Rozwiązania przewidziane dla większych systemów są często dodatkowo płatne.

Przyszłość CCTV IP oraz systemów analogowo-cyfrowych

Wysoka rozdzielczość oraz dobra jakość obrazu to nie jedyna zaleta systemów IP. Nie bez znaczenia jest fakt zmniejszenia ilości potrzebnych do stworzenia systemu kabli oraz skalowalność systemu, do którego niezwykle łatwo można dodać kolejną kamerę. Zdalny dostęp do każdego elementu składowego systemu niezwykle ułatwia zarządzanie i konserwację poszczególnych podzespołów. Czy należy zatem oczekiwać, że systemy IP szybko zastąpią swoje starsze odpowiedniki?

Mimo ciągłego poszerzania oferty, oferowanych na rynku urządzeń IP jest niestety nadal mniej niż elementów systemów analogowo-cyfrowych. Rynek podzespołów IP dopiero kształtuje się, co ma swoje odbicie również w wysokich cenach tego typu urządzeń. Za wzrastającymi możliwościami kamer IP nie nadąża infrastruktura sieciowa. Dla systemów kilkukamerowych, pracujących w rozdzielczościach megapikselowych, wskazane jest stosowanie sieci o gigabitowej przepustowości. W polskich realiach internetowych obserwowanie obrazów z kamer o wysokich rozdzielczościach spoza sieci lokalnej może okazać się dosyć frustrującym zajęciem. Wiele z aktualnie działających rozwiązań CCTV stanowi element większego, zintegrowanego systemu. Wymiana urządzeń na system IP będzie wymagała przebudowy pozostałych elementów (kontrola dostępu, systemy sygnalizacji pożaru itp.) wchodzących w skład inteligentnego budynku. Należy również pamiętać, że systemy IP buduje się, bazując na innych rozwiązaniach niż dotychczas stosowana telewizja dozorowa. Silna informatyzacja branży CCTV zmusza instalatorów do ciągłego podnoszenia swych kwalifikacji i zaznajamiania się z nowościami sprzętowymi, co wymaga czasu.



Podsumowanie

Wszystko raczej wskazuje na powolne dostosowywanie się rynku do rozwiązań IP niż intensywną wymianę dotychczasowych systemów CCTV na ich nowsze odpowiedniki. Bardzo podobnie przedstawia się sytuacja na rynkach zachodnich, gdzie, mimo wyższego poziomu infrastruktury internetowej, systemy IP – choć wdrażane coraz częściej – nie wyparły z rynku sprzętu analogowo-cyfrowego. Stosowane są przede wszystkim w obiektach rozproszonych, stanowiących inwestycje o dużej skali, w których trudno byłoby zastosować analogowe rozwiązania.

Marcin Gierszner

www.ivs-system.pl

NOVUS®

Profesjonalne rozwiązanie dla systemów CCTV

Bezpieczne osiedle

Firma Novus, działając w obszarze technicznej ochrony osób i mienia, specjalizuje się w systemach monitoringu wizyjnego gwarantując najwyższą jakość i nowoczesność oferowanych wyrobów. Posiadamy doświadczenie w realizacji systemów monitoringu wizyjnego typu „bezpieczne miasto", dużych osiedli i kompleksów mieszkaniowych. Koncepcja systemu monitoringu firmy Novus dla osiedli cechuje się elastyczną konfiguracją, najwyższą jakością materiału rejestrowanego oraz możliwością udostępniania strumieni wideo różnym użytkownikom w zależności od posiadanych uprawnień.

>> Lokalizacja rejestratorów w pobliżu miejsc montażu kamer. Brak konieczności realizacji skomplikowanych i dalekich połączeń kablowych.

>> Możliwość elastycznego tworzenia dodatkowych centrów monitoringu i przenoszenia już istniejących w inne lokalizacje.

>> Połączenie typu „multisite". Za pomocą aplikacji RAS istnieje możliwość tworzenia „wirtualnych" lokalizacji składających się z wybranych kamer z różnych rejestratorów. Możliwość realizacji równoczesnego połączenia z kilkudziesięcioma rejestratorami lub automatycznego przełączania lokalizacji.

>> Graficzne interfejsy użytkownika. W celu intuicyjnego zarządzania systemem istnieje możliwość tworzenia map osiedli i zarządzania elementami systemu (kamerami, wyjściami przekaźnikowym, wejściami alarmowymi) za pomocą graficznych ikon.

>> Możliwość tworzenia 256 grup użytkowników o różnych poziomach dostępu do poszczególnych rejestratorów. Możliwość ograniczenia uprawnień m.in. dostępu do menu, podglądu kamer ukrytych, sterowania kamerami obrotowymi i moto-zoom, odtwarzania zapisanych materiałów itp.

>> Ustawienia menu. Wszystkie ustawienia menu rejestratora mogą być dokonywane zdalnie za pomocą dedykowanego oprogramowania. Pozwala to na skoncentrowanie obsługi rejestratorów w centrum monitoringu.

>> Funkcje autodiagnostyki i powiadamiania. Automonitoring stanu systemu (m.in. temperatura dysku, uszkodzenie partycji, ocena procesu nagrywania). Dla zdarzeń systemowych i alarmowych rejestrator może uruchamiać akcję powiadamiania do 5 zdalnych hostów lub na adres e-mail. Pozwala to na optymalizację pracy operatorów i reakcję tylko na rzeczywiste zagrożenia w obiekcie.

>> Integracja z innymi systemami. Możliwość integracji z systemami kontroli dostępu, ppoż, automatyki (otwieranie / zamykanie bram, sterowanie oświetleniem).

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

Monitoring wizyjny

osiedli mieszkaniowych

Systemy telewizji dozorowej są standardowymi systemami bezpieczeństwa w nowo oddawanych do użytku budynkach mieszkalnych i użyteczności publicznej oraz realizowanych osiedlach mieszkaniowych. Oczywiste zalety telewizji dozorowej dla mieszkańców powodują, że również istniejące już osiedla oraz spółdzielnie mieszkaniowe w celu poprawy bezpieczeństwa i komfortu mieszkańców decydują się na instalację systemu kamer.

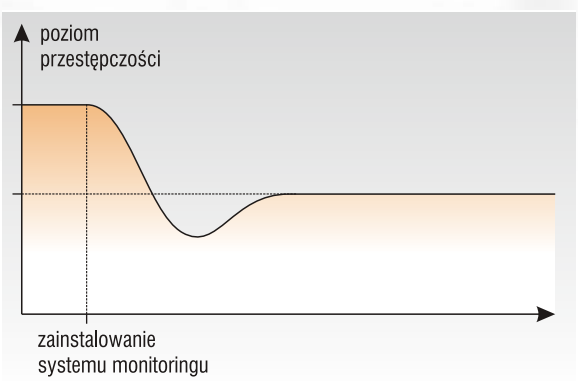
W związku z coraz większym naciskiem społeczeństw na kwestie bezpieczeństwa oraz stosunkowo wysokim poziomem akceptacji dla monitoringu wizyjnego miejsc publicznych należy oczekiwać coraz większego upowszechniania się takich systemów. Dodatkowo stale spadające koszty urządzeń CCTV powodują, że nawet niewielkie osiedla i wspólnoty mogą sobie pozwolić na zainstalowanie takich systemów bez nadmiernego obciążenia budżetu.

Realizacja systemów monitoringu ma na celu:

- zniechęcanie potencjalnych przestępców do podejmowania działań w rejonie objętym monitoringiem (prewencja);
- nadzór nad miejscami mającymi kluczowe znaczenie dla bezpieczeństwa mieszkańców, ciągami komunikacyjnymi, parkingami itp.;
- uzyskiwanie materiału filmowego o jakości pozwalającej na ewentualne wykorzystanie go w procesie sądowym;
- zapewnienie skutecznych i szybkich interwencji w sytuacjach kryzysowych (we współpracy z policją oraz innymi służbami porządkowymi).

Przeprowadzone badania dowodzą, że instalacja systemu monitoringu pozwala zredukować przestępczość nawet o 80%. Jeżeli nawet przestępczość wzrasta, na obszarach monitorowanych jest zawsze niższa, niż tam, gdzie nadzoru wizyjnego brak. Po instalacji systemu istnieje tendencja do migracji przestępczości w obszary nie objęte takim nadzorem, dlatego szczególnie ważne jest zastosowanie monitoringu na całym obszarze osiedla.

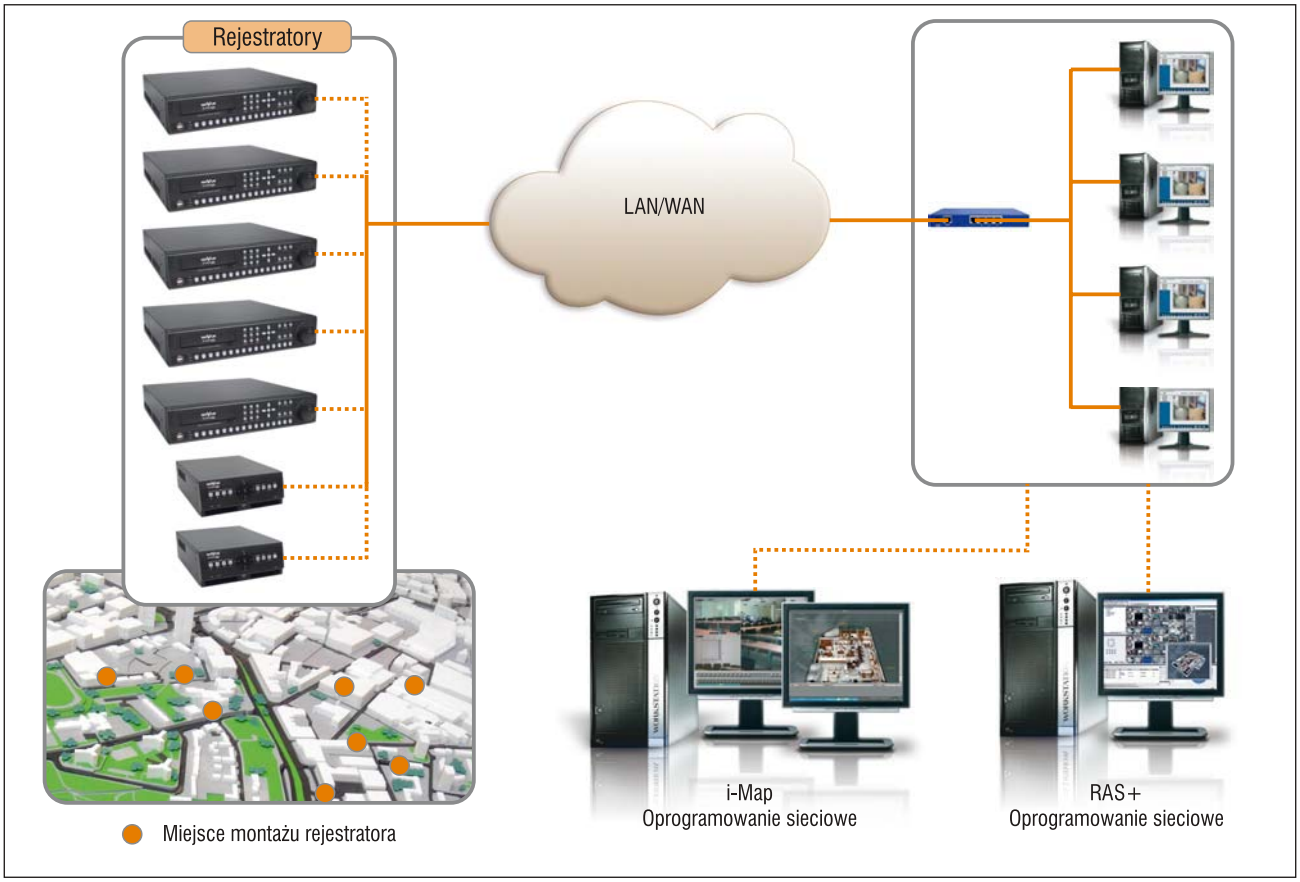
W niniejszym artykule chciałbym skoncentrować uwagę Czytelnika na technicznych aspektach realizacji prawidłowego systemu monitoringu. Równie ważne przy realizacji systemów monitoringu, zwłaszcza w kontekście ostatniego z wymienionych wyżej celów, są kwestie organizacyjne oraz ustanowione przez administratora systemu procedury działania w określonych sytuacjach. Wynikają one jednakże z lokalnych uwarunkowań, polityki bezpieczeństwa władz dzielnicy lub miasta i możliwości integracji danego systemu monitoringu z systemem monitoringu miasta.



Rys. 1. Poziom przestępczości po zainstalowaniu sytemu monitoringu wizyjnego

Aby zbudować efektywny system monitoringu, należy w pierwszej kolejności stworzyć jego koncepcję. Trzeba m.in.:

- ustalić na podstawie rozmów z mieszkańcami oraz organami porządkowymi liczbę punktów kamerowych oraz ich typy (kamery stacjonarne, obrotowe, kolorowe, typu dzień/noc);
- określić, czy system będzie bezobsługowy, czy będzie posiadał centra nadzoru (oraz ustalić dokładną ich liczbę); udostępnić sygnały wizji innym użytkownikom, np. policji, mieszkańcom itp.
- dokonać wyboru medium transmisyjnego (światłowód, droga radiowa lub kable miedziane) oraz typu przesyłanych sygnałów (sygnał analogowy czy sygnał cyfrowy); ustalić sposób dystrybucji poszczególnych obrazów z kamer do centrów monitoringu oraz możliwości wykorzystania już istniejącej kanalizacji teletechnicznej;
- określić sposób oraz parametry archiwizacji, kopiowania i udostępniania nagranego materiału (czas archiwizacji, rozdzielczość, jakość);
- określić, czy budowany system jest docelowy, czy powinna istnieć możliwość jego rozbudowy i ewentualnej integracji z elementami już działającego systemu bezpieczeństwa.



Rys. 2. Przykładowy schemat połączeń systemu rozproszonego

Takie sformułowanie koncepcji pozwala wstępnie oszacować koszty jej realizacji. Na podstawie powyższych ustaleń należy sporządzić mapę z naniesionymi wszystkimi elementami tej koncepcji. Dzięki niej będzie można stworzyć szczegółowy projekt systemu monitoringu z precyzyjnym opisem każdego punktu kamerowego, proponowanych urządzeń i sposobu ich funkcjonowania oraz przebiegu tras kablowych i związanych z tym prac.

Zakończenie budowy systemu monitoringu wizyjnego wiąże się z procedurami testowania i odbioru. Należy potwierdzić zgodność zastosowanych urządzeń z projektem (dokumentacją techniczną), prawidłowość ich montażu oraz poprowadzenia okablowania. Dodatkowo należy określić, czy sceny obserwowane przez kamery odpowiadają założeniom koncepcyjnym oraz czy sygnał wizyjny jest zgodny z normami telewizji dozorowej i odpowiednimi przepisami dotyczącymi warunków rozpoznania i identyfikacji osób. Niespełnienie powyższych standardów uniemożliwi wykorzystanie zarchiwizowanych materiałów w procesie dowodowym.

Aby zapewnić nieprzerwane działanie systemu, należy zadbać o serwisowe i techniczne wsparcie wykonawcy po oddaniu systemu do użytkowania. Jeśli w umowie wykonawczej brakuje zapisów dotyczących okresowych testów sprawności w okresie gwarancyjnym oraz po tym okresie, system jest skazany na stopniową utratę funkcjonalności i powolne umieranie. Jeśli nie dokonuje się okresowych przeglądów i napraw oraz nie czyści kamer i obudów (kloszy), komfort i efekty pracy operatorów są ograniczone.

Firma Novus specjalizuje się w systemach monitoringu wizyjnego. Bazując na urządzeniach oraz autorskich opracowaniach firmy, zrealizowano wiele systemów nadzoru dla osiedli oraz systemów typu „bezpieczne miasto". Novus posiada doświadczenie w realizacji systemów monitorujących złożonych z kilku do kilkudziesięciu punktów kamerowych. Każde osiedle lub dzielnica, ze względu na swoje położenie, stopień zagrożenia przestępczością, dostęp do infrastruktury telekomunikacyjnej, określa własne wymagania dotyczące sposobu funkcjonowania sprzętu. Dzięki pełnemu nadzorowi nad procesem projektowania urządzeń oraz oprogramowania, jesteśmy w stanie dokonać zmian w produkcie w zależności od postawionych wymagań.

Szczególnej uwadze realizujących systemy monitoringu wizyjnego polecane są kamery szybkoobrotowe serii CAMA-I, rejestratory serii NV-DVR3000 i NV-DVR5000, a także systemy wykorzystujące karty przechwytujące Novus.

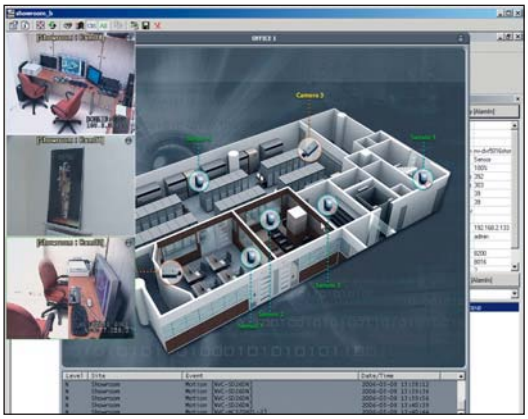
W obrębie serii zintegrowanych kamer szybkoobrotowych CAMA-I można wyróżnić trzy modele:

- NVC-SD18DNA – typu dzień/noc (zoom 18x, przetwornik CCD 1/4" ExViewHAD SONY);
- NVC-SD22DN – typu dzień/noc (zoom 22x, przetwornik CCD 1/4" SuperHAD SONY);
- NVC-SD26DN – typu dzień/noc (zoom 23x, przetwornik 1/4" ExViewHAD SONY).

Wszystkie modele serii posiadają identyczny wygląd i funkcje, a różnice dotyczą jedynie zastosowanego modułu kamerowego i, tym samym, różnych ustawień automatyki ekspozycji. Zastosowane przetworniki CCD 752 (H) x 582 (V) pikseli umożliwiają generowanie obrazu wideo wysokiej rozdzielczości (480 linii telewizyjnych w trybie kolorowym oraz 570 w trybie monochromatycznym). Zmiany ogniskowej w szerokim zakresie (dla modelu NVC-SD26DN w granicach 3,5–91 mm) umożliwiają zarówno obserwację szerokich planów (poziomy kąt widzenia 54,2°), jak i realizację dużych zbliżeń (poziomy kąt widzenia 2,2°). Oprogramowanie kamery pozwala również na realizację zoomu cyfrowego o krotności od 10 do 12 razy, w zależności od modelu. Zapewnia to uzyskiwanie zbliżeń nawet 312-krotnych.

Seria kamer szybkoobrotowych CAMA-I jest przeznaczona do pracy w warunkach słabego oświetlenia. Sprawdza się bardzo

dobrze zwłaszcza w systemach monitoringu wizyjnego miast, które stawiają przed kamerami najwyższe wymagania w zakresie niezawodności elementów mechanicznych i optycznych oraz odporności na niekorzystne i zmienne warunki atmosferyczne. W kamerach CAMA-I można zaprogramować ujęcia programowalne, które umożliwiają szybką i sprawną obsługę urządzenia (do 240 presetów), a także cztery trasy obserwacji. Trasa obserwacji jest to ciąg zaprogramowanych funkcji (uchył, obrót, przybliżenie itp.). Maksymalny czas potrzebny do wykonania zadań na wszystkich trasach wynosi 240 s (cztery minuty). Połączenie powyższych funkcji umożliwia tzw. patrol. Jest to schemat obserwacji składający się z 42 elementów (presetów, tras obserwacji, funkcji automatycznego skanowania oraz samych funkcji patrolu).



Rys. 3. Mapa obiektu z podglądem obrazu z kamer

Choć ramy niniejszego artykułu nie pozwalają na przedstawienie wszystkich dostępnych sposobów rejestracji oraz zarządzania poszczególnymi strumieniami wizji, warto rozważyć zbudowanie systemu rozproszonego bazującego na serii rejestratorów NV-DVR5000.

Dostarczane wraz z urządzeniem zaawansowane aplikacje sieciowe umożliwiają budowę centralnych stacji monitorowania, zdolnych do nadzoru i podglądu obrazów z kamer z wielu lokalizacji rozproszonych. Możliwości zdalnej konfiguracji oraz monitorowania stanu pracy urządzeń pozwalają na wyeliminowanie lokalnej obsługi i skupienie wszystkich funkcji zarządzających w jednym lub kilku oddalonych centrach zarządzania. Automatyczne nawiązywanie przez rejestrator połączeń ze zdefiniowanymi lokalizacjami pozwala na efektywne wykorzystanie pracy operatora i obserwację obrazów z kamer tylko z lokalizacji, w których nastąpiły zdefiniowane uprzednio zdarzenia krytyczne, takie jak aktywacja wejścia alarmowego czy detekcja ruchu.

Dodatkowo, aby usprawnić pracę operatorów, aplikacje sieciowe umożliwiają wykorzystanie samodzielnie przygotowanych przez administratora systemu podkładów graficznych – map. Dzięki łatwości i intuicyjności obsługi oraz unikatowym cechom użytkowym, oprogramowanie to pozwala na zwiększenie efektywności pracy operatorów i tym samym lepszy dozór monitorowanych obiektów.

Od zastosowanych rozwiązań oraz wyboru wykonawcy systemu monitoringu wizyjnego zależy poczucie bezpieczeństwa mieszkańców. Aby to bezpieczeństwo umocnić i profesjonalnie chronić wspólne mienie mieszkańców oraz ich samych, należy zaufać partnerom sprawdzonym, posiadającym doświadczenie w realizacji takich systemów oraz dysponującym najbardziej zaawansowanymi rozwiązaniami technologicznymi, gwarantującymi najwyższą jakość i niezawodność. Firma Novus zapewnia najwyższą jakość oferowanych rozwiązań oraz pomoc w planowaniu i realizacji takich systemów.

Patryk Gańko
Novus

C & C

T<H GROUP

Monitoring dla małych firm

SID-450

Kamera kopułkowa
o wysokiej rozdzielczości
do pracy w dzień i w nocy
z możliwością obrotu
w 3 osiach.
Do montażu ściennego
lub sufitowego,
z wbudowanym obiektywem
zmiennoogniskowym
3x (ogniskowa 3-9 mm).
Wysoka rozdzielczość
530 linii TV.
Wysoka czułość
0,002 Lx (Sens-up).

SID-50

Kamera kopułkowa
o wysokiej rozdzielczości
do pracy w dzień i w nocy.
Stały obiektyw
(ogniskowa 3 mm).
Wysoka rozdzielczość
530 linii TV.
Wysoka czułość
0,002 Lx (Sens-up).

SDC-415

Kamera o wysokiej
rozdzielczości
do pracy w dzień i w nocy.
Wysoka rozdzielczość
530 linii TV.
Wysoka czułość
0,002 Lx (Sens-up).

SOC-4030

Kamera o wysokiej
rozdzielczości
do pracy w dzień i w nocy
z wbudowanym obiektywem
zmiennoogniskowym.
Szybka, prosta w instalacji
z wbudowanym obiektywem
zmiennoogniskowym
3x (ogniskowa 3-9 mm).
Wysoka rozdzielczość
530 linii TV.
Wysoka czułość
0,002 Lx (Sens-up).

SVR-440

Rejestrator cyfrowy

W komplecie taniej!

SAMSUNG TECHWIN

Autoryzowany dystrybutor Samsung Techwin w Polsce:
C&C Partners Telecom Sp. z o.o.

www.samsungcctv.ccpartners.pl

Siedziba: ul. 17 Stycznia 119, 121, 64-100 Leszno, tel. 065 525 55 55, fax 065 525 56 66, e-mail: cctv@ccpartners.pl

Oddział Gdańsk
ul. Szymanowskiego 2, 80-280 Gdańsk
tel. 048 583 45 08 57, fax 048 585 52 30 61

Oddział Katowice
ul. Kościuszki 175, 40-524 Katowice
tel. 032 201 78 90, fax 032 201 78 95

Oddział Warszawa
Ursynów Business Park
ul. Puławska 303 wejście B, 02-785 Warszawa
tel. 022 549 70 00, fax 022 549 70 10

artykuł sponsorowany

Rejestratory Novus serii 5000 – OPROGRAMOWANIE SIECIOWE (cz. 4)

W numerze 2/2006 *Zabezpieczeń* zakończona została prezentacja rejestratora Novus serii NV-DVR5000 oraz współpracujących z nim aplikacji sieciowych. W podsumowaniu poinformowano, że trwają prace nad kolejnymi generacjami oprogramowania zwiększającego funkcjonalność systemu. Obecnie zakończono już prace nad aplikacją RAS+. Niniejszy artykuł ma na celu przedstawienie jej najważniejszych funkcji oraz zachęcenie do zastąpienia nią dotychczas używanych aplikacji RAS oraz IMAP.

W oprogramowaniu RAS+ zostały scalone moduły do zarządzania, podglądu na żywo i odtwarzania oraz moduł graficznych interfejsów użytkownika (map), co pozwala na równoczesny dostęp do powyższych funkcji oraz daje większą swobodę operatorom systemu w procesach nadzoru i obsłudze systemu.

Interfejs graficzny aplikacji nie ma predefiniowanej rozdzielczości i może być skalowany w zależności od potrzeb operatora. Dodatkowo oprogramowanie umożliwia pracę dwumonitorową. Poszczególne okna mogą być przenoszone w dowolne miejsce ekranów, zagnieżdżane w innych oknach lub automatycznie ukrywane, jeżeli nie są używane. Pozwala to na pełne dostosowanie aplikacji do aktualnych potrzeb lub zadań operatora i jego efektywną pracę.

W obrębie jednego programu instalacyjnego zostały zebrane wszystkie dostępne wersje językowe, pozwalając na wybór wersji językowej przed każdym uruchomieniem lub zdefiniowanie domyślnej wersji językowej. Dostępne języki to m.in. polski, hiszpański, rosyjski, niemiecki.

Aplikacja umożliwia łączenie się z wieloma rejestratorami równocześnie. Dowolne kamery mogą być powielane w wielu oknach. Stworzone przez użytkownika widoki z kamer z różnych rejestratorów (do 64) mogą być zapamiętywane i następnie automatycznie wywoływane. Dodatkowo w widokach użytkownik może nadać poszczególnym kamerom dowolną nazwę, niezależną od nazwy przyporządkowywanej przez rejestrator. Szczególnie przydatną funkcją jest możliwość jednoczesnego podglądu i odtwarzania wybranych kamer z wielu rejestratorów. Pozwala to na obserwację sytuacji na żywo oraz, dodatkowo, w drugim oknie, ze zdefiniowanym opóźnieniem.

W przypadku nagłych zdarzeń operatorzy systemu posiadają możliwość lokalnej rejestracji wyświetlanych na ekranie monitora obrazów z kamer w znanym już formacie minibank. Administrator systemu może zdefiniować maksymalną pojemność zapisanych danych i włączyć funkcję nadpisywania.

Do aplikacji RAS+ została dodana obsługa graficznych interfejsów użytkownika, czyli map. Obraz z kamer podłączonych do ikon mapy można wyświetlać w niezależnych oknach lub przeciągać do okien głównego programu. Najbardziej efektywnym sposobem nadzoru jest wykorzystanie podczas pracy dwóch monitorów (karta graficzna typu *dual head*) – z główną aplikacją na jednym z nich oraz aplikacjami dodatkowymi (np. obsługą map, alarmów lub odtwarzania) na drugim.

Raporty stanu pracy rejestratorów mogą być generowane automatycznie z zadanym przedziałem czasowym. Rozszerzona została lista sprawdzanych zdalnie elementów: m.in. praca kamer, działanie alarmów, stan nagrywania oraz zakres dostępnych nagrań.

Odbierane przez aplikację z rejestratorów informacje o zdarzeniach krytycznych mogą być wyświetlane w dowolnych oknach podziału metodą przeciągnij i upuść. Pozwala to na szybką reakcję na zdarzenia w systemie. Funkcjonalność ta będzie zwiększana m.in. poprzez określanie czasu reakcji operatora od momentu otrzymania alarmu do momentu połączenia się z krytyczną lokalizacją, dodanie podstawowych informacji o lokalizacji i telefonach kontaktowych oraz zmianę statusu alarmu w momencie realizacji połączenia.

Zoptymalizowano również wyświetlanie zdarzeń alarmowych w module odtwarzania Dzięki temu można szybko wyszukiwać zarejestrowane zdarzenia krytyczne w systemie.

Przedstawienie w artykule zasadniczych zalet RAS+, tzn. pełnej skalowalności oraz elastyczności, jest nader trudne. Najlepszym sposobem realizacji tego zamierzenia byłby pokaz lub osobiste przetestowanie oprogramowania. Dlatego wszystkich użytkowników rejestratorów serii NV-DVR5000 zachęcam do poprawienia funkcjonalności tych urządzeń poprzez zainstalowanie aplikacji RAS+.

Patryk Gańko
Novus

Przykładowy screen z aplikacji RAS+

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

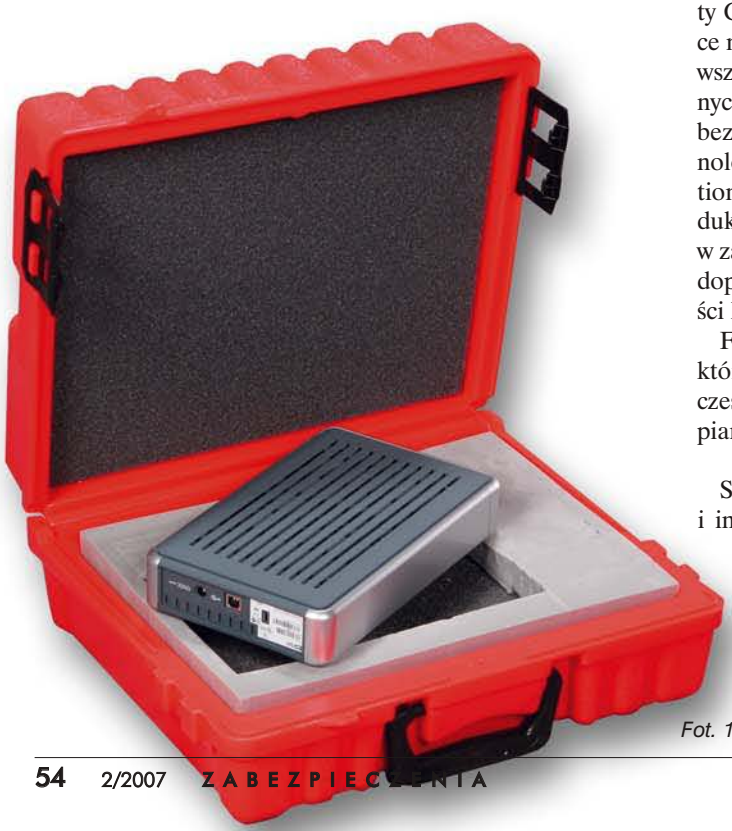
Jak uchronić dane znajdujące się na dysku twardym w trakcie jego przenoszenia?

Dyski twarde należą do najbardziej wrażliwych na wstrząsy nośników danych. Dlatego nie są zalecane przez producentów do przenoszenia danych na odległość. Niekiedy jednak jesteśmy do tego zmuszeni. Dysk jest wówczas narażony na wstrząs, istnieje także ryzyko upuszczenia dysku. Również oddając go w obce ręce, chcielibyśmy mieć pewność, że nie ulegnie uszkodzeniu, a nasze dane pozostaną nienaruszone.

Profesjonalne zabezpieczenie danych

Profesjonaliści zajmujący się przechowywaniem i transportowaniem dużej ilości danych rozumieją, że wartość i bezpieczeństwo informacji na nośnikach wymagają zastosowania specjalnej ochrony. Właśnie ze względu na potrzeby centrów danych zaczęto rozwijać technologie mające zapewniać odpowiednie warunki do przechowywania i przenoszenia nośników. Oprócz ochrony przed uderzeniami i upadkami, zaczęto oczekiwać również szczelnego zabezpieczenia dysków przed wilgocią i cząstkami unoszącymi się w powietrzu. Do przechowywania nośników solidne rozwiązania ognioodporne oferuje firma Phoenix Safe (*www.phoenixsafe.pl*).

W dziedzinie produktów służących do transportu nośników wyspecjalizowała się firma Turtle Case (*www.turtle.mtstorage.pl*). Jej produkty, zabezpieczające dodatkowo przed wyładowaniami elektrostatycznymi i promieniowaniem UV, spełniają wszystkie wspomniane wymogi dotyczące właściwego przenoszenia danych. Walizki Turtle Case stanowią idealny środek transportu dzięki trwałości tworzywa polietylenowego. Jednocześnie, ponieważ jest ono lekkie, koszty bezpiecznego przewożenia większej liczby dysków są niskie. Brak ostrych krawędzi i wygodne wgłębienia ułatwiają przenoszenie i układanie walizek. Możliwość oplombowania każdej walizki stanowi dodatkowy atut.



Fot. 1. Walizka Turtle Case RHD 2 Multi

Dysk twardy chroniony jak nigdy dotąd

Duży asortyment produktów Turtle Case do przenoszenia różnych nośników informacji, w tym także dysków twardych, uwzględnia również potrzeby indywidualnego użytkownika – w ofercie producenta znajdziemy między innymi małe walizki, do przenoszenia jednego czy dwóch dysków twardych.

Hermetycznie zamykana kasetka Turtle Case Multi2 redukuje szkodliwe dla zapisanych na dysku danych zmiany temperatury i dostęp wilgoci. Podwójne ścianki, wykonane z tworzywa o unikatowych właściwościach, pochłaniają siłę uderzenia i niwelują wstrząsy przenoszone na dysk, zapewniając zarazem izolację termiczną. Samoblokujące się podwójne zamki stanowią dodatkowe zabezpieczenie. W efekcie użytkownik otrzymuje lekką, ważącą zaledwie 1,8 kg, a jednocześnie bardzo trwałą kasetkę. Przenoszenie w niej twardego dysku jest komfortowe, nie trzeba obawiać się o zapisane na nim dane.

Korzystający z większej liczby dysków twardych będą zadowoleni z walizki Turtle Case RHD 10. W specjalnych przegrodach można w niej umieścić dziesięć niestykających się ze sobą nośników.

Technologia Turtle Case dla każdego nośnika

Turtle Case może chronić także dyski optyczne – płyty CD, DVD, Blu-ray HD-DVD czy UDO. W jednej walizce można przenieść aż do 55 nośników optycznych. Również wszystkie rodzaje taśm magnetycznych do archiwizacji danych (DDS, 8 mm, AIT, VXA, LTO, DLT, SLDT) mogą być bezpiecznie przenoszone w produktach Turtle Case. Technologię wykonania walizek rekomendują firmy IBM i Imation – najwięksi producenci nośników magnetycznych. Produkty Turtle Case mogą pomieścić od jednej aż do 20 kaset, w zależności od ich rodzaju. Trwale wyżłobione przegrody są dopasowane do ich rozmiarów, co daje gwarancję stabilności każdej taśmy w walizce.

Firma Turtle Case zaspokaja również potrzeby klientów, którzy chcą transportować różne rodzaje nośników jednocześnie. Jest to możliwe dzięki zastosowaniu wypełnienia piankowego w modelach Multi.

Specyfikację techniczną dotyczącą produktów Turtle Case i innych technologii zabezpieczania nośników można uzyskać u konsultantów MT Storage:
tel. (012) 414 07 40, e-mail biuro@mtstorage.pl
i pod adresem *http://www.turtle.mtstorage.pl.*

MT Storage

firma ATLine®

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

CODELOCK TYP 525

Mechaniczny zamek szyfrowy typ 525, bez baterii, bez zasilania, łatwy montaż i zmiana kodu (8000 kodów do wyboru). Blokada zamka w pozycji „zamek otwarty".

438,- netto

ERMO 482, ERMO 482XPRO

S klasa

ERMO 482
jest bistatycznym detektorem mikrofalowym służącym do ochrony zewnętrznej. Zasięg: 50 m, 80m, 120m, 200m

ERMO 482X PRO
jest barierą mikrofalową z cyfrową obróbką sygnału o zasięgu 50, 80, 120 i 200m. Mikroprocesor zawarty w urządzeniu wykorzystuje zaawansowaną analizę sygnału uzyskując dzięki temu znakomite osiągi w detekcji sygnałów i odporności na fałszywe alarmy.

TYP 481

44,- netto

Czarna mata naciskowa typ 481, wymiary 350mm x 150mm, minimalny nacisk powodujący zadziałanie maty to 1.5 kg, wyjście NO

ALFA

S klasa

210,- netto

Wewnętrzna czujka mikrofalowa (efekt Doppler'a), zasięg 15 m

MEDUSA

9860,- netto za 4 strefy

Zewnętrzna bariera mikrofalowa w obudowie „lampy", zasięg między nadajnikiem a odbiornikiem do 50 mb.

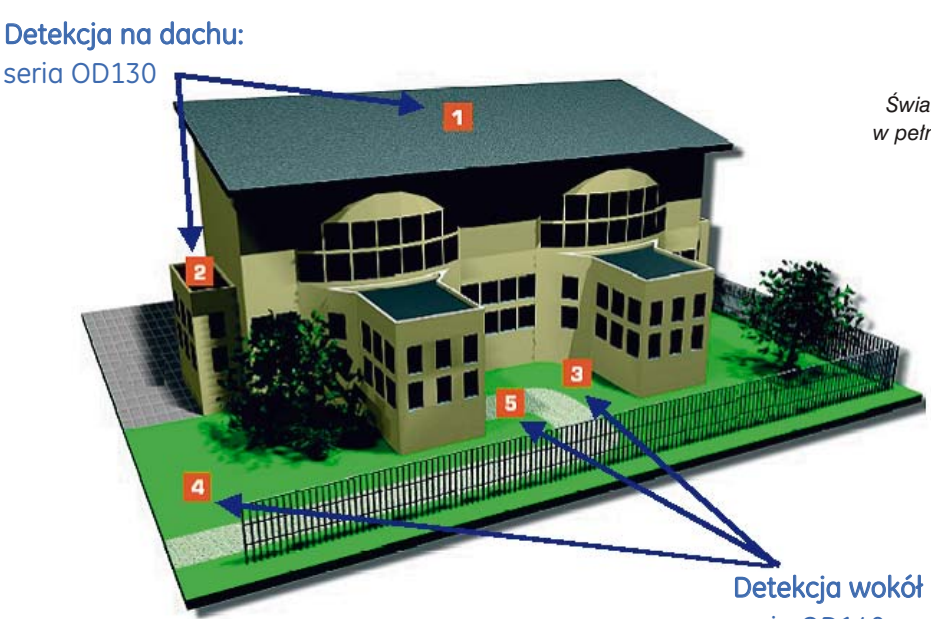
GE Security

Światłowód detekcyjny

Fot. 1. Moduły siatkowe dedykowane do ochrony dachu

Na rynku zabezpieczeń pojawił się nowy produkt: światłowód detekcyjny firmy GE Security. Jest to niewidzialne z zewnątrz rozwiązanie, pozwalające na skuteczne wykrycie intruza, zanim wejdzie on do środka obiektu.
Zapraszam do bliższego zapoznania się z tym interesującym systemem ochrony obwodowej.

Każdy z producentów systemów zabezpieczeń chwali się, że jego czujki nie powodują fałszywych alarmów. Można się też spotkać z określeniami typu „inteligentna czujka", czy „system rozróżniający człowieka od innych obiektów". Oczywiście informacje marketingowe to często jedynie teoria. W praktyce niestety nadal występują fałszywe alarmy. Zdarza się, że czujka bierze psa za człowieka i generuje alarm. Tak było, jest i pewnie jeszcze długo będzie przy zastosowaniu systemów bazujących jedynie na czujkach. Ponadto często zdarza się, że informacja o alarmie jest przekazywana użytkownikowi w momencie gdy intruz znajduje się już na terenie obiektu. Włamywacz może oczywiście się spłoszyć po usłyszeniu syreny, ale, zanim przyjedzie patrol interwencyjny, złodziej może zdążyć coś ukraść i oddalić się. Firma GE Security postanowiła zmierzyć się z tym problemem i właśnie wprowadza na rynek system wykorzystujący światłowód detekcyjny. System ten wykrywa uginanie się przewodu światłowodowego pod poruszającym się intruzem, po czym zgłasza informacje o alarmie. Przeznaczony jest do montażu w postaci modułów składających się z mat zakopywanych



Rys. 1. Światłowód detekcyjny w pełni ochrania dostęp do domu

Fot. 2. Maty ze światłowodem – „niewidzialny" system detekcji wokół obiektu

w ziemi lub paneli (siatek) do ochrony dachów, sufitów itp. (które można wykorzystać również w celu zapewnienia ochrony wewnątrz pomieszczeń).

System ten wyróżniają cztery cechy:

1) łatwość instalacji,
2) bardzo małe prawdopodobieństwo wystąpienia fałszywego alarmu,
3) łatwość integracji z istniejącym systemem bezpieczeństwa,
4) niewrażliwość na zakłócenia elektromagnetyczne, przepięcia itp.

Ochrona podłoża – jak to dokładnie działa?

Intruz praktycznie zawsze wchodzi na teren posiadłości pieszo lub wjeżdża pojazdem. Oznacza to, że idealnym miejscem do zastosowania systemu zabezpieczeń jest ziemia. Światłowód detekcyjny umieszczony pomiędzy dwiema matami wprowadza nas w inny świat systemów zabezpieczeń. Można teraz śmiało powiedzieć, że mamy do czynienia z niewidzialnym systemem detekcji. Osoba wchodząca na teren chronionego obiektu zostaje wykryta znacznie wcześniej, niż w przypadku użycia typowych nieperyferyjnych systemów alarmowych – jeszcze zanim zbliży się do obiektu. Maty ze światłowodem (fot. 2) można zastosować pod piaskiem, żwirem lub pod nawierzchnią brukowaną. W momencie, kiedy intruz nadepnie na taką matę, nastąpi ugięcie kabla, przy jednoczesnej zmianie intensywności przesyłanego światła. Zmiana ta jest rozpoznawana przez moduł detekcyjny OD117, który jest sercem całego systemu. Moduł porównuje strumień światła z wyjścia przewodu detekcyjnego z poziomem sygnału, który jest wprowadzany do wejścia przewodu detekcyjnego. Zmiana natężenia światła powoduje zadziałanie przekaźnika, a tym samym alarm. Oczywiście przewód detekcyjny musi być odpowiednio zabezpieczony. W tym celu zastosowana jest gumowa osłona, która chroni przewód przed mechanicznym uszkodzeniem. Może zdarzyć się taka sytuacja, że właściciel obiektu będzie chciał położyć coś w miejscu, gdzie została umieszczona mata ze światłowodem (np. krzesła i stół ogrodowy). W takim przypadku inteligentny moduł analizatora po pewnym czasie „przyzwyczai się" do obecności spoczywającego na nim przedmiotu.

Instalator może wybrać jedną z trzech wielkości zestawu do montażu ziemnego:

- OD140 – zestaw do montażu ziemnego – obszar 50 x 1,25 m,
- OD143 – zestaw do montażu ziemnego – obszar 25 x 1,25 m,
- OD146 – zestaw do montażu ziemnego – obszar 4 x 1,25 m.

Rozwiązanie to doskonale nadaje się do zastosowania w jednostkach bankowych, domach, biurach, magazynach i innych obiektach.

System wykrywa zarówno lekkie obciążenie, np. ludzi, jak i o wiele cięższe, np. ciężarówki.

Koniec kłopotów związanych z dachem

Badania wykazały, że dach budynku jest jednym z najsłabiej chronionych miejsc w systemie zabezpieczeń. Zastosowanie optycznej detekcji gwarantuje nam pełne bezpieczeństwo od strony dachu. Dzięki swojej oryginalnej konstrukcji system światłowodowy jest odporny na zakłócenia elektromagnetyczne i warunki atmosferyczne.

Chroniona powierzchnia pokryta jest modułami siatkowymi (zdjęcie nr 1), które są połączone między sobą. Róg każdej siatki leży na okrągłym pasywnym czujniku naciskowym. Przez każdy czujnik prowadzony jest światłowód detekcyjny, który łączy optyczny nadajnik z optycznym odbiornikiem. Oba te elementy znajdują się w module detekcyjnym. Wkroczenie intruza na siatkę powoduje powstanie napięcia na pasywnym czujniku. Napięcie to jest zamieniane na sygnał „zgięcia przewodu detekcyjnego", co zmienia natężenie światła. Rezultatem zmiany natężenia światła jest wygenerowanie sygnału alarmowego przez moduł detekcyjny (OD117). Czułość modułu detekcyjnego można regulować.

Do Państwa dyspozycji są obecnie dwie wielkości zestawów dachowych:

- OD130 – zestaw dachowy na powierzchnię 10 m^2,
- OD131 – zestaw dachowy na powierzchnię 25 m^2.

System ten można stosować na dachach o niskiej wytrzymałości.

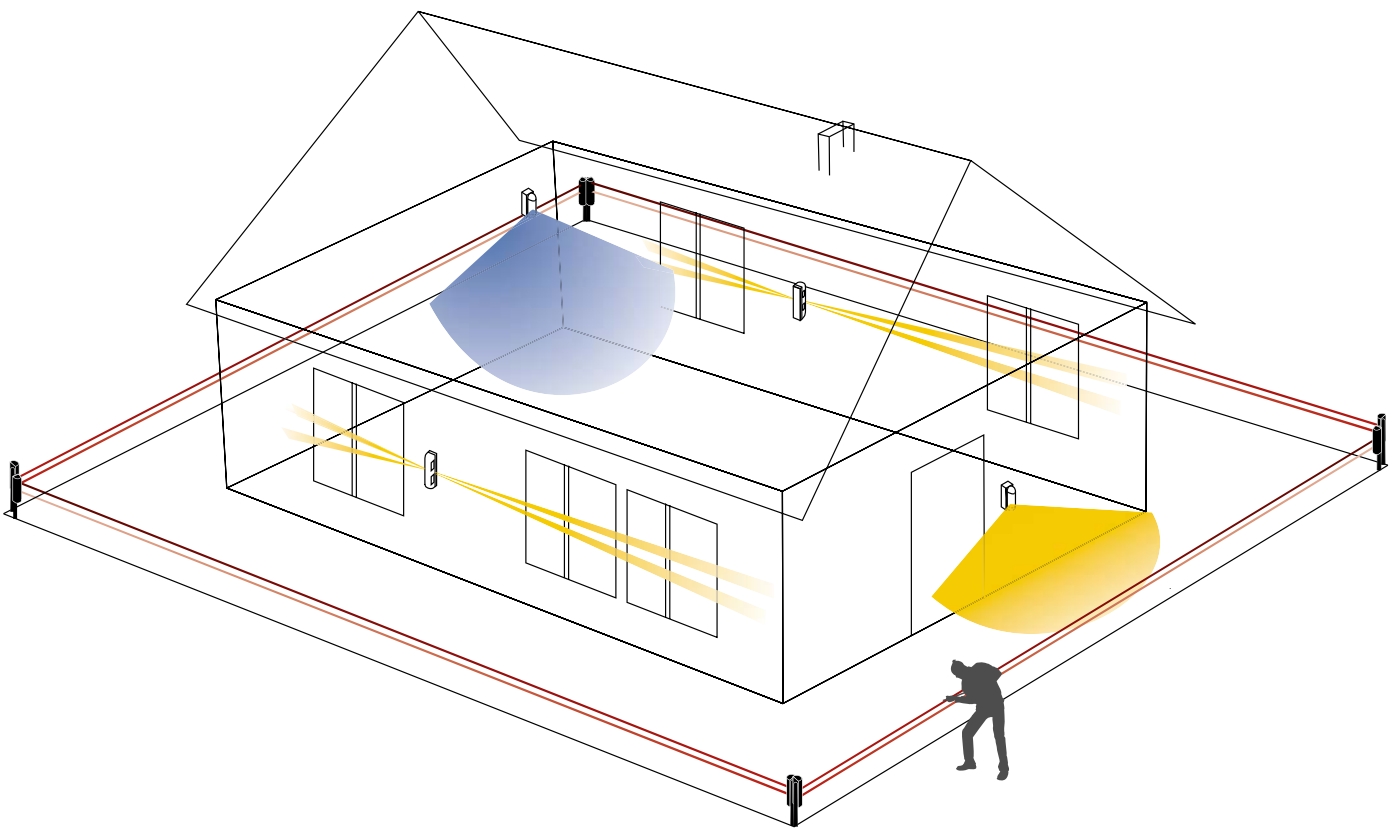
Aby zapewnić odpowiedni styk pomiędzy przewodem detekcyjnym a optycznym nadajnikiem lub odbiornikiem, przewód musi być na końcu bardzo dokładnie obcięty za pomocą odpowiedniego narzędzia. Narzędzie to (nóż) jest dostarczane w komplecie z modułem detekcyjnym. Ostrze musi być oczywiście zawsze ostre i może być użyte ograniczoną liczbę razy.

Omawiany system ochrony umożliwia nie tylko wykrycie intruza, ale także – opcjonalnie, po podłączeniu systemu rejestracji wideo – zarejestrowanie próby dokonania włamania. Oczywiście rejestrację wideo można zapewnić zarówno w przypadku zestawu do montażu ziemnego, jak i dachowego.

Jak można zauważyć, system ochrony bazujący na światłowodzie detekcyjnym jest ciekawym rozwiązaniem, które cechuje się łatwością instalacji, bardzo małym prawdopodobieństwem wygenerowania fałszywego alarmu oraz łatwością integracji z istniejącym systemem bezpieczeństwa. Aby uzyskać informacje na temat cen poszczególnych modułów, proszę skontaktować się z przedstawicielami handlowymi firmy GE Security.

Łukasz Wojtukiewicz
GE Security Polska

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

Uniwersalna centrala sterująca

UCS 4000

Firma Polon-Alfa systematycznie rozszerza asortyment urządzeń przeznaczonych do ochrony przeciwpożarowej. Tym razem przygotowała wyspecjalizowaną centralę, służącą do sterowania przeciwpożarowymi urządzeniami zabezpieczającymi. Uniwersalna centrala sterująca UCS 4000 stanowi jednocześnie uzupełnienie i rozszerzenie systemu sygnalizacji pożarowej Polon 4000.

Uniwersalna centrala sterująca UCS 4000 jest najnowszym urządzeniem w ofercie firmy Polon-Alfa, które zostało w całości opracowane i skonstruowane przez inżynierów firmy. UCS 4000 stanowi element rozszerzający możliwości produkowanych systemów sygnalizacji pożarowej o funkcję sterowania wentylacją i oddymianiem. Centrala spełnia wymagania norm pr EN 12101-9 i EN 12101-10.

Przeznaczenie

Centrala jest przeznaczona do uruchamiania zewnętrznych zabezpieczających urządzeń przeciwpożarowych, szczególnie tych, które służą do oddymiania grawitacyjnego i mechanicznego. Ponadto umożliwia:

1) wykrywanie pożaru (zadymienia),
2) automatyczne lub ręczne uruchamianie urządzeń przeciwpożarowych,
3) automatyczną kontrolę zadziałania urządzeń przeciwpożarowych i wykonawczych (siłowniki, wentylatory, elektromagnesy itp.),
3) sygnalizowanie akustyczne i optyczne stanów pracy urządzeń (alarm, uszkodzenie, blokowanie, testowanie),
4) automatyczną kontrolę własnych układów i obwodów,
5) przekazywanie podstawowych informacji – o alarmie, uszkodzeniu, testowaniu, stanie urządzeń przeciwpożarowych i wykonawczych – do systemów nadrzędnych (np. systemu Polon 4000, systemu IGNIS 1000 lub innych).

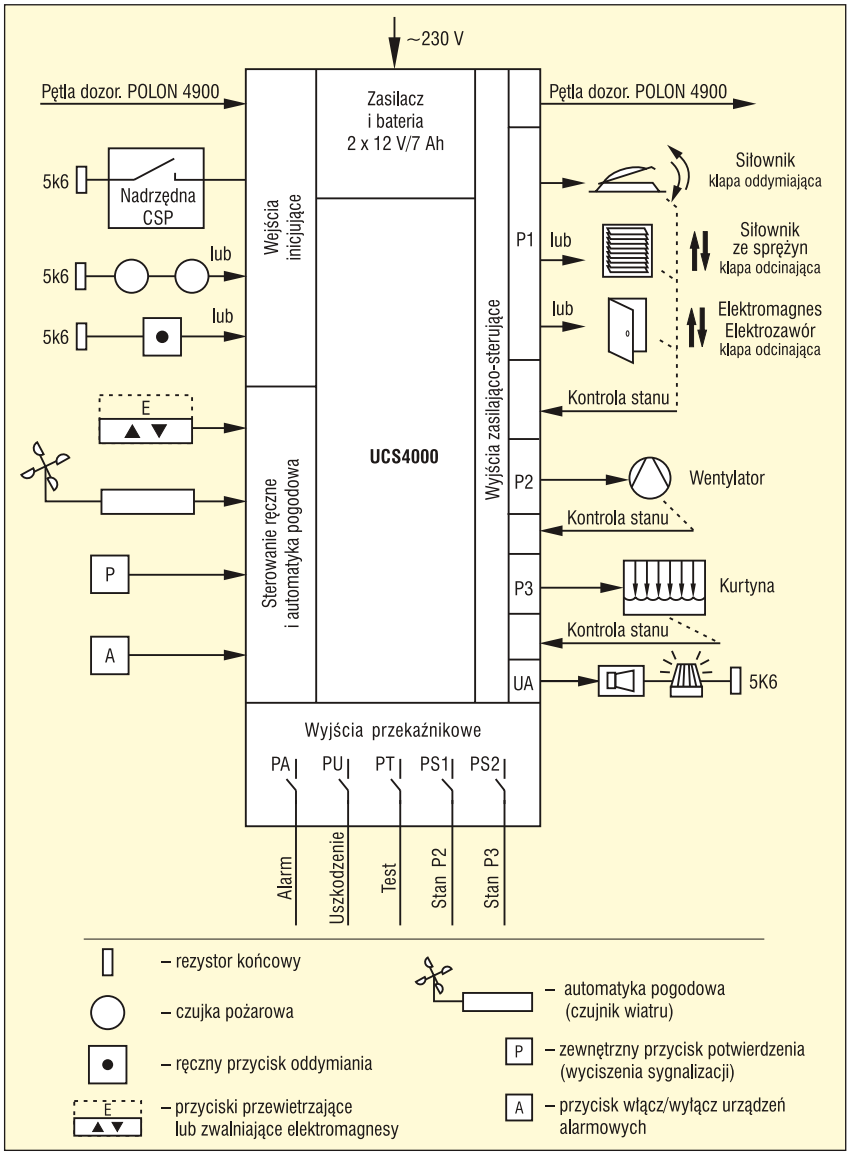
Uniwersalna centrala sterująca UCS 4000 może pracować indywidualnie, jako uniwersalny jednostrefowy sterownik oddymiania, wykorzystując własną linię dozorową z czujkami. Może również stanowić adresowalny element wykonawczy, zainstalowany w adresowalnych liniach/pętlach dozorowych central sygnalizacji pożarowej Polon 4900. W tym trybie pracy programowanie centrali oraz jej kontrola przeprowadzane są z poziomu centrali sygnalizacji pożarowej. Wszelkie komunikaty odnośnie stanu pracy centrali UCS są widoczne w centrali pożarowej. UCS 4000 może pracować również jako centrala podrzędna w konwencjonalnym systemie sygnalizacji pożarowej IGNIS 1000, a także w innych systemach – wówczas do uruchomienia centrali wykorzystuje się jej inicjujące wejście alarmowe.

Wyposażenie centrali

Centrala wyposażona jest w następujące elementy:

– konwencjonalną linię dozorową, na której instaluje się czujki pożarowe szeregu 40 produkcji Polon-Alfa; dzięki temu centrala ma możliwość samodzielnego wykrycia zagrożenia pożarowego (pojawienia się dymu lub płomienia, wzrostu temperatury – w zależności od rodzaju zastosowanych czujek) i automatycznego, bez ingerencji człowieka, uruchomienia przeciwpożarowych urządzeń zabezpieczających, np. klap oddymiających;
– konwencjonalną linię ręcznych przycisków oddymiania (przyciski szeregu PO-6X); dzięki temu możliwe staje się ręczne uruchomienie urządzeń zabezpieczających w sytuacji zagrożenia lub pożaru przez osobę, która to zagrożenie dostrzegła; jest to działanie analogiczne do uruchomienia ręcznych ostrzegaczy pożarowych w systemach sygnalizacji pożarowej;
– moduł komunikacyjny do systemu Polon 4000; umożliwia on cyfrową komunikację z centralami sygnalizacji pożarowej Polon 4900 oraz programowanie i kontrolę stanu centrali poprzez adresowalną linię dozorową;
– nadzorowaną linię, przyjmującą sygnał alarmu z zewnętrznej centrali sygnalizacji pożarowej; w przypadku gdy centrala UCS 4000 pracuje jako podrzędna w stosunku do centrali sygnalizacji pożarowej, może ona przyjmować sygnał alarmu pożarowego z przekaźników centrali SAP lub zewnętrznych elementów wykonawczych z nią współpracujących; nadzorowanie połączenia gwarantuje jego ciągłą kontrolę na wypadek przerwy lub zwarcia;

– potencjałowy przekaźnik główny P1 uniwersalnego zastosowania, o obciążalności 2 A, do zasilania urządzeń przeciwpożarowych (siłowników i napędów klap przeciwpożarowych, elektromagnesów oddzieleń przeciwpożarowych itp.) i sterowania nimi;
– linie kontrolne stanu przełączników krańcowych urządzeń przeciwpożarowych, sterowanych i zasilanych przez przekaźnik główny P1; informacja pochodząca z tych linii pozwala na kontrolę zadziałania urządzenia sterowanego;
– dwa bezpotencjałowe, nadzorowane przekaźniki dodatkowe P2 i P3, które można zaprogramować do sterowania urządzeniami instalowanymi w systemach oddymiania (wentylatorami, kurtynami itp.);
– potencjałowe wyjście nadzorowane, przeznaczone do dołączenia pożarowych urządzeń alarmowych (sygnalizatorów optycznych lub akustycznych);
– pięć bezpotencjałowych przekaźników do przekazywania informacji do systemów nadrzędnych: przekaźnik alarmu PA, przekaźnik uszkodzenia PU, przekaźnik aktywnej funkcji testowania PT, dwa przekaźniki stanu przełączników krańcowych urządzeń przeciwpożarowych PS1 i PS2;
– linię zasilającą czujnik deszczu lub wiatru; informacje z czujników deszczu i wiatru są wykorzystywane jedynie w sytuacji dziennego przewietrzania; padający deszcz mógłby dostać się do wewnątrz obiektu, a zbyt duży wiatr – uszkodzić mechanizm klapy, dlatego w sytuacji dziennego przewietrzania sygnał z czujników deszczu/wiatru blokuje otwarcie klap; w przypadku pożaru ta informacja jest ignorowana;
– linie przyjmujące sygnały z przycisków przewietrzających („otwórz”, „zamknij”) lub sygnał wywołany przez wciśnięcie przycisku zwalniającego elektromagnesy.



Po otrzymaniu sygnału inicjującego następuje uruchomienie procedury oddymiania. Blokowane są przyciski przewietrzania, ignorowane są sygnały z czujnika deszczu lub wiatru.

Uruchomienie urządzeń przeciwpożarowych przez centralę UCS 4000 jest możliwe w wyniku:
1) zadziałania czujki na konwencjonalnej linii dozorowej,
2) zadziałania ręcznego przycisku oddymiania,
3) pojawienia się sygnału z zewnętrznej centrali sygnalizacji pożarowej (np. IGNIS 1000),
4) otrzymania rozkazu z systemu Polon 4000.

Po otrzymaniu sygnału inicjującego następuje uruchomienie procedury oddymiania. Blokowane są przyciski przewietrzania, ignorowane są sygnały z czujnika deszczu lub wiatru. Zgodnie z ustalonym, przyjętym i zaprogramowanym scenariuszem pożarowym następuje:
– uruchomienie przekaźnika głównego P1,
– wysterowanie programowanych przekaźników dodatkowych P2 i P3,
– wysterowanie informacyjnego przekaźnika alarmu PA,
– wysterowanie pożarowych urządzeń alarmowych.

Sterowanie urządzeniami przeciwpożarowymi przez przekaźnik główny P1

Głównym zadaniem centrali UCS 4000 jest zasilanie wykonawczych urządzeń przeciwpożarowych w postaci wszelkiego rodzaju klap i okien przeciwpożarowych (wyposażonych w napędy lub siłowniki elektryczne), oddzieleń przeciwpożarowych (elektromagnesów) itp., oraz sterowanie nimi.

Zadanie to jest spełniane dzięki dedykowanemu wyjściu przekaźnika głównego P1. Jest to wyjście uniwersalne i może być zaprogramowane w czterech trybach pracy z różnymi parametrami czasowymi (T1 – czas opóźnienia wysterowania, T2 – czas trwania wysterowania):

1. Tryb pracy 1 – przeznaczony jest dla urządzeń przeciwpożarowych wyposażonych w siłowniki (napędy) elektryczne dwukierunkowe, sterowane dwu- lub trójprzewodowo, zasilane napięciem stałym 24 V. Siłowniki tego rodzaju są stosowane w klapach i oknach oddymiających, wentylacyjnych.

2. Tryb pracy 2 – przeznaczony jest dla urządzeń przeciwpożarowych wyposażonych w siłowniki (napędy) elektryczne (24 V) ze sprężyną. Siłowniki tego rodzaju są stosowane w klapach przeciwpożarowych odcinających.

3. Tryb pracy 3 – przeznaczony jest dla urządzeń przeciwpożarowych sterowanych przerwą prądową, wyposażonych w elektromagnesy zasilane napięciem 24 V. Sterowanie tego rodzaju jest stosowane powszechnie w systemach drzwi przeciwpożarowych.

4. Tryb pracy 4 – przeznaczony jest dla urządzeń przeciwpożarowych sterowanych impulsem prądowym, wyposażonych w elektromagnesy (lub elektrozawory) zasilane napięciem stałym 24 V. Sterowanie tego rodzaju jest stosowane w systemach oddzieleń lub odgrodzeń przeciwpożarowych.

Dodatkowo można zaprogramować kontrolę ciągłości zasilania oraz kontrolę stanu przekaźników krańcowych urządzeń przeciwpożarowych, sterowanych i zasilanych poprzez wyjście przekaźnika głównego P1.

Przy niekorzystnych warunkach atmosferycznych zewnętrzne klapy lub okna mogą przymarznąć. Centrala UCS 4000 umożliwia zaprogramowanie funkcji przeciwoblodzeniowej. Funkcja działa w stanie alarmu pożarowego. W przypadku przymarznięcia klapy centrala sygnalizuje jej uszkodzenie oraz w ciągu 30 minut, w odstępach co dwie minuty, próbuje ją otworzyć.

Sterowanie urządzeniami przeciwpożarowymi przez przekaźniki dodatkowe P2 i P3

Jeśli klapy przeciwpożarowe (oddymiające, odcinające) są sterowane i zasilane poprzez przekaźnik główny P1, można dodatkowo wykorzystać przekaźniki programowane P2 i P3 do sterowania (załączania lub wyłączania) urządzeniami wykonawczymi instalacji wentylacji i oddymiania, między innymi:

– wentylatorami oddymiającymi (nawiewnymi lub wyciągowymi),
– kurtynami i roletami dymowymi,
– oddzieleniami i grodziami przeciwpożarowymi.

Przekaźnikom P2 i P3 można zaprogramować uzależnienie czasowe (czas opóźnienia i czas trwania wysterowania) oraz kontrolę potwierdzenia zadziałania w czasie 5 s albo 30 s. Dzięki temu można uzależnić czasowo wysterowanie np. wentylatorów oddymiających względem sygnału sterującego klapami przeciwpożarowymi. W przypadku braku potwierdzenia zadziałania urządzeń wykonawczych w odpowiednim czasie centrala UCS 4000 zgłasza uszkodzenie.

Dzienna wentylacja (przewietrzanie)

Centrala umożliwia dodatkowo realizowanie dziennego przewietrzania. Do sterowania oknem lub klapą wentylacyjną (otwieranie i zamykanie) służą programowalne przyciski, podłączone do odpowiednich wejść (tzw. przyciski przewietrzające). Dodatkowo w miejsce tych przycisków można podłączyć zewnętrzny programowalny zegar, sterujący wentylacją. W ten sposób umożliwia się niezależne sterowanie przewietrzaniem, które może być dodatkowo wspomagane automatyką pogodową – poprzez czujnik deszczu lub wiatru (zbyt silny wiatr lub deszcz blokują przewietrzanie). W przypadku alarmu pożarowego działanie zarówno przycisków przewietrzających, jak i automatyki pogodowej jest zablokowane.

ZUD POLON-ALFA

Zabezpieczenie pieniędzy oraz informacji w firmie

Wiele firm działających na rynku można zaliczyć do kategorii obiektów o wysokim ryzyku zagrożenia włamaniem lub kradzieżą. Dlatego ich właściciele oraz kadra kierownicza powinni pamiętać, że profilaktyka jest tańsza od leczenia i należy zawczasu odpowiednio chronić obiekt oraz zabezpieczyć cały proces obrotu pieniędzmi i informacjami.

W kierowaniu i zarządzaniu firmą ogromne znaczenie ma ład organizacyjny, informacyjny i dokumentacyjny w trójkącie współzależności. Już sam odpowiednio zorganizowany i nadzorowany obieg dokumentów, informacji i pieniędzy pozwoli uniknąć wielu zagrożeń. Ogromne znaczenie ma tu również właściwie zorganizowana kontrola dostępu oraz zarządzanie kluczami. Praktyka dostarcza wielu przykładów rezygnacji z włamań czy kradzieży z uwagi na wysoką jakość zabezpieczeń technicznych czy należyte wyszkolenie pracowników. Większe firmy posiadają zazwyczaj pomieszczenia specjalne (archiwa, kasy, pracownie komputerowe, pomieszczenia służące do przechowywania ważnych dokumentów lub cennych albo specyficznych towarów). Pomieszczenia takie powinny być zabezpieczone przynajmniej jednymi drzwiami o podwyższonej odporności na włamanie, najlepiej klasy C. Okres gwarancji, jakiej podlegają takie drzwi, trwa zazwyczaj 24 miesiące. Po tym czasie trzeba pamiętać o okresowych przeglądach i konserwacjach.

Dobór i montaż drzwi należy powierzać licencjonowanym pracownikom zabezpieczenia technicznego. Montaż zapewniają również producenci lub sprzedawcy drzwi. Licencje wydają, a także ewentualnie zawieszają i cofają, komendanci wojewódzcy Policji. Licencja jest wydawana w trybie urzędowym, po przeprowadzeniu postępowania. Osoby posiadające licencję pracownika zabezpieczenia technicznego z reguły mają długoletni staż pracy i doświadczenie. Wielu z nich to członkowie Polskiego Stowarzyszenia Licencjonowanych Serwisów Kluczowych.

Istotnym elementem zabezpieczenia pomieszczeń specjalnych jest zapewnienie dostępu do tych pomieszczeń tylko osobom upoważnionym. Możemy to osiągnąć poprzez zamontowanie zamków elektronicznych działających na zasadzie wprowadzenia kodu cyfrowego, karty magnetycznej lub odczytu linii papilarnych. Zamki tego typu cieszą się na polskim rynku coraz większą popularnością. Dostęp do pomieszczeń specjalnych powinien być obserwowany przez ochronę. Bardzo skutecznym rozwiązaniem może tu być zastosowanie bezprzewodowego zestawu obserwacyjnego. Zestaw taki składa się z kamery, nadajnika i odbiornika radiowego. Może być podłączony do urządzeń TV i wideo, jak również do komputerów, magnetowidów czy nagrywarki DVD.

Obecnie nawet nieduże firmy nie mogą właściwie funkcjonować bez urządzeń służących do zabezpieczania wartości czy też ważnych dla firmy dokumentów i informacji. Podstawową grupą urządzeń służących do ochrony wartości oraz informacji przechowywanych na różnych nośnikach są sejfy, kasy pancerne, szafy na dokumenty, skrytki ścienne, sejfy do zabezpieczania komputerów, kasety metalowe do zabezpieczania magnetowidów i notebooków, kasety metalowe na walutę, pojemniki do transportu wartości.

Na rynku jest bardzo szeroka oferta tego typu urządzeń. Jak w tym gąszczu ofert, z których każda (zdaniem producentów i sprzedających) jest doskonała, znaleźć odpowiednią?

Przed zakupem należy dokładnie rozpoznać trzy aspekty:

1) przeznaczenie urządzenia – do przechowywania czego ma być wykorzystane – w zależności od tego trzeba dobrać jego rodzaj, klasę odporności na włamanie i wielkość;
2) gdzie dane urządzenie zostanie umieszczone (trzeba uwzględnić wytrzymałość ścian, podłóg, stropów), czy istnieje możliwość przytwierdzenia go do podłoża;
3) w jaki zamek (lub zamki) powinno być wyposażone urządzenie zabezpieczające.

Ponadto powinniśmy brać pod uwagę to, jak urządzenie to będzie wykorzystywane w przyszłości. Należy również pamiętać o tym, że stawianym przez firmy ubezpieczeniowe wymogiem w przypadku ubezpieczenia jest zastosowanie sejfów i szaf pancernych do przechowywania walorów.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 14 października 1998 r., opublikowane w Dzienniku Ustaw Nr 129 poz. 858 „w sprawie szczegółowych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne", ustala wielkości przechowywanych wartości w zależności od klasy wyrobu i rodzaju systemu alarmowego, jeżeli urządzenie taki posiada. Wielkości te przedstawia tabela 1. Jedna jednostka obliczeniowa to równowartość 120 średnich pensji krajowych za ubiegły kwartał, wg danych GUS ogłaszanych w Monitorze Polskim.

Sejfy lub kasy możemy uzbroić w instalację alarmową. Celem montowania instalacji alarmowej w sejfach jest zabezpieczenie przed próbami niepowołanego dostępu. Instalacja alarmowa składa się zazwyczaj z następujących czujników:

- czujniki wstrząsowe, umieszcza się je na drzwiach i korpusie sejfu (wyzwalają alarm w przypadku wykrycia zbyt dużych wstrząsów),
- czujnik wysunięcia języka zamka (wyzwala alarm w przypadku próby nieuprawnionego otwarcia zamka),

Klasa odporności na włamanie	Minimalna wartość odporności na włamanie (RU)		Klasa zamka	Dopuszczalny limit wartości pieniężnych (w jednostkach obliczeniowych) przechowywanych w pomieszczeniach i urządzeniach			
	Dostęp częściowy	Dostęp całkowity		Pomieszczenia i urządzenia niechronione systemem alarmowym lub chronione systemem alarmowym klasy niższej od SA3		Pomieszczenia i urządzenia chronione systemem alarmowym klasy co najmniej SA3	
				Pomieszczenia	Urządzenia	Pomieszczenia	Urządzenia
0	poniżej 30	poniżej 50	1xA	–	–	–	–
I	30	50	1xA	–	0,5	–	1,3
II	50	80	1xA	–	1,5	–	3
III	80	120	1xB	–	3	–	6
IV	120	180	2xB	–	5	–	10
V	180	270	2xB	8	8	15	15
VI	270	400	2xC	12	12	20	20
VII	400	600	2xC	16	16	30	30
VIII	550	825	2xC	20	20	40	40
IX	700	1050	2xC	30	–	60	60
X	900	1350	2xC	40	–	100	100
XI		2000	3xC lub 2xD	60	–	bez ograniczeń	–
XII		3000	3xC lub 2xD	–	–	bez ograniczeń	–
XIII		4500	2xD	–	–	bez ograniczeń	–

Tab. 1. Podział pomieszczeń i urządzeń w zależności od odporności na włamanie, wyrażonej w jednostkach odporności (RU) oraz ze względu na limit przechowywanych wartości pieniężnych, wyrażony w jednostkach obliczeniowych (źródło: DzU nr 129 poz. 858 zał. nr 2)

– czujnik zamknięcia drzwi (wyzwala alarm w przypadku próby nieuprawnionego otwarcia drzwi),
– czujnik zerwania (wyzwala alarm w przypadku próby zerwania sejfu z mocowań).

Wszystkie czujniki przygotowane są do podłączenia centrali alarmowej, a sygnały wyprowadzone na zewnątrz sejfu.

Podstawową normą, na podstawie której wydawane są certyfikaty na urządzenia do zabezpieczania wartości, jest polska norma PN-EN 1143-1, która określa również warunki badań. Norma ta podaje zasady i wymagania, jakim powinny odpowiadać pomieszczenia i urządzenia służące do przechowywania wartości.

Dostępne na polskim rynku wyroby posiadają certyfikaty Instytutu Mechaniki Precyzyjnej w Warszawie, które potwierdzają wysoką jakość i niezawodność wyrobu. Certyfikaty wydawane są na okres trzech lat. Certyfikat jest przyznawany producentowi i dotyczy jego produkcji. W okresie ważności certyfikatu Instytut sprawuje nadzór na przebiegiem produkcji. W celu przedłużenia ważności certyfikatu producent musi ponownie zgłosić wyrób do badań. Limit czasowy ważności certyfikatu umożliwia Instytutowi właściwe nadzorowanie procesu produkcji. Wyroby, które zostały wyprodukowane, zakupione i zainstalowane w okresie ważności certyfikatu, zachowują ważność przez cały okres eksploatacji. Do właściwej identyfikacji urządzeń zabezpieczających lub pomieszczeń do przechowywania wartości służą tabliczki znamionowe, zawierające podstawowe informacje o wyrobie. Tabliczka znamionowa montowana jest w wyrobach certyfikowanych. Podaje się na niej: oznaczenie producenta, znak wyrobu, numer fabryczny, rok produkcji, masę wyrobu, numer certyfikatu oraz klasę odporności i nazwę jednostki certyfikującej.

Niezwykle ważny jest rodzaj zamka stosowanego w pomieszczeniach specjalnych oraz urządzeniach zabezpieczających.

Najprostszym rodzajem jest wielozapadkowy zamek mechaniczny. Zazwyczaj w zestawie znajduje się komplet dwóch kluczy. Często zdarza się, że jeden klucz przechowywany jest w sejfie. Wówczas w przypadku zagubienia drugiego istnieje konieczność awaryjnego otwarcia. Zdarzają się również przypadki, w których pracownik zwalniany z firmy, a dysponujący kluczem, twierdzi, że zgubił klucz (istnieje także ryzyko nieuprawnionego dorobienia klucza). Trzeba wówczas zwrócić się do producenta o wymianę zamka w sejfie. Bardzo dobrym rozwiązaniem jest system klucza centralnego Master Key, nazywany często „w cztery oczy". Polega on na tym, że zamek może zostać otworzony jedynie za pomocą dwóch różnych kluczy jednocześnie, z których jeden może posiadać np. przełożony, a drugi – pracownik. Kolejnym rodzajem zamków są mechaniczne zamki szyfrowe (układ tarcz i pokrętło obsługujące) – trzy- lub czterotarczowe, dające mnóstwo możliwych kombinacji. Zamki posiadają tę zaletę, iż umożliwiają zmianę szyfru otwierającego. Za pomocą klucza do zmiany szyfrów przełożony może zmienić kod otwierający bez wiedzy pracownika korzystającego z sejfu. Ma to na celu odcięcie pracownika od dostępu do sejfu w przypadku pojawienia się nieprawidłowości. Stosowanie szyfru otwierającego zamek jest również jednym z rodzajów kontroli dostępu do sejfu. Zaletą mechanicznego zamka szyfrowego jest brak konieczności zarządzania kluczami. Wadą tego rozwiązania może być dla niektórych użytkowników zbyt „skomplikowana" obsługa.

Jeszcze innym rodzajem zamków są elektroniczne zamki szyfrowe, sterowane przyciskami, co jest znaczącym ułatwieniem w codziennej obsłudze. Niektóre z tych zamków mają możliwość odczytu w czasie rzeczywistym 4999 otwarć i dopuszczają obsługę przez 99 użytkowników, z których każdy może posługiwać się swoim sześciocyfrowym kodem. W przypadku zamków elektronicznych istnieje możliwość wprowadzenia specjalnego kodu alarmowego, który również

otwiera sejf. Wówczas informacja o napadzie dociera do centrali i powiadamiana jest policja lub agencja ochrony (napastnik nic o tym nie wie). Zamek otwiera się po czasie oczekiwania, który wywołany jest pierwszym wprowadzeniem kodu. W tym czasie trzeba ponownie wprowadzić kod otwarcia. Czasy oczekiwania i otwarcia ustawiamy w zależności od indywidualnych potrzeb. W codziennej pracy bardzo istotne jest zabezpieczenie pieczątek, druków i wybranej dokumentacji. Można to łatwo zrobić, stosując dodatkową skrytkę w sejfie.

W związku z dynamicznym rozwojem sieci i systemów komputerowych, z którymi Państwo na co dzień współpracują, istnieje rosnąca konieczność ochrony danych zawartych na nośnikach magnetycznych. W związku z tym producenci oferują specjalne sejfy do ochrony magnetycznych nośników informacji. Sejfy te są dostępne na rynku w różnych rozmiarach i z różnorodnym wyposażeniem wewnętrznym, w zależności od potrzeb klienta.

Sejfy na komputer stacjonarny, montowane w miejscu pracy czy zamieszkania, zabezpieczają komputer przed kradzieżą i zapewniają kontrolę dostępu, zwłaszcza jeśli posiadają zamki z możliwością rejestracji i odczytu otwarć. Od niedawna dostępne są na naszym rynku kasety zabezpieczające komputery przenośne, które posiadają podstawę kotwiącą. Podstawę taką można zamontować w miejscu pracy, w samochodzie czy w domu. Sejfy na nośniki magnetyczne przede wszystkim muszą zabezpieczać przed kradzieżą. Wypełnienie przestrzeni między ścianami materiałem ognioodpornym oraz próg ogniowy na obwodzie drzwi gwarantują bezpieczeństwo w przypadku pożaru albo zalania wodą. Urządzenia te zabezpieczają również przed rozmagnesowaniem nośników informacji.

W wielu sklepach i hurtowniach stosowane są sejfy wrzutowe lub działające na podobnej zasadzie sejfy kasjerskie. Umożliwiają one deponowanie gotówki, dokumentów, weksli, papierów wartościowych i czeków przez poszczególnych pracowników poprzez wrzucenie ich do środka takich sejfów przez otwór, bez potrzeby otwierania. Zamykają dostęp do całości zdeponowanych walorów. Stanowią skuteczną ochronę nadmiaru gotówki w kasach lub boksach kasjerskich w przypadku napadu lub kradzieży. Otwory wrzutowe umożliwiają swobodne złożenie depozytu, a ich konstrukcja chroni przed wyławianiem chronionej zawartości.

Stosowanie certyfikowanych sejfów i kas oraz ich prawidłowe użytkowanie jest bardzo dobrym sposobem zabezpieczenia pieniędzy, dokumentów i informacji. Nie można dziś wyobrazić sobie właściwie funkcjonujących firm, nie posiadających urządzeń zabezpieczających tego typu.

Nadkom. mgr Henryk Gabryelczyk
Ekspert Wydziału Prewencji KWP w Poznaniu

Zewnętrzne czujki dualne

serii OPM firmy Optex

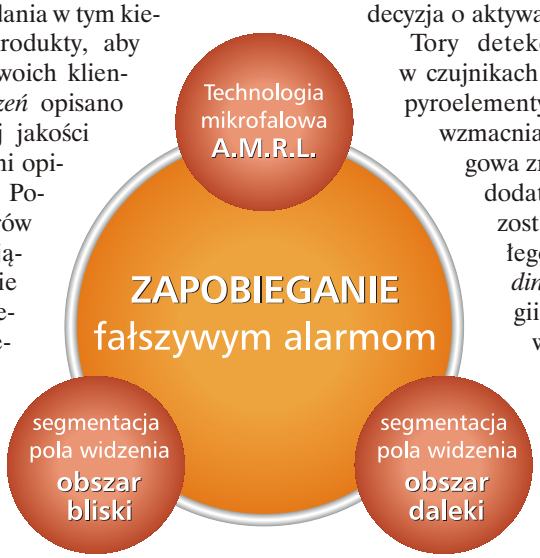
Nieuzasadnione alarmy spowodowane aktywacją zewnętrznych pasywnych czujek podczerwieni (PCP), pojawiające się wskutek działania naturalnych czynników otoczenia, spędzają sen z powiek instalatorów i producentów detektorów. Poszukiwania sposobów skutecznej walki z tym problemem doprowadziły do powstania wielu różnych rozwiązań technicznych, które minimalizują to zjawisko.

Przykładowe rozwiązania to: zwielokrotnienie torów detekcji PCP, zastosowanie dwóch lub rzadziej trzech technologii wykrywania intruza, zastosowanie zdalnej weryfikacji audio i wideo itd. Zastosowanie zdalnej wideoweryfikacji stało się możliwe dzięki dynamicznemu rozwojowi technologii komunikacyjnych oraz coraz większym możliwościom systemów monitoringu wizyjnego. Ostatnie dokonania w zakresie analizy sygnału wizyjnego pod kątem wykrywania postaci człowieka, a nawet jego identyfikacji (na podstawie bazy danych biometrycznych twarzy), dają nadzieję na nowe rozwiązania w zakresie ochrony zewnętrznej i systemów *security* w ogóle. Zanim jednak to nastąpi, a potem trafi „pod strzechy", skuteczna detekcja intruza przy użyciu sprawdzonych czujników pozostanie niezastąpiona.

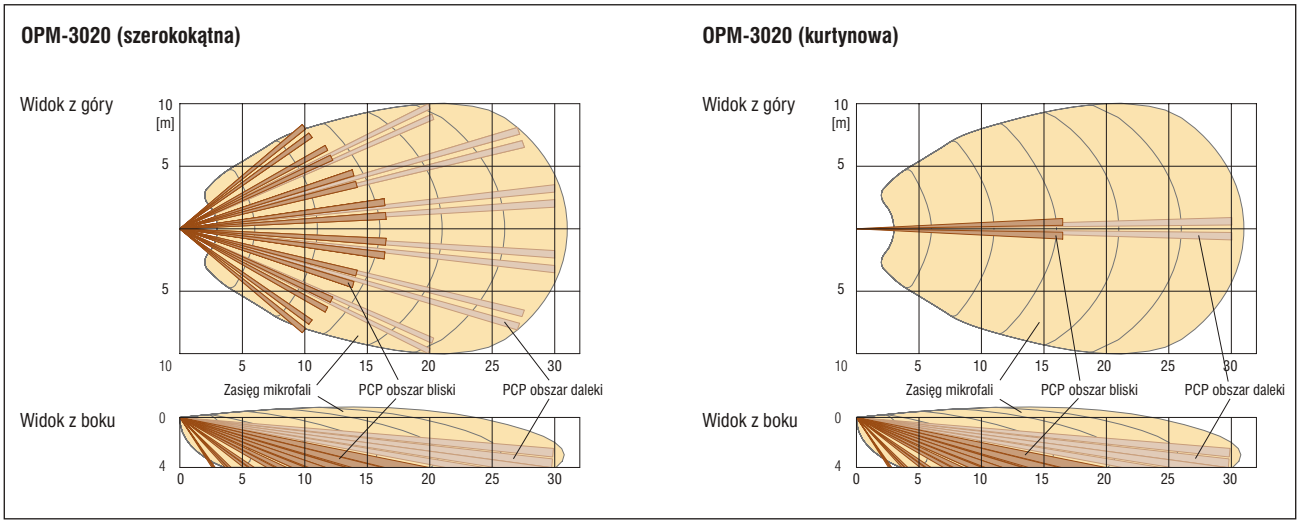
Firma Optex od lat zajmuje się produkcją urządzeń ochrony zewnętrznej. Prowadząc badania w tym kierunku, ciągle udoskonala swoje produkty, aby sprostać rosnącym oczekiwaniom swoich klientów. W numerze 6/2006 *Zabezpieczeń* opisano czujki PCP serii LRP. Te wysokiej jakości urządzenia cieszą się bardzo dobrymi opiniami instalatorów i użytkowników. Pomimo wyjątkowo dobrych parametrów pracy urządzeń serii LRP, zapewniających stabilną detekcję niezależnie od warunków środowiskowych, oczekiwania klientów skierowały zainteresowanie firmy w stronę technologii mikrofalowej. Rezultatem tego jest nowa seria dualnych czujek zewnętrznych OPM. Nowa seria czujników bazuje na sprawdzonych rozwiązaniach serii LRP w dziedzinie detekcji PCP oraz najnowszych osiągnięciach w pracach nad detekcją mikrofalową. Szeroko zakrojone prace nad tymi urządzeniami zaowocowały pięcioma postępowaniami patentowymi dotyczącymi nowatorskich rozwiązań zastosowanych w produktach japońskiej firmy. Pomimo zewnętrznych podobieństw seria OPM jest całkiem nowym produktem, dziedziczącym tylko najlepsze cechy swojego poprzednika.

Technologie

Wzorem czujek LRP czujki OPM wyposażone są w trzy niezależne tory detekcji: dwa tory detekcji pasywnej podczerwieni (PCP) oraz tor detekcji mikrofalowej (μW). Każdy kanał dokonuje detekcji intruza absolutnie niezależnie. Sygnały wyjściowe wszystkich torów poddawane są analizie, w której na podstawie algorytmów podejmowana jest decyzja o aktywacji alarmu.



Tory detekcji podczerwieni, podobnie jak w czujnikach LRP, wyposażone są w podwójne pyroelementy oraz posiadają wysokiej jakości wzmacniacze analogowe. Cała część analogowa znajduje się w głowicy czujnika i jest dodatkowo ekranowana. Obydwa tory zostały wyposażone w filtry światła białego (ang. *Double Conductive Shielding*). Filtry wykonane w tej technologii skutecznie oddzielają promieniowanie podczerwone od innych źródeł promieniowania oraz pełnią rolę ekranu chroniącego przed zakłóceniami elektromagnetycznymi. Zastosowanie technologii segmentacji pola widzenia czujki (ang. *Quad Zone Logic*), dobrze znanej z czujników



Rys. 1. Charakterystyki czujek OPM-3020 i OPM-303

wewnętrznych, pozwala wykorzystać efekt zwielokrotnienia sygnału docierającego do pyroelementu. Dzięki tej technologii obiekty duże (wielkości człowieka) generują kilkukrotnie większy sygnał użyteczny niż obiekty małe (zwierzęta). Niezwykle istotne jest to, że zwielokrotnienie sygnału realizowane jest w torze optycznym, więc nie ma wpływu na poziom szumów pochodzących ze wzmacniaczy.

Tory detekcji podczerwieni, dzięki zastosowanym w nich najlepszym technologiom firmy Optex, charakteryzują się wysoką skutecznością detekcji oraz niskim odsetkiem fałszywych pobudzeń. Pole detekcji czujek podczerwieni, inaczej niż w czujkach serii LRP, zostało rozdzielone na obszar bliski, do 16 m, oraz daleki, do 30 m. W ten sposób utrzymano wysokie zagęszczenie stref detekcji niezależnie od odległości od detektora.

Zewnętrzne czujki dualne zazwyczaj posiadają regulację zasięgu części mikrofalowej jedynie w niewielkim zakresie (zwykle od 2 do 4 ustawień). Skutkuje to na ogół zwiększonym ryzykiem występowania fałszywych alarmów lub utratą czułości. Zakłócenia pracy czujek mogą być spowodowane np. wzajemnym zakłócaniem się czujników znajdujących się w swoim bezpośrednim sąsiedztwie (w razie ustawienia zbyt dużej czułości detektora) lub spadkiem zdolności wykrywania intruza (w przypadku ustawienia zbyt niskiej czułości detektora). Lekarstwem na tego rodzaju bolączki jest zastosowanie technologii AMRL (ang. *Adjustable Microwave Range Limiter*), pozwalającej na regulację zasięgu detekcji mikrofal od 0 do 30 m w odstępach co 5 m. To proste w użyciu a zarazem bardzo skuteczne rozwiązanie pozwala dostosować zasięg czujki do aktualnych potrzeb instalacji.

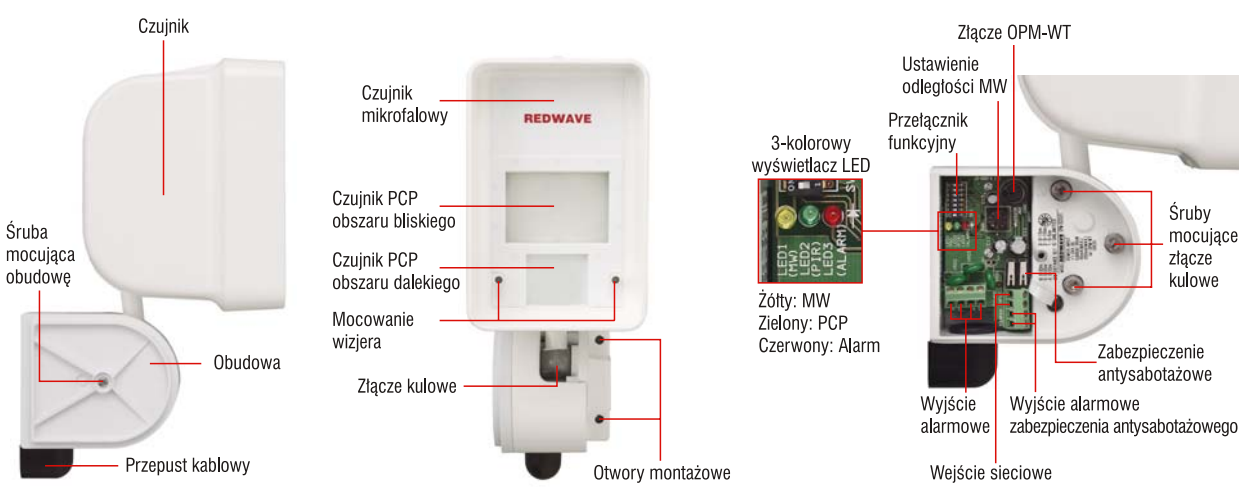
Z natury działania dopplerowskich detektorów mikrofalowych wynika ich czułość na wykrywanie ruchu nie tylko intruzów, ale również ruchu wszelkich obiektów czy mediów. W celu skutecznej i wiarygodnej detekcji intruza należy wprowadzić kryteria oceny sygnału wyjściowego, które pozwolą wyeliminować jak największą ilość pozostałych źródeł. Pomaga w tym zastosowanie algorytmu eliminującego składniki sygnału pochodzące od ruchów cyklicznych (ang. *Repetitive Movement Discrimination*). Przy pomocy tego narzędzia minimalizuje się wpływ stałego otoczenia czujki (drzewa, krzewy, flagi itd.) na sygnały alarmowe.

Analiza wtórna, decydująca o generowaniu alarmów, poza realizowaniem iloczynu logicznego sygnałów z trzech kanałów detekcji, pozwala na zdefiniowanie dodatkowych funkcji zwiększających jej odporność na fałszywe pobudzenia.

Zastosowanie

Czujki OPM mogą być stosowane wszędzie tam, gdzie istnieje ryzyko występowania dużej liczby fałszywych alarmów, np. w lokalizacjach o wyjątkowo trudnych warunkach pracy dla czujek podczerwieni oraz tam, gdzie minimalizacja fałszywych alarmów jest sprawą priorytetową. Oferta firmy

Budowa czujki



Optex zawiera szeroki asortyment urządzeń. Dostępne są produkty o dwóch różnych charakterystykach pokrycia: szerokokątnej OPM-3020 30 m x 20 m oraz kurtynowej OPM-303 30 m x 3 m. Każda z nich jest dostępna w dwóch pasmach mikrofal: 10,587 GHz (w wersji E) oraz 9,900 GHz (w wersji F), a każde z pasm zostało dodatkowo podzielone na kanały, aby wyeliminować ryzyko wystąpienia interferencji pomiędzy czujnikami. Oferowany zakres częstotliwości mikrofal pozwala na stosowanie tych czujek w większości krajów europejskich, między innymi w Polsce.

W stosunku do czujek LRP rozszerzono również zakres wysokości montażu czujek, (możliwość montażu na wysokości od 2,4 m do 4 m).

Podsumowanie

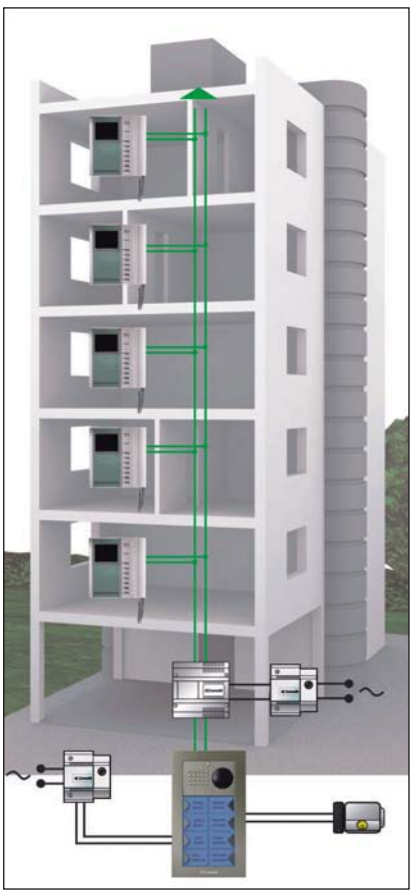
Starania inżynierów firmy Optex dały oczekiwany rezultat. Tam, gdzie zastosowano czujki OPM, zazwyczaj notowano kilkunasto-, a czasem nawet kilkudziesięcioprocentowy spadek fałszywych pobudzeń, przy zachowaniu tego samego poziomu wykrywalności intruzów. To dowodzi, iż nowe urządzenie pracuje niezawodnie, tak jak na produkty czołowego producenta zabezpieczeń zewnętrznych przystało. Motto firmy – *Product Excellence for Peace of Mind* – znowu zmaterializowało się w postaci wspaniałego urządzenia.

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

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

Drukarka TEMPO MAGICARD firmy Ultra Electronics

Tempo

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.

Możliwość kodowania pasków magnetycznych (drukarka Tempo M).

Taśmy kolorowe – nadruk 250 kart
Taśmy monochromatyczne – nadruk 500 kart

Kolory taśm monochromatycznych:
czarny, czerwony, niebieski, zielony, biały, złoty i srebrny

SPECYFIKACJA TECHNICZNA:

Prędkość nadruku
Kolorowy wydruk karty od krawędzi do krawędzi w 40 sekund.
Monochromatyczny wydruk karty w 6 sekund.

Cykl działania
Ciągły

Wbudowane zabezpieczenie
Holokote™ anti-coping znak wodny na całej powierzchni karty

Typy taśm
TM1: Pełny kolor YMCKO – nadruk 250 szt.
PF3: Monochromatyczne – nadruk 500 szt.

Karty
Drukarka akceptuje karty samoprzylepne i PVC formatu CR80 o grubości od 0,51 do 1,02 mm.
Karty z HoloPatch™

Głowica
300 dpi wymienna

Interface do PC
USB rev.1.1 (kompatybilny z USB 2.0)

Sterowniki
Windows 2000, XP

Kompatybilność Elektromagnetyczna i certyfikat
EN 50 081-1 i EN 50 082-1 (Europa) / CE

Zasilanie
90–265 V; 47–63 Hz

Wymiary
(177 x 200 x 211) mm

Masa
około 3,2 kg

Kolor
Srebrny metalik/niebieski

Temperatura pracy
10 – 30ºC

Gwarancja
2 lata (łącznie z głowicą)

TEMPO M DRUKARKA Z KODEREM PASKA MAGNETYCZNEGO

Prędkość
Nadruk w kolorze i zakodowanie karty (ścieżki 1 i 2) w 45 sekund

Koder paska magnetycznego
Standard ISO 7811 koder HiCO ścieżki 1 i 2

DYSTRYBUTOR w Polsce:

ACSS

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

Ultra ELECTRONICS

REJESTRATORY CYFROWE 4-, 8- i 16-kanałowe

seria JPEG2000

- Algorytm kompresji JPEG2000
- Najlepsza jakość zapisanego materiału
- Tryby pracy – duplex/triplex
- Nagrywarka CD-RW
- Łącze USB do archiwizacji
- Sterowanie PTZ
- Wygodne wyszukiwanie i przeglądanie materiału
- Łącze USB do aktualizacji oprogramowania
- Menu w języku polskim
- Zdalne oprogramowanie
- Pilot
- Wyjście VGA w opcji
- Audio w opcji
- Regulowana prędkość transmisji sieciowej

JPEG2000 – najlepsza jakość zapisanego obrazu

Specyfikacja techniczna:

Model	4SEC2004	4SEC2008	4SEC2016
Ilość wejść wideo	4 przelotowe	8 przelotowych	16 przelotowych
Kompresja	JPEG2000		
Wyjścia wideo	Monitor/VCR		
Wyjście VGA	1 wyjście w opcji		
Audio (opcja)	4 wejścia (mono); 1 wyjście (mono)		
Dyski	Do 2 dysków – bez ograniczenia pojemności		
Podział ekranu	1, 4	1, 4, 6, 8, 9	1, 4, 6, 8, 9, 13, 16
Rozdzielczość zapisu	720x288, 360x288		
Jakość zapisu	Wielkość pliku i rozmiar klatki	W porównaniu z innymi algorytmami kompresji, JPEG2000 gwarantuje lepszą jakość zapisanego materiału przy takiej samej rozdzielczości i rozmiarze ramki.	
Podstawowa	14 kB (720x288)		
Normalna	19 kB (720x288)		
Oszczędna	24 kB (720x288)		
Dobra	29 kB (720x288)		
Bardzo dobra	32 kB (720x288)		
Prędkość zapisu (PAL)	50 fps (720x288), 100 fps (360x288)	100 fps (720x288), 200 (360x288)	
Prędkość podglądu	W czasie rzeczywistym dla wszystkich kanałów		
Wielozadaniowość	Triplex (odtwarzanie/zapis/ethernet)		
PIP/ZOOM	Tak/tak		
Detekcja ruchu	Strefy 16x12		
Tryby zapisu	Ciągły/detekcja/harmonogram/alarm/ręczny		
Wyszukiwanie zapisu	Wg daty, czasu i zdarzeń		
Zabezpieczenie	Poziomy dostępu: Administrator, Manager, użytkownik (maks. 8)		
Wejścia alarmowe	4 (NO/NC)	8 (NO/NC)	16 (NO/NC)
Wyjścia	1 przekaźnikowe		
Archiwizacja	CD-RW/Zdalne oprogramowanie/VCR/USB		
Temperatura pracy	od 5 do 40°C		
Wilgotność	< 90%		
Wymiary	430x400x92 mm		
Masa	ok. 7,5 kg (bez dysków)	ok. 8 kg (bez dysków)	
Zasilanie	12 V DC (zasilacz w komplecie)		

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

ALARMTECH POLSKA Sp. z o.o.

VD 400
detektor sejsmiczny

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

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

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

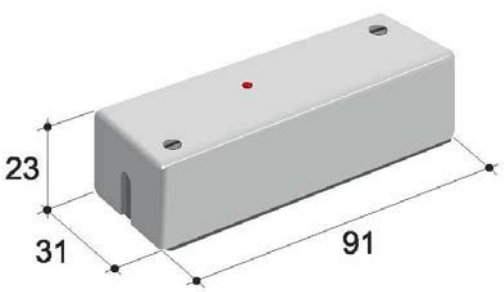
VD 400 oferowany jest także w zestawach VD 400-Z1 oraz VD 400-Z2, z puszką przyłączeniową JB 102.

Montaż detektora na betonowych i ceglanych ścianach powinien być przeprowadzany przy użyciu płyty montażowej MP 400 – wraz z dodatkowymi śrubami i bolcem.

Przy montażu na wolnym powietrzu w niedogodnych warunkach atmosferycznych lub w chłodnych pomieszczeniach, należy skorzystać z obudowy WH 400 zawierającej element grzewczy utrzymujący odpowiednią temperaturę w otoczeniu detektora i wilgotność poniżej wartości krytycznej.

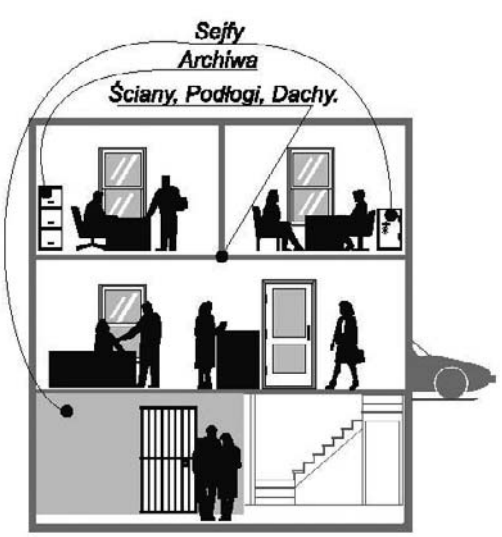
Detektor sejsmiczny VD 400 jest wyposażony w sygnalizator alarmu w postaci diody LED, zabezpieczenie przed zdjęciem pokrywy oraz posiada wewnętrzny rejestrator zdarzeń – „czarną skrzynkę”.

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



Materiał	stal	beton
Promień detekcji	5 m	4 m

Typowe miejsca montażu:



80-299 Gdańsk – Osowa, ul. Kielnieńska 115
tel. (0-58) 340 24 40, fax (0-58) 340 24 49
http://www.alarmtech.pl, e-mail: info@alarmtech.pl

Kamera serii ICE firmy BAXALL
ICE+CM2UATP/LV i ICE+CM2UATP/M

- Kamera kolor/mono z funkcją DSP
- Przetwornik 1/2"
- Rozdzielczość – 540 TVL
- Wyjście wideo UTP

DANE TECHNICZNE	
Przetwornik	1/2" Sony Super HAD CCD
Obróbka obrazu	cyfrowa DSP
Efektywna liczba pikseli	752 (H) x 582 (V)
Czułość	0,6 lx dla obrazu użytecznego z włączoną automatyczną regulacją wzmocnienia (AGC), przysłona obiektywu F1.2
Rozdzielczość	540 TVL
Wyjście wizyjne	1 Vp-p composite video, 75Ω, BNC
Stosunek sygnał/szum	> 50 dB
Balans bieli	2500 K ~ 9500 K/manualny
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)	7 okien konfiguracji, z możliwością włączenia/wyłączenia
Korekcja gamma	0,45
Synchronizacja	line-lock lub wewnętrzna
Dodatkowe funkcje	zmiana progu przełączania pomiędzy trybami kolor/mono, regulacja balansu bieli, tryb zapisu cyfrowego (DRM)

OBIEKTYW	
Mocowanie obiektywu	C lub CS 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. (22) 649 60 95, faks (22) 649 61 00
e-mail: sales@ide.com.pl
www.ide.com.pl

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

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

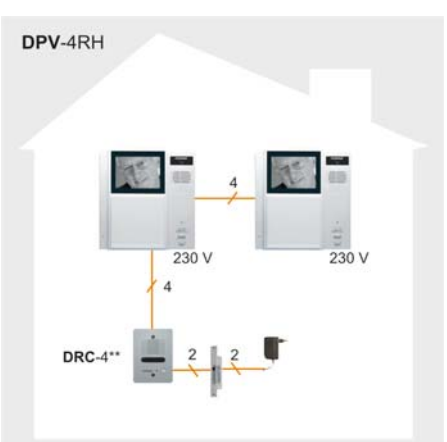
Charakterystyka monitora:

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

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

Charakterystyka kamery:

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



Przykładowy schemat podłączenia

GDE POLSKA
Global Distributor of Electronics

GDE Polska
ul. Koniecznego 46
32-040 Świątniki Górne

tel./fax: 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

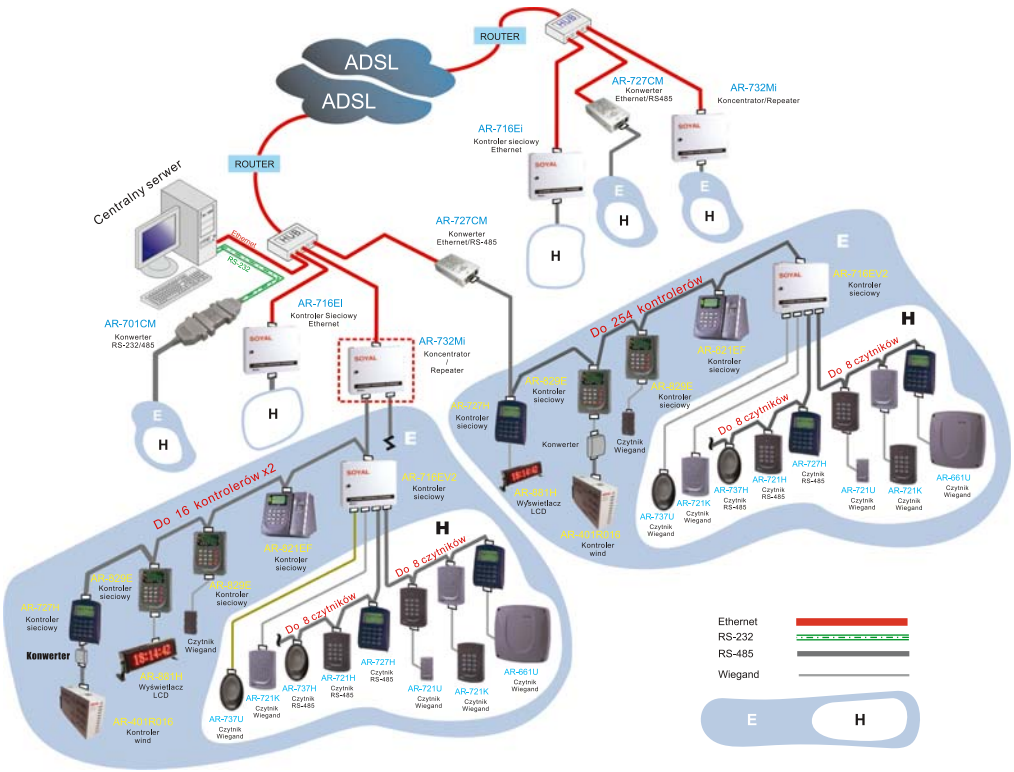
GDE POLSKA
Global Distributor of Electronics

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

System kontroli dostępu i rozliczania czasu pracy z elementami automatyki SOYAL

System kontroli dostępu „SOYAL” jest uniwersalnym systemem kontroli dostępu przeznaczonym do wszystkich typów obiektów, zarówno małych, średnich jak i bardzo dużych. System ten oprócz funkcji kontroli dostępu posiada funkcję rozliczania czasu pracy oraz moduły automatyki przemysłowej (kontrola 512 wejść i wyjść z własnym programowanym sterownikiem). Funkcje te pozwalają na użycie systemu we wszystkich typach obiektów, np.: w obiektach specjalnych, przemysłowych, hotelowych, biurowcach.



Główne cechy systemu to:

- wielofunkcyjny program obsługi systemu
- nieograniczona liczba „klientów” (stacji podległych)
- praca systemu w oparciu o RS485, LAN lub w układzie mieszanym
- duża pojemność systemu – do 15 tysięcy użytkowników
- duża liczba kontrolerów przejść – do 254 (jeden kontroler może nadzorować do 16 przejść)
- praca kontrolerów samodzielna lub w sieci
- pojemność zapisu zdarzeń w trybie on-line ograniczona pojemnością dysku twardego
- pojemność zapisu zdarzeń w pojedynczym kontrolerze do 17 tysięcy zdarzeń
- możliwość kontroli 4064 drzwi
- możliwość tworzenia 255 grup drzwi
- możliwość tworzenia 63 stref czasowych
- możliwość określenia 120 dni wolnych
- funkcja Anti-pass-back
- zakres temperatur pracy kontrolerów od -10°C
- zakres temperatur pracy czytników od -20°C
- monitorowane wejścia czujników drzwi, przycisków wyjścia itd.
- współpraca z wieloma czytnikami w różnych formatach – WG26/34, ABA, 125 kHz, 13,56 MHz Mifare, 2,4 GHz
- współpraca z czytnikiem biometrycznym – odcisk palca
- możliwość kontroli wind na 63 poziomach
- bogate wyposażenie dodatkowe w postaci tablic LED, zwór, zamków, solenoidów itp.
- zasilanie systemu od 9 V do 24 V DC
- współpraca z systemami hotelowymi
- prosta i przejrzysta konfiguracja systemu
- obsługa wielu formatów kart

Protector Polska Sp. z o.o.
ul. Tyniecka 28, 71-019 Szczecin
tel.: +48 (091) 431 83 10, faks +48 (091) 431 83 11
www.protector-polska.pl, e-mail: biuro@protector-polska.pl

Urządzenia kontroli dostępu

Kontroler sieciowy AR-716Ei

- Kontroler 18 przejść
- Przejścia kontrolowane jedno lub dwustronne
- Funkcja Anti-pass-back (kontrola wejścia/wyjścia)
- Ethernet 10 Base T
- Magistrala RS485
- Obsługa formatów Wiegand 26, 34, ABA
- Do 15000 użytkowników w systemie
- Pamięć 11000 zdarzeń
- 63 strefy czasowe, 255 grup drzwi
- Temperatura pracy: od -20°C do +75°C

Czytnik kart zbliżeniowych AR-737U

- Standard 125 kHz (dostępny również w wersji Mifare 13,56 MHz)
- Dostępny również w wersji wodoodpornej (opcja)
- Możliwość integracji z kontrolą dostępu innych producentów
- Magistrala RS232/RS485
- Obsługa formatów Wiegand 26, 34, ABA
- Temperatura pracy od -20°C do +75°C

Kontroler biometryczny z klawiaturą zintegrowany z czytnikiem kart zbliżeniowych AR-821EF

- Kontrola wind
- Funkcja Anti-pass-back (kontrola wejścia/wyjścia)
- Czytnik kart zbliżeniowych w standardzie 125 kHz (dostępny również w wersji Mifare 13,56 MHz)
- Czytnik odcisku palca
- Do 1450 użytkowników
- Wyświetlacz LCD
- Magistrala RS-485
- Ethernet 10 Base T (opcja)
- Obsługa formatów Wiegand 26, 34, ABA
- Temperatura pracy: -20°C do +75°C

Kontroler z wewnętrznym czytnikiem i wyświetlaczem LCD AR-747H

- Wewnętrzny czytnik kart zbliżeniowych
- Wyświetlacz LCD
- Standard 125 kHz (opcja Mifare 13,56 MHz)
- Dostępny również w wersji wodoodpornej IP 54
- Do 1024 użytkowników/3000 zdarzeń
- Kontrola wind
- System rozliczania czasu pracy
- Możliwość zmiany oprogramowania
- Magistrala RS485
- Obsługa formatów Wiegand 26, 34, ABA
- Temperatura pracy: od -20°C do +75°C

Kontroler z wewnętrznym czytnikiem AR-721H

- Wewnętrzny czytnik kart zbliżeniowych
- Podwójne przejście
- Standard 125 kHz (opcja Mifare 13,56 MHz)
- Magistrala RS485
- Obsługa formatów Wiegand 26, 34, ABA
- Kontrola wind
- System rozliczania czasu pracy
- Możliwość zmiany oprogramowania
- Możliwość dołączenia drugiego czytnika
- Temperatura pracy: -20°C do +75°C

Breloki, karty

- Karta standardowa 125K (tylko odczyt, sekwencyjna)
- Specjalna do AR-661U
- Karta ISO (tylko odczyt) 125K
- Mifare – ultra cienka, L10 384 bity EEPROM (odczyt i zapis)
- Mifare – standard Mf1, S50 (1 kB) EEPROM
- Brelok – tylko odczyt

PROTECTOR

Protector Polska Sp. z o.o.
ul. Tyniecka 28, 71-019 Szczecin
tel.: +48 (091) 431 83 10, faks +48 (091) 431 83 11
www.protector-polska.pl, e-mail: biuro@protector-polska.pl

Radiowy czytnik Wieganda RW-1

o zasięgu do 150 m

Radiowy Czytnik Wieganda RW-1 jest urządzeniem pozwalającym na wykorzystanie w systemach kontroli dostępu pilotów radiowych, w taki sam sposób jak kart zbliżeniowych.

Radiowy czytniki Wieganda pozwala na zaprogramowanie wielu cztero, dwu lub jednokanałowych pilotów, gdzie każdy kanał pilota (przycisk) może być traktowany jako osobna karta zbliżeniowa z indywidualnym numerem karty (*site code*+*card code*).

Liczba zaprogramowanych pilotów zależna jest tylko od typu systemu kontroli dostępu jakim dysponujemy i zależna jest od pojemności danego systemu. Danemu pilotowi można przydzielić takie uprawnienia dla użytkownika, jak dla typowej karty zbliżeniowej.

RW-1 ma zastosowanie wszędzie tam, gdzie występuje problem ze sterowaniem dalekiego zasięgu. Nadaje się do sterowania systemami parkingowymi, bramami garażowymi itp.

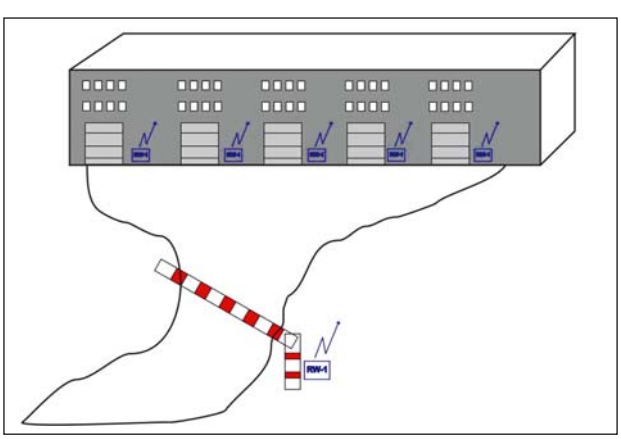
RW-1 jest urządzeniem uniwersalnym i może być podłączony do każdej kontroli dostępu wykorzystującej protokół Wieganda. Może być stosowany zarówno w nowo budowanych systemach kontroli dostępu, jak i już istniejących.

W celu zapewnienia wysokiego poziomu bezpieczeństwa, użyte urządzenia radiowe pracują z wykorzystaniem dynamicznie zmiennego kodu.

Dane techniczne:

1. Zasięg: do 150 m w terenie otwartym
2. Liczba pilotów w systemie – zależna od pojemności systemu kontroli dostępu
3. Obudowa czytnika – ABS IP 65
4. Zakres temperatury pracy – od -25°C do +55°C
5. Format transmisji: Wiegand (26,32)
6. Wymiary: 120 mm x 170 mm x 80 mm
7. Zasilanie 12 V AC/DC
8. Pobór mocy: maks. 100 mA (przy 12 V DC)

Uwaga: W części radiowej wykorzystano urządzenia firmy DTM.



Przykład wykorzystania czytników RW-1 w systemach parkingowych i sterowania bram wjazdowych

Protector Polska Sp. z o.o.
ul. Tyniecka 28, 71-019 Szczecin
tel.: +48 (091) 431 83 10, faks +48 (091) 431 83 11
www.protector-polska.pl, e-mail: biuro@protector-polska.pl

Tytan

ZAKŁAD FIZYKOTERAPII I ODNOWY BIOLOGICZNEJ

Tytan Rehabilitacja

7 lat na rynku - nowoczesny sprzęt - szeroka oferta zabiegów - wykwalifikowana kadra
Drugie miejsce w rankingu warszawskich placówek rehabilitacyjnych, wg NFZ




OFERTA

dla firm świadczących usługi ochrony:

- abonament na rehabilitację, niedostępną w większości placówek medycznych ubezpieczających firmy wysokiej klasy, specjalistyczny sprzęt do rehabilitacji oraz nowoczesne wyposażenie medyczne
- opieka wykwalifikowanej kadry
- dostępność: 8:00-21:00 w dni robocze oraz 9:00-14:00 w soboty
- możliwość odpisania naszego abonamentu od funduszu socjalnego oraz kosztów uzyskania przychodów
- lokalizacja w Centrum miasta, dogodny dojazd i komunikacja

NASZA OFERTA ZABIEGÓW

- elektroterapia (zastosowanie: urazy, stany zwyrodnieniowe)
- kinezyterapia (bóle krzyża, otyłość)
- krioterapia (obrzęki pourazowe, skręcenia, zwichnięcia)
- magnetoterapia (osteoporoza, wczesne leczenie złamań w gipsie)
- laseroterapia (leczenie zatok)
- światłolecznictwo (przykurcze i napięcia mięśniowe)
- hydroterapia (obrzęki, zaburzenia krążenia)
- gimnastyka lecznicza - stretching (wzmacnianie i odbudowa masy mięśniowej)

Wykupienie abonamentu dla grupy pracowników zapewni uzyskanie atrakcyjnych warunków finansowych.

Więcej informacji: Grażyna Kozanowska-Salamon,
Tytan, Al. 3-go Maja 2 (wejście od Potockiego), tel.: (22) 625 05 09, 625 51 50.

CENNIK USŁUG bez abonamentu - 20% zniżki dla branży ochrony!

- Konsultacja medyczna	120 zł
- Konsultacja rehabilitacja medyczna	80 zł
- Magnetoterapia	20 zł
- Laseroterapia	20-30 zł
- Ultradźwięki	20-30 zł
- Elektroterapia	20 zł
- Krioterapia	30 zł
- Wirówka	25 zł
- Kinezyterapia	50 zł
- Masaż całościowy (1 godzina)	120 zł
- Masaż kręgosłupa (30 minut)	60 zł
- Masaż częściowy (15 minut)	30 zł
- Injekcja stawowa, okołostawowa	60 zł

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.
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. Cieszyńska 3, 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
30-954 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

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

PRZEDSIĘBIORSTWO HANDLOWO-USŁUGOWE MERX
D. MIGACZ, K. PORĘBA, A. STRÓŻIK Sp. J.
ul. Nawojowska 88 b
33-300 Nowy Sącz
tel. (18) 443 86 60
faks (18) 443 86 65
e-mail: biuro@merx.com.pl
www.merx.com.pl

PRZEDSIĘBIORSTWO „COMERX" Sp. z o.o.
ul. Nawojowska 88 b
33-300 Nowy Sącz
tel. (18) 443 86 60
faks (18) 443 86 65
e-mail: pkolodziej@comerx.com.pl
www.comerx.com.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 ŚLĄZAK Sp. J.
ul. Wita Stwosza 28
50-149 Wrocław
tel./faks (71) 343 16 76, 341 78 52, 344 82 61
tel. kom. (0) 660 727 438
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

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. Grunwaldzka 48/50
80-241 **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

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 03
faks (71) 340 58 02

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

www.tac.com/pl

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
faks (32) 205 39 71
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
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

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

VIDICON Sp. z o.o.
ul. Bema 7-9
50-265 Wrocław
tel. (71) 327 80 13
faks (71) 327 90 60
e-mail: wroclaw@vidicon.pl

Oddział:
ul. Powązkowska 15, 01-797 **Warszawa**
tel. (22) 562 30 00
faks (22) 562 30 30
e-mail: vidicon@vidicon.pl
www.vidicon.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	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 s.c.	-	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
Merx	-	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	-	-
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
Wizja	-	-	TAK	TAK	-
Vidicon	-	-	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	-
C&C Partners	-	TAK	-	-	-	-	TAK	-	-
CAMSAT	-	TAK	-	-	-	-	TAK	-	-
CBC Poland	-	TAK	-	-	-	-	-	-	-
Cezim	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	-	-	-	-	-
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
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 s.c.	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
Merx	-	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	-
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	-	-
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	-
Wizja	-	-	-	-	-	-	-	-	TAK
Vidicon	TAK	TAK	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
Henryk Gabryelczyk
Patryk Gańko
Norbert Góra
Daniel Kamiński
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
Sławomir Wagner
Marcin Pyclik
Dział DTP
Jarosław Witkowski
jarek@zabezpieczenia.com.pl
Korekta
Paweł Karczmarzyk
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

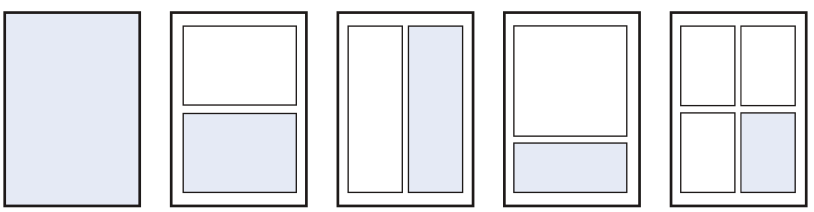
jednorazowy wpis	– 60 zł

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

urmet
MIWI

iProtect™

ZINTEGROWANY SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM

Kontrola Dostępu

Rejestracja Czasu Pracy

CCTV IP

SSWiN

Parking

Ochrona Osób

Integracja z systemem PPOŻ

Rejestracja Gości

TCP/IP

MIWI-URMET sp. z o.o., 91-341 Łódź, ul. Pojezierska 90A, www.miwiurmet.com.pl, e-mail:miwi@miwiurmet.com.pl

Czujka zewnętrzna OD850 technologia TriTech
Niezawodna ochrona obwodowa

Przedstawimy jedną z najbardziej niezawodnych technologii wśród systemów antywłamaniowych.

- Detektory TriTech serii OD850 są przeznaczone do zastosowań zewnętrznych, w niesprzyjających warunkach fizycznych.
- Działanie czujek opiera się na kombinacji wykrywania za pomocą pasywnej podczerwieni (PIR) i promieniowania mikrofalowego (MV) z zaawansowanymi technologiami przetwarzania sygnałów.
- Dzięki skutecznej, zewnętrznej ochronie, intruz jest wykrywany na terenie, przed włamaniem do domu, co zapewnia dłuższy czas na interwencje.
- Liniowy pomiar przemieszczających się obiektów, które w konsekwencji nie zmieniają swojego położenia. Zapobiega to wywoływaniu alarmu przez obiekty, które wprawdzie się poruszają, ale nie przemieszczają, takie jak gałęzie drzew czy wiszące szyldy.
- Możliwość wysterowania dodatkowego przekaźnika, dzięki czemu może być włączane oświetlenie oraz sygnalizator akustyczny lub optyczny.
- Możliwość sprawdzenia działania czujki nawet przy silnym oświetleniu, dzięki diodzie LED o podwyższonej jasności.
- Obszar pokrycia 15x15m

BOSCH
Technologia bliżej nas

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